

# **BiPAC 8700AX(L)-1600**

# Triple-WAN Wireless 1600Mbps 3G/4G LTE (VPN) VDSL2/ADSL2+ Firewall Router

# **User Manual**

Version Released: 2.52.d1

Last revised date: August 30, 2017

# **Table of Contents**

Chapter 1: Introduction	1
Introduction to your Router	
Features	
VDSL2/ADSL2+ Compliance	
Network Protocols and Features	
Firewall	
Quality of Service Control	5
ATM and PPP Protocols	5
IPTV Applications	
Wireless LAN	5
Virtual Private Network (VPN)	
USB Application Server	
Management	
Hardware Specifications	
Physical Interface	
Chapter 2: Installing the Router	
Package Contents	
Important note for using this router	
Device Description	
The Front LEDs	
The Rear Ports	
Cabling	
Chapter 3: Basic Installation	
Connecting Your Router	
Network Configuration	
Configuring a PC in Windows 7/ 8/ 10	
Configuring a PC in Windows // & 10	
Configuring a PC in Windows XP	
Factory Default Settings	
Information from your ISP	
Easy Sign On (EZSO)	
Chapter 4: Configuration	
Configuration via Web Interface	
Status	
Summary	
WAN	
Statistics	
LAN	
WAN Service	
xTM	
xDSL	
Bandwidth Usage	
LAN	45
WAN Service	47
3G/4G LTE Status	49
Route	50
ARP	51
DHCP	52
VPN	53
IPSec	53

РРТР	
L2TP	
OpenVPN	
GRE	
Log	
System Log	
Security Log	
Quick Start	
Quick Start	
Configuration	
LAN - Local Area Network	
Ethernet	
IPv6 Autoconfig	
Interface Grouping	
Wireless 5G(wl0) & 2.4G(Wl1)	
Basic	
Security	
MAC Filter	
Wireless Bridge	
Advanced	
Station Info	
Schedule Control	
WAN-Wide Area Network	
WAN Service	
DSL	
Ethernet	
3G/4G LTE	
Failover	
DSL	
SNR	
System	
Internet Time	
Firmware Upgrade	
Backup / Update	146
Access Control	147
Mail Alert	
SMS Alert	
Configure Log	150
USB	
Storage Device Info	151
User Account	152
Print Server	157
DLNA	162
IP Tunnel	
IPv6inIPv4	
IPv4inIPv6	
Security	
IP Filtering Outgoing	
IP Filtering Incoming	
MAC Filtering	
Blocking WAN PING	
Time Restriction	
URL Filter	
Parental Control Provider	
	······································

QoS - Quality of Service	180
Quality of Service	180
QoS Port Shaping	185
NAT	186
Exceptional Rule Group	186
Virtual Servers	187
DMZ Host	
One-to-One NAT	192
Port Triggering	
ALG	
Wake On LAN	
VPN	
IPSec	
VPN Account	
Exceptional Rule Group	
PPTP	
PPTP Server	
PPTP Client	
L2TP	
L2TP Server	
L2TP Client	
OpenVPN	
OpenVPN Server	
OpenVPN CA	
OpenVPN Client	
GRE	
Advanced Setup	
Routing	
Default Gateway	
Static Route	
Policy Routing	256
RIP	257
DNS	258
DNS	258
Dynamic DNS	260
DNS Proxy	263
Static DNS	
Static ARP	265
UPnP	266
Certificate	272
Trusted CA	272
Multicast	275
Management	278
SNMP Agent	
TR- 069 Client	
HTTP Port	
Remote Access	
Mobile Network	
3G/4G LTE Usage Allowance	
Power Management	
Time Schedule	
Auto Reboot	
Diagnostics	
Diagnostics Tools	

Push Service	
Diagnostics	
Ethernet OAM	
Restart	
Chapter 5: Troubleshooting	
Appendix: Product Support & Contact	

# **Chapter 1: Introduction**

## **Introduction to your Router**

The Billion BiPAC 8700AX(L)-1600 is a multi-service VDSL2 router featuring fiber-ready triple-WAN VDSL2 supports backward compatibility to ADSL2+for a longer reach distance, an all-in-one advanced device including concurrent dual-band 802.11ac (5GHz) 1300Mbps and 802.11n (2.4GHz) 300Mbps, Gigabit Ethernet, connections to 3G/4G LTE and NAS (Network Attached Storage) in one unit. As well as being IPv6-capable, the BiPAC 8700AX(L)-1600 VDSL2 router supports superfast fiber connections via a Gigabit Ethernet WAN port. It also has one USB port, allowing the device to act as a NAS (Network Attached Storage) device with DLNA (Digital Living Network Alliance) and FTP (File Transfer Protocol) access. Moreover, the USB port can host a 3G/4G LTE modem connecting to the 3G/4G LTE network for Internet access. With an array of advanced features, the Billion BiPAC 8700AX(L)-1600 delivers a future-proof solution for VDSL2 connections, superfast FTTC and ultra-speed FTTH (Fiber-To-The-Home) network deployment and services.

### **Flexible Deployment Options**

The BiPAC 8700AX(L)-1600 provides users with flexible, scalable deployment options optimized to both reduce costs and provide the longest possible lifespan for the investment. The BiPAC 8700AX(L)-1600 integrates triple WAN options; a VDSL2/ADSL2+ interface, a 10/100/1000 Ethernet WAN interface which can be used for broadband connectivity to any other Ethernet broadband device., as well as the 3G/4G LTE mobile connectivity. Operators can now deploy one device to support current and future network migration.

### Maximum wireless performance

Featured with simultaneous dual-band technology, the BiPAC 8700AX(L)-1600 can run both 2.4GHz and 5GHz frequency bands at the same time, offering ultra-fast wireless speeds of up to 1600Mbps (1300+300) and multiple SSIDs on both bands. The BiPAC 8700AX(L)-1600, by adopting this state-of-the-art technology, allows for multiple-demand applications, such as streaming HD videos and multiplayer gaming simultaneously. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

### 3G/4G LTE mobility and Always-on Connectivity

With an embedded 3G/4G LTE-based Internet connection (insert an external 3G/4G LTE USB modem to its built-in USB port), user can access internet through 3G/4G LTE, whether you are seated at your desk or taking a cross-country trip. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/LTE network in the event that you ADSL/Fibre/Cable line fails. The BiPAC 8700AX(L)-1600 will then automatically reconnect to the xDSL/Fibre/Cable connection when it is restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

### Experience Gigabit WAN

The BiPAC 8700AX(L)-1600 has one Gigabit WAN port. This WAN offers broadband connectivity option for connecting to a cable, DSL, fibre modem. The BiPAC 8700AX(L)-1600 again offers users convenience and optimal network performance with data rates reaching up to 1Gbps.

### Pathway to the Future

IPv6 (Internet Protocol Version 6), launched as the current IPv4 is getting filled up, gradually becomes the indispensible addressing system for the savvy cloud computing users. Equipped with IPv6, the BiPAC 8700AX(L)-1600 eagerly provides users a better working environment to work with, a shortcut to upgrade and a more efficient solution to save budget. For the customers during this transition period, dual stack (IPv4 and IPv6) feature enables the hosts a convenient way to reserve both address to smooth over this coexistent period.

### Web Based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with online help. It also supports remote management capability for remote users to configure and manage this product.

### Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

# **Features**

- Compliant with all ADSL2+/VDSL2 standards
- IPv6 ready (IPv4/IPv6 dual stack)
- Triple WAN approach VDSL2/ADSL2+, 3G/4G LTE mobile connection, and Ethernet WAN for Broadband Connectivity
- Ethernet: 5-port 10/100/1000M auto-crossover (MDI/MDI-X) switch
- 1-port Gigabit WAN (EWAN) port for broadband connectivity, also servers as a LAN port
- USB port for NAS, DLNA media server, and 3G/4G LTE modem
- Compliant with IEEE 802.11a/b/g/n/ac standards
- Simultaneous dual-band Wireless 1300Mbps (5GHz) and 300Mbps (2.4GHz)
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless security with WPA-PSK/WPA2-PSK
- Supports WDS repeater function
- Multiple wireless SSIDs with wireless guest access and client isolation
- Secured IPSec VPN with powerful DES/ 3DES/ AES
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication
- Pure L2TP and L2TP over IPSec

OpenVPN with CA authentication and extensive OpenSSL encryption

- GRE tunnel
- SNR adjustments to achieve highest sync speeds
- Universal Plug and Play (UPnP) Compliance
- · QoS for traffic prioritization and bandwidth management
- SOHO firewall security
- Auto failover and failback
- Supports IPTV application<sup>\*2</sup>
- · Ease of use with quick installation wizard (EZSO)
- Ideal for Home and SOHO users

### VDSL2/ADSL2+ Compliance

- Compliant with xDSL Standard
- ITU-T G.993.2 (VDSL2)
- ITU-T G.998.4 (G.inp)
- ITU-T G.993.5 (G.vector)
- ITU-T G.992.5 (G.dmt.bis plus, Annex M )
- (ADSL2+ Annex M, available for BiPAC 8700AX(L)-1600 A model only)
- ITU-T G.992.3 (G.dmt.bis, Annex M, ADSL2

Annex M, available for BiPAC 8700AX(L)-1600 A model only)

- Full-rate ANSI T1.413 Issue 2
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- ITU-T G.994.1 (G.hs)
- Supports VDSL2 band plan: 997 and 998
- ADSL/2/2+ fallback modes
- Supports VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a
- Supports ATM and PTM modes

### **Network Protocols and Features**

- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- IPv6 over PPP
- DHCPv6
- IP Tunnel IPv6 in IPv4(6RD)
- IP Tunnel IPv4 in IPv6(DS-Lite)
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- MLD snooping and MLD proxy for video service
- · Management based-on IP protocol, port number and address
- Support port-based Interface Grouping (VLAN)

### Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- MAC Filter
- URL Content Filtering (v4/v6) string or domain name detection in URL string
- Remote access control for web base access
- Packet filtering (v4/v6) port, source IP address, destination IP address, MAC address
- URL content filtering (v4/v6) string or domain name detection in URL string
- MAC filtering

· Password protection for system management

### **Quality of Service Control**

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IPv4/IPv6 protocol, port number and address

### **ATM and PPP Protocols**

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over ALL5 (RFC 268, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4 / F5

### **IPTV Applications**<sup>\*2</sup>

- IGMP Snooping and IGMP Proxy
- MLD Snooping and MLD Proxy
- Interface Grouping (VLAN)
- Quality of Service (QoS)

### Wireless LAN

- Compliant with IEEE 802.11 a/ b/ g/ n/ac standards
- 2.4 GHz and 5GHz frequency range
- Up to 300+1300 Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Supports WPS v2
- Wireless Security with WPA-PSK / WPA2-PSK support
- Multiple wireless SSIDs with wireless guest access and client isolation
- WDS repeater function support

### Virtual Private Network (VPN)

- IKE key management
- DES, 3DES and AES encryption for IPSec
- L2TP over IPSec
- Pap/ Chap/ MS-CHAPv2 authentication for PPTP
- IPSec pass-through
- OpenVPN with CA authentication and extensive OpenSSL encryption
- GRE tunnel

### **USB Application Server**

- 3G/4G LTE USB modem
- Storage/NAS: FTP server, samba server, DLNA media server
- Printer Server

### Management

- Easy Sign-on (EZSO)
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client / relay
- Supports SNMP v1,v2, MIB-I and MIB-II
- TR-069\*1 supports remote management
- Available Syslog
- Mail alert for WAN IP changed
- Auto failover and fallback
- Push Service for diagnostics and debug usage



- 1. On request for Telco / ISP projects
- 2. IPTV application may require subscription to IPTV services from a Telco / ISP.
- 3. Specifications on this datasheet are subject to change without prior notice.

# **Hardware Specifications**

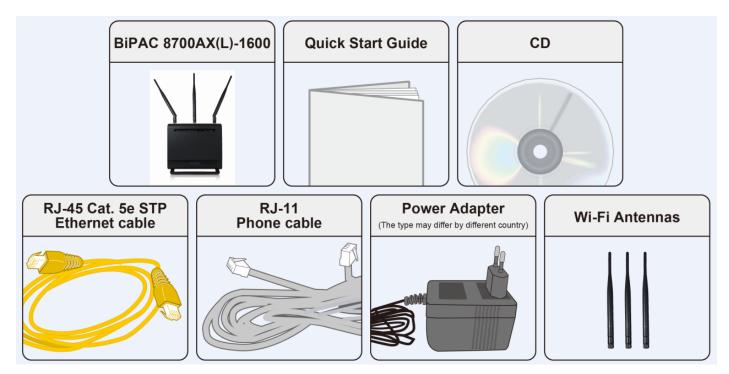
## **Physical Interface**

- WLAN antennas: 3 external antennas for 5G and 2 internal antennas for 2.4G
- DSL: VDSL/ADSL port
- Ethernet: 5-port 10/100/1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: 1 Gigabit Ethernet port (port#5) for connecting directly to Fiber/ xDSL/ Cable modem, also serving as a Ethernet port#5 when not in EWAN use. It is a LAN/WAN configurable port.
- USB 2.0 supports storage service and 3G/4G LTE USB modem
- Wireless on/off and WPS push button
- Power jack
- Power switch
- Factory default reset button

# **Chapter 2: Installing the Router**

# Package Contents

- BiPAC 8700AX(L)-1600 Triple-WAN Wireless 1600Mbps 3G/4G LTE (VPN) VDSL2/ADSL2+
   Firewall Router
- Vertical Stand
- Quick Start Guide
- •CD containing the on-line manual
- Three detachable external Wi-Fi Antennas for 5G
- RJ-45 Cat. 5e STP Ethernet cable
- •RJ-11 telephone cable
- Power adapter
- Splitter / Micro-filter (Optional)



# Important note for using this router

	<ol> <li>Do not use the router in high humidity or high temperatures.</li> <li>Do not use the same power source for the router as other equipment.</li> <li>Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.</li> <li>Avoid using this product and all accessories outdoors.</li> </ol>
Warning	



Place the router on a stable surface.
 Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

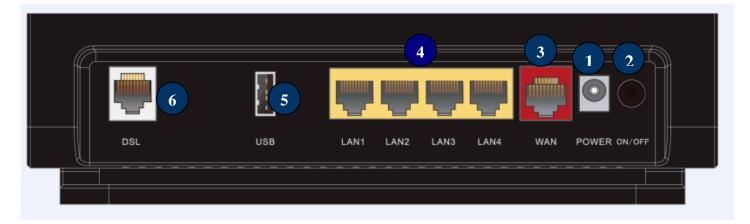
# **Device Description**

## The Front LEDs



LED	Status	Meaning				
POWER	Red	Boot failure or in emergency mode				
Green		System ready				
LAN1~4	Green	Successfully connected to a LAN device				
EANT	Off	Data being transmitted / received				
WLAN(2.4G / 5G)	Green	Wireless enabled (either 2.4G or 5G wireless).				
WEAR(2.407 30)	Blinking	Data being transmitted / received.				
WPS	Green Blinking	WPS is enabled and trying to establish a WPS connection.				
Off		WPS process completed or WPS is off.				
		Successfully connected to a USB device (Printer, USB 2.0 storage, 3G/LTE 3G USB modem)				
WAN	Green	Successfully connected to an Ethernet device or to a broadband device.				
Blinking		Data being transmitted / received				
	Green	Successfully connected to an xDSL DSLAM (Line Synced)				
DSL Green Blinking		xDSL synchronizing or waiting for DSL synchronizing				
	Off	xDSL cable unplugged				
	Green	IP connected and traffic is passing through the device				
Internet	Blinking	Data being transmitted / received				
Internet	Red	The router fails to obtain and IP.				
	Off	The router is either in bridged mode or WAN/DSL connection is not ready				

## The Rear Ports





	Port	Meaning
1	POWER	Connect the supplied Power Adapter to this port.
2	ON/OFF	Power ON/OFF switch
3	Gigabit WAN	Connect to Fibre/ Cable/ xDSL Modem with a RJ-45 cable, for broadband connectivity * Note: this port is a LAN/WAN configurable port.
4	LAN1~4	Connect a STP Ethernet cable to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps /1000Mbps
5	USB	Connect the USB device (Printer, USB 2.0 storage, 3G/LTE 3G USB modem) to this port.
6	DSL	Connect to the xDSL/ telephone network with RJ-11 cable(telephone)
7	WPS	Press & hold the button for <b>2 seconds</b> to trigger WPS function * For WPS configuration, please refer to the WPS section in the User Manual.
8	WLAN	Press & hold the button for <b>more than 6 seconds</b> to enable/disable wireless
9	Reset	Push and hold the reset button for 5 seconds to restore to its factory default settings (this is used when you cannot login to the router, e.g. forgot your password).
8	WiFi Antennas	3 Fixed antennas for 5G. Screw the supplied 3G/4G LTE antennas onto the antenna connectors on both sides

# Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are all lit. If they are not, verify if you are using the proper cables. If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Make sure you have a line filter with all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

# **Chapter 3: Basic Installation**

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS / Windows 10/ Windows 8, Windows 7 / XP / / Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

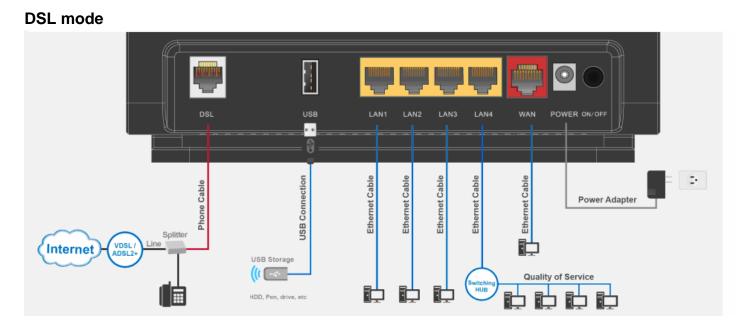
Please follow the following steps to configure your PC network environment.



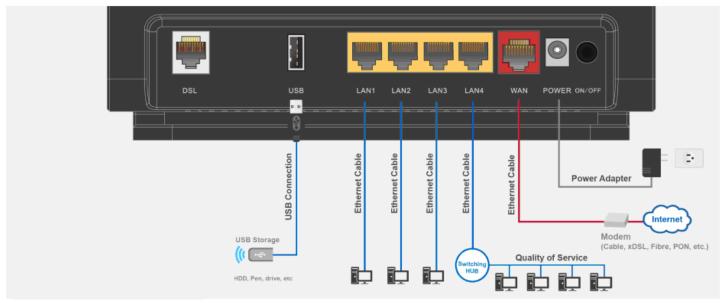
Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

# **Connecting Your Router**

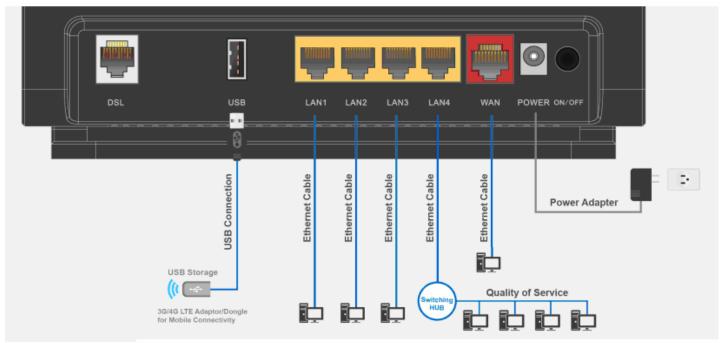
Users can connect the VDSL2/ADSL2+ router as the following.



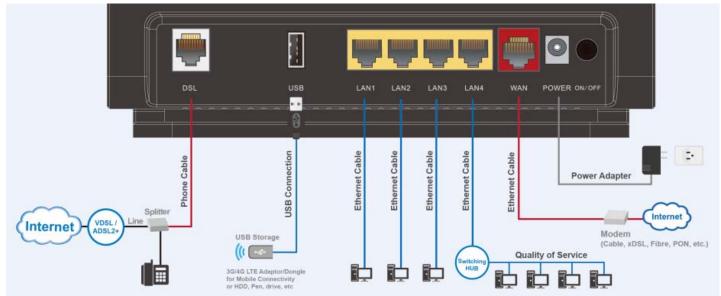
### **Broadband mode**



### 3G/4G LTE mode



### Failover/fallback mode



# **Network Configuration**

### Configuring a PC in Windows 7/8/10

- 1. For Windows 7/8, go to **Start**. Click on **Control Panel**.
- 2. For Windows 10, Users can click Start then click on Settings; or right click the mouse when it points at Windows ICON (Start), then click Control Panel.



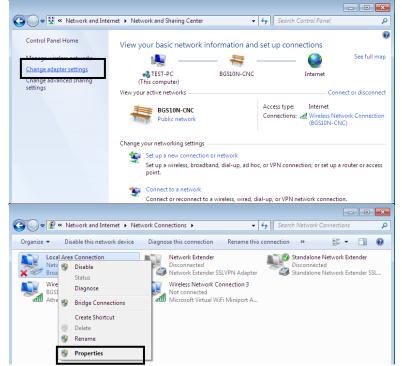
#### Settings of Windows 10

3. Click on Network and Internet.



4. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

5. Select the Local Area Connection, and right click the icon to select Properties.



### IPv4:

6. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties

- 7. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
- 8. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Networking Sharing Connect using: Broadcom 570x Gigabit Integrated Controller Configure
Broadcom 570x Gigabit Integrated Controller
Configure
oor ingero
This connection uses the following items:
Client for Microsoft Networks
<ul> <li>✓ ■ QoS Packet Scheduler</li> <li>✓ ■ File and Printer Sharing for Microsoft Networks</li> </ul>
A Internet Protocol Version 6 (TCP/IPv6)     A Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
🗹 📥 Link-Layer Topology Discovery Responder
Install Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication
across diverse interconnected networks.
OK Cancel
nternet Protocol Version 4 (TCP/IPv4) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
OUse the following IP address:
IP address:
Subnet mask:
Subnet mask:      Default gateway:
Default gateway:
Default gateway:          Obtain DNS server address automatically
Obtain DNS server address automatically     Use the following DNS server addresses:
Default gateway:          Image: Obtain DNS server address automatically         Image: Obtain DNS server addresses:         Preferred DNS server:

### IPv6:

6. Select Internet Protocol Version 6 (TCP/IPv6) then click Properties

- In the TCP/IPv6 properties window, select the Obtain an IPv6 address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
- 8. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

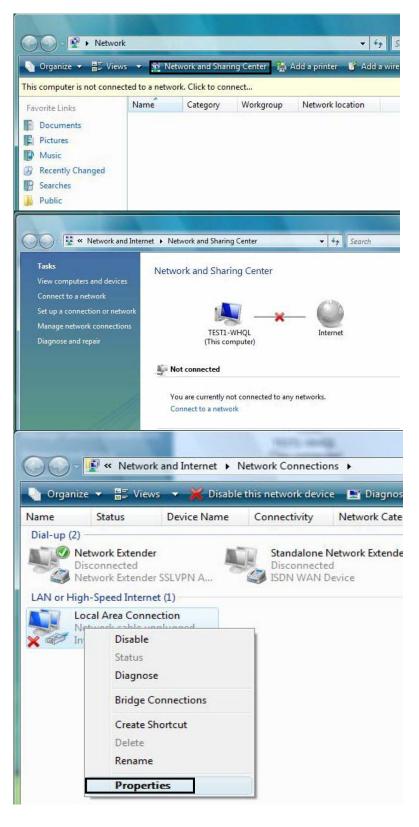
🔋 Local Area Connectio	on Properties	<b>X</b>
Networking Sharing		
Connect using:		
Broadcom 570x C	Sigabit Integrated Controller	
This connection uses th	e following items:	Configure
🗹 🏪 Client for Micro	soft Networks	
🗹 💂 Qo S Packet S		
	Sharing for Microsoft Netwo col Version 6 (TCP/IPv6)	orks
	col Version 6 (TCP/IPv4)	
	ology Discovery Mapper I/C	D Driver
🗹 🔺 Link-Layer Top	ology Discovery Responder	·
Install	Uninstall	Properties
Description		
	e next-genetion version s communication across	
interconnected netw		suiverse
	ОК	Cancel
		2 ×
ternet Protocol Version 6 (TCP/IPv6	) Properties	
General		
	utomatically if your network supports th work administrator for the appropriate I	
Obtain an IPv6 address automa	tically	
O Use the following IPv6 address:		
IPv6 address:		
Subnet prefix length: Default gateway:		
Obtain DNS server address auto		
Use the following DNS server ad	dresses:	
Preferred DNS server: Alternate DNS server:		
Alternate DNS server:		
Validate settings upon exit		Advanced
		OK Cancel

## **Configuring a PC in Windows Vista**

- 1. Go to Start. Click on Network.
- 2. Then click on **Network and Sharing Center** at the top bar.

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.

4. Select the Local Area Connection, and right click the icon to select Properties.



### IPv4:

5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.

- 6. In the **TCP/IPv4 properties** window, select the Obtain an **IP** address automatically and **Obtain DNS Server address** automatically radio buttons. Then click **OK** to exit the setting.
- 7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Sec. 2014										
etwork	ing									
Conne	ct us	ing:								
<b>Q</b>	Intel(	R) 82566	DM Gig	abit N	etwork	Conr	nection	٦		ĺ
								Config	11.179	
This co	onne	ction uses	s the foll	owing	items	:		Coning	jaie	
		ient for Mi			nrks					
		oS Packe e and Prir			r Mion	facet	Notwo	dea		
	in Int	ternet Pro	tocol Ve	rsion	<mark>e (TC</mark> P		6)	in S		
	1.00	ternet Pro	ARNAL AL ALL AND			8 . 7 . 8	12241	Drive		
		nk-Layer nk-Layer	10000	20 (A. 197	10.00 P. 10 P. 3				1	
			er in							
1	Insta	əll		Unin	stall			Prope	rties	
Desc						ر در میلیگور				
		sion Cont								
		a network iverse inte					minuh	Catio	ų.	
					-			-		
						0	K		Cano	cel
_					-	- 1.5				
ant D		al Vari	- A (TC	D/ID					9	2
	otoc	ol Versio	n 4 (TC	P/IPv4	4) Proj	pertie	s		6	2
	1	col Versio ernate Cor		_	4) Proj	pertie	s		6	2
neral ou car	Alte	ernate Cor IP setting	nfigurations assign	on ed aut	tomatic	ally f	your n		< supp	orts
neral ou car nis cap	Alte get pabilit	ernate Cor	nfiguratio s assign vise, you	on ed aut	tomatic	ally f	your n		< supp	orts
neral ou car his cap or the	Alte aget appr	ernate Cor IP setting ty. Otherw opriate IP	nfiguratio s assign vise, you settings	on ed aut i need	tomatic to ask	ally f	your n		< supp	orts
neral ou car nis cap or the () Oł	Alte appr appr	ernate Cor IP setting cy. Otherw opriate IP an IP add	nfigurations assign vise, you settings ress aut	on ed aut i need i, comatic	tomatic to ask	ally f	your n		< supp	orts
neral ou car his cap or the O Us	Alte abilit appr otain se the	ernate Cor IP setting ty. Otherw opriate IP an IP add e following	nfigurations assign vise, you settings ress aut	on ed aut i need i, comatic	tomatic to ask	ally f	your n		< supp	orts
neral ou car nis cap or the O Us IP ac	Alte appr otain se the	ernate Cor IP setting ty. Otherw opriate IP an IP add e following	nfigurations assign vise, you settings ress aut	on ed aut i need i, comatic	tomatic to ask	ally f	your n		< supp	orts
neral ou car his cap or the O O Us IP ac Subr	Alte abilit appr otain se the ddres	ernate Cor IP setting cy. Otherw opriate IP an IP add e following is: ask:	nfigurations assign vise, you settings ress aut	on ed aut i need i, comatic	tomatic to ask	ally f	your n		< supp	orts
neral ou car his cap or the O O Us IP ac Subr	Alte abilit appr otain se the ddres	ernate Cor IP setting ty. Otherw opriate IP an IP add e following	nfigurations assign vise, you settings ress aut	on ed aut i need i, comatic	tomatic to ask	ally f	your n		< supp	orts
neral ou car nis cap or the O O O Us IP ac Subr Defa	Alter pabilit appr otain se the ddres	ernate Cor IP setting cy. Otherw opriate IP an IP add e following is: ask:	nfiguration s assign vise, you settings ress aut IP addr	on ed aut need omatic ess:	comatic to ask	ally f your r	your n		< supp	orts
neral ou car is cap or the O Ol DP ac Subr Defa	Alte pabilit appr btain se the ddres net m ult g	ernate Cor IP setting ty. Otherw opriate IP an IP add e following is: ask: ateway:	nfiguration s assign vise, you settings ress aut IP addr IP addre	on ed aut need omatic ess:	comatic to ask cally	ally f	your n		< supp	orts
neral ou car nis cap or the O O Us Subr Defa O O Us	Alte abilit appr btain se the ddres net m ult g	ernate Cor IP setting cy. Otherw opriate IP an IP add e following is: ask: ask: ateway: DNS serve	nfiguration s assign vise, you settings ress aut IP addr IP addre	on ed aut need omatic ess:	comatic to ask cally	ally f	your n		< supp	orts
eral ou car is cap or the O Ol O Us Subr Defa O Ol O Ol O Ol O Ol O Ol O Ol O Ol O O	Altern get abiliti approtain se the ddress and m ult g- btain se the se the	ernate Cor IP setting cy. Otherw opriate IP an IP add e following ss: ask: ateway: DNS serve e following	nfiguration s assign vise, you settings ress aut ress aut r IP addr r IP addre er addre DNS se er:	on ed aut need omatic ess:	comatic to ask cally	ally f	your n		< supp	orts
eral ou car is cap or the O Ol O Us Subr Defa O Ol O Ol O Ol O Ol O Ol O Ol O Ol O O	Altern get abiliti approtain se the ddress and m ult g- btain se the se the	ernate Cor IP setting ty. Otherw opriate IP an IP add e following is: ask: ateway: DNS serve e following I DNS serve	nfiguration s assign vise, you settings ress aut ress aut r IP addr r IP addre er addre DNS se er:	on ed aut need omatic ess:	comatic to ask cally	ally f	your n	k admi	< supp inistra	orts
eral ou car is cap or the O Ol O Us Subr Defa O Ol O Ol O Ol O Ol O Ol O Ol O Ol O O	Altern get abiliti approtain se the ddress and m ult g- btain se the se the	ernate Cor IP setting ty. Otherw opriate IP an IP add e following is: ask: ateway: DNS serve e following I DNS serve	nfiguration s assign vise, you settings ress aut ress aut r IP addr r IP addre er addre DNS se er:	on ed aut need omatic ess:	comatic to ask cally	ally f	your n	k admi	< supp	orts
eral ou car is cap or the O Ol O Us Subr Defa O Ol O Ol O Ol O Ol O Ol O Ol O Ol O O	Altern get abiliti approtain se the ddress and m ult g- btain se the se the	ernate Cor IP setting ty. Otherw opriate IP an IP add e following is: ask: ateway: DNS serve e following I DNS serve	nfiguration s assign vise, you settings ress aut ress aut r IP addr r IP addre er addre DNS se er:	on ed aut need omatic ess:	comatic to ask cally	ally f	your n	k admi	< supp inistra	orts

### IPv6:

5. Select Internet Protocol Version 6 (TCP/IPv6) then click Properties.

- In the TCP/IPv6 properties window, select the Obtain an IPv6 address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
- 7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

Local Area Connection	n Properties	×
Networking Sharing		
Connect using:		
_	Circle Network Com	
Intel(R) 82566DM	Gigabit Network Conn	hection
This connection uses the	following items:	Configure
	_	
Client for Micros		
✓ ♣ File and Printer		letworks
<ul> <li>Internet Protoco</li> </ul>	-	
Internet Protoco		
✓ Link-Layer Topo		
<ul> <li>Link-Layer Topo</li> </ul>		
	logy biscovery ricspo	
Install	Uninstall	Properties
Description		
TCP/IP version 6. The	next-genetion vers	ion of the internet
	-	
protocol that provides		cross diverse
interconnected netwo	orks.	
	ОК	Cancel
ternet Protocol Version 6 (TCP/IPv6)	Properties	9 ×
General		
You can get IPv6 settings assigned au		
Otherwise, you need to ask your net	work administrator for the appro	opnate 1996 setungs.
	1002070	
Obtain an IPv6 address automat	ically	
O Use the following IPv6 address:	-	
IPv6 address:		
Subnet prefix length:		
Default gateway:		
Obtain DNS server address auto	matically	
Use the following DNS server ad		
Preferred DNS server:		
Alternate DNS server:		
Alternate DNS SerVer:		
Validate settings upon exit		
		Advanced
		Advanced OK Cancel

## Configuring a PC in Windows XP

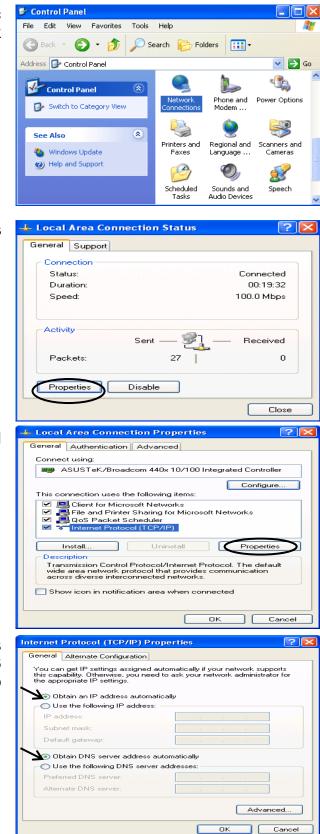
### IPv4:

- 1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
- 2. Double-click Local Area Connection.

3. In the Local Area Connection Status window, click Properties.

4. Select Internet Protocol (TCP/IP) and click Properties.

- 5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
- 6. Click OK to finish the configuration.



### IPv6:

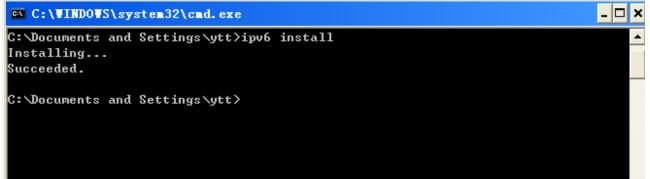
IPv6 is supported by Windows XP, but you should install it first.

Act as shown below:

1. On the desktop, Click Start > Run, type cmd, then press Enter key in the keyboard, the following screen appears.



2. Key in command ipv6 install



Configuration is OK now, you can test whether it works ok.

# **Factory Default Settings**

Before configuring your router, you need to know the following default settings.

### Web Interface (Username and Password)

Three user levels are provided by this router, namely **Administrator**, **Remote** and **Local** respectively. See <u>Access Control</u>.

#### Administrator

- Username: admin
- Password: admin

#### Local

- Username: user
- Password: user

#### Remote

- Username: support
- Password: support



If you have forgotten the username and/or password of the router, you can restore the device to its default setting by pressing the **Reset Button** more than **5** seconds.

#### **Device LAN IPv4 settings**

- IPv4 Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

#### **Device LAN IPv6 settings**

▶ IPv6 Address / prefix: Default is a link-local address and is different from each other as MAC address is different from one to one. For example: fe80:0000:0000:0204:edff:fe01:0001 / 64, the prefix initiates by fe80::

#### **DHCP server for IPv4**

- DHCP server is enabled.
- Start IP Address: 192.168.1.254
- IP pool counts: 100

### LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

### IPv4

LAN Port		WAN Port
IPv4 address	192.168.1.254	
Subnet Mask	255.255.255.0	The PPPoE function is
DHCP server function	Enabled	enabled to automatically get
IP addresses for distribution to PCs		the WAN port configuration from the ISP.

### IPv6

LAN Port		WAN Port
	address is different from one to one. For example :	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
DHCP server function	Enabled	

# Information from your ISP

Г

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided.

٦

Gather the information as illustrated in the following table and keep it for reference.

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
DHCP Client	VPI/VCI, VC / LLC-based multiplexing, Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

# Easy Sign On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

### EZSO window pops up:

**Step1:** Set the administration password.

Easy Sign On		
▼Administrator Password		
Configure Administrator Password		
New Password	(maximum length is 15)	
Confirm Password	(maximum length is 15)	
Continue		

### Step 2: Set the Time Zone.

Easy Sign On		
* Time Zone		
Configure Time Zone Offset		
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 💌	
Continue		

Step 3: Configure the WAN interface.

### DSL mode (ADSL mode, please choose ATM; VDSL, please choose PTM)

Here take ADSL for example.

Before configuring with DSL mode, please confirm you have correctly connected the DSL line, and it is now synchronized.

Easy Sign On		
• WAN Interface (WAN > Wireless)		
Select WAN Interface		
Main Port	DSL 💟 (Current Main Port: DSL)	
Layer2 Interface	⊙ ATM ○ PTM	
VPI/VCI	8/35	
Туре	PPPoE	
Username	username	
WAN IP Address	Obtain an IP Address Automatically	
Continue Done		

Select DSL, press Continue to go on to next step, press "Done" to quit the setting.

**1.** Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.

Easy Sign On		
<pre> • WAN Interface (WAN &gt; Wireless) </pre>		
WAN Service		
Туре	PPP over Ethernet (PPPoE)	
VPI / VCI	[0-255] / [32-65535]	
Username		
Password		
Service Name		
Encapsulation Mode	LLC/SNAP-BRIDGING	
Authentication Method	AUTO 💌	
IPv4 Address	Static	
IP Address		
IPv6 for this service	✓ Enable	
IPv6 Address	□ Static	
IP Address		
МТО	1492	
Continue		

If the DLS line doesn't synchronize, the page will pop up warning of the DSL connection failure.

Easy Sign On	
▼ WAN Interface (WAN > Wireless)	
DSL Line Is Not Ready. Please Check your DSL Line and wait for a while.	

3. Wait while the device is configured (DSL synchronized).

Easy Sign On	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

**4.** WAN port configuration is success and next to wireless, if you want skip wireless setting, click **Done**.



Click **Done**, web configuration will be loaded, you will enter the web configuration page.

Easy Sign On	
*WAN Interface	
Stop EZSO	
You stopped the EZSO procedure. Web Configuration will now load.	

configure the Wireless setting. The 8700AX(L)-1600 supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key. (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wl0)	
Wireless	✓ Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
▼ Wireless (WAN > Wireless)		
Please wait while the device is configured.		

### 6. Continue to set 2.4GHz wireless.

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	2.4GHz (wl1)	
Wireless	☑ Enable	
SSID	wlan-ap-2.4g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
Wireless (WAN > Wireless)		
Please wait while the device is configured.		

### **7.** Success in configuring the EZSO.

Easy Sign On	
* Process finished	
Success.	
The Easy-Sign-On process is finished. Your device has been successfully configured.	
You can now:	
1. Log onto the router management interface for more advanced settings on 192.168.1.254 2. Continue to wpad.home.gateway/wpad.dat	

#### **Ethernet mode**

1. Select Ethernet, press Continue to go on to next step.

Easy Sign On	
<ul> <li>WAN Interface (WAN &gt; Wireless)</li> <li>Select WAN Interface</li> </ul>	
	Ethernet 🖌 (Current Main Port: DSL)
Continue Done	

**2.** Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.

Easy Sign On		
<pre> WAN Interface (WAN &gt; Wireless) </pre>		
WAN Service		
Туре	PPP over Ethernet (PPPoE) 💌	
Username		
Password		
Service Name		
Authentication Method	AUTO 💌	
IPv4 Address	Static	
IP Address		
IPv6 for this service	Enable	
IPv6 Address	Static	
IP Address		
МТО	1492	
Continue		

### **3.** Wait while the device is configured.

Easy Sign On	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

### **4.** WAN port configuration is success.

Easy Sign On	
WAN Interface (WAN > Wireless)	
Congratulations !	
Your WAN port has been successfully configured.	
Next to Wireless Done	

Click **Done**, web configuration will be loaded, you will enter the web configuration page.

**5.** After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8700AX(L)-1600 supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wi0)	
Wireless	Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
Wireless (WAN > Wireless)		
Please wait while the device is configured.		

#### 6. Continue to set 2.4GHz wireless.

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	2.4GHz (wl1)	
Wireless	✓ Enable	
SSID	wlan-ap-2.4g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
▼ Wireless (WAN > Wireless)		
Please wait while the device is configured.		

#### **7.** Success in configuring the EZSO.

Easy Sign On	
* Process finished	
Success.	
The Easy-Sign-On process is finished. Your device has been successfully configured.	
You can now:	
1. Log onto the router management interface for more advanced settings on 192.168.1.254 2. Continue to wpad.home.gateway/wpad.dat	

3G/4G LTE

1. Select 3G/4G LTE, press Continue to go on to next step.

Easy Sign On		
WAN Interface (WAN > Wireless)		
Select WAN Interface		
Main Port	3G/4G LTE 💙 (Current Main Port: DSL)	
Username		
APN	internet	
Continue Done		

**2.** Enter the APN, username, password from your ISP, for settings about Authentication method, PIN, etc, also refer to your ISP.

Easy Sign On		
▼WAN Interface (WAN > Wireless)		
Parameters		
Mode	Use 3G/4G LTE dongle settings 💌	
APN	internet	
Username		
Password		
Authentication Method	AUTO 💌	
PIN		
Obtain DNS	Use WAN Interface     O Use Static DNS     O Parent Controls	
Primary DNS / Secondary DNS		
мти	1500	
*Warning: Entering the wrong PIN code three times will lock the SIM.		
Continue		

#### **3.** Wait while the device is configured.

Easy Sign On	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

#### 4. WAN port configuration is success.

Easy Sign On	
WAN Interface (WAN > Wireless)	
Congratulations !	
Your WAN port has been successfully configured.	
Next to Wireless Done	

Click **Done**, web configuration will be loaded, you will enter the web configuration page.

Easy Sign On	
▼WAN Interface	
Stop EZSO	
You stopped the EZSO procedure. Web Configuration will now load.	

**5.** After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8700AX(L)-1600 supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wl0)	
Wireless	✓ Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
Wireless (WAN > Wireless)		
Please wait while the device is configured.		

#### 6. Continue to set 2.4GHz wireless.

Easy Sign On		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	2.4GHz (wl1)	
Wireless	✓ Enable	
SSID	wlan-ap-2.4g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Easy Sign On		
▼ Wireless (WAN > Wireless)		
Please wait while the device is configured.		

#### 7. Success in configuring the EZSO.

Easy Sign On	
▼ Process finished	
Success.	
The Easy-Sign-On process is finished. Your device has been successfully configured.	
You can now:	
Log onto the router management interface for more advanced settings on 192.168.1.254     Continue to www.sohu.com/	

# **Chapter 4: Configuration**

# **Configuration via Web Interface**

Open your web browser; enter the IP address of your router, which by default is 192.168.1.254, and click or press 'Enter' key on the keyboard, a login prompt window will appear. The default root username and password are "admin" and "admin" respectively.

Windows Security		
The server 192.168.1.254 is asking for your user name and password. The server reports that it is from BiPAC 8700AX.		
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.		
admin  admin  Remember my credentials		
OK Cancel		

Congratulations! You are now successfully logged in to the VDSL2/ADSL2+ Router!

Once you have logged on to your BiPAC 8700AX(L)-1600 Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

Status (Summary, WAN, Statistics, Bandwidth Usage, 3G/4G LTE Status, Route, ARP, DHCP, VPN, Log)

Quick Start (Quick Start)

Configuration (LAN, Wireless 5G(wl0), Wireless 2.4G(wl1), WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)

**VPN** (IPSec, VPN Account, Exceptional Rule Group, PPTP, L2TP, OpenVPN, GRE)

Advanced Setup (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)

# **Status**

This Section gives users an easy access to the information about the working router and access to view the current status of the router. Here **Summary**, **WAN**, **Statistics**, **Bandwidth Usage**, **3G/4G LTE Status**, **Route**, **ARP**, **DHCP**, **VPN** and **Log** subsections are included.

✓ Status
Summary
• WAN
Statistics
Bandwidth Usage
<ul> <li>3G/4G LTE Status</li> </ul>
Route
• ARP
• DHCP
▶ VPN
▶ Log
Quick Start
Configuration
► VPN
►Advanced Setup

# Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).

Status		
Device Information		
Model Name	8700AXL	
Host Name	home.gateway	
System Up-Time	0D 2H 37M 11S	
Date/Time	Fri Feb 17 05:17:20 2017 Sync	
Software Version	2.52.d2	
LAN IPv4 Address	192.168.1.254	
LAN IPv6 Address	fe80::223:b8ff:fed6:9635/64	
MAC Address	00:23:b8:d6:96:35	
DSL PHY and Driver Version	A2pv6F039v.d26m	
Wireless Driver Version	7.49.6	
▼ WAN		
Line Rate - Upstream (Kbps)	0	
Line Rate - Downstream (Kbps)	0	
Default Gateway / IPv4 Address	ppp0.1 (Ethernet) / 123.204.172.185	
Connection Time	02:36:11	
Primary DNS Server	139.175.1.1	
Secondary DNS Server	8.8.8.8	
IPv6 Gateway / IPv6 Address		

#### **Device Information**

Model Name: Displays the model name.

Host Name: Displays the name of the router.

System Up-Time: Displays the elapsed time since the device is on.

Date/Time: Displays the current exact date and time. Sync button is to synchronize the

Date/Time with your PC time without regard to connecting to internet or not.

Software Version: Firmware version.

LAN IPv4 Address: Displays the LAN IPv4 address.

**LAN IPv6 Address:** Displays the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

MAC Address: Displays the MAC address.

**DSL PHY and Driver Version:** Display DSL PHY and Driver version.

Wireless Driver Version: Displays wireless driver version.

#### WAN

Line Rate – Upstream (Kbps): Displays Upstream line Rate in Kbps.

Line Rate – Downstream (Kbps): Displays Downstream line Rate in Kbps.

Default Gateway/IPv4 Address: Display Default Gateway and the IPv4 address.

**Connection Time:** Displays the elapsed time since ADSL connection is up.

Primary DNS Server: Displays IPV4 address of Primary DNS Server.

Secondary DNS Server: Displays IPV4 address of Secondary DNS Server.

**Default IPv6 Gateway/IPv6 Address:** Display the IPv6 Gateway and the obtained IPv6 address.

# WAN

This table displays the information of the WAN connections, users can turn here for WAN connection information.

Status							
WAN							
Wan Info							
Interface	Description	Туре	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64	218.2.135.1
USB3G0			3G/LTE Card not found				

Interface: The WAN connection interface.

**Description:** The description of this connection.

**Type:** The protocol used by this connection.

Status: To disconnect or connect the link.

**Connection Time:** The WAN connection time since WAN is up.

**IPv4 Address:** The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

**DNS:** The DNS address the device obtained.

# **Statistics**

#### LAN

The table shows the statistics of LAN.

Note: P5 is a configurable WAN/LAN port.

LAN Statistics														
	Received							Transmitte	ed					
Interface	Total				Multicast	Unicast	Broadcast	Total				Multicast	Unicast	Broadcast
	Bytes	Packets	Errors	Drops	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Packets	Packets	Packets
P1	1073478	7658	0	0	971	6641	46	4992894	7008	0	0	112	6881	15
P2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P3	120968	820	0	353	318	329	173	156280	373	0	0	4	359	10
P4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P5/EWAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wIO	0	0	0	3	0	0	0	389475	1226	0	0	0	0	0
wl1	0	0	0	2	0	0	0	373076	1112	0	0	1052	0	66

**Interface:** List each LAN interface. P1-P4 indicates the LAN interfaces (P5/WAN can work as a LAN port).

Bytes: Display the total Received and Transmitted traffic statistics in Bytes for each interface.

Packets: Display the total Received and Transmitted traffic statistics in Packets for each interface.

**Errors:** Display the total statistics of errors arising in Receiving or Transmitting data for each interface.

**Drops:** Display the total statistics of drops arising in Receiving or Transmitting data for each interface.

Multicast (packets): Display the Received and Transmitted multicast Packets for each interface.

Unicast (packets): Display the Received and Transmitted unicast Packets for each interface.

Broadcast (packets): Display the Received and Transmitted broadcast Packets for each interface.

Reset: Press this button to refresh the statistics.

#### **WAN Service**

#### The table shows the statistics of WAN.

WAN Se	ervice																
Statistic	S																
		Receive	d							Transmi	itted						
Interface	Description	Total				Multica	ast	Unicast	Broadcast	Total				Multica	ast	Unicast	Broadcast
		Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
ppp0.1	pppoe_0_0_33	209804	2671	0	0	0	0	2671	0	593212	2133	0	0	0	0	2133	0

Interface: Display the connection interface.

**Description:** The description for the connection.

Bytes: Display the Received and Transmitted traffic statistics in Bytes for every WAN interface.

Packets: Display the Received and Transmitted traffic statistics in Packests for every WAN interface.

**Errors:** Display the statistics of errors arising in Receiving or Transmitting data for every WAN interface.

**Drops:** Display the statistics of drops arising in Receiving or Transmitting data for every WAN interface.

**Multicast (packets):** Display the Received and Transmitted multicast Packets for every WAN interface.

Unicast (packets): Display the Received and Transmitted unicast Packets for every WAN interface.

**Broadcast (packets):** Display the Received and Transmitted broadcast Packets for every WAN interface.

**Reset:** Press this button to refresh the statistics.

#### хТМ

The Statistics-xTM screen displays all the xTM statistics

XTM										
	inting									
Interface Stat	100 070 077									
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
62 -	14467180	1330512	11347	7340	2	4	0	0	0	0

**Port Number:** Shows number of the port for xTM.

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received.

Out OAM Cells: Number of OAM cells transmitted.

In ASM Cells: Number of ASM cells received.

Out ASM Cells: Number of ASM cells transmitted.

In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

**Reset:** Click to reset the statistics.

#### xDSL

* xDSL			
xDSL			
Mode	ADSL_2plus		
Traffic Type	ATM		
Status	Up		
Link Power State	LO		
	Downstream	Upstream	
Line Coding (Trellis)	On	On	
SNR Margin (dB)	6.4	6.0	
Attenuation (dB)	2.0	0.7	
Output Power (dBm)	17.6	2.6	
Attainable Rate (Kbps)	24452	1104	
Rate (Kbps)	24328	1071	
MSGc (# of bytes in overhead channel message)	58	66	
B (# of bytes in Mux Data Frame)	254	33	
M (# of Mux Data Frames in FEC Data Frame)	1	1	
T (Mux Data Frames over sync bytes)	3	1	
R (# of check bytes in FEC Data Frame)	0	0	
S (ratio of FEC over PMD Data Frame length)	0.3349	0.9855	
L (# of bits in PMD Data Frame)	6090	276	
D (interleaver depth)	1	1	
Delay (msec)	0	0	
INP (DMT symbol)	0.00	0.00	
Super Frames	0	0	
Super Frame Errors	39	3	
RS Words	0	1722778	
RS Correctable Errors	0	0	
RS Uncorrectable Errors	0	0	
HEC Errors	1215	2	
OCD Errors	15	0	
LCD Errors	15	0	
Total Cells	420733366	402229838	
Data Cells	878484	358776	
Bit Errors	67717	0	
Total ES	30	3	
Total SES	0	0	
Total UAS	23	23	

**Mode:** Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM. **Traffic Type:** Transfer mode, here supports ATM and PTM.

**Status:** Show the status of DSL link.

Link Power State: Show link output power state.

Line Coding (Trellis): Trellis on/off.

**SNR Margin (dB):** Show the Signal to Noise Ratio(SNR) margin.

Attenuation (dB): This is estimate of average loop attenuation of signal.

Output Power (dBm): Show the output power.

Attainable Rate (Kbps): The sync rate you would obtain.

Rate (Kbps): Show the downstream and upstream rate in Kbps.

MSGc (#of bytes in overhead channel message): The number of bytes in overhead channel message.

**B (# of bytes in Mux Data Frame):** The number of bytes in Mux Data frame.

M (# of Mux Data Frames in FEC Data Frame): The number of Mux Data frames in FEC frame.

T (Mux Data Frames over sync bytes): The number of Mux Data frames over all the sync bytes.

R (# of check bytes in FEC Data Frame): The number of check bytes in FEC frame.

S (ratio of FEC over PMD Data Frame length): The ratio of FEC over PMD Data frame length

L (# of bits in PMD Data Frame): The number of bit in PMD Data frame

D (interleaver depth): Show the interleaver depth.

Delay (msec): Show the delay time in msec.

**INP (DMT symbol):** Show the DMT symbol.

Super Frames: The total number of super frames.

Super Frame Errors: the total number of super frame errors.

**RS Words:** Total number of Reed-Solomon code errors.

**RS Correctable Errors:** Total number of RS with correctable errors.

RS Uncorrectable Errors: Total number of RS words with uncorrectable errors.

HEC Errors: Total number of Header Error Checksum errors.

**OCD Errors:** Total number of out-of-cell Delineation errors.

LCD Errors: Total number of Loss of Cell Delineation.

Total Cells: Total number of cells.

Data Cells: Total number of data cells.

Bit Errors: Total number of bit errors.

Total ES: Total Number of Errored Seconds.

Total SES: Total Number of Severely Errored Seconds.

Total UAS: Total Number of Unavailable Seconds.

**xDSL BER Test:** Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.Tested Time (sec)20
Tested Time (sec) 20 -
Start Close

Select the Tested Time(sec), press **Start** to start test.

ADSL BER Test Run	ning
The xDSL BER test is	n progress.
Connection Speed	27447 Kbps
The test will run for	20 seconds
Stop Close	

When it is OK, the following test result window will appear. You can view the quality of ADSL connection. Here the connection is OK.

ADSL BER Test Resu	lt
The ADSL BER test cor	npleted successfully.
Test Time	20 seconds
Total Transferred Bits	0x00000001DA1F500
Error Ratio	0.00e+00
Close	

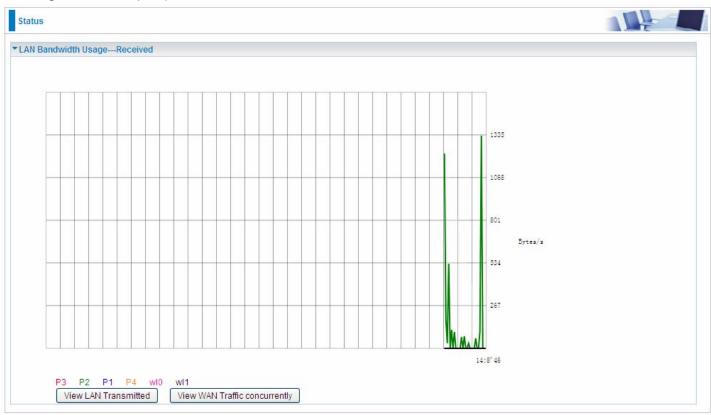
Reset: Click this button to reset the statistics.

### **Bandwidth Usage**

Bandwidth Usage provides users direct view of bandwidth usage with simple diagram. Bandwidth usage shows the use of the bandwidth from two angles: Transmitted and Received, giving users a clear idea of the usage.

#### LAN

**Note:** P5 is a configurable WAN/LAN port (here the example is in broadband WAN mode, p5 working as a WAN port).

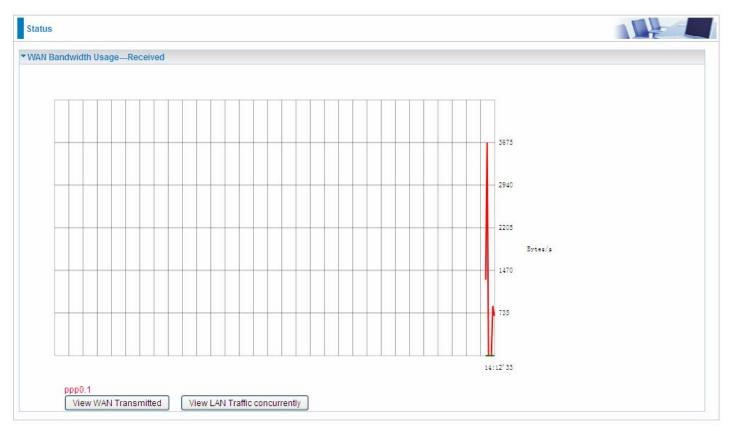


Press **View LAN Transmitted** button to change the diagram to the statistics of the LAN Transmitted Bytes. (**Note:** <u>P2</u> means Ethernet port #2, and the traffic information of the port #2 is identified with blue, the same color with port#2 in the diagram; other ports all take the same mechanism.)

When you press **View WAN Traffic concurrently** button, the WAN Bandwidth Usage pops up so that users can view the WAN traffic concurrently.



#### **WAN Service**



Press **View WAN Transmitted** button to change the diagram to the statistics of the WAN Transmitted Bytes.

Press **View LAN Traffic concurrently** button to directly switch to the LAN Bandwidth Usage page to view the LAN traffic concurrently.



### 3G/4G LTE Status

Status		
▼ 3G/4G LTE Status		
Parameters		
Status	3G/4G LTE Card not found	
Signal Strength		
Network Name	N/A	
Network Mode	N/A	
Card Name		
Card Firmware		
Current TX Bytes / Packets	0/0	
Current RX Bytes / Packets	0/0	
Total TX Bytes / Packets	0/0	
Total RX Bytes / Packets	0/0	
Total Connection Time	00:00:00	

Status: The current status of the 3G/4G LTE connection.

**Signal Strength:** The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G LTE Signal Strength LED indicates the signal strength as well.

**Network Name:** The name of the 3G/4G LTE network the router is connecting to.

**Network Mode:** The current operation mode for 3G/4G LTE module, it depends on service provider and card's limitation, GSM or UMTS.

Card Name: Given a name for the embedded 3G/4G LTE module.

Card Firmware: Current used FW in the 3G/4G LTE module.

Current Received (RX) /Transmitted (TX) Bytes: Current Rx/TX (receive/transmit) packets in Byte

Total Received (RX) /Transmitted (TX) Bytes: The total Rx/TX (receive/transmit) packets in Byte

**Total Connection Time:** The total of 3G/4G LTE dongle connection time since the 3G/4G LTE is up and running

# Route

Status						
▼Route						
Flags: U - up, ! - re	ject, G - gateway, H - ho	st, R - reinstate, D - dynamic (redir	ect), M - modified (r	redirect)		
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.46	0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp0.1
		255 255 255 0		0		br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		DIO

Destination: The IP address of destination network.

Gateway: The IP address of the gateway this route uses.

Subnet Mask: The destination subnet mask.

Flag: Show the status of the route.

- ① U: Show the route is activated or enabled.
- (i) **H** (host): destination is host not the subnet.
- **G**: Show that the outside gateway is needed to forward packets in this route.
- ① R: Show that the route is reinstated from dynamic routing.
- ① D: Show that the route is dynamically installed by daemon or redirecting.
- ① M: Show the route is modified from routing daemon or redirect.

Metric: Display the number of hops counted as the Metric of the route.

Service: Display the service that this route uses.

Interface: Display the existing interface this route uses.

# ARP

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Security** – **MAC Filtering** function. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.

▼ ARP					
ARP Table					
IP Address	Flag	MAC Address	Device	Mark	
192.168.1.100	Complete	00:18:de:ce:8f:5b	br0	wlan-ap-2.4g (2.4G)	
192.168.1.102	Complete	18:a9:05:38:04:03	br0		
172.16.1.254	Complete	00:50:7f.e0:b1:14	eth0.1		
Neighbor Cache Table					
IPv6 Address		MAC Address	Device	Mark	
fe80::d160:5adb:9009:8	7ae	00:22:64:1b:6ffd	br0		
2000:1211:1002:4f0b:bc	194:aa1e:3567:9759	00:22:64:1b:6ffd	br0		

#### **ARP table**

IP Address: Shows the IP Address of the device that the MAC address maps to.

Flag: Shows the current status of the ARP entries.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① P (publish entry): publish this route item.

**MAC Address:** Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

**Device:** here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".

Mark: Show clearly the SSID (WLAN) the device is in.

#### **Neighbor Cache Table**

IPv6 address: Shows the IPv6 Address of the device that the MAC address maps to.

**MAC Address:** Shows the MAC address that is corresponded to the IPv6 address of the device it is mapped to.

**Device:** here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".

Mark: Show clearly the SSID (WLAN) the device is in.

# DHCP

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Status				
▼ DHCP				
Leased Table				
Host Name	MAC Address	IP Address	Expires In	Mark
billion-17bc6f1	18:a9:05:38:04:03	192.168.1.100	15890 days, 4 hours, 20 minutes, 52 seconds	
vtt-PC	00:18:de:ce:8f:5b	192,168,1,101	23 hours, 56 minutes, 23 seconds	wlan-ap-2.4g (2.4G)

Host Name: The Host Name of DHCP client.

MAC Address: The MAC Address of internal DHCP client host.

IP Address: The IP address which is assigned to the host with this MAC address.

**Expires in:** Show the remaining time after registration.

Mark: Show clearly the SSID (WLAN) the device is in.

## VPN

VPN status viewing section provides users IPSec, PPTP, L2TP and GRE VPN status.

#### **IPSec**

PSec Status						
VPN Tunnels						
Name	Active	Local Subnet	Remote Subnet	Remote Gateway	SA	
11	×	192.168.1.0 255.255.255.0	192.168.0.0 255.255.255.0	172.16.1.235		

Name: The IPSec connection name.

Active: Display the connection status.

Local Subnet: Display the local network.

**Remote Subnet:** Display the remote network.

Remote Gateway: The remote gateway address.

**SA:** The Security Association for this IPSec entry.

#### PPTP

▼PPTP Status						
PPTP Server •						
Name 🕨	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test	$\checkmark$	Connected	Remote Access		172.16.1.207	Drop
PPTP Client •						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action

#### **PPTP Server**

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

**Peer Network IP:** Display the remote (client side) network and subnet mask in LAN to LAN PPTP connection.

Connected By: Display the IP of remotely connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

#### **PPTP Client**

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

**Peer Network IP:** Display the remote (server side) network and subnet mask.

**Client:** Assigned IP by PPTP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

L2TP Status						
L2TP Server	•					
Name 🕨	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test1	$\checkmark$	Connected	Remote Access		192.168.1.10	Drop
L2TP Client •						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action

#### **L2TP Server**

Name: The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

**Peer Network IP:** Display the remote (client side) network and subnet mask in LAN to LAN L2TP connection.

Connected By: Display the IP of remotely connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

#### **L2TP Client**

**Name:** The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the network and subnet mask of server side.

Client: Assigned IP by L2TP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

#### OpenVPN

OpenVPN S	tatus						
OpenVPN Se	rver 🕨						
Name 🕨	Enable	Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
test1	$\checkmark$	Connected	Remote Access		192.168.15.1	192.168.15.22	Drop
OpenVPN Cli	ent⊁						
Name	Enable	Status	Peer Network IP	Client IP	Action		
Refresh							
Status	tatus						L.
Status ▼ OpenVPN S						1	E
Status • OpenVPN S OpenVPN Se		Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
Status ▼OpenVPN S OpenVPN Se Name ►	rver • Enable	Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
Refresh Status • OpenVPN Se Name • OpenVPN Cli Name	rver • Enable	Status	Connection Type Peer Network IP	Peer Network IP Client IP	Server IP Action	Connect By	Action

#### **OpenVPN Server**

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the subnet address of client side in LAN to LAN mode.

Server IP: The tunnel virtual IP of server side assigned by server itself.

**Connected By:** The assigned tunnel virtual IP to remotely connected OpenVPN client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

#### **OpenVPN Client**

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the tunnel virtual address (WAN address) of server side.

Client: Assigned tunnel virtual IP by OpenVPN server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

GRE

GRE Status				
Name	Enable	Status	Remote Gateway IP	
test3	1	Connected	69.121.1.22	

Name: The GRE connection name.

Enable: Display the connection status with icons.

Status: The connection status, connected or disable.

Remote Gateway: The IP of remote gateway.

# Log

#### System Log

Display system logs accumulated up to the present time. You can trace historical information with this function. And the log policy can be configured in <u>Configure Log</u> section.

item Log		
	Jan 1 00:03:52 daemon err FDNSLOGIN: FakedDnsProxy is closed Jan 1 00:03:52 daemon info FDNSLOGIN: shutdown Jan 1 00:04:03 kern crit kernel: eth4 (Int switch port: 3) (Logical Port: 3) Link UP 100 mbps full duplex Jan 1 00:04:03 kern warn kernel: ADDRCONF(NETDEV_CHANGE): eth4: link becomes ready Jan 1 00:04:03 kern warn kernel: eth4.1 MAC address set to 00:04:ED:36:96:8A Jan 1 00:04:03 kern warn kernel: netdev path : eth4.1 -> eth4 Jan 1 00:04:03 kern warn kernel: BCMVLAN : eth4 mode was set to RG Jan 1 00:04:03 kern info kernel: device eth4 entered promiscuous mode May 27 05:30:56 kern crit kernel: eth1 (Ext switch port: 2) (Logical Port: 10) Link DOWN. May 27 05:30:56 kern info kernel: br0: port 2(eth1.0) entered disabled state May 27 05:31:14 kern crit kernel: eth1 (Ext switch port: 2) (Logical Port: 10) Link UP 1000 mbps full duplex May 27 05:31:14 kern info kernel: ADDRCONF(NETDEV_CHANGE): eth1.0: link becomes ready May 27 05:31:14 kern info kernel: br0: port 2(eth1.0) entered forwarding state May 27 05:31:14 kern info kernel: br0: port 2(eth1.0) entered forwarding state	

**Refresh:** Click to update the system log. **Clear:** Click to clear the current log from the screen.

#### Security Log

Security log displays the message logged about security, like filter messages and some firewall message. You can turn to <u>IP Filtering Outgoing</u>, <u>IP Filtering Incoming</u>, <u>URL Filter</u> to determine if you want to log this information. Also you can turn to Configure Log section below to determine the level to log the message. You can use this to track potential threats to your system and network.

Status	
▼ Security Log	
Refresh Clear	

Refresh: Click to update the security log.

**Clear:** Click to clear the current log from the screen.

# **Quick Start**

### **Quick Start**

This part allows you to quickly configure and connect your router to internet.

#### DSL mode (ADSL mode, please choose ATM; VDSL, please choose PTM)

Here take ADSL for example.

Quick Start		
WAN Interface (WAN > Wireless		
Select WAN Interface		
Main Port	DSL (Current Main Port: DSL)	
Layer2 Interface	⊙ ATM ○ PTM	
VPI/VCI	8/35	
Туре	PPPoE	
Username	username	
WAN IP Address	Obtain an IP Address Automatically	
Continue		

Select DSL, press **Continue** to go on to next step. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.

Quick Start		
<pre>wan interface (WAN &gt; Wireless)</pre>		
WAN Service		
Туре	PPP over Ethernet (PPPoE)	
VPI/VCI	[0-255] / [32-65535]	
Username		
Password		
Service Name		
Encapsulation Mode	LLC/SNAP-BRIDGING	
Authentication Method	AUTO	
IPv4 Address	Static	
IP Address		
IPv6 for this service	✓ Enable	
IPv6 Address	Static	
IP Address		
МТО	1492	
Continue		

If the DLS line is not synchronized, the page will pop up warning of the DSL connection failure.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
DSL Line Is Not Ready. Please Check your DSL Line and wait for a while.	

#### 3. Wait while the device is configured.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

#### 4. WAN port configuration is successful.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
Congratulations !	
Your WAN port has been successfully configured.	
Next to Wireless	

**5**. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8700AX(L)-1600 supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Quick Start		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wi0)	
Wireless	✓ Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Quick Start		
Wireless (WAN > Wireless)		
Please wait while the device is configur	ha	

#### 6. Continue to set 2.4GHz wireless.

Quick Start		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	2.4GHz (wl1)	
Wireless	Enable	
SSID	wlan-ap-2.4g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Quick Start		
▼ Wireless (WAN > Wireless)		
Please wait while the device is configure	d.	

#### 7. Success.

Quick Start

Process finished
 Success.

Go back to **Status** > **Summary** for more information.

#### **Ethernet mode**

1. Select Ethernet, press Continue to go on to next step.

Quick Start		
▼ WAN Interface (WAN > Wireless)		
Select WAN Interface		
Main Port	Ethernet 🗹 (Current Main Port: DSL)	
Continue		

**2.** Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.

Quick Start		
<pre>wan interface (WAN &gt; Wireless)</pre>		
WAN Service		
Туре	PPP over Ethernet (PPPoE)	
Username		
Password		
Service Name		
Authentication Method	AUTO 💌	
IPv4 Address	Static	
IP Address		
IPv6 for this service	✓ Enable	
IPv6 Address	Static	
IP Address		
МТО	1492	
Continue		

#### **3.** Wait while the device is configured.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

#### **4.** WAN port configuration is successful.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
Congratulations !	
Your WAN port has been successfully configured.	
Next to Wireless	

**5.** After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The device supports dual-band wireless connections, in Quick Start part, users can only enable or disable the wireless on the band and the exact SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES). For detail setting, please go to the Wireless part in this Manual.

Quick Start		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wi0)	
Wireless	Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Quick Start		
Wireless (WAN > Wireless)		
Please wait while the device is configured		

#### 6. Continue to set 2.4GHz wireless.

Quick Start		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	2.4GHz (wl1)	
Wireless	Enable	
SSID	wlan-ap-2.4g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Quick Start		
Wireless (WAN > Wireless)		
Please wait while the device is configured.		

#### 7. Success.

Quick Start	
▼ Process finished	
Success.	

Go back to Status > Summary for more information

#### 3G/4G LTE

#### 1. Select 3G/4G LTE, press Continue to go on to next step.

Quick Start		
WAN Interface (WAN > Wireless)		
Select WAN Interface		
Main Port	3G/4G LTE 💟 (Current Main Port: DSL)	
Username		
APN	internet	
Continue		

**2.** Select the 3G mode, and enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting.

Quick Start		
▼WAN Interface (WAN > Wireless)		
Parameters		
Mode	Use 3G/4G LTE dongle settings 👻	
APN	internet	
Username		
Password		
Authentication Method	AUTO 🔽	
PIN		
МТО	1500	
Obtain DNS	⊙ Use WAN Interface O Use Static DNS O Parent 0	Controls
Primary DNS / Secondary DNS	/	
*Warning: Entering the wrong PIN code three tim	as will lock the SIM.	
Continue		

#### **3.** Wait while the device is configured.

Quick Start	
▼ WAN Interface (WAN > Wireless)	
Please wait while the device is configured.	

#### 4. WAN port configuration is successful.

Quick Start	
WAN Interface (WAN > Wireless)	
Congratulations !	
Your WAN port has been successfully configured.	
Next to Wireless	

**5.** After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The device supports dual-band wireless connections, in Quick Start part, users can only enable or disable the wireless on the band and the exact SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES). For detail setting, please go to the Wireless part in this Manual.

Quick Start		
▼Wireless (WAN > Wireless > VOIP)		
Parameters		
Band	5GHz (wi0)	
Wireless	✓ Enable	
SSID	wlan-ap-5g	
WPA2 Pre-Shared Key	Click here to display	
Continue		
Quick Start		
Wireless (WAN > Wireless)		
Please wait while the device is configured	í.	

#### 6. Continue to set 2.4 GHz wireless.

Quick Start	
2.4GHz (wl1)	
Enable	
wlan-ap-2.4g	
Click here to display	
	Enable wlan-ap-2.4g

#### 7. Success.

Quick Start	
▼ Process finished	
Success.	

Go back to **Status > Summary** for more information.

# Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

LAN, Wireless 5G (wl0), Wireless 2.4G (wl1), WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT and Wake On LAN.

▶ Status
· Quick Start
<ul> <li>Configuration</li> </ul>
LAN
Wireless 5G (wl0)
Wireless 2.4G (wl1)
▶ WAN
System
▶ USB
IP Tunnel
Security
Quality of Service
▶ NAT
• Wake On LAN
▶ VPN
►Advanced Setup

The function of each configuration sub-item is described in the following sections.

# LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

# Ethernet

Configuration				
▼LAN				
Parameters				
Group Name	Default 💌			
IP Address	192.168.1.254			
Subnet Mask	255.255.255.0			
IGMP Snooping	Enable			
IGMP Snooping Mode	O Standard Mode 💿 Block	ing Mode		
IGMP LAN to LAN Multicast	Enable(LAN to LAN Multica	ast is enabled until the first WAN service	is connected, regardless of th	is setting.)
LAN side firewall	Enable			
DHCP Server				
DHCP Server	Enable 💌			
Start IP Address	192.168.1.100			
End IP Address	192.168.1.199			
Leased Time (hour)	24			
Option 66	Enable			
Use Router's setting as DNS Server				
Primary DNS server				
Secondary DNS server				
Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
Add				
IP Alias				
IP Alias	Enable Enable			
IP Address				
Subnet Mask				
Apply Cancel				

# **Parameters**

**Group Name:** This refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group via the drop-down box. For more information please refer to Interface Grouping of this manual.

**IP address:** the IP address of the router. Default is 192.168.1.254.

Subnet Mask: the default Subnet mask on the router.

**IGMP Snooping:** Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

When enabled, you will see two modes:

- Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ③ Blocking Mode: In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

**IGMP LAN to LAN Multicast:** Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he wants to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

**LAN side firewall:** Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to <u>IP Filtering Incoming</u> to add the allowing rules. **Note** that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this CPE from the specified LAN group.

#### **DHCP Server**

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

#### i) Disable

DHCP Server	
DHCP Server	Disable 💌

Disable the DHCP Server function.

# i Enable

Enable the DHCP function, enter the information wanted. Here as default.

DHCP Server	
DHCP Server	Enable 🗸
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Leased Time (hour)	24
Option 66	Enable
Use Router's setting as DNS Server	
Primary DNS server	
Secondary DNS server	

Start IP Address: The start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: The end IP address f the range the DHCP Server used to assign to the Clients.

Leased Time (hour): The leased time for each DHCP Client.

**Option 66:** Click Enable to activate DHCP option 66 for some special devices, like IPTV Set Box. The devices can get firmware or some special service from the TFTP server. User needs to set the IP or hostname of the TFTP server.

**User Router's setting as DNS server:** Select whether to enable use router's setting as DNS server, if enabled, the PCs on the LAN side obtain the router's setting as DNS server. If disabled, please specify exactly the primary/secondary DNS server.

Primary/Secondary DNS server: Specify your primary/secondary DNS server for your LAN devices.

#### **(i)** DHCP Server Relay

DHCP Server	
DHCP Server	DHCP Server Relay 🗸
DHCP Server IP Address	

DHCP Server IP Address: Please enter the DHCP Server IP address.

#### **Static IP List**

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients.

Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
Add				

#### Press Add to the Static IP List.

Configuration	
▼ Static IP	
Parameters	
Host Label	
MAC Address	
IP Address	
Apply Cancel	

Enter the MAC Address, IP Address, and then click Apply to confirm your settings. But the IP assigned should be outside the range of 192.168.1.100-192.168.1.199.

Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
HP	18:a9:05:38:04:05	192.168.1.200		Edit

#### **IP** Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node.

IP Alias		
IP Alias	Enable	
IP Address		
Subnet Mask		
Apply Cancel		

**IP Alias:** Check whether to enable this function.

**IP Address:** Specify an IP address on this virtual interface.

Subnet Mask: Specify a subnet mask on this virtual interface.

Click **Apply** to apply your settings.

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is "stateful" configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful autoconfiguration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is "stateless" configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

Configuration	
▼ IPv6 Autoconfig	
Parameters	
Note: Interface ID does NOT support ZERO COMPRESSIO For exampe: Please enter "0:0:0:2" instead of "::2".	IN "::". Please enter the complete information.
Group Name	Default 💌
Static LAN IPv6 Address Configuration	
Interface Address / Prefix Length	
IPv6 LAN Applications	
DHCPv6 Server	✓ Enable
DHCPv6 Server Type	
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	✓ Enable
ULA Prefix Advertisement	
RADVD Type	
Prefix	
Preferred Life Time	-1
Valid Life Time	-1
MLD Snooping	✓ Enable
MLD Snooping Mode	O Standard Mode 💿 Blocking Mode
MLD LAN to LAN Multicast	Enable(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
Apply Cancel	

**Group Name:** Here group refers to the group you set in **Interface Grouping** section, you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

#### Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

#### **IPv6 LAN application**

**DHCPv6 Server:** Check whether to enable DHCPv6 server.

**DHCPv6 Server Type:** Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available. **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server. **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

**Start interface ID:** Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID.

**Note:** Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.

For example: Please enter "0:0:0:2" instead of "::2".

**Leased Time (hour):** The leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

**Issue Router Advertisement:** Check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

**ULA Prefix Advertisement:** Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

**RADVD Type:** The way that ULA prefix is generated.

- Randomly Generated
- ① Statically Configured: select to set manually in the following parameters.

**Prefix:** Set the prefix manually.

**Preferred Life Time:** The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

**Valid Life Time:** It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

**MLD snooping:** Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

- ③ Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ③ Blocking Mode: In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

**MLD LAN to LAN Multicast:** Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled

Stateless: Two methods can be carried.

③ With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv	6 Server	Enable
Issue F	Router Advertisements	🗹 Enable

With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

③ With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	🗹 Enable
DHCPv6 Server Type	⊙ Stateless ○ Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	Enable

With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

#### Stateful: two methods can be adopted.

With only DHCPv6 enabled

DHCPv6 Server	🗹 Enable
DHCPv6 Server Type	🔘 Stateless 💿 Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	Enable

With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are assigned by DHCPv6 server.

#### () With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	🗹 Enable
DHCPv6 Server Type	🔘 Stateless 💿 Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	Enable

With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

(Please **Note:** P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.)

Interface Grouping				
Groups Isolation		Enable 🗌		
Apply				
Group Configuration				
Maximum number of entries car	n be configured : 16			
Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
		ppp0.1	P1	
Default		P2		
		P3		
		P4		
		P5/EWAN		
		wlan-ap-2.4g		
		wlan-ap-5g		

Groups Isolation: If enabled, devices in one group are not able to access those in the other group.

# Click **Add** to add groups.

Configuration	
▼ Interface grouping Configuration	
Parameters	
If you like to automatically add LAN clients to a WAN Interface in the By configuring a DHCP vendor ID string any DHCP client request IMPORTANT If a vendor ID is configured for a specific client device	ne new group add the DHCP vendor ID string. with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. e, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name	
Grouped WAN Interfaces	Available WAN Interfaces
	<pre>&gt;&gt; </pre>
Grouped LAN Interfaces	Available LAN Interfaces
	P1 P2 P3 P4 P5/EWAN wlan-ap-2.4g wlan-ap-5g
Automatically Add Clients With the following DHCP Vendor IDs	
Apply Cancel	

Group Name: Type a group name.

Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

**Grouped LAN Interfaces:** Select the LAN interfaces you want to group as a single group from *Available LAN Interfaces*.

Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.

In group "test", P2 and PPP0.1 are grouped in one group, they have their only network , see LAN.

Configuration				
▼Interface Grouping				
Groups Isolation		Enable 🛄		
Apply				
Group Configuration				
Maximum number of entries car	be configured : 16			
Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
		P1		
			P3	
Default		P4		
		P5/EWAN		
		wlan-ap-2.4g		
		wlan-ap-5g		
test		ppp0.1	P2	
Add Remove				

If you want to remove the group, check the box as the following and press **Remove**.

Configuration				
Interface Grouping				
Groups Isolation		Enable 🗌		
Apply				
Group Configuration				
Maximum number of entries car	n be configured : 16			
Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
		P1		
			P3	
			P4	
Default		P5/EWAN		
		wlan-ap-2.4g		
		wlan-ap-5g		
est		ppp0.1	P2	

**Note:** If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

# Wireless 5G(wl0) & 2.4G(Wl1)

BiPAC 8700AX(L)-1600 is a simultaneous dual-band (2.4G and 5G) wireless router supporting 11b/g/n/a/ac wireless standards. It allows multiple wireless users on 2.4G and 5G radio bands to surf the Internet, checking e-mail, watching video, listening to music over the Internet concurrently. You can choose the optimum radio band wireless connection base on your environment.

► Status	
Quick Start	
▼Configuration	
LAN	
Wireless 5G (wl0)	
Wireless 2.4G (wl1)	
• WAN	
System	
▶ USB	
IP Tunnel	
Security	
Quality of Service	
▶ NAT	
· Wake On LAN	
► VPN	
►Advanced Setup	

#### Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.

Configuration			
* Basic			
Parameters			
Wireless	✓ Enable		
Hide SSID	Enable		
Clients Isolation	Enable		
Disable WMM Advertise	Enable		
Wireless Multicast Forwarding (WMF)	Enable		
SSID	wlan-ap-2.4g		
BSSID	00:04:ED:01:00:02		
Country	UNITED STATES		
Country RegRev	0		
Max Clients	16 [1-16]		
Wireless - Guest/Virtual Access Points			
SSID	Hidden Clients Isolation Disable WMM Advertise WMF Max Clients BSSID Enable		
wI0_Guest1	□ □ □ 16 N/A □		
wI0_Guest2			
wI0_Guest3	□ □ □ 16 N/A □		
Apply Cancel			

**Wireless:** Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

**Hide SSID:** It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

**Clients Isolation:** if you enabled this function, then each of your wireless clients will not be able to communicate with each other.

**Disable WMM Advertise:** Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

**SSID:** The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default *wlan-ap-2.4g* to a unique ID name to the AP already builtin to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not exceed 32 characters.

**BSSID:** Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

**Country:** Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports, 1-16.

**Guest/virtual Access Points:** A "Virtual Access Point" is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple "Virtual APs", each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising

a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

# Security

Wireless security prevents unauthorized access or damage to computers using wireless network.

Configuration		
▼ Security		
If Hide Access Point enabled or Mac filter list	is empty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup		
WPS	Disable 🖌 (Current Disable)	
Manual Setup AP		
Select SSID	wlan-ap-2.4g	
Network Authentication	Open	
WEP Encryption	Disabled 💌	
Apply Cancel		

#### Note:

The WPS feature will also be unavailable when the security setting is not WPA2 PSK or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

#### **Manual Setup AP**

Select SSID: select the SSID you want these settings apply to.

#### **Network Authentication**

Open

Network Authentication	Open 🗸	
WEP Encryption	Enable 🗸	
Encryption Strength	128-bit 💌	
Current Network Key	1 🗸	
Network Key 1	1234567890123	
Network Key 2	1234567890123	
Network Key 3	1234567890123	
Network Key 4	1234567890123	
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.		

**WEP Encryption:** Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1-4 below.

**Network Key (1- 4):** Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

# (i) Shared

This is similar to network authentication 'Open'. But here the WEP Encryption must be enabled.

1		
Network Authentication	Shared 💌	
WEP Encryption	Enable 🗸	
Encryption Strength	128-bit 💌	
Current Network Key	2 💌	
Network Key 1	1234567890123	
Network Key 2	1234567890123	
Network Key 3	1234567890123	
Network Key 4	1234567890123	
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.		

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

# i) 802.1x

Network Authentication	802.1X 🗸	
RADIUS Server IP Address	0.0.0.0	
RADIUS Port	1812	
RADIUS Key		
WEP Encryption	Enable 🗸	
Encryption Strength	128-bit 💌	
Current Network Key	2 🗸	
Network Key 1	1234567890123	
Network Key 2	1234567890123	
Network Key 3	1234567890123	
Network Key 4	1234567890123	
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.		

**RADIUS Server IP Address:** RADIUS( Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2-3 below.

**Network Key (1- 4):** Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Network Authentication	WPA2
Protected Management Frames	Disable 🗸
WPA2 Preauthentication	Disable 💌
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled 🕑

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**WPA2 Preauthentication:** When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

**WPA Group ReKey Internal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

**RADIUS Server IP Address:** RADIUS( Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. This is in seconds.

**RADIUS Server Port:** Enter the port number of RADIUS authentication server here.

**RADIUS Key:** Enter the password of RADIUS authentication server.

**WPA/WAPI Encryption:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

# **WPA2-PSK**

Network Authentication	WPA2 -PSK	¥
Protected Management Frames	Disable 💌	
WPA/WAPI passphrase	•••••	Click here to display
WPA Group Rekey Interval	3600	[0-2147483647]
WPA/WAPI Encryption	AES 🗸	
WEP Encryption	Disabled \vee	

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can click here to display to view it.

**WPA Group ReKey Internal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

**WPA/WAPI Encryption:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

# Mixed WPA2/WPA

Network Authentication	Mixed WPA2/WPA
Protected Management Frames	Disable 🗸
WPA2 Preauthentication	Disable 💌
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled 🔽

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**WPA2 Preauthentication:** When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

**WPA Group ReKey Internal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

**RADIUS Server IP Address:** RADIUS( Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

**RADIUS Server Port:** Enter the port number of RADIUS authentication server here.

**RADIUS Key:** Enter the password of RADIUS authentication server.

**WPA/WAPI Encryption:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

# **i** Mixed WPA2/WPA-PSk

Network Authentication	Mixed WPA2/WPA -PSK		
Protected Management Frames	Disable 💌		
WPA/WAPI passphrase	•••••	Click here to display	
WPA Group Rekey Interval	3600	[0-2147483647]	
WPA/WAPI Encryption	AES 💌		
WEP Encryption	Disabled \vee		

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can click here to display to view it.

**WPA Group ReKey Internal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

**WPA/WAPI Encryption:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

#### **WPS Setup**

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure Ap settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known **PIN method** is supported to configure WPS.

**WPS:** Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

#### Note:

1) WPS feature is only available when in WPA2 PSK or OPEN mode in security settings.

2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select "Configured" in the WPS AP Mode below, and default WPS AP Mode is "Configured". When AP is configured as Enrollee, the WPS AP Mode below should be changed to "Unconfigured". Follow the following steps.

Configuration	
* Security	
If Hide Access Point enabled or Mac filter li	st is empty with 'allow' chosen, WPS2 will be disabled.
WPS Setup	
WPS	Enable V (Current: Disable)
Add Client	Use STA PIN OUse AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	Help
Authorized Station MAC	Help
WPS AP Mode	Configured V
Setup AP (Configure all security settings with	th an external registrar)
Device PIN	10864111 Help
Manual Setup AP	
Select SSID	wian-ap-2.4g 🗸
Network Authentication	Open 🗸
WEP Encryption	Disabled V
Apply Cancel	

# **Configure AP as Registrar**

# Add Enrollee with PIN method

- 1. Select radio button "Enter STA PIN".
- 2. Input PIN from Enrollee Station (16837546 in this example), Or else users can **alternatively** enter the authorized station MAC *Help:* it is to help users to understand the concept and correct operation.

Configuration	
▼ Security	
If Hide Access Point enabled or Mac filter list	st is empty with 'allow' chosen, WPS2 will be disabled.
WPS Setup	
WPS	Enable V (Current: Disable)
Add Client	Use STA PIN Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEI mode is configured)
PIN	16837546 Help
Authorized Station MAC	Help
WPS AP Mode	Configured
Setup AP (Configure all security settings wi	th an external registrar)
Device PIN	10864111 Help
Manual Setup AP	
Select SSID	wlan-ap-2.4g 🗸
Network Authentication	Open 🗸
WEP Encryption	Disabled V

# (Station PIN)

Configuration	
* Security	
If Hide Access Point enabled or Mac filter list	st is empty with 'allow' chosen, WPS2 will be disabled.
WPS Setup	
WPS	Enable V (Current: Disable)
Add Client	Use STA PIN OUse AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	Help
Authorized Station MAC	18:A9:05:38:04:08
WPS AP Mode	Configured V
Setup AP (Configure all security settings wi	th an external registrar)
Device PIN	10864111 Help
Manual Setup AP	
Select SSID	wlan-ap-2.4g 🗸
Network Authentication	Open 🗸
WEP Encryption	Disabled V
Apply Cancel	

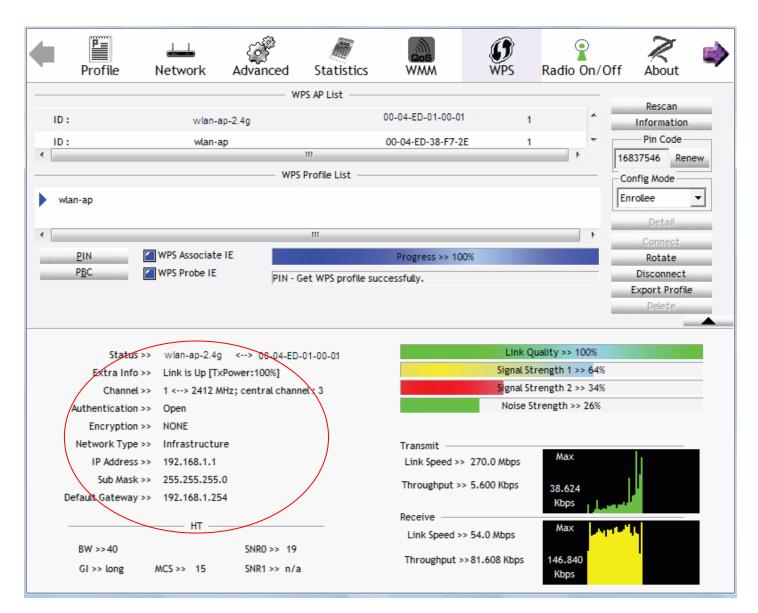
# (Station MAC)

Note: Users can alternatively input PIN from Enrollee Station or enter the authorized station MAC.

4. Operate Station to start WPS Adding Enrollee. Launch the wireless client's WPS utility (eg.Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. Wlan-ap-2.4g) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

Profile	e Netw	vork	ر Advanced	Statistics	WMM	<b>Ø</b> WPS	Radio On/	/Off Ab	≷ I
				PS AP List					scan
ID:0x0000		wlan-ap			00-04-ED-01-00-02	1	^	ALL A LA ALL AND A	mation
ID:		wlan-ap	-2.4g		00-04-ED-00-00-01	1	-	Pin	Code
				111			•	16837546	Renew
			WPS	Profile List				Config M	ode
								Enrollee	•
								De	tail
		_					•	Con	nect
PIN	wps 🖉	ssociate IE			Progress >> 0%			Rol	tate
PBC	🔬 📶 WPS F	Probe IE	WPS st	tatus is disconne	cted			and the second s	onnect
								Export	t Profile
								the second se	
								the second se	lete
Extra	Info >>	onnected				Signal S	Quality >> 0% trength 1 >> 0%	<u>De</u>	
Extra	a Info >> annel >>	onnected				Signal S Signal S	trength 1 >> 09 trength 2 >> 09	<u>D</u> d %	
Extra Ch Authentic	annel >> ation >>	onnected				Signal S Signal S	trength 1 >> 09	<u>D</u> d %	
Extra Ch Authentic Encry	a Info >> annel >> ation >> ption >>	onnected				Signal S Signal S	trength 1 >> 09 trength 2 >> 09	<u>D</u> d %	
Extra Ch Authentic Encry Network	annel >> ation >> ption >> Type >>	onnected			Transmit	Signal S Signal S	trength 1 >> 09 trength 2 >> 09	<u>D</u> d %	
Extra Ch Authentic Encry Network IP Ad	annel >> ation >> ption >> Type >> dress >>	onnected			Link Speed >>	Signal S Signal S	trength 1 >> 09 trength 2 >> 09 Strength >> 0%	<u>D</u> d %	
Extra Ch Authentic Encry Network IP Ad Sub	annel >> ation >> ption >> Type >> dress >> Mask >>	onnected				Signal S Signal S	trength 1 >> 09 trength 2 >> 09 Strength >> 0% Max 0.000	<u>D</u> d %	
Extra Ch Authentic Encry Network IP Ad	annel >> ation >> ption >> Type >> dress >> Mask >>	onnected			Link Speed >> Throughput >>	Signal S Signal S	trength 1 >> 09 trength 2 >> 09 Strength >> 0%	<u>D</u> d %	
Extra Ch Authentic Encry Network IP Ad Sub	annel >> ation >> ption >> Type >> dress >> Mask >>	onnected			Link Speed >> Throughput >> Receive	Signal S Signal S	trength 1 >> 09 trength 2 >> 09 Strength >> 0% Max 0.000	<u>D</u> d %	
Extra Ch Authentic Encry Network IP Ad Sub	annel >> ation >> ption >> Type >> dress >> Mask >> eway >>		SNR0 >> n/a		Link Speed >> Throughput >>	Signal S Signal S	trength 1 >> 09 trength 2 >> 09 Strength >> 0% Max 0,000 Kbps	<u>D</u> d %	

4. The client's SSID and security settings will now be configured to match the SSID and security settings of the registrar.



You can check the message in the red ellipse with the security parameters you set, here we all use the default.

# Configure AP as Enrollee

# Add Registrar with PIN Method

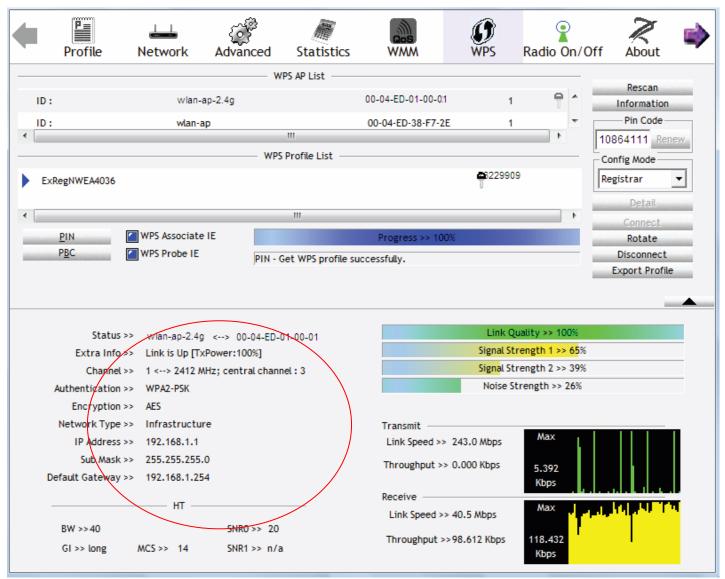
# 1. Set AP to "*Unconfigured Mode*".

Configuration	
* Security	
If Hide Access Point enabled or Mac filter lis	st is empty with 'allow' chosen, WPS2 will be disabled.
WPS Setup	
WPS	Enable V (Current: Disable)
Add Client	O Use STA PIN Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
WPS AP Mode	Unconfigured V
Setup AP (Configure all security settings wi	th an external registrar)
Device PIN	10864111 Help
Manual Setup AP	
Select SSID	wlan-ap-2.4g 🗸
Network Authentication	Open 🗸
WEP Encryption	Disabled V
Apply Cancel	

2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as **Registrar**. Enter the **PIN** number (10864111 (device) for example) in the PIN Code column then choose the correct AP (eg. wlan-ap-2.4g) from the WPS AP List section before pressing the PIN button to run the scan.

•	Profile	LLL Network	ر Advanced	Statistics	Cos WMM	() WPS	Radio On/	Off About	
			w	PS AP List					
ID	: 0x0000	wlan-a	ap-2.4g		00-04-ED-01-00-01			Rescan	
ID		D2-VP			00-1B-11-E4-DA-D5	,	• •	Pin Code	
•		02.411	`		001011240803			10864111 Renew	
			WPS	Profile		(		Config Mode	
E	xRegNWEA4036					•		Registrar 🔻	
	B							Detail	
•				III			+	Connect	
-	<u>P</u> IN	WPS Associate	IE		Progress >> 0%			Rotate	
100000	P <u>B</u> C	WPS Probe IE	·					Disconnect	
			1					Export Profile	
	Status	>> Disconnected				Link	Quality >> 0%		
	Extra Info	>>				Signal	Strength 1 >> 0%		
	Channel	>>				Signal	Strength 2 >> 0%		
	Authentication	>>				Noise	Strength >> 0%		
	Encryption	>>							
	Network Type	>>			Transmit —				
	IP Address	>>			Link Speed >>		Max		
	Sub Mask	>>			Throughput >>		0.000		
	Default Gateway	>>					Kbps		
		— нт —			Receive		Max		
					Link Speed >>		Max		
	BW >>n/a		SNR0 >> n/a		Throughput >>		0.000		
	GI >> n/a	MCS >> n/a	SNR1 >> n/a	L			Kbps		

3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

#### **MAC Filter**

Configuration		
▼MAC Filter		
Parameters		
Select SSID	wlan-ap-2.4g 💌	
MAC Restrict Mode *	● Disable ○ Allow ○ Deny	
* If 'allow' is chosen and mac filter is emp	ty, WPS will be disabled.	
MAC Address	Remove	Edit
Add Remove		

Select SSID: select the SSID you want this filter applies to.

#### **MAC Restrict Mode:**

- ① **Disable:** disable the MAC Filter function.
- (i) Allow: allow the hosts with the following listed MACs to access the wireless network.
- (i) **Deny**: deny the hosts with the following listed MACs to access the wireless network.

Click Add to add the MACs.

Configuration		
▼MAC Filter		
Parameters		
MAC Address	f0:de:f1:31:36:68 < <type from="" listbo<="" or="" select="" td=""><td>)X 🗸</td></type>	)X 🗸
Apply Cancel		

Click **Apply** to apply your settings and the item will be listed below.

Configuration			
▼MAC Filter			
Parameters			
Select SSID	wlan-ap-2.4g 💌		
MAC Restrict Mode *	O Disable   Allow O Deny		
* If 'allow' is chosen and mac filter is empty	WPS will be disabled.		
MAC Address	Remove	Edit	
F0:DE:F1:31:36:68		Edit	
Add Remove			

To delete entries , check the remove checkbox and press **Remove** to delete it. To make changes, click **Edit** of a MAC address to reconfigure the MAC as needed.

#### Wireless Bridge

WDS (wireless distributed system) is a system enabling the wireless interconnection of access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Configuration		
▼Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables wirele Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless Only those bridges selected in Remote Bridges will be e	pridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address		
Apply Refresh		

**Bridge Restrict:** It determines whether the gateway will communicate with all other bridges or only specific ones:

① Enable: to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.

Bridge Restrict	Enable
Remote Bridges MAC Address	
Apply Refresh	

**Remote Bridge MAC Address:** enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

① Enabled (Scan): to enable wireless bridge restriction. Only those scanned by the gateway can communicate.

Bridge Restrict	Enabled(Scan)	~	
Remote Bridges MAC Address		SSID wlan-ap	BSSID 00:04:ED:14:27:13
Apply Refresh			

**Remote Bridge MAC Address:** select the remote bridge MAC addresses.

① Disable: Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.

Bridge Restrict	Disable 🗸
Apply Refresh	

Click **Apply** to apply your settings.

#### Example: How to set up WDS/Wireless Bridge

Before setting up WDS:

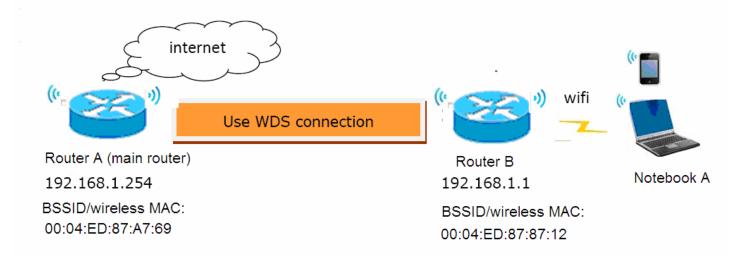
1). The router involved should all support **WDS/Wireless Bridge** feature.

2). To ensure better compatibility, please use the router of the same brand, or better the same model.

#### Point to Point wireless bridge

Router B needs to bridge to Router A using wireless bridge for internet access and wireless coverage extension.

Router B shares the same Wireless SSID, Country, Security, Channel setting with Router A.



# **Router A setup**

1). Login to Router A (LAN IP Address: 192.168.1.254), enable DHCP server.

Configuration			
TLAN			
Parameters			
Group Name	Default 🗸		
P Address	192.168.1.254		
Subnet Mask	255.255.255.0		
GMP Snooping	I Enable		
GMP Snooping Mode	O Standard Mode   Block	king Mode	
GMP LAN to LAN Multicast	Enable(LAN to LAN Multio	ast is enabled until the first WAN service is	connected, regardless of this setting.)
LAN side firewall	Enable		
DHCP Server			
DHCP Server	Enable		
Start IP Address	192.168.1.100		
End IP Address	192.168.1.199		
eased Time (hour)	24		
Option 66	Enable		
Jse Router's setting as DNS Server			
Primary DNS server			
Secondary DNS server			
Static IP Lease List			
Host Label	MAC Address	IP Address	Remove Edi
Add			
P Alias			
P Alias	Enable		
P Address			
Subnet Mask			

# 2). Configure WAN Interface for Router A (ADSL PPPoE). See WAN Service.

Status							
*WAN							
Wan Info							
Interface	Description	Туре	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_0_33	PPPoE	Disconnect	00:03:25	111.251.238.198	2001:b011:700a:07ab:d191:5238:6e54:6e00/64	168.95.195.100,168.95.195.160

# 3). Configure wireless for Router A (SSID, Country, Security, Channel.)

I.	Basic	configuration	(SSID,	Country,	etc)
••	Daoio	ooningaradori	(0010)	oound y,	0.0,

Configuration								
Basic								
Parameters								
Wireless	🗹 Enat	☑ Enable						
Hide SSID	Enat	Enable						
Clients Isolation	Enat	ble						
Disable WMM Advertise	Enak	ble						
Wireless Multicast Forwarding (WMF)	Enat	ole						
SSID	test-ap-	test-ap-2.4g						
BSSID	00:04:ED	00:04:ED:87:A7:69						
Country	UNITE							
Country RegRev	0	]		141				
Max Clients	16	[1-16]						
Wireless - Guest/Virtual Access Points								
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable	
wI0_Guest1					16	N/A		
wI0_Guest2					16	N/A		
wI0_Guest3					16	N/A		

II. Wireless security configuration for Router A. Configure Network Authentication as WPA2-PSK and WPA/WAPI passphrase as 1234567890. (Users configure wireless security parameters according to their own needs.)

Configuration		
* Security		
If Hide Access Point enabled or Mac filter list is e	npty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup		
WPS	Disable V (Current: Disable)	
Manual Setup AP		
Select SSID	test-ap-2.4g 🗸	
Network Authentication	WPA2 -PSK	
Protected Management Frames	Disable V	
WPA/WAPI passphrase	Click here to display	
WPA Group Rekey Interval	3600 [0-2147483647]	
WPA/WAPI Encryption	AES V	
Apply Cancel		

III. Advanced wireless configuration for Router A (Channel 1, Bandwidth 20MHz/40MHz , OBSS Coexistence Disable ). Note: Select your own bandwidth, but both sides need to be same.

Configuration	
Advanced	
Parameters	
Band	2.4GHz V
Channel	1 Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	20MHz / 40MHz V Current: 40MHz
Control Sideband	Lower V Current: Lower
802.11n Rate	Auto
802.11n Protection	Auto 🗸
Support 802.11n Client Only	Off V
RIFS Advertisement	Auto 🗸
OBSS Coexistence	Disable V
RX Chain Power Save	Enable V Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps 🗸
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable V
Transmit Power	100% 🗸
WMM(Wi-Fi Multimedia)	Enable V
WMM No Acknowledgement	Disable V
WMM APSD	Enable V

4). Configure Wireless Bridge for Router A, by scanning or inputting Router B's wireless MAC address.

Make sure you know Router B's wireless MAC. If not, go to **Wireless > Basic**. Check BSSID which is Router B's wireless MAC.

Configuration								
Basic								
Parameters								
Wireless	I Enable	e						
Hide SSID	Enable	e						
Clients Isolation								
Disable WMM Advertise	Enable	e						
Wireless Multicast Forwarding (WMF)	Enable	e						
SSID	test-ap-2	test-ap-2.4g						
BSSID	00:04:ED:	00:04:ED:87:87:12						
Country	UNITED	STATES		~				
Country RegRev	0							
Max Clients	16	[1-16]						
Wireless - Guest/Virtual Access Points								
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable	
wI0_Guest1					16	N/A		
wI0_Guest2					16	N/A		
wI0_Guest3					16	N/A		

# (Router B's wireless basic configuration)

Configuration		
Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables w Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wirele Only those bridges selected in Remote Bridges will	ess bridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address	Enabled(Scan) Disable	
Apply Refresh		
Configuration		
Configuration • Wireless Bridge Parameters		
• Wireless Bridge	ess bridge restriction.	
Wireless Bridge Parameters Select Disabled in Bridge Restrict which disables w Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wirele	ess bridge restriction.	
Wireless Bridge Parameters Select Disabled in Bridge Restrict which disables w Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wirele Only those bridges selected in Remote Bridges will	ess bridge restriction. be granted access.	

WDS Configuration finished for Router A.

# Router B setup

1). Login to Router B (LAN IP Address: 192.168.1.1. Here if the LAN is same with router A, please change it to 192.168.1.X which needs to be on the same subnet with router A), disable DHCP server.

Configuration	
*LAN	
Parameters	
Group Name	Default V
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IGMP Snooping	☑ Enable
IGMP Snooping Mode	O Standard Mode    Blocking Mode
IGMP LAN to LAN Multicast	Enable(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
LAN side firewall	Enable
DHCP Server	
DHCP Server	Disable V
IP Alias	
IP Alias	
IP Address	
Subnet Mask	
Apply Cancel	

2). Configure wireless for Router B (SSID, Country, Security, Channel which need to be same as set in Router A.)

I. Basic configuration	(SSID,	Country,	etc)
------------------------	--------	----------	------

Configuration								
Basic								
Parameters								
Wireless	I Enal	ble						
Hide SSID	Enal	ble						
Clients Isolation	Enal	ble						
Disable WMM Advertise	Enal	Enable Enable test-ap-2.4g						
Wireless Multicast Forwarding (WMF)	Enal							
SSID	test-ap-							
BSSID	00:04:EI	D:87:87:12						
Country	UNITED	O STATES		~				
Country RegRev	0							
Max Clients	16	[1-16]						
Wireless - Guest/Virtual Access Points								
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable	
wI0_Guest1					16	N/A		
wl0_Guest2					16	N/A		
wI0_Guest3					16	N/A		

II. Wireless security configuration for Router B. Configure Network Authentication the same as Router A.

Configuration		
* Security		
If Hide Access Point enabled or Mac filter list is a	empty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup		
WPS	Disable V (Current: Disable)	
Manual Setup AP		
Select SSID	test-ap-2.4g 🗸	
Network Authentication	WPA2 -PSK	
Protected Management Frames		
WPA/WAPI passphrase	Click here to display	
WPA Group Rekey Interval	3600 [0-2147483647]	
WPA/WAPI Encryption	AES V	
Apply Cancel		

III. Advanced wireless configuration for Router B, the same as set in Router A (Channel 1, Bandwidth 20MHz/40MHz, OBSS Coexistence Disable ).

Configuration	
*Advanced	
Parameters	
Band	2.4GHz V
Channel	1 Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	20MHz / 40MHz V Current: 40MHz
Control Sideband	Lower V Current: Lower
802.11n Rate	Auto
802.11n Protection	Auto V
Support 802.11n Client Only	Off V
RIFS Advertisement	Auto 🗸
OBSS Coexistence	Disable V
RX Chain Power Save	Enable V Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps 🗸
Multicast Rate	Auto 🗸
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress <sup>™</sup> Technology	Disable V
Transmit Power	100% 🗸
WMM(Wi-Fi Multimedia)	Enable V
WMM No Acknowledgement	Disable V
WMM APSD	Enable V

3). Configure Wireless Bridge for Router B, by scanning or inputting Router A's wireless MAC address.

Make sure you know Router A's wireless MAC. If not, go to **Wireless > Basic**. Check BSSID which is A's wireless MAC.

Basic								
Parameters								
Wireless	I Enat	☑ Enable						
Hide SSID	Enat							
Clients Isolation								
Disable WMM Advertise	Enat	ole						
Wireless Multicast Forwarding (WMF)	Enat	Enable						
SSID	test-ap-	test-ap-2.4g						
BSSID	00:04:E0	D:04:ED:87:A7:69						
Country	UNITE							
Country RegRev	0	]						
Max Clients	16	[1-16]						
Wireless - Guest/Virtual Access Points								
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable	
wI0_Guest1					16	N/A		
wl0_Guest2					16	N/A		
wI0_Guest3					16	N/A		

# (Router A's wireless basic configuration)

Configuration		
• Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables wir Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireles Only those bridges selected in Remote Bridges will b	s bridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address	Enabled(Scan) Disable	
Apply Refresh		
Configuration  • Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables win Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireles Only those bridges selected in Remote Bridges will b	ss bridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address	00:04:ED:87:A7:69 ×	
Apply Refresh		

# WDS Configuration finished for Router B.

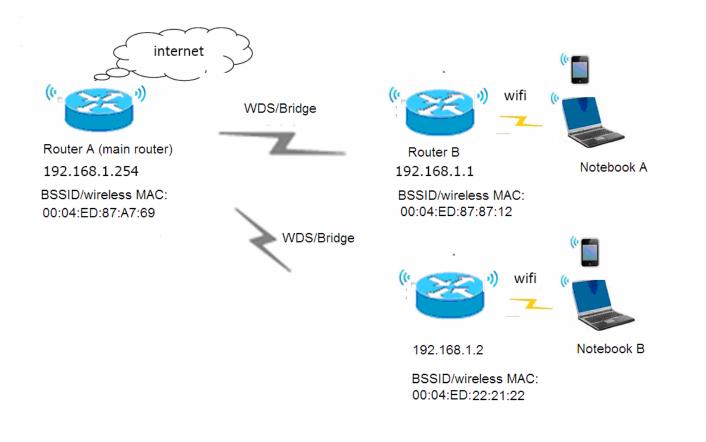
As for now, the WDS connection between Router A and B is established. Connect a wireless client to Router B with the SSID "test-ap-2.4g" to test the connectivity.

Configuration				
Station Info				
Associated Stations				
MAC Address	Associated	Authorized	SSID	Interface
	Yes	Yes	test-ap-2.4g	wIO

# One-to-Multiple wireless bridge

Router B and C need to bridge to Router A using wireless bridge for internet access and wireless coverage extension.

Router B and C share the same Wireless SSID, Country, Security, Channel setting with Router A.



# Router A setup

1). Login to Router A (LAN IP Address: 192.168.1.254), enable DHCP server.

Configuration				
TLAN				
Parameters				
Group Name	Default 🗸			
IP Address	192.168.1.254			
Subnet Mask	255.255.255.0			
GMP Snooping	I Enable			
GMP Snooping Mode	O Standard Mode    Blockin	ng Mode		
GMP LAN to LAN Multicast	Enable(LAN to LAN Multica	st is enabled until the first WAN service is	connected, regardless of this s	etting.)
LAN side firewall	Enable			
DHCP Server				
OHCP Server	Enable 🔻			
Start IP Address	192.168.1.100			
End IP Address	192.168.1.199			
eased Time (hour)	24			
Option 66	Enable			
Jse Router's setting as DNS Server	 ✓			
Primary DNS server				
Secondary DNS server				
Static IP Lease List	The second se			
Host Label	MAC Address	IP Address	Remove	Edit
Add				
P Alias				
P Alias	Enable			
P Address				
Subnet Mask				

# 2). Configure WAN Interface for Router A (ADSL PPPoE). See <u>WAN Service</u>.

Status							
*WAN							
Wan Info							
Interface	Description	Туре	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_0_33	PPPoE	Disconnect	00:03:25	111.251.238.198	2001:b011:700a:07ab:d191:5238:6e54:6e00/64	168.95.195.100,168.95.195.160

## 3). Configure wireless for Router A (SSID, Country, Security, Channel.)

## I. Basic configuration (SSID, Country, etc)

Configuration							
* Basic							
Parameters							
Wireless	Enat	ole					
Hide SSID	Enat	ole					
Clients Isolation	Enat	ble					
Disable WMM Advertise	Enat	ble					
Wireless Multicast Forwarding (WMF)	Enat	ble					
SSID	test-ap-	2.4g					
BSSID	00:04:E0	D:87:A7:69					
Country	UNITE	D STATES		~			
Country RegRev	0	]		(4)			
Max Clients	16	[1-16]					
Wireless - Guest/Virtual Access Points							
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
wI0_Guest1					16	N/A	
wl0_Guest2					16	N/A	
wl0_Guest3					16	N/A	

II. Wireless security configuration for Router A. Configure Network Authentication as WPA2-PSK and WPA/WAPI passphrase as 1234567890. (Users configure wireless security parameters according to their own needs.)

Configuration		
* Security		
If Hide Access Point enabled or Mac filter list is e	mpty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup		
WPS	Disable V (Current: Disable)	
Manual Setup AP		
Select SSID	test-ap-2.4g 🗸	
Network Authentication	WPA2 -PSK	
Protected Management Frames	Disable V	
WPA/WAPI passphrase	Click here to display	
WPA Group Rekey Interval	3600 [0-2147483647]	
WPA/WAPI Encryption	AES	
Apply Cancel		

III. Advanced wireless configuration for Router A (Channel 1, Bandwidth 20MHz/40MHz , OBSS Coexistence Disable ) Note: Select your own bandwidth, but all sides need to be same.

Configuration	
Advanced	
Parameters	
Band	2.4GHz V
Channel	1 Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	20MHz / 40MHz V Current: 40MHz
Control Sideband	Lower V Current: Lower
802.11n Rate	Auto
802.11n Protection	Auto 🗸
Support 802.11n Client Only	Off V
RIFS Advertisement	Auto 🗸
OBSS Coexistence	Disable V
RX Chain Power Save	Enable V Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps 🗸
Multicast Rate	Auto 🗸
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	[2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable V
Transmit Power	100% 🗸
WMM(Wi-Fi Multimedia)	Enable V
WMM No Acknowledgement	Disable V
WMM APSD	

4). Configure Wireless Bridge for Router A, by scanning or inputting Router B and C's wireless MAC addresses.

Make sure you know Router B and C's wireless MACs. If not, go to **Wireless > Basic**. Check BSSID which is Router B's wireless MAC. Router B for example

Configuration							
Basic							
Parameters							
Wireless	Enat	ble					
Hide SSID	Enat	ble					
Clients Isolation	Enat	ole					
Disable WMM Advertise	Enat	ble					
Wireless Multicast Forwarding (WMF)	Enat	ble					
SSID	test-ap-	2.4g					
BSSID	00:04:E0	0:87:87:12					
Country	UNITED	STATES		~			
Country RegRev	0	]					
Max Clients	16	[1-16]					
Wireless - Guest/Virtual Access Points							
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
wI0_Guest1					16	N/A	
wl0_Guest2					16	N/A	
wI0_Guest3					16	N/A	

## (Router B's wireless basic configuration)

Configuration		
▼Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables wire Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless Only those bridges selected in Remote Bridges will be	s bridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address	Enabled(Scan) Disable	
Apply Refresh		
Configuration		
Wireless Bridge		
▼Wireless Bridge		
• Wireless Bridge Parameters Select Disabled in Bridge Restrict which disables wire Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless Only those bridges selected in Remote Bridges will be	s bridge restriction.	
Parameters Select Disabled in Bridge Restrict which disables wire Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless	s bridge restriction.	
Parameters Select Disabled in Bridge Restrict which disables wire Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless Only those bridges selected in Remote Bridges will be	s bridge restriction. e granted access.	

WDS Configuration finished for Router A.

## Router B setup

1). Login to Router B (LAN IP Address: 192.168.1.1. Here if the LAN is same with router A, please change it to 192.168.1.X which needs to be on the same subnet with router A), disable DHCP server.

Configuration	
*LAN	
Parameters	
Group Name	Default V
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IGMP Snooping	☑ Enable
IGMP Snooping Mode	O Standard Mode   Blocking Mode
IGMP LAN to LAN Multicast	Enable(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
LAN side firewall	Enable
DHCP Server	
DHCP Server	Disable V
IP Alias	
IP Alias	
IP Address	
Subnet Mask	
Apply Cancel	

2). Configure wireless for Router B (SSID, Country, Security, Channel which need to be same as set in Router A.)

Configuration								
Basic								
Parameters								
Wireless	Б	- Enab	le					
Hide SSID	[	Enab	le					
Clients Isolation	[	Enab	le					
Disable WMM Advertise	Γ	Enab	le					
Wireless Multicast Forwarding (WMF	) [	Enab	le					
SSID	t	est-ap-2	2.4g					
BSSID	0	0:04:ED	0:87:87:12					
Country		JNITEL	STATES		~			
Country RegRev	0	,			site.			
Max Clients	1	16	[1-16]					
Wireless - Guest/Virtual Access Po	vints		·					
SSID	Hi	idden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
wI0_Guest1						16	N/A	
wl0_Guest2						16	N/A	
						16	N/A	

I. Basic configuration (SSID, Country, etc)

II. Wireless security configuration for Router B. Configure Network Authentication the same as Router A.

Configuration		
* Security		
If Hide Access Point enabled or Mac filter list is e	mpty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup		
WPS	Disable V (Current: Disable)	
Manual Setup AP		
Select SSID	test-ap-2.4g V	
Network Authentication	WPA2 -PSK	
Protected Management Frames		
WPA/WAPI passphrase	Click here to display	
WPA Group Rekey Interval	3600 [0-2147483647]	
WPA/WAPI Encryption	AES V	
Apply Cancel		

III. Advanced wireless configuration for Router B, the same as set in Router A (Channel 1, Bandwidth 20MHz/40MHz, OBSS Coexistence Disable ).

Configuration	
*Advanced	
Parameters	
Band	2.4GHz 🗸
Channel	1 V Curlent: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	20MHz / 40MHz V Current: 40MHz
Control Sideband	Lower V Current: Lower
802.11n Rate	Auto
802.11n Protection	Auto V
Support 802.11n Client Only	Off V
RIFS Advertisement	Auto 🗸
OBSS Coexistence	Disable V
RX Chain Power Save	Enable V Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps 🗸
Multicast Rate	Auto 🗸
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable V
Transmit Power	100% 🗸
WMM(Wi-Fi Multimedia)	
WMM No Acknowledgement	Disable 🗸
WMM APSD	

3). Configure Wireless Bridge for Router B, by scanning or inputting Router A's wireless MAC address. Make sure you know Router A's wireless MAC. If not, go to **Wireless > Basic**. Check BSSID which is A's wireless MAC.

Configuration						1	
* Basic							
Parameters							
Wireless	Enat	ole					
Hide SSID	Enat	ble					
Clients Isolation	Enat	ble					
Disable WMM Advertise	Enat	ble					
Wireless Multicast Forwarding (WMF)	Enat	ble					
SSID	test-ap-	2.4g					
BSSID	00:04;E0	D:87:A7:69					
Country	UNITE	D STATES		~			
Country RegRev	0						
Max Clients	16	[1-16]					
Wireless - Guest/Virtual Access Points							
SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
wI0_Guest1					16	N/A	
wl0_Guest2					16	N/A	
wl0_Guest3					16	N/A	

## (Router A's wireless basic configuration)

Configuration		
▼Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables win Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireles Only those bridges selected in Remote Bridges will b	s bridge restriction.	
Bridge Restrict Remote Bridges MAC Address	Enabled(Scan) Disable	
Apply Refresh		
Configuration		
▼Wireless Bridge		
Parameters		
Select Disabled in Bridge Restrict which disables win Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireles Only those bridges selected in Remote Bridges will b	s bridge restriction.	
Bridge Restrict	Enable	
Remote Bridges MAC Address	00:04:ED:87:A7:69 ×	
Apply Refresh	· · · · ·	

WDS Configuration finished for Router B.

As for now, the WDS connection between Router A and B is established. Connect a wireless client to Router B with the SSID "test-ap-2.4g" to test the connectivity.

Configuration				
Station Info				
Associated Stations				
MAC Address	Associated	Authorized	SSID	Interface

Router C setup Refer to Router B setup

### Advanced

#### – 2.4GHz Wireless

Configuration

Advanced	
Parameters	
Band	2.4GHz 🔻
Channel	1 Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	40MHz  Current 20MHz
Control Sideband	Lower  Current: N/A
802.11n Rate	Auto
802.11n Protection	Auto 🔻
Support 802.11n Client Only	Off •
RIFS Advertisement	Auto 🔻
OBSS Coexistence	Enable V
RX Chain Power Save	Enable V Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps 🔻
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable <b>T</b>
Transmit Power	100% -
WMM(Wi-Fi Multimedia)	Enable <b>v</b>
WMM No Acknowledgement	Disable <b>•</b>
WMM APSD	Enable •
Beamforming Transmission (BFR)	Disable V
Beamforming Reception (BFE)	Disable 🔻

Band: In the 2.4 GHz radio frequency.

Channel: Choose a channel to use. Here is a list of available channels or select Auto mode instead.

Scan Used Channel: Press the button to scan and list all channels being used.

Auto Channel Timer (min): Available when Auto Channel is selected. The auto channel times length it takes to scan in minutes.

802.11n/EWC: select to auto enable or disable 802.11n.

**Bandwidth:** The higher the bandwidth the better the performance will be but greater interference with other wireless devices.

**Control Sideband:** only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower** 

**sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

**802.11n Rate:** This allows you to select the fixed transmission rate or auto.

**802.11n Protection:** turn off for maximize throughput.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients

operating at 802.11n speeds.

**RIFS Advertisement:** Reduced Inter-frame Spacing (RIFS) is an 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

**OBSS Co-Existence:** coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

**RX Chain Power Save:** Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

**RX Chain Power Save Quiet Time:** The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

**RX Chain Power Save PPS:** The maximum number of packets per seconds that can be processed by the WLAN interface for duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

**54g<sup>™</sup> Rate:** Available after changing **802.11n Rate** to "Use 54g Rate" in **802.11n Rate**. It is used to limit 11n speed to a specific rate, e.g. 1M, 6M, 12M, 24M, 48M, etc.

Multicast Rate: Setting for multicast packets transmission rate.

**Basic Rate:** Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

**Fragmentation Threshold:** A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

**RTS Threshold:** Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

**DTIM Interval:** Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

**Beacon Interval:** The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

**Global Max Clients:** Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

**XPress™ Technology:** It has been designed to improve the wireless network efficiency. Default is disabled.

Transmit Power: select the transmitting power of your wireless signal.

**WMM (Wi-Fi Multimedia):** you can choose to enable or disable this function which allows for priority of certain data over wireless network.

**WMM No Acknowledgement:** Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

**Beamforming Transmission (BFR) / Beamforming Reception (BFE):** Enable to increase wireless speed by focusing and concentrating transmitted (send) and/or receive signals with a wireless client instead of broadcast signals in all directions. **Note**: Both router and client wireless must support beamforming technology.

### – 5GHz Wireless

Configuration	
Advanced	
Parameters	
Band	5GHz 💌
Channel	36/80 👻 Current: 36 Scan Used Channel
Auto Channel Timer	15 minutes
802.11n/EWC	Auto 💌
Bandwidth	80MHz in 5G 🗸 Current: 80MHz
Control Sideband	Lower V Current N/A
802.11n Rate	Auto 💌
802.11n Protection	Auto 💌
Support 802.11n Client Only	Off 💌
RIFS Advertisement	Auto 💌
OBSS Coexistence	Enable 💌
RX Chain Power Save	Enable 🖌 Power Save status: Low Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	6 Mbps 👻
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable 🗸
Regulatory Mode	Disable 🗸
Pre-Network Radar Check	-1 [0-99]
In-Network Radar Check	-1 [10-99]
TPC Mitigation(db)	0(Off) 🗸
Transmit Power	100% 🗸
WMM(Wi-Fi Multimedia)	Enable 🗸
WMM No Acknowledgement	Disable 🗸
WMM APSD	Enable 🔽
Beamforming Transmission (BFR)	Disable 🔽
Beamforming Reception (BFE)	Disable 🗸

Band: In the 5GHz radio frequency.

Channel: Choose a channel to use. Here is a list of available channels or select Auto mode instead.

Scan Used Channel: Press the button to scan and list all channels being used.

Auto Channel Timer (min): Available when Auto Channel is selected. The auto channel times length it takes to scan in minutes.

802.11n/EWC: select to auto enable or disable 802.11n.

**Bandwidth:** The higher the bandwidth the better the performance will be but greater interference with other wireless devices. Select **20MHz** for lessen radio interference.

**Control Sideband:** only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower** 

**sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

**802.11n Rate:** This allows you to select the fixed transmission rate or auto.

**802.11n Protection:** turn off for maximize throughput.

**Support 802.11n Client Only:** turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

**RIFS Advertisement:** Reduced Inter-frame Spacing (RIFS) is an 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

**OBSS Co-Existence:** coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

**RX Chain Power Save:** Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

**RX Chain Power Save Quiet Time:** The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

**RX Chain Power Save PPS:** The maximum number of packets per seconds that can be processed by the WLAN interface for duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

**54g<sup>™</sup> Rate:** Available after changing **802.11n Rate** to "Use 54g Rate" in **802.11n Rate**. It is used to limit 11n speed to a specific rate, e.g. 6M, 12M, 24M, 48, etc.

Multicast Rate: Setting for multicast packets transmission rate.

**Basic Rate:** Setting for basic transmission rate. It is not a specific kind of rate but a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

**Fragmentation Threshold:** A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

**RTS Threshold:** Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

**DTIM Interval:** Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

**Beacon Interval:** The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

**Global Max Clients:** Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

**XPress™ Technology:** It has been designed to improve the wireless network efficiency. Default is disabled.

**Regulatory Mode:** Select to deny any regulatory mode, which is only for **5GHz** band wireless. There are two regulatory modes: **Configuring Your Router Wireless 5G(wl0) & 2.4G(wl1) – Advanced for 5G Wireless** 

802.11h: The standard solves interference problems with e.g. satellites and radar using the same 5 GHz band as 802.11a or 802.11n dual-band access points.

802.11d: This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.

Pre-Network Radar Check (Used for 802.11h only): Specifies a period of time in seconds [0-99] to

check for radar on a channel before the Access Point establishes a wireless network with the channel.

**In-Network Radar Check (Used for 802.11h only):** After the wireless network got established, specifies a period of time in seconds [10-99] to check for radar when switching to another non-radar channel.

**TPC Mitigation (db):** Known as Transmitter Power Control mitigation to reduce unnecessary transmitting power radio and possible radio interference to other users.

**Transmit Power:** select the transmitting power of your wireless signal.

**WMM (Wi-Fi Multimedia):** you can choose to enable or disable this function which allows for priority of certain data over wireless network.

**WMM No Acknowledgement:** Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

**Beamforming Transmission (BFR) / Beamforming Reception (BFE):** Enable to increase wireless speed by focusing and concentrating transmitted (send) and/or receive signals with a wireless client instead of broadcast signals in all directions. **Note**: Both router and client wireless must support beamforming technology.

## **Station Info**

Here you can view information about the wireless clients.

Configuration				
▼ Station Info				
Associated Stations				
MAC Address	Associated	Authorized	SSID	Interface
Refresh				

MAC Address: The MAC address of the wireless clients.

**Associated:** List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access.

**SSID:** Show the current SSID of the client.

Interface: To show which interface the wireless client is connected to.

**Refresh:** To get the latest information.

### Schedule Control

Schedule control is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access.

The Wireless schedule only functions whilst Wireless is enabled. The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

For detail setting the timeslot, user can turn to Time Schedule .

Configuration	
* Schedule Control	
	edule only functions whilst Wireless is enabled. AP schedule control only operates whilst the associated AP is enabled.
wlan-ap-5g	Enable
T	1. Always On Sun Mon Tue Wed Thu Fri Sat From 00 😪 : 00 😪 : 00 😪
Time Schedule	2. Check or select from listbox 💙 🛛 Sun 🗍 Mon 🗍 Tue 🗍 Wed 🗍 Thu 🗍 Fri 🗋 Sat From 00 😒 : 00 💙 To 00 👽 : 00 👽
Wireless - Guest/V	/irtual Access Points
wI0_Guest1	Disable
	1. Always On Sun Mon Tue Wed Thu Fri Sat From 00 🗸 : 00 🗸 To 00 🗸 : 00 🗸
Time Schedule	2. Check or select from listbox 💙 Sun Mon Tue Wed Thu Fri Sat From 00 🔍 : 00 🗸 : 00 🗸 : 00 🗸
wI0_Guest2	Disable
T	1. Always On Sun Mon Tue Wed Thu Fri Sat From 00 - : 00 - To 00 - : 00 -
Time Schedule	2. Check or select from listbox 💙 Sun Mon Tue Wed Thu Fri Sat From 00 🗸 : 00 💙 : 00 💙 : 00 💙
wI0_Guest3	Disable
	1. Always On Sun Mon Tue Wed Thu Fri Sat From 00 😴 : 00 🛩 To 00 😴 : 00 🛩
Time Schedule	2 check or select from listbox v Sun Mon Tue Wed Thu Fri Sat From 00 v: 00 v To 00 v: 00 v
Apply	

**Time Schedule:** Set when the SSID works. If user wants the SSID works all the time, please select "Always On"; if not, please set or select the exact time your want the SSID works. Here user can set two separate intervals.

For example: user wants the SSID "*wlan-ap-5g*" to work on weekdays except for Wednesday, under this circumstance, user can set as shown below. (8700AX(L)-1600 offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals.)

wlan-ap-5g	Enable
Time Cehedule	1. check or select from listbox 💙 🗌 Sun 🗹 Mon 🗹 Tue 🗋 Wed 🗋 Thu 📄 Fri 🛄 Sat 🛛 From 00 💙 : 00 🔍 To 23 🔍 : 59 💌
Time Schedule	2. 🗹 check or select from listbox 💌 🗌 Sun 🗋 Mon 💭 Tue 🗋 Wed 🗹 Thu 🗹 Fri 🗋 Sat 🛛 From 00 🔍 : 00 🔍 To 23 🔍 : 59 💌

# **WAN-Wide Area Network**

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems.

#### **WAN Service**

Three WAN interfaces are provided for WAN connection: DSL (VDSL/ADSL), Ethernet and 3G/4G LTE.

WAN Servic	e							
G/4G LTE Inte	erface							
nterface	Description	TEL No.	APN	Username	NAT	Firewall	Dial on demand	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Click Add to add new WAN connections.

#### (i) DSL

In DSL mode, there are two transfer modes for you to configure for WAN connection, namely **ATM** (**ADSL**) and **PTM** (**VDSL**) configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.

Configuration			
▼WAN Service			
Parameters			
WAN Port	DSL 💌		
Layer2 Interface	● ATM ○ PTM		
Туре	PPP over Ethernet (PPPoE) 🐱		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING V
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO 💌	Firewall	✓ Enable
NAT	Enable	Fullcone NAT	Enable
IPv4 Address	Static	IP Address	
Dial on demand	Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	Enable		
IPv6 Address	Static	IP Address	
MTU	1492		
PPPoE with Pass-through	Enable		
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable
MLD Multicast Proxy	Enable	MLD Multicast Source	Enable
Next			

Layer2 Interface: 2 transfer mode, ATM (ADSL) or PTM (VDSL).

## 

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.

Configuration			
*WAN Service			
Parameters			
WAN Port	DSL 💌		
Layer2 Interface	● ATM ○ PTM		
Туре	PPP over Ethernet (PPPoE) 💌		
VPI/VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING V
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO 🗸	Firewall	Enable
NAT	Enable	Fullcone NAT	Enable
IPv4 Address	Static	IP Address	
Dial on demand	Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	Enable		
IPv6 Address	Static	IP Address	
MTU	1492		
PPPoE with Pass-through	Enable		
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable
	Enable	MLD Multicast Source	Enable

**VPI/VCI:** Enter the VPI/VCI combination from you ISP.

**Encapsulation Mode:** Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

**Description:** User-defined description for the connection, commonly for friendly use.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

**Username:** Enter the account obtained from the ISP.

**Password:** Enter the password obtained from the ISP.

Service Name: The item is for identification purposes, user can define this.

Authentication Method: Default is Auto. Or else your ISP will advise you the appropriate mode.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Note:** In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

**IP Address:** If *Static* is enabled in the above field, enter the static IPv4 address get from the ISP.

**Dial on demand:** It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

**Inactivity Timeout:** The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

**IPv6 for this service:** Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If Static is enabled in the above field, enter the static IPv4 address.

**MTU:** Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**PPPoE with Pass-through:** Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only" from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

Click Next to continue to set the default gateway and DNS for IPv4 and IPv6.

Configuration	
▼ Default Gateway / DNS	
Default Gateway	
Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	3G0/USB3G0
Selected WAN Interface As The System Default IPv6 Gateway	pppoe_0_8_35/ppp0.1 💌
DNS	
DNS Server Interface	Available WAN Interfaces     O Static DNS Address     O Parent Controls
Selected DNS Server Interfaces	Available WAN Interfaces
ppp0.1	3G0/USB3G0
Primary DNS server	
Secondary DNS server	
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6	Client on that interface.
DNS Server Interface	Available WAN Interfaces     O Static DNS IPv6 Address
WAN Interface selected	pppoe_0_8_35/ppp0.1 💌
Primary IPv6 DNS server	
Secondary IPv6 DNS server	
Next	

## **Default Gateway**

Select default gateway for you connection (IPv4 and IPv6).

#### DNS

#### > IPv4

#### Three ways to set an IPv4 DNS server

- (i) Available WAN interfaces: Select a desirable WAN interface as the IPv4 DNS server.
- (i) **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① Parental Controls: If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at <u>Parental Control Provider</u>).

#### > IPv6

### **Obtain IPv6 DNS info from a WAN interface**

**WAN Interface selected:** Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

#### Static DNS IPv6 Address

**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** Type the specific primary and secondary IPv6 DNS Server address.

If you don't need a service, select the item you want to remove, check the checkbox, then press **Remove**.

Press Edit button to re-edit this service settings.

WAN Ser	vice											
ATM Interf	ace											
Interface	Description	Туре	VPI/VCI	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MId	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8/35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled		Edit
3G/4G LTE	Interface											
Interface	Description	TEL No.		APN	Username		NAT	Firewall	Dial on de	emand		Edit
USB3G0		*99***1#	ŧ	internet			Enabled	Enabled	Enabled			Edit

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address). (IPv4 or IPv6)

 Status

 \*WAN

 Wan Info

 Interface
 Description
 Type
 Status
 Connection Time
 IPv4 Address
 IPv6 Address
 DNS

 ppp0.1
 ppp0e\_0\_8\_35
 PPPoE
 Disconnect
 00:04:03
 10:40:90:211
 2000:db98:1000:1000:29ac:afc6:59a4:5816/64
 218.2.135.1

 USB3G0
 3G/LTE Card not found
 0
 0
 0
 0
 0

## PPPoA

Configuration			
WAN Service			
Parameters			
WAN Port	DSL		
Layer2 Interface	⊙АТМ ○РТМ		
Туре	PPPoA 💌		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	VC/MUX
Description			
Jsername			
Password			
Authentication Method	AUTO 💌	Firewall	Enable
NAT	Enable	Fullcone NAT	Enable
Pv4 Address	Static	IP Address	
Dial on demand	Enable	Inactivity Timeout	(minutes) [1-4320]
Pv6 for this service	Enable		
Pv6 Address	Static	IP Address	
итu	1500		
WI O			
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable

VPI/VCI: Enter the VPI/VCI combination from you ISP.

**Encapsulation Mode:** Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

**Description:** User-defined description for the connection.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Authentication Method: Default is Auto. Or else your ISP will advise you the appropriate mode.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Note:** In this connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. With Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

**IPv4 Address:** Select whether to set static IPv4 address or obtain automatically.

**IP Address:** If *Static* is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is

useful when saving internet fees.

**Inactivity Timeout:** The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

**IP Address:** If **Static** is enabled in the above field, enter the static IPv4 address.

**MTU:** Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.

## IP over Ethernet

Configuration				
*WAN Service				
Parameters				
WAN Port	DSL			
Layer2 Interface	⊙ ATM ○ PTM			
Туре	IP over Ethernet			
VPI/VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNA	P-BRIDGING 💌
Description				
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1	[tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	✓ Enable			
Option 60 Vendor ID				
Option 77 User ID				
Option 61 Client ID				
Option 125	⊙ Disable O Enable			
Option 50 Request IP Address				
Option 51 Request Leased Time	0			
Option 54 Request Server Address				
WAN IP Address				
WAN Subnet Mask				
WAN gateway IP Address				
IPv6 for this service	Enable			
Obtain an IPv6 address automatically	✓ Enable			
WAN IPv6 Address/Prefix Length				
WAN Next-Hop IPv6 Address				
NAT	Enable	Fullcone NAT	Enable	e
Firewall	Enable			
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable	e
No Multicast VLAN Filter	Enable			
MLD Multicast Proxy	Enable	MLD Multicast Source	Enable	e
MTU	1500	MAC Spoofing		
Next				

VPI/VCI: Enter the VPI/VCI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

**Description:** User-defined description for the connection, commonly for friendly use.

Authentication Method: Default is Auto. Or else your ISP will advise you the appropriate mode.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

**Option 60 Vendor ID:** Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a

string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

**Option 77 User ID:** Set the User ID, which identifies the request DHCP user.

**Option 61 Client ID:** Set the client ID., which identifies the request DHCP client.

**Option 125:** Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is *Disable*.

**Option 50 Request IP Address:** Set the particular request IP address to be assigned from the DHCP.

**Option 51 Request Leased Time:** Set the request lease time for the requested IP address.

Option 54 Request Server Address: Set request Server Address.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

**IPv6 for this service:** Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**No Multicast VLAN Filter:** Enable to deactivate the multicast VLAN filter which allows users to filter on all multicast packets or on specific multicast groups.

MLD Multicast Proxy: check whether to enable this function. MLD (Multicast Listener Discovery

Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2. **Note:** It works only on MLD version 2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system.

**MTU:** Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**MAC Spoofing:** This option is required by some service providers specifying some specific MAC allowed for joining network. You must fill in the MAC address specified by your service provider when this information is required.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Configuration			
*WAN Service			
Parameters			
WAN Port	DSL 💌		
Layer2 Interface	⊙ ATM ○ PTM		
Туре	IPoA 💌		
VPI/VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-ROUTING
Description			
WAN gateway IP Address			
NAT	Enable	Fullcone NAT	Enable
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable
No Multicast VLAN Filter	Enable		
Next			

VPI/VCI: Enter the VPI/VCI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

**Description:** User-defined description for the connection, commonly for friendly use.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**No Multicast VLAN Filter:** Enable to deactivate the multicast VLAN filter which allows users to filter on all multicast packets or on specific multicast groups.

## Bridging

Configuration			
▼WAN Service			
Parameters			
WAN Port	DSL 💌		
Layer2 Interface	⊙ ATM ○ PTM		
Туре	Bridging		
VPI/VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Allow as IGMP Multicast Source	Enable	Allow as MLD Multicast Source	Enable
Next			

VPI/VCI: Enter the VPI/VCI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Allow as IGMP Multicast Source: Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. Note: It works only on IGMP version 3.

**Allow as MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

## (i) Ethernet

#### Ethernet WAN connection is well known as directly broadband WAN connection.

Configuration			
▼WAN Service			
Parameters			
WAN Port	Ethernet 🔽		
Туре	PPP over Ethernet (PPPoE) 💌		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO 💌	Firewall	Enable
NAT	Enable	Fullcone NAT	Enable
IPv4 Address	Static	IP Address	
Dial on demand	Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	Enable		
IPv6 Address	Static	IP Address	
MTU	1492		
PPPoE with Pass-through	Enable		
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable
MLD Multicast Proxy	Enable	MLD Multicast Source	Enable
Next			

## PPPoE

Configuration			
• WAN Service			
Parameters			
WAN Port	Ethernet 🔽		
Туре	PPP over Ethernet (PPPoE) 💌		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO 💌	Firewall	Enable
TAV	Enable	Fullcone NAT	Enable
Pv4 Address	Static	IP Address	
Dial on demand	Enable	Inactivity Timeout	(minutes) [1-4320]
Pv6 for this service	Enable		
Pv6 Address	Static	IP Address	
MTU	1492		
PPPoE with Pass-through	Enable		
	Enable	IGMP Multicast Source	Enable
GMP Multicast Proxy			Enable

**Description:** User-defined description for the connection, commonly for friendly use.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID

identification, tagged: 0-4094, untagged : -1.

**Username:** Enter the account obtained from the ISP.

**Password:** Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is Auto. Or else your ISP will advise you the appropriate mode.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Note:** In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. and while you disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted or Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

**IPv4 Address:** Select whether to set static IPv4 address or obtain automatically.

**IP Address:** If *Static* is enabled in the above field, enter the static IPv4 address get from the ISP.

**Dial on demand:** It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

**Inactivity Timeout:** The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

**IP Address:** If **Static** is enabled in the above field, enter the static IPv4 address.

**MTU:** Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**PPPoE with Pass-through:** Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.

Configuration	
▼ Default Gateway / DNS	
Default Gateway	
Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	-> 3G0/USB3G0
Selected WAN Interface As The System Default IPv6 Gateway	pppoe_eth0/ppp0.1 😪
DNS	
DNS Server Interface	Available WAN Interfaces     O Static DNS Address     O Parent Controls
Selected DNS Server Interfaces	Available WAN Interfaces
ppp0.1	3G0/USB3G0
Primary DNS server	
Secondary DNS server	
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6	6 Client on that interface.
DNS Server Interface	Available WAN Interfaces     O Static DNS IPv6 Address
WAN Interface selected	pppoe_eth0/ppp0.1 💌
Primary IPv6 DNS server	
Secondary IPv6 DNS server	
Next	

## **Default Gateway**

Select default gateway for you connection (IPv4 and IPv6).

## DNS

#### IPv4

#### Three ways to set an IPv4 DNS server

- ① Available WAN interfaces: Select a desirable WAN interface as the IPv4 DNS server.
- (i) **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① Parental Controls: If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at <u>Parental Control Provider</u>).

#### > IPv6

#### Obtain IPv6 DNS info from a WAN interface

**WAN Interface selected:** Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

#### Static DNS IPv6 Address

**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** Type the specific primary and secondary IPv6 DNS Server address.

If you don't need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Press Edit button to re-edit this service settings.

WAN Sen	vice										
ETH Interfa	ice										
Interface	Description	Туре	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MId	Remove	Edit
ppp0.1	pppoe_eth4	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled		Edit
3G/4G LTE	Interface										
Interface	Description	TEL No.		APN	Username		NAT	Firewall	Dial on dem	hand	Edit
USB3G0		*99***1#		internet			Enabled	Enabled	Enabled		Edit

Here the corresponding WAN Service have been configured, if it is OK, you can access the internet. You can go to **Status>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).

## (IPv4 or IPv6)

Status							
• WAN							
Wan Info							
Interface	Description	Туре	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_eth4	PPPoE	Disconnect	00:04:03	10.40.90.211	2000:db98:1000:1000:29ac:afc6:59a4:5816/64	218.2.135.1
USB3G0			3G/LTE Card not found				

## IP over Ethernet

Configuration			
▼WAN Service			
Parameters			
WAN Port	Ethernet V		
Туре	IP over Ethernet		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	Enable		
Option 60 Vendor ID			
Option 77 User ID			
Option 61 Client ID			
Option 125	Disable     Disable		
Option 50 Request IP Address			
Option 51 Request Leased Time	0		
Option 54 Request Server Address			
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	Enable		
Obtain an IPv6 address automatically	Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	Enable	Fullcone NAT	Enable
Firewall	Enable		
IGMP Multicast Proxy	Enable	IGMP Multicast Source	Enable
No Multicast VLAN Filter	Enable		
MLD Multicast Proxy	Enable	MLD Multicast Source	Enable
мти	1500	MAC Spoofing	
Next			

**Description:** User-defined description for the connection, commonly for friendly use.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

**Option 60 Vendor ID:** Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

**Option 77 User ID:** Set the User ID, which identifies the request DHCP user.

**Option 61 Client ID:** Set the client ID., which identifies the request DHCP client.

**Option 125:** Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function.

Default setting is *Disable*.

**Option 50 Request IP Address:** Set the particular request IP address to be assigned from the DHCP.

**Option 51 Request Leased Time:** Set the request lease time for the requested IP address.

Option 54 Request Server Address: Set request Server Address.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**IGMP Multicast:** IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**No Multicast VLAN Filter:** Enable to deactivate the multicast VLAN filter which allows users to filter on all multicast packets or on specific multicast groups.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

**MTU:** Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

**MAC Spoofing:** This option is required by some service providers specifying some specific MAC allowed to join in network. You must fill in the MAC address specified by your service provider when this information is required.

## Bridging

Configuration			
▼WAN Service			
Parameters			
WAN Port	Ethernet 💌		
Туре	Bridging		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Allow as IGMP Multicast Source	Enable .	Allow as MLD Multicast Source	Enable
Next			

**Description:** User-defined description for the connection, commonly for friendly use.

**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Allow as IGMP Multicast Source: Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. Note: It works only on IGMP version 3.

Allow as MLD Multicast Source: Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. Note: It works only on MLD version 2.

## **3G/4G LTE**

Select 3G/4G LTE to configure the route to enjoy the mobility. By default the 3G/4G LTE interface is on, user can edit the parameters to meet your own requirements.

WAN Ser	vice											
ATM Interf	face											
Interface	Description	Туре	VPI/VCI	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MId	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8/35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled		Edit
3G/4G LTE	Interface											
Interface	Description	TEL No.		APN	Username		NAT	Firewall	Dial on de	mand		Edit
USB3G0		*99***1#		internet			Enabled	Enabled	Enabled			Edit

Click Edit button to enter the 3G/4G LTE configuration page.

Configuration					
▼WAN Service					
Parameters					
Dial on demand	🗹 Enable				
Mode	Use 3G/4G LTE dongle s	settings 💌			
Use PPP	Enable Enable				
TEL No.	*99***1#		APN	internet	
Username			Password		
Authentication Method	AUTO 🔽		PIN		
Dial on demand	Enable				
Keep Alive	Enable 7	seconds [1-86400]			
IP Address	8.8.8.8				
мто	1500				
NAT	Enable		Firewall	Enable	
Selected Default Gatewa	y Interfaces			Available Routed WAN Interfaces	
USB3G0		×		ppp0.1	8
Obtain DNS	Ose WAN Interface	O Use Static DNS	O Parent Controls		
Selected DNS Server Inte	erfaces			Available WAN Interfaces	
USB3G0		8		ppp0.1	< ×
Primary DNS			Secondary DNS		
*Warning: Entering the w	rong PIN code three times v	vill lock the SIM.			
Apply Cancel					

**Dial on demand:** If enabled, the 3G/4G LTE will work in dial on demand mode and be brought up only when there is no active default route. In this mode, 3G/4G LTE work as a backup for the WAN connectivity. While if disabled, 3G/4G LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G

preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

**TEL No.:** The dial string to make a 3G/LTE user internetworking call. It may provide by your mobile service provider.

**APN:** An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

**Username/Password:** Enter the username and password provided by your service provider. The username and password are case sensitive.

**Authentication Protocol:** Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

**PIN:** PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/ service provider.

① Connect on Demand: If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

**Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 600 seconds.

Dial on demand	Enable	
Idle Timeout	600	seconds [10-86400]

(i) **Keep Alive:** Check Enable to allow the router to send message out every 7 seconds (can be changed base on need) to prevent the connection being dropped by ISP.

**IP Address:** The IP address is used to "ping", and router will ping the IP to find whether the connection is still on.

Dial on demand	Enable
Keep Alive	Enable 7 seconds [1-86400]
IP Address	8.8.8.8

**NAT:** Check to enable the NAT function.

**Firewall:** Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to <u>IP Filtering Incoming</u> to add allowing rules.

**MTU:** MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

**Select default gateway interfaces:** Select from the interfaces the default gateway, here commonly we select USB3G0.

Selected DNS Server Interfaces: Three ways to set a DNS server.

- (i) Available WAN interfaces: Select a desirable WAN interface as the DNS server.
- ③ Static DNS Address: To specify DNS server manually by entering your primary and

secondary DNS server addresses.

① Parental Controls: If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at <u>Parental Control Provider</u>).

Click **Apply** to confirm the settings.

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (Here user can see the 3G/LTE failover).

Status							
▼ WAN							
Wan Info							
Interface	Description	Туре	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured				
USB3G0	3G0	PPP	Connected	00:01:10	10,44,183,197		221.5.4.55

## Failover

Auto failover/failback is to ensure an always-on internet connection. Users can set a Master WAN interface (main WAN) and a slave interface (backup WAN), and when Master WAN fails, it will switch to slave WAN, and when master WAN restores, it will switch to master WAN interface again.

Configuration	
▼ Failover	
Parameters	
L3 WAN Failover	O Enable   Disable
Master Interface	pppoe_0_8_35/ppp0.1 V Ping Ocateway O Host
Slave Interface	pppoe_0_8_35/ppp0.1 V Ping Ocateway O Host
Probe Cycle	30 seconds [3~86400]
Connectivity Decision	Fail after 3 times[1~32]
Fall back	
Apply Cancel	

L3 WAN Failover: Check Enable to activate L3 WAN failover.

Master Interface: Select a master WAN interface.

Ping: To ping to check the master WAN inteface's connectivity.

- Gateway: It will send ping packets to gateway of master interface and wait for response from it in every "Probe Cycle" to check the connectivity of the gateway of master interface.
- () Host: It will send ping packets to specific host and wait for response in every "Probe Cycle".

Slave Interface: Select a slave WAN interface as backup port.

Ping: To ping to check the slave WAN inteface's connectivity.

- Gateway: It will send ping packets to gateway of slave interface and wait for response from it in every "Probe Cycle" to check the connectivity of the gateway of slave interface.
- (1) Host: It will send ping packets to specific host and wait for response in every "Probe Cycle".

**Probe Cycle:** Set the time duration for the **Probe Cycle** to determine when the router will switch to the backup connection once the main connection (main port) fails. For example, when set to 30 seconds, the probe will be conducted every 30 seconds.

**Connectivity Decision:** Set how many times of probing failure to switch to backup port.

# Note:

1) The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle** multiplied by **connection Decision amount** (e.g. From the image above it will be 30 seconds multiplied by 3 consecutive fails, the router will determine failover to slave interface.

2).The failback setting follow the same decision policy as the failover. For example, according to settings above in the screenshot, the connection probe will be carried out every 30 seconds, and 3 consecutive times of probe success is found, the router will determine failback to master interface.

# DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.

DSL	
Parameters	
Modulation	G.Dmt IG.lite IT1.413 ADSL2 AnnexL ADSL2+ AnnexM VDSL2
Profile	🛛 🖉 8a 🔍 8b 🔍 8c 🔍 8d 🔍 12a 🔍 12b 🗹 17a
US0	✓ Enable
Phone line pair	
Capability	Bitswap SRA
PhyR	Upstream 🗹 Downstream
*** If DSL line is not ready, related config	juration cannot successfully set.

**Modulation:** There are 8 modes "G.Dmt", "G.lite", "T1.413", "ADSL2", "AnnexL", "ADSL2+", "AnnexM", "VDSL2" that user can select for this connection.

Profile: VDSL profiles up to 17a.

**US0:** Select to enable US0. In VDSL mode, profiles like 8a, 8b, 8c, 8d, 12a and 17a need users to enable US0 band.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

**Capability:** There are 2 options "Bitswap Enable" and "SRA Enable" that user can select for this connection.

- Bitswap Enable: Allows bitswaping function.
- ③ SRA Enable: Allows seamless rate adaptation.

PhyR: A new technology to control impulse and noise to improve the BER and DSL data quality.

Click **Apply** to confirm the settings.

## SNR

**Signal-to-noise ratio** (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

Configuration			
▼ SNR			
Parameters			
Note that a value set too low ma There are no set values recomm	y affect stability, a balance needs to nended as each ADSL line will be o		nest possible sync speed whilst still maintaining stability.
SNR	-1	dB [ Auto : -1 ]	
Apply			

**SNR:** Change the value to adjust the DSL link rate, more suitable for an advanced user.

# System

## **Internet Time**

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.

Configuration				
▼ Internet Time				
Parameters				
Synchronize with Internet time servers	🗹 Enable			
First NTP time server	Other	~	192.43.244.18	
Second NTP time server	Other	*	128.138.140.44	
Third NTP time server	Other	*	129.6.15.29	
Fourth NTP time server	Other	*	131.107.1.10	
Fifth NTP time server	None	*		
Time zone offset	(GMT-00:00) Gree	enwich Mear	n Time: Dublin, Edinburgh, Lisbon, Lon	don 💌
Apply Cancel				

Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to apply your settings.

# Firmware Upgrade

Software upgrading lets you experience new and integral functions of your router.

Configuration		
▼Firmware Upgrade		
You may upgrade the system sof	tware on your network device.	
After upgrading, let your device re	start with factory default settings or current settings.	
Restart device with	Factory Default Settings	
Restant device with	O Current Settings	
New Firmware Image	Browse	
Upgrade		

#### **Restart device with:**

- **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- Current Settings: Restart the device with the current settings automatically when finishing upgrading.

Your router's "firmware" is the software that allows it to operate and provides all its functionality.

Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click **Upgrade** to update the firmware in your router.



DO NOT power down the router or interrupt the firmware upgarding while it is still in process. Improper operation could damage the router.

### **Backup / Update**

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

Configuration	
▼Backup / Update	
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.	
Backup Configuration	
Backup DSL router configurations. You may save your router configurations to a file on your PC.	
Backup Settings	
Restore Configuration	
Configuration File Browse	
Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save	e current configuration.
Update Settings	

Click **Backup Settings**, a window appears, click save , then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open.** Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.

progress		
progress Do not switch off device during flash update or rebo	ooting	
total :	6%	

#### Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.

Configuration			
* Access Control			
Parameters			
Level	Administrator 💌		
Username	admin		
Old Password		(maximum length is 15)	
New Password		(maximum length is 15)	
Confirm Password		(maximum length is 15)	
Apply Cancel			

Level: select which level you want to change password to. There are three default levels.

- ① Administrator: the root user, corresponding default username and password are admin and admin respectively.
- ③ Remote: username for the remote user to login, corresponding default username and password are support and support respectively.
- ① Local: username for the general user, when logon to the web page, only few items would be listed for common user, corresponding default username password are user and user respectively.

**Username:** The default username for each user level.

Old Password: Enter the old password.

New Password: Enter the new password.

**Confirm Password:** Enter again the new password to confirm.

**Note:** By default the accounts of **Remote** and **Local** are disabled, please click **Valid** check-box to activate the accounts.

Configuration			
▼Access Control			
Parameters			
Level	Remote 💙		
Valid			
Username	support		
Old Password		(maximum length is 15)	
New Password		(maximum length is 15)	
Confirm Password		(maximum length is 15)	
Apply Cancel			

Click **Apply** to apply your new settings.

#### Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.

Configuration	
▼Mail Alert	
Server Information	
WAN Port	DSL V
Apply all the settings to	Ethernet 3G/4G LTE
SMTP Server	
Username	
Password	
Sender's E-mail	(Must be xxx@yyy.zzz)
SSL / TLS	Enable
Port	25
Account Test	
Failover / Failback	
Recipient's E-mail	(Must be xxx@yyy.zzz)
WAN IP Change Alert	
Recipient's E-mail	(Must be xxx@yyy.zzz)
3G/4G LTE Usage Allowance	
Recipient's E-mail	(Must be xxx@yyy.zzz)
SIM lost	
Recipient's E-mail	(Must be xxx@yyy.zzz)
Apply Cancel	

**WAN Port:** Mail Alert feature can be applicable to every WAN mode: Ethernet, DSL and 3G/LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

**Apply all settings to:** check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

**SMTP Server:** Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

**Password:** Enter the password of your email account.

Sender's Email: Enter your email address.

**SSL:** Check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

**Recipient's Email (Failover / Failback):** Enter the email address that will receive the alert message once the failover or failback has been detected.

**Recipient's Email (WAN IP Change Alert):** Enter the email address that will receive the alert message once a WAN IP change has been detected.

**Recipient's Email (3G/4G LTE Usage Allowance ):** Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

**Recipient's Email (SIM lost):** Enter the email address that will receive the alert message once the SIM card loss has been detected.

#### SMS Alert

SMS, Short Message Service, is to inform clients the information clients subscribe. The BiPAC 8700AX(L)-1600 offers SMS alert sending clients alert messages when a WAN IP change is detected.

Configuration	
▼ SMS Alert	
WAN IP Change Alert	
Recipient's Number	
Арріу	

**Recipient's Number (WAN IP Change Alert):** Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

# **Configure Log**

Configuration		
▼ Configure Log		
Parameters		
Log		
Log Level	Informational 💌	
Display Level	Informational 💌	
Mode	Local 💌	
Apply Cancel		

Log: Enable or disable this function.

**Log level:** Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- **(i)** Emergency = system is unusable
- ① Alert = action must be taken immediately
- (i) **Critical** = critical conditions
- (i) **Error** = error conditions
- Warning = warning conditions
- (i) Notice = normal but significant conditions
- Informational = information events
- ① Debugging = debug-level messages

The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

**Display Level:** Display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: Select the mode the system log adopted. Three modes: local, Remote and Both.

- ① Local: Select this mode to store the logs in the router's local memory.
- ③ Remote: Select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- () **Both**: Logs stored adopting above two ways.

Click **Apply** to save your settings.

# USB

Storage here refers to network sharing in the network environment. USB devices act as the storage carrier for common file sharing, DLNA. With a USB-based printer, the 8700AX(L)-1600 can also serve as a network printer offering printing service for every client on the network.

# **Storage Device Info**

This part provides users direct access to the storage information like the total volume, the used and the remaining capacity of the device.

Configuration				
* Storage Device Info				
Storage Device Info				
Volume Name	FileSystem	Total Space	Used Space	Unmount
disk1_1	fat	15354	518	Unmount

Volume Name: Display the storage volume name

FileSystem: Display the storage device's file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

Used Space: Display the remaining space of each partition, unit MB.

**Unmount:** Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

#### **User Account**

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data. Default user admin.

Configuration			
▼User Accounts			
User Accounts			
A maximum accounts can be c	onfigured: 16		
Username	Home Directory	Remove	Edit
admin	1		
Add Remove			

#### Click Add button, enter the user account-adding page:

Configuration		
▼ User Accounts		
Parameters		
Username		
Password		
Confirm Password		
Volume Name	disk1_1 🗸	
Apply Cancel		

**Username:** user-defined name, but simpler and more convenient to remember would be favorable. **Password:** Set the password.

Confirm Password: Reset the password for confirmation.

**Volume Name:** Select Volume name, as to create access to the volume of the specified partition of the storage.

For example, a user *test* is setup behind the disk1\_1.

Configuration			
▼User Accounts			
User Accounts			
A maximum accounts can be	configured: 16		
Username	Home Directory	Remove	Edit
admin	1		
test	disk1_1/test		Edit
Add Remove			

# Accessing mechanism of Storage:

In your computer, Click **Start > Run**, enter <u>\\192.168.1.254</u>

192.168.1.254\/

\_\_\_\_

<b>₩</b> (192.168.1.254	
₽ See more results	
\\192. 168. 1. 254  ×	Shut down 🕨

When accessing the network storage, you can see a folder named "*public*", users should have the account to enter, and the account can be set at the User Accounts section.

When first logged on to the network folder, you will see the "*public*" folder.

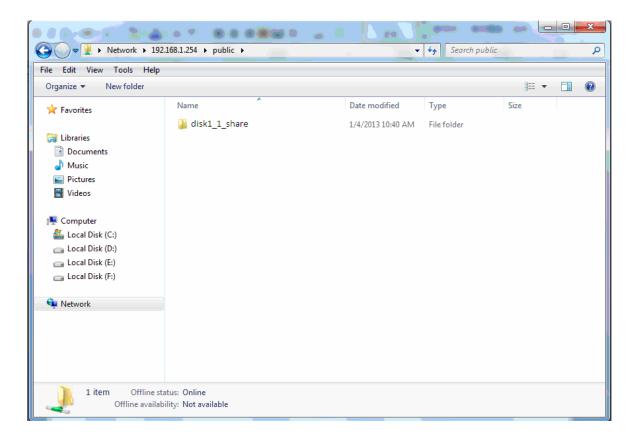
Public: The public sharing space for each user in the USB Storage.

When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.

Network	192.168.1.254 >	<b>▼</b>	47 Search 192.168.1.254
File Edit View Tools	Help		
Organize 🔻 Network an	d Sharing Center View remote p	inters	iii 🔹 🗖 🔞
🚖 Favorites	Name	Туре	Comments
Libraries Documents Music Pictures Videos Computer Computer Local Disk (C:) Local Disk (E:) Local Disk (F:)	🚆 public	Share	shared folders on each volume
🙀 Network		m	
1 item			

#### Access the folder *public*.

Windows Security
Enter Network Password Enter your password to connect to: 192.168.1.254
test •••• Domain: WIN7-64 Remember my credentials
🐼 Access is denied.
OK Cancel



When successfully accessed, the private folder of each user is established, and user can see from the following picture. The *test* fold in the picture is the private space for each user.

le Edit View Tools H	lelp		
Organize 🔻 Network and	d Sharing Center View remote	printers	i
😭 Favorites	Name	Туре	Comments
🖳 Recent Places	👰 public	Share	shared folders on each volun
🧱 Desktop	🤰 test	Share	Home Directory
<ul> <li>□ Libraries</li> <li>□ Documents</li> <li>↓ Music</li> <li>□ Pictures</li> <li>■ Videos</li> </ul>			
<ul> <li>Computer</li> <li>Local Disk (C:)</li> <li>Local Disk (D:)</li> <li>Local Disk (E:)</li> <li>Local Disk (F:)</li> </ul>			
🗣 Network			
	•	m	

### **Print Server**

The Print Server feature allows you to share a printer on your network by connecting a USB cable from your printer to the USB port on the 8700AX(L)-1600 This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 3 step process (8700AX-1600 for example)

- 1. Connect the printer to the 8700AX-1600 's USB port
- 2. Enable the print server on the 8700AX-1600
- 3. Install the printer drivers on the PC you want to print from

Configuration		
▼ Print Server		
Parameters		
On-board Print Server	Enable	
Printer Name	OfficePrinter	
Make And Model	Epson Stylus Photo R2	
Apply Cancel		

On-board Print Server: Check Enable to activate the print server

Printer Name: Enter the Printer name, for example, OfficePrinter

**Make and Model:** Enter in the Make and Model information for the printer, for example, *Epson Stylus Photo R290* 

#### Note:

The *Printer name* can be any text string up to **40** characters. It cannot contain spaces. The *Make and Mode* can be any text string up to **128** characters.

Setup of Printer client (Windows 7)

Step 1: Click Start and select "Devices and Printers"



#### Step 2: Click "Add a Printer".



Step 3: Click "Add a network, wireless or Bluetooth printer

Wha	at type of printer do you want to install?
•	Add a local printer Use this option only if you don't have a USB printer. (Windows automatically installs USB printe when you plug them in.)
•	Add a network, wireless or Bluetooth printer Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

Step 4: Click "The printer that I want isn't listed"

Printer Name	Address	

**Step 5:** Select "Select a shared printer by name" Enter <u>http://8700AX-1600</u> - LAN-IP:631/printers/printer-name or. Make sure printer's name is the same as what you set in the 8700AX earlier

For Example: *http://192.168.1.254:631/printers/OfficePrinter* OfficePrinter is the Printer Name we set up earlier

0	Add Printer	x
	Find a printer by name or TCP/IP address	
	Browse for a printer	
	Select a shared printer by name	
	http://192.168.1.254:631/printers/OfficePrinter	B <u>r</u> owse
	Example: \\computername\printername or http://computername/printers/printername/.printer	
	Add a printer using a TCP/IP address or hostname	
	Ne	xt Cancel

**Step 6:** Click "Next" to add the printer driver. If your printer is not listed and your printer came with an installation disk, click "Have Disk" find it and install the driver.

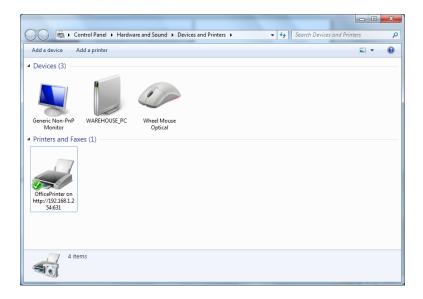
Add Printer Wizard	8 ×
an installation dis	acturer and model of your printer. If your printer came with k, click Have Disk. If your printer is not listed, consult your ation for a compatible printer.
Manufacturer	Printers
Brother	Epson Stylus Photo R200 (M)
Canon	Epson Stylus Photo R210 (M)
Epson	EPSON Stylus Photo R290 Series
Fuji Xerox	Epson Stylus Photo R300 (M)
Generic	El Enson Stylus Photo R310 (M)
This driver is digitally si <u>Tell me why driver sign</u>	Have Disk
	OK Cancel

#### Step 7: Click "Next"

6	🖶 Add Printer	-	x
	You've successful	ly added OfficePrinter on http://192.168.1.254:631	
	<u>P</u> rinter name:	OfficePrinter on http://192.168.1.254:631	
	This printer has been ir	stalled with the EPSON Stylus Photo R290 Series driver.	
		<u>N</u> ext	ancel

🕞 🖶 Add Printer
You've successfully added OfficePrinter on http://192.168.1.254:631
To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.
<u>F</u> inish Cancel

You will now be able to see your printer on the Devices and Printers Page



The Digital Living Network Alliance (DLNA) is a non-profit collaborative trade organization established by Sony in June 2003, which is responsible for defining interoperability guidelines to enable sharing of digital media between consumer devices such as computers, printers, cameras, cell phones and other multiple devices.

DLNA uses Universal Plug and Play (UPnP) for media management, discovery and control. UPnP defines the types of devices ('server', 'renderer', 'controller') that DLNA supports and the mechanism for accessing media over a network.

Overall, DLNA allows more convenience, more choices and enjoyment of your digital content through DLNA certified devices. Any DLNA certified devices or software can access the DLNA server.

With USB storage, 8700AX(L)-1600 can serve as a DLNA server.

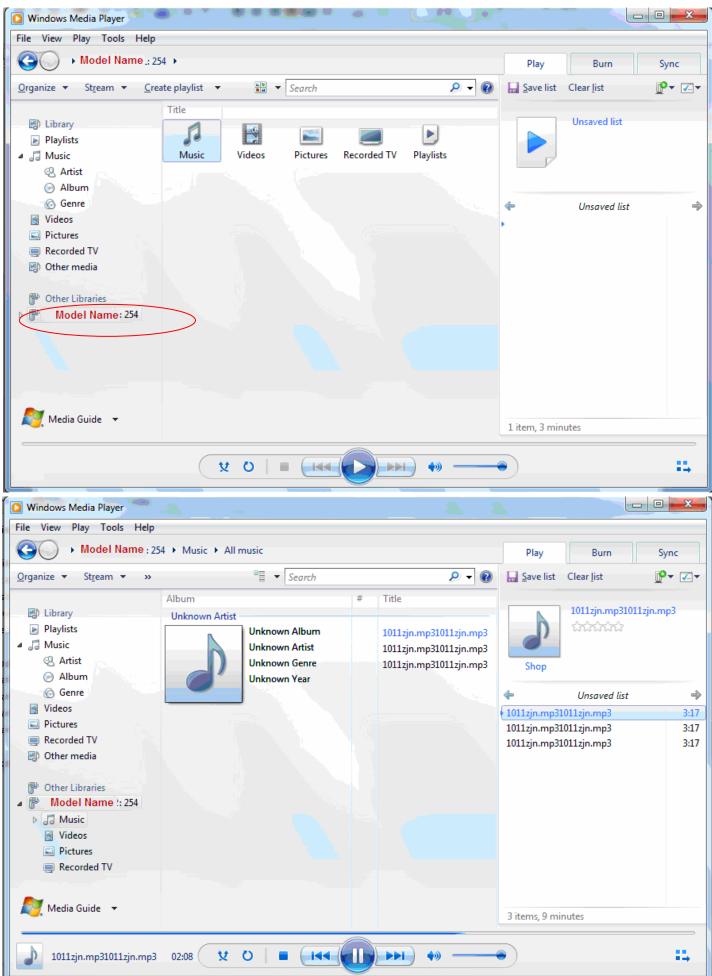
Configuration		
▼Digital Media Server settings		
Parameters		
On-board digital media server	Enable	
Interface	Default 💌	
Media Library Path	disk1_1 💌	
Apply Cancel		

**On-board digital media server:** Enable to share the device as a DLNA server.

Interface: The VLAN group, it is the bound interface for DLNA server accessing.

**Media Library Path:** Default is disk1\_1, total USB space (pictures, videos, music, etc, all can be accessed with this path).

Take Windows media player in Windows 7 accessing the DLNA server for example for usage of DLNA .



# **IP Tunnel**

An IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets. IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 internet.

#### IPv6inIPv4

6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP Protocol number set to 41. This protocol number is specifically designated for IPv6 capsulation.

#### 6RD:

6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the enduser's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.

Pv6inll							
6in4 Tun Name	nel Confi	-					
	WAN	LAN	Dynamic	V4 Common Bit Length	6rd Prefix with Prefix Length	Border Relay Address	Remove

#### Click Add button to manually add the 6in4 rules.

Configuration		
▼ 6in4 Tunnel Configuration		
Parameters		
Tunnel Name		
Mechanism	6RD 💌	
Associated WAN Interface	×	
Associated LAN Interface	LAN/br0 💌	
Method		
V4 Common Bit Length		
6rd Prefix with Prefix Length		
Border Relay IPv4		
Apply Cancel		

Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are

packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

**Method:** 6rd operation mechanism: manually configured or automatically configured. If manually, please fill out the following 6rd parameters.

**V4 Common Bit Length:** Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

**6rd Prefix with Prefix Length:** Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP( The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

**Border Relay IPv4 Address:** The IPv4 address of the border relay. The relay is used to unwrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

### IPv4inIPv6

4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

### DS – Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.

Configuration					
▼IPv4inIPv6					
4in6 Tunnel Confi	iguration				
Name	WAN	LAN	Dynamic	AFTR	Remove
Add Rem	iove				

Click Add button to manually add the 4in6 rules.

Configuration		
▼ 4in6 Tunnel Configuration		
Parameters		
Tunnel Name		
Mechanism	DS-Lite 💌	
Associated WAN Interface	×	
Associated LAN Interface	LAN/br0 💌	
Method		
AFTR		
Apply Cancel		

Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

**Associated WAN Interface:** The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

**Method:** Manually to specify the AFTP (Address Family Transition Router) address or Automatic. **AFTR:** Specify the address of AFTP (Address Family Transition Router) from your ISP.

# Security

# **IP Filtering Outgoing**

IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is "**or**" operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Note: The maximum number of entries: 32.

IP Filte	ering									
Dutgoir	ng IP Filtering Setup									
A maxin	num entries can be c	configured: 32								
Dedoe		IP	Drotocol	Source IP address	Source Port	Action	Lon	Disable	Domouo	Edit
Order	Filter Name	Version	Protocol	Destination IP address	Destination Port	Action	Log	Disable	Remove	Edit

Click **Add** button to enter the exact rule setting page.

Configuration					
Outgoing IP Filtering Se	tup				
Parameters					
Filter Name		<type from<="" or="" select="" td=""><td>i listbox 😒</td><td></td><td></td></type>	i listbox 😒		
IP Version	IPv4 💌				
Protocol	TCP/UDP 💌			Protocol Number	[0 - 254]
Source IP address		~		Source Port	[port or port:port]
Destination IP address		~		Destination Port	[port or port:port]
Time Schedule	Always On	Sun Mo	n 🔲 Tue 💭 Wed 🔲 Thu	Fri Sat From 00 V:	00 🗸 To 00 🗸 : 00 🗸
Action	drop 🖌			Log	
Apply					
(					

**Filter Name:** A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

**Protocol:** Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any) rule applies to.

**Source IP address:** This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

**Source Port [port or port:port]:** The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

**Destination IP address:** Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

**Destination Port [port or port: port]:** Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 –

65535.

**Time Schedule:** Select or set exactly when the rule works. When set to "Always On", the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in "**Time Schedule**" during which the rule works. And when set to "Disable", the rule is disabled or inactive and there will be an icon"

" in list table indicating the rule is inactive. See <u>Time Schedule</u>.

Action: Select to drop or forward the packets fit the outgoing filtering rule.

Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

**Example:** For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be forwarded. Or exactly in the rule below, all traffic trying to access FTP will be forwarded.

Configuration						
▼Outgoing IP Filtering Se	tup					
Parameters						
Filter Name	FTP	< <type fro<="" or="" select="" td=""><td>om listbox 💌</td><td></td><td></td><td></td></type>	om listbox 💌			
IP Version	IPv4 💌					
Protocol	TCP/UDP			Protocol Number		[0 - 254]
Source IP address		~		Source Port		[port or port:port]
Destination IP address		~		Destination Port	21	[port or port:port]
Time Schedule	Always On	Sun 🗆 N	Non 🗌 Tue 🗌 Wed 🗌 Thu 🔲 Fri	Sat From 00 🗸 :	00 🗸 To 00	- : 00 -
Action	forward 💌			Log	Image: A start of the start	

P IP Filt	ering									
Outgoi	ng IP Filtering Setup									
A maxir	num entries can be (	configured: 32								
Order	Citere Manage	IP	Protocol	Source IP address	Source Port	Antina	Log	Disable	Remove	Edit
Order	Filter Name	Version		Destination IP address	Destination Port	Action				
	ETD		TCP	Any	Any	forward	Disable			Edit
	FTP 4	4	ICF	Any	21	lorward	Disable			

(The rule is active; disable field shows the status of the rule, active or inactive)

Add another Outgoing IP Filtering rule, users will find the "arrow" icon to change the IP outgoing filter rule working orders.

▼ IP Filt	ering									
Outgoin	ng IP Filtering Setup									
A maxir	num entries can be c	configured: 32								
Order	Filter Name IP Versio	IP	Protocol	Source IP address	Source Port	Action	Les	Disable	Demous	<b>F</b> 40
Order		Version	Protocol	Destination IP address Destinatio		Action	Log	Disable	Remove	Eun
1	FTP		TOP	Any	Any	forward	Disable			Edit
*	r i r	P 4 TCP Any	Any	21	forward Disabl				Eult	
	LITTO			Any	Any	dran	Disable			C T dit
•	HTTP 4	TCP	Any	80	drop	Disable			Edit	

# How to disable set rule.

Configuration									1		
• Outgoing IP Filtering S	etup										
Parameters											
Filter Name	FTP	<	<	listbox 👻							
IP Version	IPv4 💌										
Protocol	TCP 🗸					Protocol Nu	mber		[0	- 254]	
Source IP address		~				Source Port				[port or p	ort:port]
Destination IP address		~				Destination	Port	21		[port or p	ort:port]
						Sat From	00 ~	: 00 V T	0 00 ~	00 🗸	
Time Schedule 🤇	Disable		Sun 🗌 Mon	n 🗌 Tue 🗌 Wed	Thu Fri	- Out I for					
Time Schedule ( Action Apply	Disable forward 💌		Sun 🗆 Mon	n ∟]Tue ∟IWed	L Thu L Fr	Log					
Action			Sun 🗆 Mon	n ∟Tue ∟Wed	_ Thu _ Fri			and the second s			4
Action Apply Configuration			Sun 🗆 Mon	n ∟Tue ∟Wed	□ Thu □ Fri			and the second s			
Action Apply Configuration IP Filtering	forward 💌		Sun 🗆 Mon	h ∟Tue ∟Wed	□ Thu □ Fri			and the second s			4
Action Apply	forward 💌		Sun Mon	h ∟ Tue ∟ Wed	Thu     Fri			and the second s			4
Action Apply Configuration IP Filtering utgoing IP Filtering Setu maximum entries can b	forward 💌		Source IP address	h ∟ Tue ∟ Wed							4
Action Apply Configuration IP Filtering Putgoing IP Filtering Setu maximum entries can b	forward v	Protocol			So	Log		Contraction of the local distance of the loc	Disable	Remove	Edit
Action Apply Configuration IP Filtering Dutgoing IP Filtering Setu maximum entries can b	forward  forward forwa	Protocol	Source IP address		So	Log urce Port istination Port y		Log	Disable	Remove	Edit

(Rule inactive)

# **IP Filtering Incoming**

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to forward the specific incoming traffic.

#### Note:

1. The maximum number of entries: 32.

2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.

▼ IP Filtering							
Incoming IP Filte	ring Setup						
A maximum entri	es can be configured:	32					
Filter Name	Interfaces		Source IP address	Source Port	1.00	Dischle	Remove Edi
Filter Marne		IP Version Protocol	Destination IP address	Destination Port	Log	Disable	Remove Edi

Click **Add** button to enter the exact rule setting page.

Configuration			
Incoming IP Filtering Se	tup		
Parameters			
Filter Name	<type from="" listbox-<="" or="" select="" td=""><td>- 🗸</td><td></td></type>	- 🗸	
IP Version	IPv4 💌		
Protocol	TCP/UDP	Protocol Number	[0 - 254]
Source IP address	~	Source Port	[port or port:port]
Destination IP address	~	Destination Port	[port or port:port]
Interfaces	All Dipoe_eth4/eth4.1 Dpppoe_0_0_35/ppp0.1	23G0/USB3G0	
Time Schedule	Always On 💽 Sun 🗌 Mon 🗌 Tu	e 🗌 Wed 🛄 Thu 🛄 Fri 🛄 Sat From 00 💌 : 00 💌	To 00 🗸 : 00 🗸
Log			
Apply			

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

**IP Version:** Select the IP Version, IPv4 or IPv6.

**Protocol:** Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any ) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port : port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 -65535

Interfaces: Check if the filter rule applies to all interfaces. User can base on need select interfaces to make the rule take effect with those interfaces.

**Time Schedule:** Select or set exactly when the rule works. When set to "Always On", the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in "**Time Schedule**" during which the rule works. And when set to "Disable", the rule is disabled or inactive and there will be an icon"

" in the list table indicating the rule is inactive. See <u>Time Schedule</u>.

Log: check the check-box to record the security log. To check the log, users can turn to <u>Security Log</u>.

### **MAC Filtering**

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

**FORWARDED** means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.

**BLOCKED** means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.

Configuration					
MAC Filtering					
MAC Filtering S	etup				
		Cs configured in Bridge mode. FORWA OCKED means that all MAC layer frame			
MAC Filtering P	olicy For Each Interface				
Interface	Policy	Change			
atm0.1	FORWARD				
WARNING: Cha for the new polic		another of an interface will cause all d	efined rules for that interface to t	De REMOVED AUTOMATICALLY! Yo	u will need to create new rules
Change Polic					
MAC filtering ru	les				
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
Add Re	move				

By default, all MAC frames of the interface in Bridge Mode will be **forwarded**, you can check **Change** checkbox and then press **Change Policy** to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode, and all the MAC layer frames will be **forward**, but you can set some rules to let some item matched the rules to be **blocked**.

Click Add button to add the rules.

Configuration		
▼MAC filtering rules		
Parameters		
Protocol	✓	
Destination MAC		
Source MAC		
Frame Direction	LAN<=>WAN	
WAN Interface	br_eth0/eth0.2 💌	
Apply		

**Protocol type:** Select from the drop-down menu the protocol that applies to this rule.

Destination /Source MAC Address: Enter the destination/source address.

**Frame Direction:** Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only LAN to WAN: LAN=>WAN, only WAN to LAN: WAN=>LAN.

**WAN Interfaces:** Select the interfaces configured in Bridge mode.

# **Blocking WAN PING**

This feature is enabled to let your router not respond to any ping command when someone others "Ping" your WAN IP.

Configuration		
Parameters		
Block WAN PING	O Enable 💿 Disable	
Block WAN (IPv6) PING	O Enable 💿 Disable	

## **Time Restriction**

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

This page adds time of day restriction to a special LAN device connected to the router. Please click Add button to add the device(s) to be subject to Time Restriction rules (forward or drop connection to internet). Devices Not added will not comply with the rules and access internet and router willingly.

To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.

Time Restriction												
Access Time Restriction	on											
A maximum entries can	be configured: 32											
Host Label IV	MAC Address	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Remove	Edit

#### Click Add to add the rules.

Configuration	
<ul> <li>Time Restriction</li> </ul>	
Parameters	
Host Label	
MAC Address	< <type from="" listbox="" or="" select="" td="" 💌<=""></type>
Time Schedule	drop Sun Mon Tue Wed Thu Fri Sat From 00 v : 00 v To 00 v : 00 v
Apply Cancel	

Host Label: User-defined name.

**MAC Address:** Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx or xx-xx-xx-xx. For convenience, user can select from the list box.

Time Schedule: Configure to control the PC from accessing router and internet.

- ① Drop: To drop the MAC entries always; in other words, the MACs are blocked access to router and internet always.
- Forward: To forward the MAC entries always; in other words, the MACs are granted access to the router and internet always.
- ① Check or select from listbox: To set the time duration during which the MACs are blocked from access the router and internet. "select from listbox" means that you can select the already set timeslot in "Time Schedule" section during which the MACs are blocked from access the router and internet.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

# An example:

•

Configuration												
Time Restriction												
Access Time Restriction												
A maximum entries can be o	configured: 32											
Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit
test	18:a9:05:38:04:03	forwa	rd									Edit
child-use	18:a9:05:04:12:23		x	х	х	x	x		00:00	23:59		Edit
Add Remove	)											

Here you can see that the user "child-use" with a MAC of 18:a9:05:04:12:23 is blocked to access the router from 00:00 to 23:59 Monday through Friday. The "test" can access the internet always.

If you needn't this rule, you can check the box, press Remove, it will be OK.

#### **URL Filter**

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

#### Note:

1) URL Filter rules apply to both IPv4 and IPv6 sources.

2) But in **Except IP Address** part, user can click **Detail** to set the exception IP address(es) for IPv4 and IPv6 respectively.

VRL Filter	
Parameters	
Keywords Filtering	Enable Detail >
Domains Filtering	Enable Detail •
Restrict URL Features	BLOCK 🗆 Java Applet 🔲 ActiveX 💭 Cookie 💭 Proxy
Except IP Address	Detail 🕨
Log	
Time Schedule	Always On Sun Mon Tue Wed Thu Fri Sat From 00 🗸 : 00 🗸 : 00 🗸 : 00

**Keywords Filtering:** Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g.to block any image called "advertisement.gif"). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

**Domains Filtering:** This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

**Restrict URL Features:** Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

**Except IP Address:** You can input a list of IP addresses as the exception list for URL filtering. These IPs will not be covered by the URL rules.

**Time Schedule:** Select or set exactly when the rule works. When set to "Always On", the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in "**Time Schedule**" during which the rule works. And when set to "Disable", the rule is disabled. See <u>Time Schedule</u>.

**Log:** Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to <u>Security Log</u>.

#### **Keywords Filtering**

Note: Maximum number of entries: 32.

Click Detail to add the keywords.

Configuration	
▼ Keywords Filtering	
Parameters	
Keyword	
Add Edit / Delete Return >	

Enter the Keyword, for example image, and then click Add.

Configuration		
<ul> <li>Keywords Filt</li> </ul>	ering	
Parameters		
Keyword		
Add Ed	it / Delete Return >	
Edit	Keyword	Delete
0	image	

You can add other keywords like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, and then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

#### **Domains Filtering**

Note: Maximum number of entries: 32.

Click Detail to add Domains.

Configuration			
▼ Domains Filtering			
Parameters			
Domains Filtering	Туре	Forbidden Domain 💌	
Add Edit / Delete Return >			

**Domains Filtering:** enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

- (i) **Forbidden Domain:** The domain is forbidden access.
- ① **Trusted Domain:** The domain is trusted and allowed access.

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to *Keywords* 

#### Filtering.

#### **Except IP Address**

In the section, users can set the exception IP respectively for IPv4 and IPv6.

Click Detail to add the IP Addresses.

Configuration		
* Except IP Address		
Parameters		
IP Version	IPv4 💌	
Internal IP Address	~	
Add Edit / Delete Return >		

Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the *Exception List*, and excluded from the URL filtering rules in effect. For specific process, please refer to *Keywords Filtering*.

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter ( or IPv4 clients (a range) ). And also an IPv6 client (2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients(a range ) can be the exceptions from the URL rules.

At the URL Filter page, press **Apply** to confirm your settings.

#### **Parental Control Provider**

Parental Control Provider provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider "www.opendns.com" in advance. To use parental control (DNS), user needs to configure to use parental control (DNS) provided by parental control provider) to access internet at WAN configuration or DNS page(See DNS).

Configuration		
Parental Control Provider		
Parameters		
	Neb content filtering while surfing the web safer and more reliable. e at the selected Provider in advance.	
Provider	www.opendns.com	
Host Name		
Username		
Password		
(Apply) Cancel		

Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website <u>www.opendns.com</u>.

# **QoS - Quality of Service**

#### **Quality of Service**

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

**Note:** VDSL/ADSL line speed is based on the VDSL/ADSL sync rate. But there is no QoS on 3G/4G LTE as the 3G/4G LTE line speed is various and can not be known exactly.

QoS Classification Setup									
EWAN Line Speed									
Upstream / Downstream	0	/ 0	)	(bps [0 : Disable]					
Apply									
Maximum rules can be configured: 32									
Class Name IP Version Direction II	nternal IP Address	Internal Port	Protocol	External IP Address	External Port	DSCP Mark	Rote Type	Disabled	Remove

#### **EWAN Line Speed**

**Upstream / Downstream:** Specify the upstream and downstream rate of the EWAN interface. Click **Apply** to save the EWAN rate settings.

Click Add to enter QoS rules.

Configuration					
▼Quality of Service					
Non-Assigned Bandwidth Ra	tio => Upstream (LAN to WAN) : 100%	Downstream (WAN to LAN)	: 100%		
IP Version	IPv4 🐱				
Application	< <ty< td=""><td>pe or select from listbox 💌</td><td></td><td></td><td></td></ty<>	pe or select from listbox 💌			
Direction	LAN to WAN 🗸	Protocol	Any 🗸	DSCP Marking	Disable 💌
Rate Type	Prioritization 💌	Ratio	%	Priority	Normal 💌
Internal IP Address	~		Internal Port	~	
External IP Address	~		External Port	~	
Time Schedule	Always On 💌	Sun Mon Tue	Wed Thu Fr	i 🗌 Sat From 00 🛩 :	: 00 🗸 To 00 🗸 : 00 🗸
Apply					

IP Version: Select either IPv4 or IPv6 base on need.

**Application:** Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

**Direction:** Shows the direction mode of the QoS application.

- ① LAN to WAN: You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application. Eg: you have a FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.
- () WAN to LAN: Control traffic from WAN to LAN (Downstream).

**Protocol:** Select the supported protocol from the drop down list.

**DSCP Marking:** Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

# **IP Precedence and DSCP Mapping Table**

Мар	bing Table
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP offers three levels of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four levels of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Rate Type: You can choose *Limited* or *Prioritization*.

- Limited (Maximum): Specify a limited data rate for this policy. It also is the maximum rate (j) for this policy. When you choose *Limited*, type the *Ratio* proportion. As above FTP server example, you may want to "throttle" the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- ① Prioritization: Specify the rate type control for the rule to used. If you choose Prioritization for the rule, you parameter **Priority** would be available, you can set the priority for this rule.
- Set DSCP Marking: When select Set DSCP Marking, the packets matching the rule will be  $\mathbf{\hat{I}}$ forwarded according to the pre-set DSCP marking.

**Ratio:** The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%\*256\*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8)

**Priority:** Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

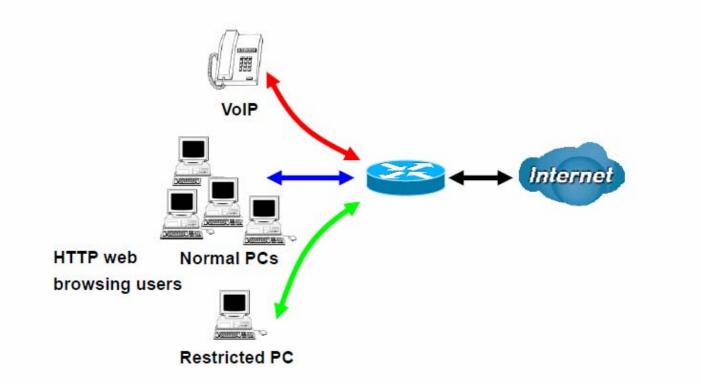
Internal Port: The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

**Time Schedule:** Select or set exactly when the rule works. When set to "Always On", the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in "**Time Schedule**" during which the rule works. And when set to "Disable", the rule is disabled or inactive and there will be an icon"

" indicating the rule is inactive. See Time Schedule.



1. Give outgoing VoIP traffic more priority.

The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.

Configuration					
Quality of Service					
Non-Assigned Bandwidth Ra	tio => Upstream (LAN to WAN) : 100	% Downstream (WAN to LAN)	):100%		
IP Version	IPv4 💌				
Application	Voip << -	-type or select from listbox 💌			
Direction	LAN to WAN 💌	Protocol	Any 🗸	DSCP Marking	EF(101110)
Rate Type	Prioritization 💌	Ratio	%	Priority	High 🔽
Internal IP Address	~		Internal Port	~	
External IP Address	~		External Port	~	
Time Schedule	timeslot1	✓ Sun ☑ Mon ☑ Tue	₩Wed . Thu . Fr	Sat From 00 🗸	: 00 🔽 To 09 🔽 : 19 🔽

2. Give regular web http access a limited rate

Configuration					
▼ Quality of Service					
Non-Assigned Bandwidth R	atio => Upstream (LAN to WAN) : 100% Do	ownstream (WAN to LAN)	:100%		
IP Version	IPv4 🐱				
Application	HTTP << HTTP(T	CP 80)			
Direction	LAN to WAN 💌	Protocol	TCP 💌	DSCP Marking	Disable 💌
Rate Type	Limited (Maximum) 💌	Ratio	20 %	Priority	Normal 🗸
Internal IP Address	~		Internal Port	~	
External IP Address	~		External Port	80 ~ 80	)
Time Schedule	timeslot1 💌 🛛	Sun 🗹 Mon 🗹 Tue [	✔Wed ♥Thu ♥Fr	i 🗌 Sat From 00 💌	: 00 💌 To 09 💌 : 19 💌
Apply					

3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.

Configuration					
▼Quality of Service					
Non-Assigned Bandwidth Ra	atio => Upstream (LAN to WAN) : 80%	Downstream (WAN to LAN) :	100%		
IP Version	IPv4 💌				
Application	P2P << -	-type or select from listbox 💌			
Direction	LAN to WAN 💌	Protocol	Any 💌	DSCP Marking	Disable 💌
Rate Type	Prioritization 💌	Ratio	%	Priority	Low 💙
Internal IP Address	~		Internal Port	~	
External IP Address	~		External Port	~	
Time Schedule	timeslot1	Sun 🗹 Mon 🗹 Tue 🛙	✔Wed ✔Thu ✔Fr	i 🗌 Sat From 00 💌	: 00 🔽 To 09 🔽 : 19 🔽

Other applications, like FTP, Mail access, users can use QoS to control based on need.

# **QoS Port Shaping**

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When "Shaping Rate" is set to "-1", no shaping will be in place and the "Burst Size" is to be ignored.

• QoS Port Shaping			
Parameters			
QoS port shaping supports	traffic shaping of Ethernet interfac	ce. If "Shaping Rate" is set to "-1", it means no shap	ing and "Burst Size" will be ignored.
Interface	Туре	QoS Shaping Rate (kbps)	Burst Size (Byte)
P1	LAN	-1	0
P2	LAN	-1	0
P3	LAN	-1	0
P4	LAN	-1	0
P5/EWAN	LAN	-1	0

Interface: P1-P5. P5 used as EWAN also covered.

**Type:** All LAN when P5 is LAN port; P5 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

Burst Size(Bytes): Set the forcefully Burst Size.

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

#### **Exceptional Rule Group**

Exceptional Rule is dedicated to giving or blocking NAT/DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.

Configuration				
• Exceptional	Rule Group			
Parameters				
Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press Edit to set the exceptional IP (IP Range).

Configuration		
* Exceptional Rule Group		
Parameters		
Group Name	Group1	
Default Action	Allow      Block	
Apply		
Exceptional Rule IP Range		
IP Address Range	~	
Add Edit / Delete		

**Default Action**: Please first set the range to make "**Default Action**" setting available. Select "Allow" to grant access to the listed IP or IPs to Virtual Server and DMZ Host.

While choose "Block" to ban the listed IP or IPs to access the Virtual Server and DMZ Host.

Apply: Press Apply button to apply the change.

#### **Exceptional Rule Range**

**IP Address Range:** Specify the IP address range; IPv4 address range can be supported.

Click Add to add the IP Range.

For instance, if user wants block IP range of 172.16.1.102-172.16.1.106 from accessing your set virtual server and DMZ host, you can add this IP range and valid it.

Configurat	tion			
<ul> <li>Exceptio</li> </ul>	onal Rule Group			
Paramete	ers			
Group Nar	me	Group1		
Default Ac	tion	O Allow 💿 Block		
Apply				
Exception	al Rule IP Range			
IP Address	s Range	~		
Add	Edit / Delete			
Edit	Action	IP Address Range	Delete	
0	Block	172.16.1.102 ~ 172.16.1.106		

#### **Virtual Servers**

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.

Virtual Servers										
Virtual Servers Setup										
Ossiasblama	External	Port	Destand	Internal Port		Opening ID Addresse	WANT late for an	Oleahlad	Deserve	<b>E</b> .40
Server Name	Start	End	Protocol	Start	Start End	Server IP Address	WAN Interface	Disabled	Remove	Edit

It is virtual server listing table as you see, Click Add to move on.

The following configuration page will appear to let you configure.

▼Virtual Server	s					
Parameters						
Interface		pppoe_0_8_35/ppp	0.1 💙	WAN IP		
Server Name		Custom Service	*			
Custom Servi	ce					
Server IP Addre	SS		<type or="" select="" t<="" td=""><td>from listbox ⊻</td><td></td><td></td></type>	from listbox ⊻		
Time Schedule		Always On : 00 🗸	Sun Mon	Tue Wed Thu	Fri Sat From 00 🗸	: 00 🗸 To 00 🖌
Exceptional Rul	e Group	None 💌				
External Port		Destand	Protocol Number	Internal Port		
Start	End	Protocol	Protocol Number	Start	End	
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
Apply C	ancel					

Interface: Select from the drop-down menu the interface you want the virtual server(s) to apply.

**WAN IP:** To specify the exact WAN IP address. It can be flexible while there are multiple WAN IPs on one interface. If the WAN IP field is empty, 8700AX(L)-1600 uses the current WAN IP of this interface.

Server Name: Select the server name from the drop-down menu.

**Custom Service:** It is a kind of service to let users customize the service they want. Enter the userdefined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.

Server IP Address: Enter your server IP Address here. User can select from the list box for quick setup.

# **External Port**

- Start: Enter a port number as the external starting number for the range you want to give access to internal network.
- ① End: Enter a port number as the external ending number for the range you want to give access to internal network.

# **Internal Port**

- ③ **Start:** Enter a port number as the internal staring number.
- (i) **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

**Protocol:** select the protocol this service used: TCP/UDP, TCP, UDP.

**Time Schedule:** Select or set exactly when the Virtual Server works. When set to "Always On", the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to "Disable", the rule is disabled and there will be an icon  $\checkmark$  in the list table indicating the rule is disabled. See <u>Time Schedule</u>.

**Exceptional Rule Group:** Select the exceptional group listed. It is to grant or block Virtual Server

access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

#### Set up

**1.** Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Virtual Serve	ers					
Parameters						
Interface		pppoe_0_8_35/ppp	0.1 💌	WAN IP		
Server Name		Custom Service	*			
Custom Ser	vice					
Server IP Add	ress		< <type or="" select<="" td=""><td>from listbox 💌</td><td></td><td></td></type>	from listbox 💌		
Time Schedul	le	Always On : 00 🛩	Sun Mon	Tue Wed Thu	Fri Sat From 00 🗸	: 00 🗸 To 00 🔨
Exceptional R	ule Group	None 💌				
External Port				Internal Port		
Start	End	Protocol	Protocol Number	Start	End	
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌		1		
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 💌				
		TCP 🗸				

# 2. Press Apply to conform, and the items will be list in the Virtual Servers Setup table.

Virtual Servers										
Virtual Servers Setup										
Server Name	External	Port	Protocol	Internal	Port	Server IP Address	WAN Interface	Disabled	Remove	Edit
Server Marrie	Start	End	FIOLOCOI	Start	End	Server IF Address	WAN Intenace	Disableu	Tremove	Lon
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1			Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1			Edit

Virtual Servers										
Virtual Servers Setup										
Server Name	External	Port	Protocol	Internal	Port	Server IP Address	WAN Interface	Disabled	Remove	Edit
Server Marrie	Start	End	FIOLOCOT	Start	End	Server II Address	WAN Interface	Disabled	Kennove	Luit
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	$\checkmark$		Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1			Edit

(✓

Means the rule is inactive)

# Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.

Virtual Servers										
Virtual Servers Setup										
Server Name	External	Port	Protocol	Internal	Port	Server IP Address	WAN Interface	Disabled	Remove	Edit
Server Marrie	Start	End	FIOLOCOI	Start	End	Server IF Address	WAN Intenace	Disableu	Kennove	Lan
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	×		Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1			Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1			Edit

#### **DMZ Host**

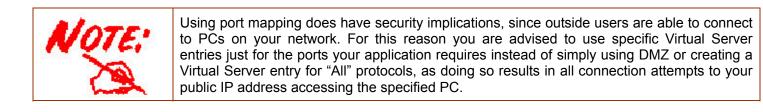
The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

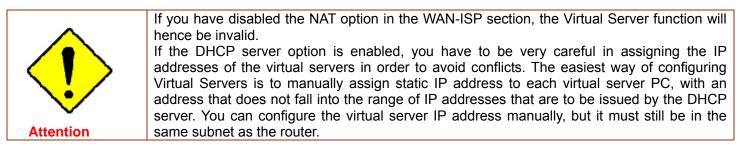
* DMZ Host		
Parameters		
DMZ Host IP Address		<<
Time Schedule	Always On	Sun Mon Tue Wed Thu Fri Sat From 00 😪 : 00 😪 : 00 😒
Exceptional Rule Group	None 🗸	

**DMZ Host IP Address:** Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

**Time Schedule:** Select or set exactly when the DMZ works. When set to "Always On", the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to "Disable", the rule is disabled. See <u>Time Schedule</u>.

**Exceptional Rule Group:** Select the exceptional group listed. It is to grant or block DMZ access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block DMZ Access to this IP range, you can select Group1.





#### One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address. If user has multiple global/public IP addresses from your ISP, you are free to use one-to-one NAT to assign some specific public IP for an internal IP like a public web server mapped with a global/public IP for outside access.

Configuration		
▼ One-to-One NAT		
Parameters		
Valid		
WAN Interface	pppoe_0_8_35/ppp0.1 🗸	
Global IP Address		
Internal IP Address		
Exceptional Rule Group	None 🖌	
Add Edit / Delete		

Valid: Check whether to valid the one-to-one NAT mapping rule.

WAN Interface: Select one based WAN interface to configure the one-to-one NAT.

**Global IP address:** The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

Internal Address: The IP address of an internal device in the LAN.

**Exceptional Rule Group:** Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 123.1.1.2.

**For example,** you have an ADSL connection of pppoe\_0\_8\_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses

#### Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.

Port Triggering									
Port Triggering Setup									
	Trigger			Open					
Application	Protocol	Port Rang	je	Destand	Port Range		WAN Interface	Remove	Edit
	Protocol	Start	End	Protocol	Start	End			

Click Add to add a port triggering rule.

Configuration											
Port Triggering											
Parameters											
Interface		pppoe_0_8_35/ppp	pppoe_0_8_35/ppp0.1 💟								
Application		Custom Application	Custom Application								
Custom Applicati	ion										
Trigger Port			Open Port								
Start	End	Trigger Protocol	Start	End	Open Protocol						
		TCP 💌			TCP 💌						
		TCP			TCP 🔽						
		TCP			TCP 💌						
		TCP 🔽			TCP 🔽						
		ТСР			TCP 💌						
		TCP			TCP 💌						
		TCP			TCP 💌						
		TCP			TCP 🗸						

**Interface:** Select from the drop-down menu the interface you want the port triggering rules apply to. **Application:** Preinstalled applications or Custom Application user can customize the utility yourself. **Custom Application:** It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

#### **Trigger Port**

- ① **Start:** Enter a port number as the triggering port starting number.
- ① End: Enter a port number as the triggering port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

# Open port

- ③ **Start:** Enter a port number as the open port staring number.
- (i) **End:** Enter a port number as the open port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the preset forwarding port or open port.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

# Set up

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

**1.** Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Configuration											
▼ Port Triggering											
Parameters											
Interface		pppoe_0_8_35/ppp	pppoe_0_8_35/ppp0.1 💟								
Application		Aim Talk	Aim Talk								
Custom Application	on										
Trigger Port			Open Port								
Start	End	Trigger Protocol	Start	End	Open Protocol						
4099	4099	TCP 💌	5191	5191	TCP 💌						
		TCP			TCP						
		TCP 💌			TCP						
		TCP 💌			TCP						
		TCP 💌			TCP 💌						
		TCP			ТСР						
		TCP 🔽			TCP 💌						
		TCP 💌			TCP						

2. Press Apply to conform, and the items will be list in the Port TriggeringSetup table.

Port Triggering									
Port Triggering Setup									
1000 H 10	Trigger			Open					
Application	Protocol	Port Range		Protocol	Port Range		WAN Interface	Remove	Edit
	FIOLOCOL	Start	End	FIOLOCOI	Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1		Edit

# Edit/Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press **Remove**.

Click **Edit** to re-edit your port-triggering rule.

Configuration									1
* Port Triggering									
Port Triggering Setup									
	Trigger			Open	27			_	
Application	Protocol	Port Ran	ge	Protocol	Port Ran	ge	WAN Interface	Remove	Edit
	FIOLOCOL	Start	End	FIOLOCOI	Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1		Edit
Add Remove									

The ALG Controls enable or disable protocols over application layer.

ALG		
Parameters		
SIP	Enable      Disable	
H.323		
IPSec	Enable O Disable	

**SIP:** Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP when SIP phone includes NAT-Traversal algorithm.

**H.323:** Enable to secure the voice communication using H.323 protocol when one or both terminals are behind a NAT.

**IPSec:** Enable IPSec ALG to allow one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation)"

# Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

▼Wake On LAN	
Parameters	
Host Label	
MAC Address	<
Wake by Schedule	Enable Schedule

Host Label: Enter identification for the host.

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

**Wake by Schedule:** Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click <u>Schedule</u> to enter time schedule configuring page to set the exact timeline.

Configuration									
Wake up Time Schedule									
Parameters									
Name									
Day in a week			Su	n 🗌 Mor	n 🗌 Tu	e 🗌 We	d 🗌 Thu	Fri 🔲 Sat	
Time			00 🗸	: 00 🗸	]				
Add Edit / Delete									
Edit Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Delete
0 11		x	x	x	х	х		09:00	

Add: After selecting, click Add then you can submit the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

"Yes" indicating the remote computer is ready for your waking up.

"No" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

Configur	ation					
▼Wake (	On LAN					
Paramet	ters					
Host Lab	pel					
MAC Add	Iress		<<	or select from listbox)		
Wake by	Schedule	Enable Schedule				
Add	Edit / Delete					
Edit	Action	Host Label	MAC Address	Ready	Delete	14 5
0	Schedule	billion-17bc6f1	18:A9:05:38:04:03	Yes		

# VPN

A **virtual private network** (**VPN**) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

# **IPSec**

**Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (**IP**) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

Note: A maximum of 16 sessions for IPSec.

VPN	/PN								
▼IPSec									
NAT Tra	iversal								
NAT Tra	NAT Traversal Enable Keep Alive 60 Second(s) [1-60]								
Apply	)								
Tunnel	Mode Con	inections							
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit		
Add	Remove	e							

# NAT Traversal

**NAT Traversal:** This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

**Keep Alive:** Type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click **Apply** to save and apply your settings.

VPN					
▼IPSec					
IPSec Settings					
L2TP over IPSec	Enable				
Connection Name		WAN Interface	Default 💌	IP Version	IPv4 💌
Local Network	Single Address 💌	IP Address		Netmask	
Remote Security Gateway		Anonyn	nous		
Remote Network	Single Address 💌	IP Address		Netmask	
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key					
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1				45	
Mode	Main 🖌				
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 💌		
DH Group	MODP1024(DH2) 💉	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 💌		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	None 💌				
мти	0 (0 : Default)				
Apply					

# **IPSec Settings**

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See L2TPover IPSec

**Connection Name:** A given name for the connection, but it should contain no spaces (e.g. "connection-to-office").

**WAN Interface:** Select the set used interface for the IPSec connection, when you select adsl pppoe\_0\_0\_35/ppp0.1 interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

**IP Version:** Select the IP version base on your network framework.

Local Network: Set the IP address or subnet of the local network.

- (i) **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- Subnet: The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

**IP Address:** The local network address.

**Netmask**: The local network netmask.

**Remote Secure Gateway:** The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

Anonymous: Enable any IP to connect in.

Remote Network: Set the IP address or subnet of the remote network.

- (i) **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ③ Subnet: The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

Key Exchange Method: Displays key exchange method.

**Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

**Local ID Type** and **Remote ID Type:** When the mode of phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

**ID content:** Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

# Phase 1

**Mode:** Select IKE mode from the drop-down menu: *Main* or *Aggressive*. This IKE provides secured key generation and key management.

**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ③ 3DES: Stands for Triple Data Encryption Standard, it uses 168 (56\*3) bits as an encryption method.
- ① AES: Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

**Integrity Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- () **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- **• SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

**DH Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

**SA Lifetime:** Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 480 minutes (28800 seconds). A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

# Phase 2

**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

**Integrity Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

**DH Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

**IPSec Lifetime:** Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Ping for Keep Alive: Select the operation methods:

- ① None: The default setting is "None". To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.
- ① DPD: Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

Detection Interval	180 864001	Second(s) [180-	Idle Timeout	5	Consecutive times [5-99]
--------------------	---------------	-----------------	--------------	---	--------------------------

**Detection Interval:** The period cycle for dead peer detection. The interval can be 180~86400 seconds.

Idle Timeout: Auto-disconnect the IPSec connection after trying several consecutive times.

Image is the second second

Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]
---------------------------	---------	----------	----	-------------------------------

**Ping IP:** Type the IP for ping operation. It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function.

**Interval:** This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

**MTU:** Maximum Transmission Unit, maximum value is 1500.

#### **IPSec for L2TP**

VPN					
▼IPSec					
IPSec Settings					
L2TP over IPSec	Enable				
Connection Name		WAN Interface	Default 💌	IP Version	IPv4 🛩
Remote Security Gateway		Anonyma	us		
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key					
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 💌		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Apply					
LTEN					

**Connection Name:** A given name for the connection, but it should contain no spaces (e.g. "connection-to-office").

**WAN Interface:** Select the set interface for the IPSec tunnel.

Remote Security Gateway: Input the IP of remote security gateway.

Key Exchange Method: Displays key exchange method.

**Pre-Shared Key:** This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

**Encryption Algorithm:** Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ③ 3DES: Stands for Triple Data Encryption Standard, it uses 168 (56\*3) bits as an encryption method.
- ① AES: Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

**Integrity Algorithm:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- **• SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

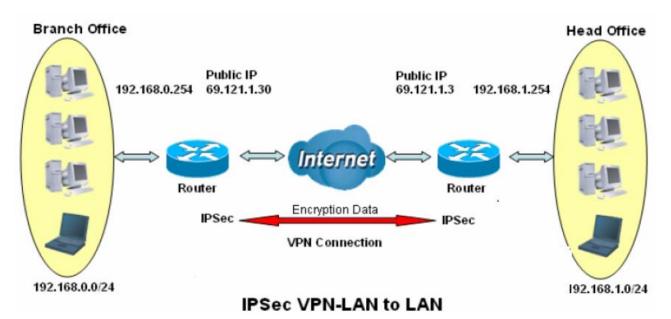
**DH Group:** It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

**IPSec Lifetime:** Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

#### **Examples:**

#### 1. LAN-to-LAN connection

Two BiPAC 8700AX-1600s want to setup a secure IPSec VPN tunnel **Note**: The IPSec Settings shall be consistent between the two routers.



# Head Office Side:

Setup de	talis.	Function	
Item		Function	Description
1	Connection Name	H-to-B	Give a name for IPSec connection
	Local Network		
2	FunctionDescriConnection NameH-to-BGive aLocal NetworkSelectSubnet192.168.1.0IP Address192.168.1.0Netmask255.255.255.0Secure Gateway Address(Hostanme)69.121.1.30Remote NetworkSelectSubnet192.168.0.0IP Address192.168.0.0Netmask255.255.255.0ProposalEsPAuthenticationMD5Encryption3DESPrefer SecurityMODP 1024(group2)	Select Subnet	
Ζ	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3		69.121.1.30	IP address of the Branch office router (on WAN side)
	Remote Network		
	Subnet		Select Subnet
4	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
	Proposal		
	Method	ESP	
	Authentication	MD5	
5	Encryption	3DES	Security Plan
		MODP 1024(group2)	
	Pre-shared Key	123456	

VPN					
▼IPSec					
IPSec Settings					
L2TP over IPSec	Enable				
Connection Name	H-to-B	WAN Interface	Default 😪	IP Version	IPv4 💌
Local Network	Subnet 😪	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	Anony	nous		
Remote Network	Subnet 😽	IP Address	192.168.0.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main 🖌				
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 🗸		
DH Group	MODP1024(DH2) 🗸	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 💌		
DH Group	None 🗸	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD 🐱				
Detection Interval	180 Second(s) [180- 86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				
Apply					

#### Branch Office Side:

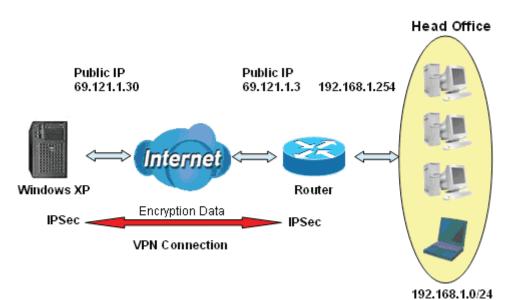
Setup details: the same operation as done in Head Office side

Item		Function	Description	
1	Connection Name	B-to-H	Give a name for IPSec connection	
	Local Network			
2	Subnet		Select Subnet	
2	IP Address	192.168.0.0	Branch Office network	
	Netmask	255.255.255.0		
3	Remote Secure Gateway Address(Hostanme)	69.121.1.3	IP address of the Head office router (on WAN side)	
	Remote Network			
	Subnet		Select Subnet	
4	IP Address	192.168.1.0	Head office network	
	Netmask	255.255.255.0		
	Proposal			
	Method	ESP		
	Authentication	MD5	Security Plan	
5	Encryption	3DES		
	Prefer Forward Security	MODP 1024(group2)		
	Pre-shared Key	123456		

VPN					
▼IPSec					
IPSec Settings					
L2TP over IPSec	Enable				
Connection Name	B-to-H	WAN Interface	Default 💌	IP Version	IPv4 💌
Local Network	Subnet 💌	IP Address	192.168.0.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.3	Anonyi	nous		
Remote Network	Subnet 👻	IP Address	192.168.1.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main 🖌				
Encryption Algorithm	3DES 💽	Integrity Algorithm	MD5 💌		
DH Group	MODP1024(DH2) 🔽	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 🐱		
DH Group	None 🗸 🗸	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD 💌				
Detection Interval	180 Second(s) [180- 86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				

# 1. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



# IPSec VPN-Host to LAN

Item		Function	Description	
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection	
	Local Network			
2	Subnet		Select Subnet	
2	IP Address	192.168.1.0	- Head Office network	
	Netmask	255.255.255.0		
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)	
4	Remote Network			
-	Single Address	69.121.1.30	Host	
	Proposal			
	Method	ESP		
	Authentication	MD5		
5	Encryption	3DES	Security Plan	
	Prefer Forward Security	MODP 1024(group2)		
	Pre-shared Key	123456		

VPN					
▼IPSec					
IP Sec Settings					
L2TP over IPSec	Enable				
Connection Name	Headoffice-to-H	WAN Interface	Default 🗸	IP Version	IPv4 💌
Local Network	Subnet 🖌	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	Anonyi	mous		
Remote Network	Single Address 🐱	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default 🗸	ID Content			
Remote ID Type	Default 😪	ID Content			
Phase 1					
Mode	Main 🖌				
Encryption Algorithm	3DES 👻	Integrity Algorithm	MD5 💌		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES 🗸	Integrity Algorithm	MD5 💌		
DH Group	None 🔽	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD 💌				
Detection Interval	180 Second(s) [180- 86400]	Idle Timeout	5 Consecutive times [5-99]		
мто	1500 (0 : Default)				
Apply					

# **VPN** Account

PPTP L2TP and OpenVPN server share the same account database set in VPN Account page.

VPN			
▼ VPN Account			
VPN Account applied to PP1	TP/L2TP/OpenVPN Server.		
Parameters			
Name		Tunnel	● Enable ○ Disable
Username		Password	
Connection Type		AN	
Peer Network IP		Peer Netmask	
Add Edit / Delete			

Name: A user-defined name for the connection.

**Tunnel**: Select **Enable** to activate the account. PPTP(L2TP/OpenVPN) server is waiting for the client to connect to this account.

**Username**: Please input the username for this account.

**Password**: Please input the password for this account.

**Connection Type**: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

# **Exceptional Rule Group**

Exceptional Rule is dedicated to giving or blocking PPTP/L2TP server access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.

Configuration				
* Exceptional	Rule Group			
Parameters				
Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

# Press Edit to set the exceptional IP (IP Range).

Configuration		
* Exceptional Rule Group		
Parameters		
Group Name	Group1	
Default Action	Allow O Block	
Apply		
Exceptional Rule IP Range		
IP Address Range	~	
Add Edit / Delete		

**Default Action**: Please first set the range to make "**Default Action**" setting available. Set "Allow" to ban the listed IP or IPs to access the PPTP and L2TP server.

Check "Block" to grant access to the listed IP or IPs to the PPTP and L2TP server.

Apply: Press Apply button to apply the change.

# **Exceptional Rule Range**

**IP Address Range:** Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your PPTP and L2TP server, you can add this IP range and valid it.

Configurat	tion			
▼Exception	al Rule Group			
Parameter	s			
Group Nam	ne	Group1		
Default Acti	on			
Apply				
Exceptiona	I Rule IP Range			
IP Address	Range	~		
Add	Edit / Delete			
Edit	Action	IP Address Range	Delete	
0	Block	172.16.1.102 ~ 172.16.1.106		
0	Block	172.16.1.108 ~ 172.16.1.108		

# PPTP

The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2 or EAP-TLS. The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2 or EAP-TLS.

Note: 4 sessions for Client and 4 sessions for Server respectively.

#### **PPTP Server**

In PPTP session, users can set the basaic parameters(authentication, encyption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitutes the PPTP Server setting.

VPN		
▼PPTP Server		
Parameters		
PPTP Function	Enable O Disable	
WAN Interface	Default	
Auth. Type	Pap or Chap 💌	
Encryption Key Length	Auto 😽	
Peer Encryption Mode	Only Stateless	
IP Addresses Assigned to Peer	start from : 192.168.1. 0	
Idle Timeout	0 [0-120] Minute(s)	
Exceptional Rule Group	None 💌	
Apply Cancel		

PPTP Funtion: Select Enable to activate PPTP Server. Disable to deactivate PPTP Server function.

**WAN Interface:** Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

**Auth. Type:** The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

**Encryption Key Length:** The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

**Peer Encryption Mode:** You may select "Only Stateless" or "Allow Stateless and Stateful" mode. The key will be changed every packet when you select Stateless mode.

**IP Addresses Assigned to Peer:** 192.168.1.x: please input the IP assigned range from 1~ 254.

Idle Timeout: Specify the time for remote peer to be disconnected without any activities, from 0~120

minutes.

**Exceptional Rule Group:** Select to grant or block access to a group of IPs to the PPTP server. See <u>Exceptional Rule Group</u>. If there is not any restriction, select none.

Click Apply to submit your PPTP Server basic settings.

#### **PPTP Client**

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.

PPTP Client			
Parameters			
Name		WAN Interface	Default
Username		Password	
Auth. Type	Pap or Chap 💌	PPTP Server Address	
Connection Type	Remote Access     CLAN to LAN	Time to Connect	O Always 💿 Manual
Peer Network IP		Peer Netmask	

Name: user-defined name for identification.

**WAN Interface:** Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

**Auth. Type:** Default is Auto if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

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

**Connection Type**: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Time to Connect: Select Always to keep the connection always on, or Manual to connect manually

any time.

Peer Network IP: Please input the subnet IP for Server peer.

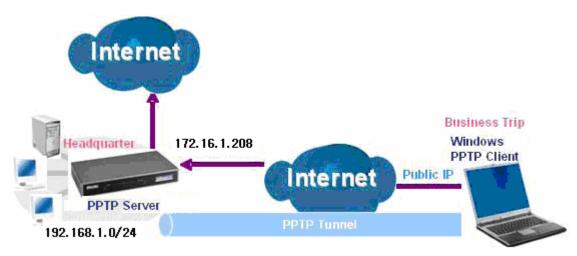
Peer Netmask: Please input the Netmask for server peer.

Click **Add** button to save your changes.

#### Example: PPTP Remote Access with Windows series

# (Note: 1. inside test with 172.16.1.208, just an example for illustration

**2.** Here is a configuration example on Windows 7; Windows series including Windows 10/ 8/ 7 vista/ also supports the application with similar steps. **)** 



Server Side:

## **1. Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

VPN		
▼PPTP Server		
Parameters		
PPTP Function	Enable O Disable	
WAN Interface	Default	
Auth. Type	MS-CHAPv2	
Encryption Key Length	Auto 🗸	
Peer Encryption Mode	Only Stateless	
IP Addresses Assigned to Peer	start from : 192.168.1.00	
Idle Timeout	10 [0-120] Minute(s)	
Exceptional Rule Group	None 💌	
Apply Cancel		

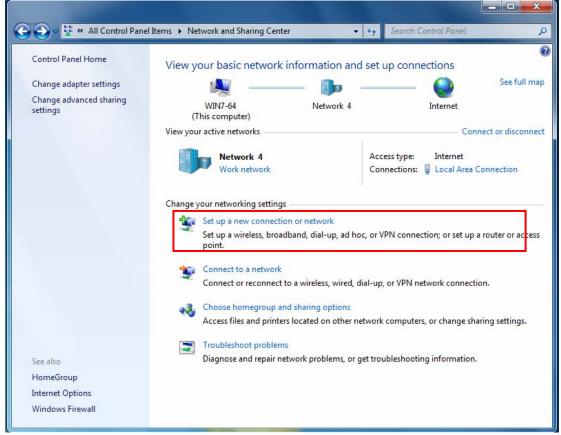
### 2. Create a PPTP Account "test".

VPN						
VPN Acc	ount					
VPN Accou	unt applied to PPTP/L	2TP/OpenVPN Server.				
Paramete	rs					
Name				Tunnel	💿 Enable 🔘 D	isable
Username	•			Password		
Connectio	n Type	Remote Access	CLAN to LAN			
Peer Netw	ork IP			Peer Netmask		
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
0	test	Enable	Remote Access			

#### **Client Side: Windows series**

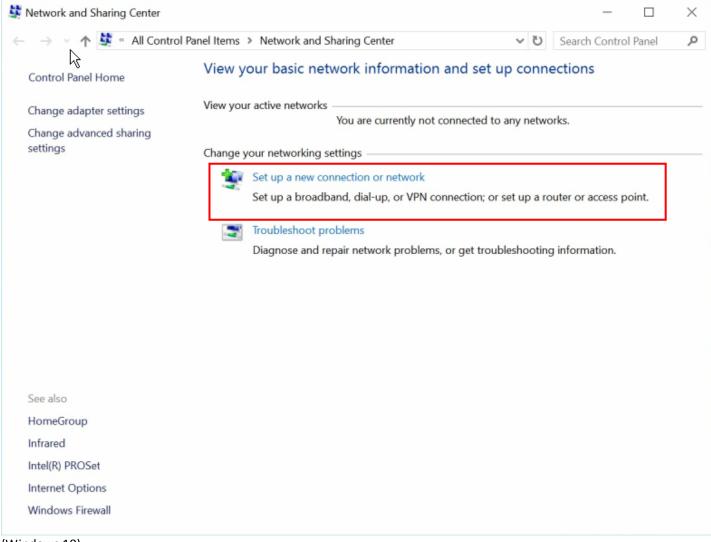
**Note:** Here is a configuration example on Windows 7; Windows series including Windows 10/ vista/ 8/ 7 also supports the application with similar steps.

1. In Windows7, click Start > Control Panel> Network and Sharing Center, Click Set up a new connection network.

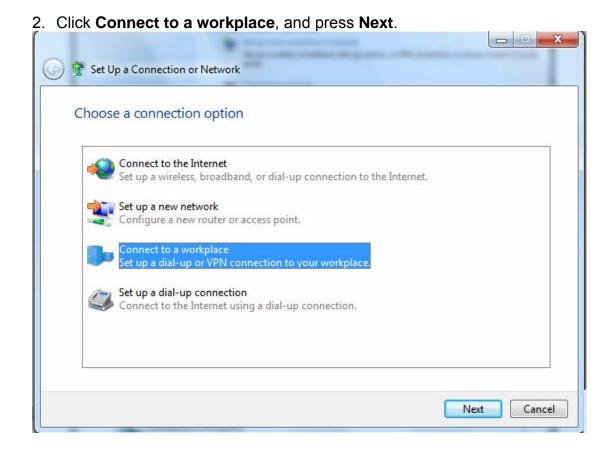




For Windows 10, Users can click **Start > Settings**; or right click the mouse when it points at Windows ICON (**Start**), then click **Control Panel > Network and Sharing Center**, then **Set up a new connection network**.



(Windows 10)



3. Select Use my Internet connection (VPN) and press Next.

🚱 🔚 Connect to a Workplace	X
How do you want to connect?	
Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.	
ių — 🍥 — ip	
Dial directly Connect directly to a phone number without going through the Internet.	
What is a VPN connection?	
	Cancel

4. Input Internet address and Destination name for this connection and press Next.

an give you this address.
Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]
VPN Connection
use this connection /one with access to this computer to use this connection. ist set it up so I can connect later

Connect to a Workpl Type the Internet a	ddress to connect to	
Your network administra	tor can give you this address.	
Internet address:	172.16.1.208	
Destination name:	test	
This option allow	ole to use this connection /s anyone with access to this computer to use this connection. ow; just set it up so I can connect later	
	Next	Cancel

5. Input the account (**user name** and **password**) and press **Create**.

Contract of the local division of the local	-	
🚱 📠 Connect to a Workpla	ace	
Time user and	as and assessment	
Type your user nar	ne and password	
User name:	1	]
Password:		
and the second second	Show characters	4
	Remember this password	-
Domain (optional):		
		Create Cancel
Connect to a Workpla	ace	
Type your user nar	ne and password	
User name:	test	
Password:	••••	
	Remember this password	
Domain (optional):		
		Create Cancel

## 6. Connect to the server.

Connect to a Workplace	
The connection is ready to use	
<b>N</b>	
Connect now	Ĵ
	Close
Connect to a Workplace	
Connecting to test	
i i	
Verifying user name and password	
Sk	ip Cancel

## 7. Successfully connected.

🚱 📠 Connect to a Workplace	
You are connected	
· · · · · · · · · · · · · · · · · · ·	
	Close

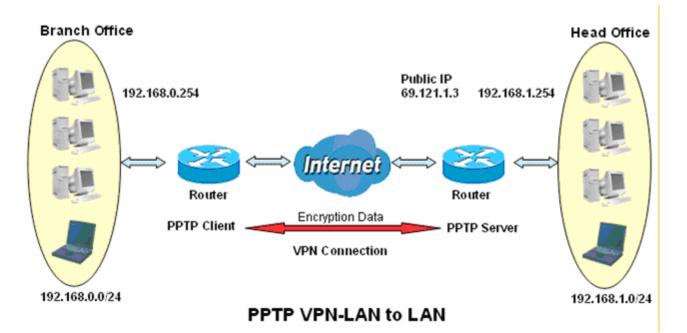
**PS**: You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "Properties" to change the security parameters (if the connection fails, users can go here to change the settings)

Organize	•		\$r • 🗔
20	Local Area Connection	Local Area Connection 2	test
	Network 4	Network cable unplugged	test 2
	Realtek RTL8168C(P)/8111C(P) Fa	Intel(R) PRO/100+ Management	WAN Miniport (PPTP)

test Properties		x
General Options Secu	rity Networking Sharing	
Type of VPN:	Hotworking Sharing	
		-
<u>(</u>		
Data encryption:	Advanced setting	gs
Require encryption (disc	connect if server declines)	-
Authentication		
Ouse Extensible Auth	nentication Protocol (EAP)	
	Properties	ň I.
. All 11 .		
Allow these protoco EAP-MSCHAPv2 w	ill be used for IKEv2 VPN type. Select	
	ols for other VPN types.	
Unencrypted pas	ssword (PAP)	
	shake Authentication Protocol (CHAP)	
	Version 2 (MS-CHAP v2)	
	vuse my Windows logon name and	
	nd domain, if any)	
	OK Canc	el
	OK Cano	
test Status	OK Cano	el X
	OK Cano	
eneral Details		
eneral Details	Value	
eneral Details Property Device Name	Value WAN Miniport (PPTP)	
eneral Details	Value	
Property Device Name Device Type	Value WAN Miniport (PPTP) vpn	
Property Property Device Name Device Type Authentication Encryption Compression	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none)	
Property Device Name Device Type Authentication Encryption Compression PPP multilink framing	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off	
Property Device Name Device Type Authentication Encryption Compression PPP multilink framing Client IPv4 address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100	
Property Device Name Device Type Authentication Encryption Compression PPP multilink framing Client IPv4 address Server IPv4 address	Value Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254	
Details       Property       Device Name       Device Type       Authentication       Encryption       Compression       PPP multilink framing       Client IPv4 address       Server IPv4 address       NAP State	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable	
Details           Property           Device Name           Device Type           Authentication           Encryption           Compression           PPP multilink framing           Client IPv4 address           Server IPv4 address           NAP State           Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
Details       Property       Device Name       Device Type       Authentication       Encryption       Compression       PPP multilink framing       Client IPv4 address       Server IPv4 address       NAP State	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable	
Details         Property         Device Name         Device Type         Authentication         Encryption         Compression         PPP multilink framing         Client IPv4 address         Server IPv4 address         NAP State         Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
Details         Property         Device Name         Device Type         Authentication         Encryption         Compression         PPP multilink framing         Client IPv4 address         Server IPv4 address         NAP State         Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
Details         Property         Device Name         Device Type         Authentication         Encryption         Compression         PPP multilink framing         Client IPv4 address         Server IPv4 address         NAP State         Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
Details           Property           Device Name           Device Type           Authentication           Encryption           Compression           PPP multilink framing           Client IPv4 address           Server IPv4 address           NAP State           Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
Property Property Device Name Device Type Authentication Encryption Compression PPP multilink framing Client IPv4 address Server IPv4 address NAP State Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	
eneral Details  Property  Device Name Device Type Authentication Encryption Compression PPP multilink framing Client IPv4 address Server IPv4 address NAP State Origin address	Value WAN Miniport (PPTP) vpn MS CHAP V2 MPPE 128 (none) Off 192.168.1.100 192.168.1.254 Not NAP-capable (unknown)	

# Example: Configuring a LAN-to-LAN PPTP VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.



## Server side: Head Office

VPN		
▼PPTP Server		
Parameters		
PPTP Function	● Enable ○ Disable	
WAN Interface	Default	
Auth. Type	MS-CHAPv2	
Encryption Key Length	Auto 💌	
Peer Encryption Mode	Only Stateless	
IP Addresses Assigned to Peer	start from : 192.168.1.00	
Idle Timeout	10 [0-120] Minute(s)	
Exceptional Rule Group	None 🗸	
Apply Cancel		

The above is the common setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

## Then the PPTP Account.

VPN						
VPN Acco	ount					
VPN Accou	nt applied to PPTP/I	L2TP/OpenVPN Server.				
Parameter	s					
Name		но		Tunnel	💿 Enable 🔘 Di:	sable
Username		HO		Password	••••	
Connection	п Туре	O Remote Access	LAN to LAN			
Peer Netwo	ork IP	192.168.0.0		Peer Netmask	255.255.255.0	
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
0	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	

#### **Client Side: Branch Office**

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.

POT	D Cline									
	P Clien									
1977	neters			N						
Name	•			BO		WAN Interface		Default	~	
Usern	iame			test		Password		••••		
Auth.	Туре			MS-CHAPv2 🔽		PPTP Server Address	3	69.121.1	.3	
Conne	ection <sup>-</sup>	Гуре		O Remote Access		Time to Connect		O Alway	s 💿 Manual	
Peerl	Vetwor	k IP		192.168.1.0		Peer Netmask		255.255.	255.0	
Add	) <u>E</u>	lit / Delete	ן							
Edit	Ena	Default Gatewa	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Netv	vork IP	Peer Netmask	Delet
0			BO	Manual	69,121,1,3	LAN to LAN	192,168,1	1.0	255.255.255.0	

**Note:** users can see the "Default Gateway" item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

# L2TP

The **Layer 2 Tunneling Protocol** (L2TP) is a Layer2 tunneling protocol for implementing virtual private networks.

L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

In L2TP section, both pure L2TP and L2TP/IPSec are supported. Users can choose your preferable option for your own needs.

Note: 4 sessions for Client and only one for Server respectively.

### L2TP Server

In L2TP session, users can set the bassic parameters(authentication, encyption, peer address, etc) for L2TP Server, and accounts in the page of VPN Account. They both constitutes the complete L2TP Server settings.

VPN		
*L2TP Server		
Parameters		
L2TP	Enable O Disable	
WAN Interface	Default or IPSec Tunnel 💌 IPSec 🕨	
Auth. Type	Pap or Chap 💌	
IP Addresses Assigned to Peer	start from : 192.168.1.0	
Tunnel Authentication		
Secret		
Remote Host Name		
Local Host Name		
Exceptional Rule Group	None 💌	
Apply Cancel		

L2TP: Select Enable to activate L2TP Server. Disable to deactivate L2TP Server.

**WAN Interface:** Select the exact WAN interface configured as source for the tunnel. Select different interfaces, you will decide whether to use L2TP over IPSec or the pure L2TP.

- ① L2TP over IPSec, Select "Default or IPSec Tunnel" only when there is IPSec for L2TP rule in place.
- ① Pure L2TP, Select Default (there is no IPSec for L2TP in place) or other interface to activate the pure L2TP.

**Auth. Type:** The authentication type, Pap or Chap, PaP, Chap. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

**IP Addresses Assigned to Peer:** 192.168.1.x: please input the IP assigned range from 1~254.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication. Enable it if needed

and set the same in the client side.

**Secret:** Enter the secretly pre-shared password for tunnel authentication.

**Remote Host Name:** Enter the remote host name (of peer) featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

**Exceptional Rule Group:** Select to grant or block access to a group of IPs to the L2TP server. See <u>Exceptional Rule Group</u>. If there is not any restriction, select none.

Click **Apply** to submit your L2TP Server basic settings.

# **L2TP Client**

L2TP client can help you dial-in the L2TP server to establish L2TP tunnel over Internet.

VPN			
►L2TP Client			
Parameters			
Name		L2TP over IPSec	Enable
WAN Interface	Default 💽		
Username		Password	
Auth. Type	Pap or Chap 💌	L2TP Server Address	
Connection Type		AN	
Peer Network IP		Peer Netmask	
Tunnel Authentication		Secret	
Remote Host Name		Local Host Name	

Name: user-defined name for identification.

**L2TP over IPSec:** If your L2TP server has used L2TP over IPSec feature, please enable this item. under this circumstance, client and server communicate using L2TP over IPSec.

#### i) Enable

*L2TP Client			
Parameters			
Name		L2TP over IPSec	Enable
IPSec Tunnel	test2 💉 IPSec 🕨		
Username		Password	
Auth. Type	Pap or Chap 🐱	L2TP Server Address	
Connection Type	Remote Access     O LAN to I	LAN	
Peer Network IP		Peer Netmask	
Tunnel Authentication		Secret	
Remote Host Name		Local Host Name	

**IPSec Tunnel:** Select the appropriate IPSec for L2TP rule configured for the L2TP Client.

Username: Enter the username provided by your L2TP Server.

**Password:** Enter the password provided by your L2TP Server.

**Auth. Type:** Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

**L2TP Server Address:** Enter the IP address of the L2TP server.

**Connection Type**: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for Server.

**Tunnel Authentication:** Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

L2TP Client					
Parameters					
Name			L2TP over IPSec	Enable	
WAN Interface	Default	*			
Usemame			Password		
Auth. Type	Pap or Chap 💌		L2TP Server Address		
Connection Type	Remote Access	O LAN to LAN			
Peer Network IP			Peer Netmask		
Tunnel Authentication			Secret		
Remote Host Name			Local Host Name		

#### i) Disable

**WAN Interface:** Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel. Under this circumstance, client and server communicate through pure L2TP server.

Username: Enter the username provided by your L2TP Server.

**Password:** Enter the password provided by your L2TP Server.

**Auth. Type:** Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

L2TP Server Address: Enter the IP address of the L2TP server.

**Connection Type**: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

**Peer Netmask**: Please input the Netmask for server.

**Tunnel Authentication:** Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

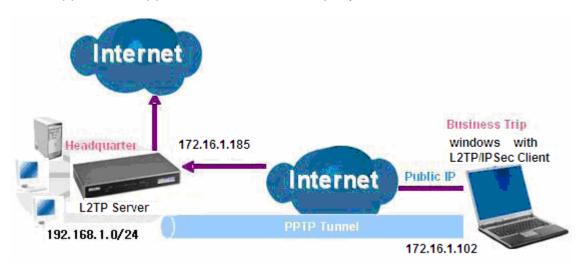
Secret: Enter the set secret password in the server side.

**Remote Host Name:** Enter the remote host name featuring the destination of the L2TP tunnel. **Local Host Name:** Enter the local host name featuring the source of the L2TP tunnel. Click **Add** button to save your changes.

#### Example: L2TP over IPSec Remote Access with Windows series

# (Note: 1. inside test with 172.16.1.185, just an example for illustration

**2.** Here is a configuration example on Windows 7; Windows series including Windows 10/ 8/ 7 vista/ also supports the application with similar steps. **)** 



Server Side:

## **1. Configuration > VPN > L2TP** and Enable the L2TP function, Click **Apply**.

VPN		
▼L2TP Server		
Parameters		
L2TP	Enable Obisable	
WAN Interface	Default or IPSec Tunnel 💙 IPSec 🕨	
Auth. Type	Chap 💌	
IP Addresses Assigned to Peer	start from : 192.168.1.10	
Tunnel Authentication		
Secret		
Remote Host Name		
Local Host Name		
Exceptional Rule Group	None 💌	
Apply Cancel		

## The IPSec for L2TP rule

VPN					
▼IPSec					
IP Sec Settings					
L2TP over IPSec	🗹 Enable				
Connection Name		WAN Interface	Default 💌	IP Version	IPv4 😒
Remote Security Gateway		Anonymo	us		
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Apply					

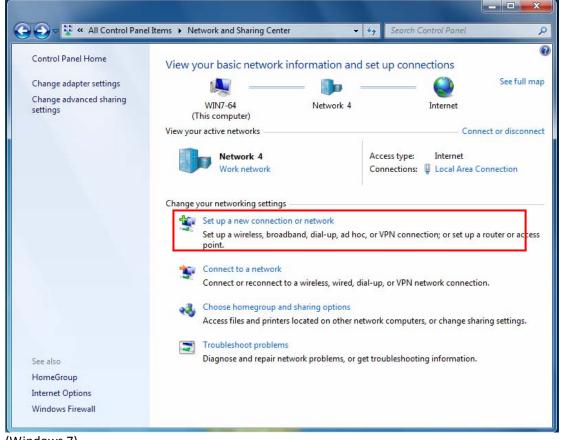
## 2. Create a L2TP Account "test1".

VPN						
VPN Acc	ount					
VPN Accou	unt applied to PPTP/L	2TP/OpenVPN Server.				
Paramete	rs					
Name		test1		Tunnel	💿 Enable 🛛 D	isable
Username	e	test1		Password	••••	
Connectio	n Type	Remote Access	CLAN to LAN			
Peer Netw	ork IP			Peer Netmask		
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
۲	test1	Enable	Remote Access			

#### **Client Side: Windows series**

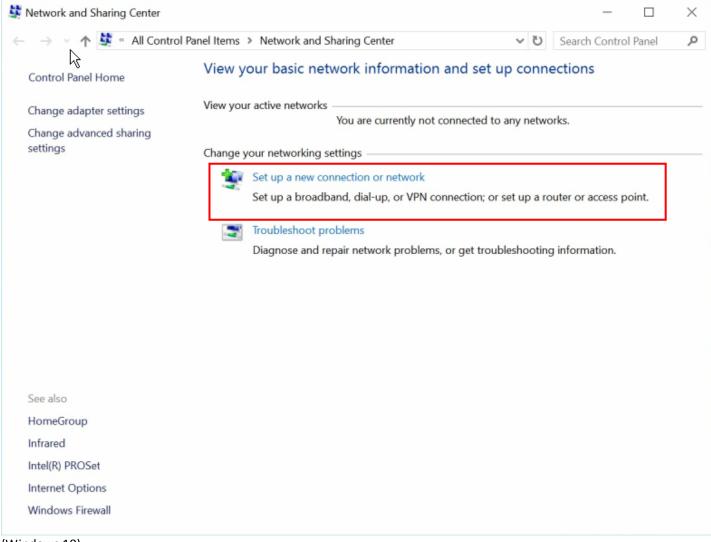
**Note:** Here is a configuration example on Windows 7; Windows series including Windows 10/ vista/ 8/ 7 also supports the application with similar steps.

1. In Windows7, click Start > Control Panel> Network and Sharing Center, Click Set up a new connection network.





For Windows 10, Users can click **Start > Settings**; or right click the mouse when it points at Windows ICON (**Start**), then click **Control Panel > Network and Sharing Center**, then **Set up a new connection network**.



(Windows 10)

# 2. Click **Connect to a workplace**, and press **Next**.

42	Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.	
2	Set up a new network Configure a new router or access point.	
•	Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
9	Set up a dial-up connection Connect to the Internet using a dial-up connection.	

3. Select Use my Internet connection (VPN) and press Next.

Connect to a Workplace	
How do you want to connect?	
<ul> <li>Use my Internet connection (VPN)</li> <li>Connect using a virtual private network (VPN) connection through the Internet</li> </ul>	t.
ing ing ing ing ing ing	
Dial directly Connect directly to a phone number without going through the Internet.	
in the second se	
What is a VPN connection?	
	Cancel

4. Input Internet address and Destination name for this connection and press Next.

Connect to a Workpl	lace
Type the Internet a	address to connect to
Your network administra	ator can give you this address.
Internet address:	[Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]
Destination name:	VPN Connection
This option allow	I ple to use this connection ws anyone with access to this computer to use this connection. ww; just set it up so I can connect later
	Next Cancel
Type the Internet a	ace address to connect to
Your network administra	ator can give you this address.
Internet address:	172.16.1.185
D <u>e</u> stination name:	L2TP_IPSec
This option allow	l ple to use this connection ws anyone with access to this computer to use this connection. ow; just set it up so I can connect later

5. Input the account (**user name** and **password**) and press **Create**.

🔒 🔚 Connect to a Workp	lace	
Type your user na	me and password	
	1	
User name:		
Password:		
	Show characters	
	Remember this password	
Domain (optional):		
		Create Cancel
the second state		- 0 X
Connectito e Worked		
Connect to a Workpl	lace	
Connect to a Workpl		
The second second second		
Type your user nar User name:	me and password	
Type your user nar	me and password test1 •••••	
Type your user nar User name:	me and password test1	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	
Type your user nar User name:	me and password test1 ••••• Show characters	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	
Type your user nar User name: Password:	me and password test1 ••••• Show characters	Create

## 6. Connection created. Press Close.

a man a filing a start	
Connect to a Workplace	
The connection is ready to use	
<b>N</b>	
Connect now	
	Close

7. Go to **Network Connections** shown below to check the detail of the connection. Right click "L2TP\_IPSec" icon, and select "**Properties**" to change the security parameters.



8. Chang the type of VPN to "Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)" and Click Advanced Settings to set the pre-shared (set in IPSec) key for authentication.

L2TP_IPSec Properties	×
General Options Security Networking Sharing	
Type of VPN:	
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)	
Advanced	settings
Data encryption:	
Require encryption (disconnect if server declines)	<b>•</b>
Authentication	
Use Extensible Authentication Protocol (EAP)	
	<b></b>
Prop	erties
Allow these protocols	
Unencrypted password (PAP)	
Challenge Handshake Authentication Protocol (CF	HAP)
Microsoft CHAP Version 2 (MS-CHAP v2)	
Automatically use my Windows logon name an	d
password (and domain, if any)	
ОК	Cancel
Advanced Properties	×
L2TP	
Use preshared key for authentication	
Key: 123456	
Use certificate for authentication	
Verify the Name and Usage attributes of the serve	er's certificate
ОК	Cancel

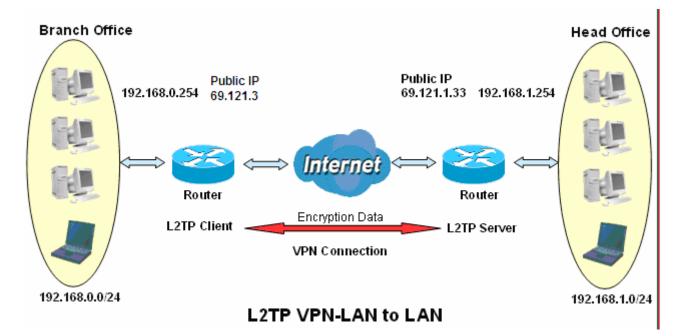
9. Go to **Network connections**, enter username and password to connect L2TP\_IPSec and check the connection status.

	PSec	
User name: te:	st1	
Password:	••••	
Domain:		
Me only	ame and password for the following users:	
L2TP_IPSec State	us	x
General Details		
Property Device Name	Value WAN Miniport (L2TP) vpn	
Device Type Authentication Encryption Compression PPP multilink frar Client IPv4 addr Server IPv4 add NAP State Network Adapte Origin address Destination addr	CHAP IPsec: AES 128 (none) ming Off ress 192.168.1.10 fress 192.168.1.254 Not NAP-capable er Used Wireless Network Connection 172.16.1.102	
Authentication Encryption Compression PPP multilink fran Client IPv4 addr Server IPv4 add NAP State Network Adapte Origin address	CHAP IPsec: AES 128 (none) ming Off ress 192.168.1.10 fress 192.168.1.254 Not NAP-capable er Used Wireless Network Connection 172.16.1.102	

## Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



## Server side: Head Office

VPN					
▼L2TP Server					
Parameters					
L2TP		●Enable C	Disable		
WAN Interface		Default or IPS	ecTunnel 💌 IPSec 🕨		
Auth. Type		Chap	~		
IP Addresses Assigned to Peer		start from : 192	.168.1.10		
Tunnel Authentication					
Secret					
Remote Host Name					
Local Host Name					
Exceptional Rule Group		None 🔽			
Apply Cancel					
VPN					
▼IPSec					
IPSec Settings					
L2TP over IPSec	Enable				
Connection Name	test2	WAN Interface	Default 🗸	IP Version	IPv4 🐱
Remote Security Gateway	69.121.1.3	Anonymo	us		
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Encryption Algorithm	3DES 💌	Integrity Algorithm	MD5 💌		
DH Group	MODP1024(DH2)	IPSec Lifetime	60 Minute(s) [60-1440]		
Apply					

Tunnel M	Tunnel Mode Connections							
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit	
	$\checkmark$	test1			Anonymous		Edit	
	$\checkmark$	test2			69.121.1.3		Edit	

The above is the commonly setting for L2TP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

# Then account the L2TP Account.

VPN						
VPN Acco	ount					
VPN Accou	int applied to PPTP/L	2TP/OpenVPN Server.				
Parameter	s					
Name		НО		Tunnel	💿 Enable 🔘 Di	sable
Username		test2		Password		
Connectior	n Type	O Remote Access	● LAN to LAN			
Peer Netwo	ork IP	192.168.0.0		Peer Netmask	255.255.255.0	
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
0	но	Enable	LAN to LAN	192.168.0.0	255.255.255.0	

#### **Client Side: Branch Office**

The client user can set up a tunnel connecting to the L2TP server, and can also set the tunnel as the default route for all outgoing traffic.

VPN							
▼L2TP Client							
Parameters							
Name	BO			L2TP ov	er IPSec	🗹 Enable	
IPSec Tunnel	test2	IPSec >					
Username	test2			Password		••••	
Auth. Type	Chap 🖌			L2TP Server Address		69.121.1.33	
Connection Type	OR	emote Access 💿 LAN to	LAN				
Peer Network IP	192.1	168.1.0		Peer Netmask		255.255.255.0	
Tunnel Authentication				Secret			
Remote Host Name			Local Host Name				
Add Edit / Delete							
Edit Enable Default Gateway Na	ne	L2TP Server Address	Connection T	ype	Peer Network IP	Peer Netmask	Delete
⊙ □ □ во		69.121.1.33	LAN to LAN		192.168.1.0	255.255.255.0	

**Note:** users can see the "Default Gateway" item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

# **OpenVPN**

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN is good at portability. OpenVPN has been ported and embedded to several systems.

#### **OpenVPN Server**

Users can set the bassic parameters(source/destination address, protocl/port, authentication, encyption, etc) for OpenVPN Server.

VPN		
▼ OpenVPN Server		
Parameters		
OpenVPN Server	O Enable 💿 Disable	
WAN Interface	Default	
Protocol	TCP 🗸	
Port Number	1194	
Tunnel Virtual Subnet		
Tunnel Netmask		
Cipher Encryption	BF-CBC	
HMAC Authentication	SHA1 🗸	
Izo Compression	Enable	
Apply Cancel		

**OpenVPN Server:** Select **Enable** to activate OpenVPN Server.

**WAN Interface:** Select the exact WAN interface configured as source for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

**Protocol:** OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports. Select the protocol.

**Port Number:** Port 1194 is the official assigned port number for OpenVPN

Tunnel Virtual Subnet: Set the tunnel virtual subnet IP for OpenVPN server.

Tunnel Network: Set the tunnel virtual subnet mask.

**Cipher Encryption:** OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select the encryption method.

**HMAC Authentication:** OpenVPN support <u>HMAC</u> authentication, please select authentication item from the list.

**Izo Compression:** Enable to use the LZO compression library to compress the data stream.

Click **Apply** to submit your OpenVPN Server basic settings.

## **OpenVPN CA**

OpenVPN offers pre-shared keys, certificate-based, and username/password-based authentication, with certificate-based being the most robust. Generally, the part offers the billion factory-defined authentication certificate.

VPN		
• OpenVPN CA		
Certificate	BEGIN CERTIFICATE MIIEMTCCA5qgAwlBAgIJAM2cArpOnGiSMA0GCSqGSlb3DQEBBQ VAMIHCMQswCQYD VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHE wdlc2luY2h1MSMwlQYD VQQKExpCaWxsaW9uIEVsZWN0cmljlENvLiwgTHRkLjEjMCEGA1U ECxMaQmlsbGlv biBFbGVjdHJpYyBDby4sIEx0ZC4xJjAkBgNVBAMTHUJpbGxpb24gR WxlY3RyaWMg Q28uLCBMdGQuIENBMR4wHAYJKoZlhvcNAQkBFg93d3cuYmlsbGl vbi5jb20wHhcN MTMwNTE2MDYxMjU2WhcNMjMwNTE0MDYxMjU2WjCBwjELMAk GA1UEBhMCVFcxDzAN BgNVBAgTBIRhaXdhbjEQMA4GA1UEBxMHSHNpbmNodTEjMCEG A1UEChMaQmlsbGlv biBFbGVjdHJpYyBDby4sIEx0ZC4xIzAhBgNVBAsTGkJpbGxpb24gR WxlY3RyaWMg Q28uLCBMdGQuMSYwJAYDVQQDEx1CaWxsaW9uIEVsZWN0cmljI ENvLiwgTHRkLiBD QTEeMBwGCSqGSlb3DQEJARYPd3d3LmJpbGxpb24uY29tMIGfMA 0GCSqGSlb3DQEB AQUAA4GNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fLf8h83M2Vc w1K51tr3UuIG ayNhDdhQAzTTifnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQUKKup vOvr0nUBt0	
Recipient's E-mail	(Must be xxx@yyy.zzz) Apply	
Export client.ovpn file	Export	

**Recipient's Email:** Set the recipient's email address to send the trusted CA to the OpenVPN client. OpenVPN server and client need matched certificate to establish trusted VPN tunnel, on client side, please import this certificate in <u>Trusted CA</u>.

Advanc	ed Setup	
▼Trusted	ICA	
Trusted	CA (Certificate Authority) Certificates	
Maximun	n certificates can be stored: 8	
Name	Subject	Type Action
CA-billio	C=TW/ST=Taiwan/L=Hsinchu/O=Billion Electric Co., Ltd./OU=Billion Electric Co., Ltd./CN=Billion Electric Co., Ltd. CA/emailAddress=www.billion.com	ca View Remove
Impor	t Certificate	

(Client side CA)

# **OpenVPN Client**

OpenVPN client can help you dial-in the OpenVPN server to establish a trusted OpenVPN tunnel over Internet.

VPN			
▼ OpenVPN Client			
Parameters			
Name		WAN Interface	Default
Username		Password	
OpenVPN Server Address			
Protocol	TCP 💌	Port Number	1194
Cipher Encryption	BF-CBC	HMAC Authentication	SHA1
Izo Compression	Enable	Certificate Authority	CA-billion V Trusted CA •
Add Edit / Delete			

Name: user-defined name for identification.

**WAN Interface:** Select the exact WAN interface configured as source for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

**Username:** Enter the username provided by your OpenVPN Server.

Password: Enter the password provided by your OpenVPN Server.

**OpenVPN Server Address:** Enter the WAN IP address of the OpenVPN server.

**Protocol**: The protocol, same as set in server side.

Port Number: 1194.

**Cipher Encryption:** Be consistent with what set on server side.

HMAC Authentication: Be consistent with what set on server side.

Izo Compression: Enable to use the LZO compression library to compress the data stream

**Certificate Authority:** Select your trusted CA from your server side to establish the trusted VPN tunnel with server.

Click Add button to save your changes.

#### How to establish OpenVPN tunnel

#### 1. Remote Access OpenVPN

(If the client wants to remotely access the OpenVPN Server, on client side, users had better install an OpenVPN client application/installer and connect to server accordingly. Here only give the configuration on server side.)

#### Server side on router

1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.

VPN		
▼ OpenVPN Server		
Parameters		
OpenVPN Server	Enable     O Disable	
WAN Interface	Default	
Protocol	TCP 💌	
Port Number	1194	
Tunnel Virtual Subnet	192.168.2.0	
Tunnel Netmask	255.255.255.0	
Cipher Encryption	BF-CBC	
HMAC Authentication	SHA1	
Izo Compression	Enable	
Apply Cancel		

2. Create an account for the OpenVPN tunnel for client to connect in.

VPN						
VPN Acco	ount					
VPN Accou	nt applied to PPTP/L	2TP/OpenVPN Server.				
P <mark>aramete</mark> r	s					
Name		test4		Tunnel	⊙ Enable O Dis	able
Jsername		tes4		Password	••••	
Connection	Туре	Remote Access	C LAN to LAN			
eer Netwo	ork IP			Peer Netmask		
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
•	test4	Enable	Remote Access			

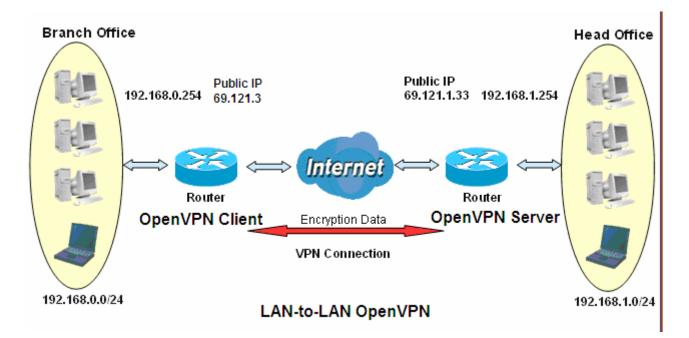
3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

CA	
BEGIN CERTIFICATE MIIEMTCCA5qgAwlBAgIJAM2cArpOnGiSMA0GCSqGSlb3DQEBBQUAMI HCMQswCQYD VQQGEwJUVZEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHEwdlc 2luY2h1MSMwlQYD VQQKExpCaWxsaW9ulEVsZWN0cmljIENvLiwgTHRkLjEjMCEGA1UECXM aQmlsbGlv biBFbGVjdHJpYyBDby4sIEx0ZC4xJjAkBgNVBAMTHUJpbGxpb24gRWxlY 3RyaWMg Q28uLCBMdGQuIENBMR4wHAYJKoZlhvcNAQkBFg93d3cuYmlsbGlvbl5j b20wHhcN MTMwNTE2MDYxMjU2WhcNMjMwNTE0MDYxMjU2WjCBwjELMAkGA1U EBhMCVFcxDzAN BgNVBAgTBIRhaXdhbjEQMA4GA1UEBxMHSHNpbmNodTEjMCEGA1UE ChMaQmlsbGiv biBFbGVjdHJpYyBDby4sIEx0ZC4xIzAhBgNVBAsTGkJpbGxpb24gRWxlY 3RyaWMg Q28uLCBMdGQuMSYwJAYDVQQDEx1CaWxsaW9uIEVsZWN0cmljIENv LiwgTHRkLIBD QTEeMBwGCSqGSlb3DQEJARYPd3d3LmJpbGxpb24uY29tMIGfMA0G CSqGSlb3DQEB AQUAA4GNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fLf8h83M2Vcw1K 51tr3UuIG ayNhDdhQAzTTifnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQUKKupvOv r0nUBt0 QByv42KrPv5b9rOaLL3Qko5yoSSaSK/vA6OtuFX4jbrz	Y Sj E Y

### 2. LAN-to-LAN OpenVPN

The branch office establishes a OpenVPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly. Configured in this way, head office and branch office can access each other.

**Note:** Both office LAN networks must be in different subnets with the LAN-to-LAN application.



## Server side: Head Office

1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.

VPN		
▼ OpenVPN Server		
Parameters		
OpenVPN Server	Enable     Disable	
WAN Interface	Default	
Protocol	TCP 💌	
Port Number	1194	
Tunnel Virtual Subnet	192.168.2.0	
Tunnel Netmask	255.255.255.0	
Cipher Encryption	BF-CBC	
HMAC Authentication	SHA1	
Izo Compression	Enable	
Apply Cancel		

2. Create an account for client to connect in

VPN						
VPN Acco	ount					
VPN Accou	int applied to PPTP/L	2TP/OpenVPN Server.				
Parameter	rs					
Name		test3		Tunnel	💿 Enable 🛛 Dis	able
Username		test3		Password	••••	
Connection	п Туре	O Remote Access	LAN to LAN			
Peer Netw	ork IP	192.168.0.0		Peer Netmask	255.255.255.0	
Add	Edit / Delete					
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
•	test3	Enable	LAN to LAN	192.168.0.0	255.255.255.0	

3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

▼OpenVPN CA		
Certificate	<ul> <li>RFGIN CFRTIFICATF MIIEMTCCA5qgAwIBAgIJAM2cArpOnGiSMA0GCSqGSIb3DQEBBQ</li> <li>VQQGEwJUVZEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHE wdlc2luY2h1MSMwIQYD</li> <li>VQQKExpCaWxsaW9uIEVsZWN0cmljIENvLiwgTHRkLjEjMCEGA1U ECxMaQmlsbGlv</li> <li>biBFbGVjdHJpYyBDby4sIEx0ZC4xJjAkBgNVBAMTHUJpbGxpb24gR</li> <li>WXY3RyaWMg</li> <li>Q28uLCBMdGQuIENBMR4wHAYJKoZIhvcNAQkBFg93d3cuYmlsbGl</li> <li>vbi5jb20wHhcN</li> <li>MTMwNTE2MDYxMjU2WhcNMjMwNTE0MDYxMjU2WjCBwjELMAk</li> <li>GA1UEBhMCVFcxDzAN</li> <li>BgNVBAgTBIRhaXdhbjEQMA4GA1UEBxMHSHNpbmNodTEJMCEG</li> <li>A1UEChMaQmlsbGiv</li> <li>biBFbGVjdHJpYyBDby4sIFx0ZC4xlzAhBgNVBASTGk.lpbGxpb24gR</li> <li>WXY3RyaWMg</li> <li>Q28uLCBMdGQuMSYwJAYDVQQDEx1CaWxsaW9uIEVsZWN0cmljI</li> <li>ENvLiwgTHRkLiBD</li> <li>QTEeMBwGCSqGSlb3DQEJARYPd3d3LmJpbGxpb24uY29tMIGfMA</li> <li>0GCSqGSlb3DQEB</li> <li>AQUAA4GNADCBIcKBgQC7V43lcYxwylv8vWI+58nq3fLf8h83M2Vc</li> <li>w1K5ttr3UuIG</li> <li>ayNhDdhQAzTTifnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQUKKup</li> </ul>	
Recipient's E-mail	gangel@gmail.com (Must be xxx@yyy.zzz) Apply	
Export client.ovpn file	Export	

#### **Client Side: Branch Office**

1. Import your trusted certificate from server side, which is used to authenticate between client and server for establishing trusted OpenVPN tunnel.

Trusted CA Import CA	certificate	
Parameters		
Name	CA-billion	
Certificate	BEGIN CERTIFICATE MIIEMTCCA5qgAwlBAgIJAM2cArpOnGiSMA0GCSqGSlb3DQE BBQUAMIHCMQswCQYD VQQGEwJUV2EPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQ QHEwdlc2luY2h1MSMwlQYD VQQKExpCaWxsaW9uIEVsZWN0cmljIENvLiwgTHRkLjEJMCEG A1UECxMaQmlsbGlv biBFbGVjdHJpYyBDby4sIEx0ZC4xJjAkBgNVBAMTHUJpbGxpb 24gRWxIY3RyaWMg Q28uLCBMdGQuIENBMR4wHAYJKoZIhvcNAQkBFg93d3cuYm IsbGlvbi5jb20wHhcN MTMwNTE2MDYxMjU2WhcNMjMwNTE0MDYxMjU2WjCBwjELM AkGA1UEBhMCVFcxDZAN BgNVBAgTBIRhaXdhbjEQMA4GA1UEBxMHSHNpbmNodTEjM CEGA1UEChMaQmlsbGlv biBFbGVjdHJpYyBDby4sIEx0ZC4xIZAhBgNVBAsTGkJpbGxpb2 4gRWxIY3RyaWMg Q28uLCBMdGQUMSYwJAYDVQQDEx1CaWxsaW9uIEVsZWN 0cmljIENvLiwgTHRkLiBD QTEeMBwGCSqGSlb3DQEJARYPd3d3LmJpbGxpb24uY29tMI GfMA0GCSqGSlb3DQEB AQUAA4GNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fLf8h83 M2Vcw1K51tr3UuIG ayNhDdhQAzTTifnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQU KKupvOvrOnUBt0 QByy42KrPv5b9rOaLL3Qko5yoSSaSK/yA6OtuFX4jbrz	

2. On the OpenVPN client side, fill in the parameters the same as set for OpenVPN server.

VPN					
▼ OpenVPN Client					
Parameters					
Name	test3		WAN Interface	Default	~
Username	test3		Password	••••	
OpenVPN Server Address	69.121.1.33				
Protocol	TCP 💌		Port Number	1194	
Cipher Encryption	BF-CBC		HMAC Authentication	SHA1 💌	
Izo Compression	Enable		Certificate Authority	CA-billion 💌 Tru:	sted CA ►
▼OpenVPN Client					
Parameters					
Name			WAN Interface	Default	~
Username			Password		
OpenVPN Server Address					
Protocol	TCP 💌		Port Number	1194	
Cipher Encryption	BF-CBC	•	HMAC Authentication	SHA1 💌	
Izo Compression	Enable		Certificate Authority	CA-billion 💌 Tru	isted CA F
Add Edit / Delete					
Edit Enable Name	WAN Interface	OpenVPN Server	Address Protocol	Port Number	Delete
O ☑ test3	default	69.121.1.33	TCP	1194	

**Note:** users can see the "Default Gateway" item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

## GRE

**Generic Routing Encapsulation** (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an Internet Protocol (IP) network. And the common use can be GRE over IPSec.

Note: up to 8 tunnels can be added, but only 4 can be activated.

GRE					
Parameters					
Name		WAN Interface	Default	*	
Local Tunnel Virtual IP		Local Netmask			
Remote Tunnel Virtual IP		Remote Gateway IP			
Remote Network	Single Address 💌	IP Address		Netmask	
Enable Keepalive		Keepalive Retry Times	10	Keepalive Interval	3 Second(s)

Name: User-defined identification.

**WAN Interface:** Select the exact WAN interface configured for the tunnel as the source tunnel IP. Select Default to use the now-working WAN interface for the tunnel.

Local Tunnel Virtual IP: Please input the virtual IP for the local tunnel.

Local Netmask: Input the netmask for the local tunnel.

Remote Tunnel Virtual IP: Please input the virtual destination IP for tunnel.

Remote Gateway IP: Set the destination IP for the tunnel.

Remote Network: Select the peer topology, Single address (client) or Subnet.

**IP Address:** Set the IP address if the peer is a client. If the peer is a subnet, please enter the IP and netmask.

**Enable Keepalive:** Normally, the tunnel interface is always up. Enable keepalive to determine when the tunnel interface is to be closed. The local router sends keepalive packets to the peer router, if keepalive response is not received from peer router within the allowed time ('retry time' multiply 'interval', based on default settings, the time interval can be 30 seconds), the local router will shut up its tunnel interface.

Keepalive Retry Times: Set the keepalive retry times, default is 10.

Keepalive Interval: Set the keepalive Interval, unit in seconds. Default is 3 seconds.

# **Advanced Setup**

There are sub-items within the System section: **Routing**, **DNS**, **Static ARP**, **UPnP**, **Certificate**, **Multicast**, **Management**, and **Diagnostics**.

Quick Start
Configuration
Advanced Setup
Routing
▶ DNS
<ul> <li>Static ARP</li> </ul>
• UPnP
Certificate
<ul> <li>Multicast</li> </ul>
Management
Diagnostics

252

## Routing

### **Default Gateway**

Advanced Setup			
r Default Gateway			
)efault Gateway Interface List			
Only one default gateway interface will be used according	to the priority with the first being	the highest and the last one the lowest priority if	the WAN interface is connected.
Selected Default Gateway Interfaces		Available Routed WAN Interfaces	
ppp0.1	*	eth4.1 USB3G0	×.
Preferred WAN Interface As The System Default IPv6 G	ateway		
Selected WAN Interface	pppoe_(	_8_35/ppp0.1 🐱	
Apply Cancel			

WAN port: Select the port this gateway applies to.

To set **Default Gateway** and **Available Routed WAN Interface**. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via or . And select a Default IPv6 Gateway from the drop-down menu.

**Note:** Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

#### **Static Route**

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.

Advanced Setup					
▼ Static Route					
Parameters					
IP Version	Dst IP / Prefix Length	Gateway	Interface	Metric	Remove
Add Remo	ve				

Above is the static route listing table, click Add to create static routing.

Advanced Setup		
▼ Static Route		
Parameters		
IP Version	IPv4 💌	
Destination IP Address / Prefix Length		
Interface	×	
Gateway IP Address		
Metric	[greater than or equal to zero]	
Apply Cancel		

IP Version: Select the IP version, IPv4 or IPv6.

**Destination IP Address / Prefix Length:** Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0/64, the prefix is 3FFE:FFFF:0:CD3.

Interface: The exit interface of local router to the next hop.

Gateway IP Address: Enter the gateway IP address/ the entry address of the next hop, .

**Metric:** Metric is the hops from local to destination, which signals the quality of the link, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.

Static Route					
Parameters					
IP Version	Dst IP/Prefix Length	Gateway	Interface	Metric	Remove
4	192.168.1.0/24		ppp0	1	

### **Policy Routing**

Here users can set a route for the host (source IP) in a LAN to access outside through a specified a WAN interface to the next hop.

The following is the policy Routing listing table.

Advanced Setup					
▼ Policy Routing					
Parameters					
Policy Name	Source IP	LAN Port	WAN	Default Gateway	Remove
Add Remove					

#### Click Add to create a policy route.

Advanced Setup		
▼ Policy Routing		
Parameters		
Policy Name		
Physical LAN Port	×	
Source IP		
Interface	pppoe_0_0_35/ppp0.1 💌	
Default Gateway		
Apply Cancel		

Policy Name: User-defined name.

Physical LAN Port: Select the LAN port.

**Source IP:** Enter the Host Source IP.

Interface: Select the WAN interface (exit interface) of local router to the next hop.

Default Gateway: Enter the gateway IP address/ the entry address of the next hop,

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press **Remove** to delete it.

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.

Advanced Setup			
▼ RIP			
Parameters			
RIP CANNOT BE CON	FIGURED on the WAN interface which has N	AT enabled (such as PPPoE).	
Interface	Version	Operation	Enable
atm0.2	2 💌	Passive 💌	
Apply Cancel	ן		

Interface: The interface the rule applies to.

Version: Select the RIP version, RIP-1, RIP-2 and both.

Operation: RIP has two operation mode.

- Passive: only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- ① Active: working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

**Enable:** check the checkbox to enable RIP rule for the interface.

**Note:** RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

Click **Apply** to apply your settings.

## DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

#### DNS

▼DNS			
In ATM mode, if only a single PVC with IPoA or static IPoE prot	R enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider for the system. tocol is configured, Static DNS server IP addresses must be entered. The as system dns servers but only one will be used according to the priority with the first being the higest and the m back in again.		
Select DNS Server Interface from available WAN interface	S		
Selected DNS Server Interfaces	Available WAN Interfaces		
ppp0.1 USB3G0			
O Use the following Static DNS IP address			
Primary DNS server			
Secondary DNS server			
O Use the IP Addresses provided by Parental Control Provid	ter		
Note that selecting a WAN interface for IPv6 DNS server will e	nable DHCPv6 Client on that interface.		
Obtain IPv6 DNS info from a WAN interface			
/AN Interface selected pppoe_0_8_35/ppp0.1 v			
O Use the following Static IPv6 DNS address			
imary IPv6 DNS server			
Secondary IPv6 DNS server			
Apply Cancel			

#### > IPv4

#### Three ways to set an IPv4 DNS server

- ③ Select DNS server from available WAN interfaces: Select a desirable WAN interface as the IPv4 DNS server.
- ① User the following Static DNS IP address: To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① Use the IP address provided by Parental Control Provider: If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at <u>Parental Control Provider</u>).

#### ➢ IPv6:

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

#### Obtain IPv6 DNS info from a WAN interface

**WAN Interface selected:** Select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

#### Use the following Static IPv6 DNS address

**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** Type the specific primary and secondary IPv6 DNS Server address.

#### **Dynamic DNS**

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es).

Advanced Setup					
▼ Dynamic DNS					
Parameters					
Host Name	Username	Service	Interface	Remove	Edit
Add Remove					

#### Click Add to register a WAN interface with the exact DNS.

Advanced Setup	
▼ Dynamic DNS	
Parameters	
Dynamic DNS Server	www.dyndns.org (custom)
Host Name	
Username	
Password	
Period	0 Day(s) 💌
Selected WAN Interface	Available WAN Interfaces
	<pre>ipoe_eth4/eth4.1 pppoe_0_8_35/ppp0.1 3G0/USB3G0</pre>
Select DDNS Server Interface from available WAN interfaces DDNS Server interface can have multiple WAN interfaces se last one the lowest priority if the WAN interface is connected. Apply	rved as system DDNS server but only one will be used according to the priority with the first being the higest and the

You will first need to register and establish an account with the Dynamic DNS provider using their

website, for example http://www.dyndns.org/

Dynamic DNS Server: Select the DDNS service you have established an account with.

Host Name, Username and Password: Enter your registered domain name and your username and password for this service.

**Period:** Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

**Selected WAN Interface:** Select the Interface that is bound to the registered Domain name.

### User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User *test* register two Dynamic Domain Names in DDNS provider <u>http://www.dyndns.org/</u>.

1. pppoe\_0\_8\_35 with DDNS: <u>www.hometest.com</u> using username/password test/test

Advanced Setup	
Dynamic DNS	
Parameters	
Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest.com
Isername	test
assword	••••
Period	25 Day(s)
Selected WAN Interface	Available WAN Interfaces
pppoe_0_8_35/ppp0.1	<pre>ipoe_eth4/eth4.1 3GO/USB3G0 </pre>
Select DDNS Server Interface from available WAN interfaces. DDNS Server interface can have multiple WAN interfaces server as to ne the lowest priority if the WAN interface is connected.	ed as system DDNS server but only one will be used according to the priority with the first being the higest and the

Auvanceu Setup					
Dynamic DNS					
Parameters					
Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1		Edit

2. ipoe\_eth4 with DDNS: <u>www.hometest1.com</u> using username/password test/test.

www.hometest1.com

Add Remove

test

Advanced Setup					
▼Dynamic DNS					
Parameters					
Dynamic DNS Server		www.dyndn	s.org (custom) 🛛 🗸		
Host Name		www.homet	est1.com		
Username		test			
Password		••••			
Period		25	Day(s) 🗸		
Selected WAN Interface			Available WAN Interfaces	:	
DDNS Server interface can h	e from available WAN interfaces. ave multiple WAN interfaces serve the WAN interface is connected.	-> <-	DDNS server but only one wil		with the first being the higest and the
Advanced Setup					
Host Name	Username		Service	Interface	Remove Edit
www.hometest.com	test		dvndns-custom	nnenace	

dyndns-custom

eth4.1

Edit

#### **DNS Proxy**

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.

Advanced Setup		
▼DNS Proxy		
Parameters		
DNS Proxy	Enable     O Disable	
Host name of the Broadband Router	home.gateway	
Domain name of the LAN network	home.gateway	
Apply Cancel		

**DNS Proxy:** Select whether to enable or disable DNS Proxy function, default is enabled.

Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway. Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

#### Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.

Advanced Setup	
▼ Static DNS	
Parameters	
Host Name	
IP Address	
(Add) Edit / Delete	

Host Name: Type the domain name (host name) for the specific IP .

**IP Address:** Type the IP address bound to the set host name above.

Click Add to save your settings.

## **Static ARP**

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And "Static ARP" here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.

Advanced Setup		
▼ Static ARP		
Parameters		
IP Address	MAC Address	
Add Edit / Delete		

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.MAC Address: Enter the MAC address that corresponds to the IP address of the device.Click Add to confirm the settings.

## **UPnP**

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Advanced Setup		
▼UPnP		
Parameters		
UPnP	● Enable ○ Disable	
Apply Cancel		

#### UPnP:

- () Enable: Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

#### Installing UPnP in Windows Example

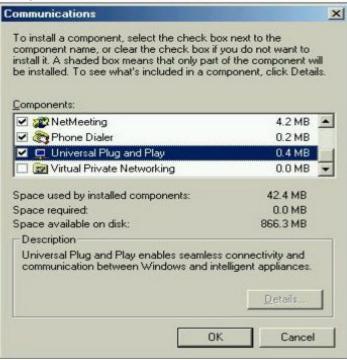
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

Add/Remove Programs Properties	? ×
Install/Uninstall Windows Setup Startup Disk	1
To add or remove a component, select or clear the check box is shaded, only part of the compo installed. To see what's included in a componer <u>C</u> omponents:	onent will be
Accessibility	0.0 MB 🔺
🗹 📻 Accessories	13.8 MB
Address Book	1.5 MB
🗹 📀 Communications	7.0 MB
🗹 🔊 Desktop Themes	5.9 MB 💌
Space used by installed components: Space required: Space available on disk: Description Includes accessories to help you connect to c	42.8 MB 0.0 MB 2574.4 MB
and online services. 5 of 9 components selected	Details Have Disk
OK Canc	el <u>Apply</u>

**Step 3:** In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

**Step 5:** Restart the computer when prompted.

#### Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

**Step 3:** In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ....

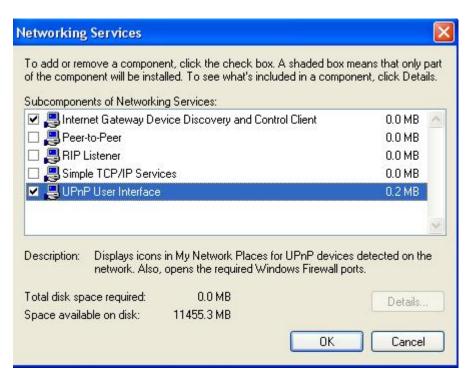


The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.

Win	dows Optional Networking	g Components Wizard		×
١	<b>∀indows Components</b> You can add or remove comp	onents of Windows XP.	Ę	1 1 1
		nt, click the checkbox. A shad nstalled. To see what's includ		
	Components:			
	🔲 불 Management and Mor	nitoring Tools	2.2 MB	
	🗹 🚉 Networking Services		0.3 MB	
	🗆 불 Other Network File an	d Print Services	0.1 MB	
			~	
			10 10 10 10 10 10 10 10 10 10 10 10 10 1	
	Description: Contains a varie	ty of specialized, network-relate	ed services and protocols.	
	Description: Contains a varie Total disk space required:	ty of specialized, network-relate	ed services and protocols.	

**Step 5:** In the Networking Services window, select the Universal Plug and Play check box. **Step 6:** Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



### Auto-discover Your UPnP-enabled Network Device

**Step 1:** Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.



**Step 3:** In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

Internet Connection Properties	? 🛛
General	
Connect to the Internet using:	
Section Internet Connection	
This connection allows you to connect to the Interne shared connection on another computer.	et through a
Show icon in notification area when connected	Settings
ОК	Cancel

Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.

Advanced Settings	
Services	
Select the services running on your network that Internet users car access.	
Services	s:
service1	
service2	Service Settings
✓ service3	Description of service:
	Test
	Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
	192.168.1.11
Add Edit Delete	External Port number for this service: 143 Internal Port number for this service: 143
OK Cancel	OK Cancel

Step 5: Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray

(i) Internet Connecti Click here for more inform	on is now connected	×	
👹 upnp2 - Pant		33	6:43 PM

Step 6: Double-click on the icon to display your current Internet connection status.

Internet Gateway —		
Status:	Connect	ed 05:50:45
Speed:		576.0 Kbps
Internet Inte	emet Gateway M	Computer
<b>()</b> —	- 🥰 ——	- 🗊
Packets Sent: Received:	68,353 64,342	- 3.056.450 4.081.813

## Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate does not match the authorized certificate of the ACS Server, the device will have no access to the server.

### **Trusted CA**

Advanced Setup			
Trusted CA			
Trusted CA (Certificate Aut	thority) Certificates		
Maximum certificates can b	e stored: 8		
Name	Subject	Туре	Action
Import Certificate			

Certificate Name: The certificate identification name.

Subject: The certificate subject.

**Type:** The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-

Key System suggested by x.509.

### Action:

- View: view the certificate.
- Remove: remove the certificate.

Click Import Certificate button to import your certificate.

Advanced Setup		
Trusted CA Imp	port CA certificate	
Parameters		
Name		
Certificate	BEGIN CERTIFICATE <insert certificate="" here=""> END CERTIFICATE</insert>	
Apply		

### Enter the certificate name and insert the certificate.

Advanced Setup		E
Trusted CA Imp	ort CA certificate	
Parameters		
Name	acscert	
Certificate	BEGIN CERTIFICATE MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQ GEwJD TjEXMBUGA1UEChMOQ02DQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc NMjAw NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBgGA1UEChMRQ02DQSBPcGV YYXRp b24gQ0Ewg28wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN ZuTJD rSwXGjaexPnBis5zNJc70SPQYGvhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/ Uu9be pUJBenxvYRgTImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73 /se+H jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVR0fBEEwPzA9oDu	
	gOaQ3 MDUxCzAJBgNVBAYTAkNOMRcwFQYDVQQKEw5DRkNBIFBvbGljeSBDQTENMAs GA1UE	
	AxMEQ1JMMTALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUL5Jufe7tBb/wveS FaAqX k1NC0tAwHQYDVR00BBYEFMMnxjZoyCdlJIevkadLJjMC5RrpMAwGA1UdEwQ	×

Trusted C	A		
Trusted CA	(Certificate Authority) Certificates		
Maximum c	ertificates can be stored: 8		
Name	Subject	Туре	Action
acscert	C=CN/O=CFCA Operation CA	ca	View Remove

## Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol**, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

Advanced Setup				
▼ Multicast				
Multicast Precedence	Disabl	e 💌 lower value, higher priority		
Multicast Strict Grouping Enforcement	Disabl	e 💙		
IGMP				
Default Version	3	[1-3]		
Query Interval	125			
Query Response Interval	10			
Last Member Query Interval	10			
Robustness Value	2			
Maximum Multicast Groups	25			
Maximum Multicast Data Sources (for IGMPv3)	10	[1-24]		
Maximum Multicast Group Members	25			
FastLeave	🗹 Ena	ble		
IGMP Group Exception List				
Group Address	Subnet I	/lask	Remove	
224.0.0.0	255.255	255.0		
239.255.255.250	255.255	255.255		
224.0.255.135	5 255.255.255			
			Add	
Remove				
MLD				
Default Version	2	[1-2]		
Query Interval	125			
Query Response Interval	10			
Last Member Query Interval	10	7		
Robustness Value	2			
	10			
Maximum Multicast Groups				
Maximum Multicast Data Sources (for MLDv2)	10	[1-24]		
Maximum Multicast Group Members				
Fast Leave	🗹 Ena	able		
MLD Group Exception List Group Address	Subnet I	lock	Remove	
ff01::0000	ffff::0000	1 - State 1 - St	Remove	
ff02::0000	ffff::0000			
ff05::0001:0003		mm.mm.mm.mm		
	intant.int		Add	
			LAUU .	
Remove				
Apply Cancel				

#### **IGMP**

**Multicast Precedence:** It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

**Robustness Value:** Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources( for IGMP v3): Enter the Maximum Multicast Data Sources, 1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

**Fast leave:** Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

#### **IGMP Exception List**

The multicast group(s) listed in the IGMP exception list will not be subject to IGMP snooping.

Here the pair of group address and the subnet mask indicates a multicast group range, and 224.0.1.0/255.255.255.0 is a multicast group range of 224.0.1.0 - 224.0.1.255.

Group Address: Set the exception multicast group address.

Subnet Mask: Set the multicast subnet mask

**Remove:** Select the group which is to be removed.

#### MLD

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

**Robustness Value:** Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources( for MLDv2): Enter the Maximum Multicast Data Sources, 1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

**Fast leave:** Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

#### MLD Exception List

The multicast group(s) listed in the MLD exception list will not be subject to MLD snooping.

Group Address: Set the exception multicast group address.

Subnet Mask: Set the multicast subnet mask

**Remove:** Select the group which is to be removed.

## Management

#### SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager, SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest, GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.

SNMP Agent		
Parameters		
SNMP Agent	O Enable 💿 Disable	
Read Community	public	
Set Community	private	
System Name	Broadcom	
System Location	unknown	
System Contact	unknown	
Trap Manager IP	0.0.0	

SNMP Agent: enable or disable SNMP Agent.

**Read Community:** Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

**Set Community:** Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

#### TR-069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones). At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

Advanced Setup			
▼TR-069 Client			
Parameters			
Inform	O Enable 💿	Disable	
Inform Interval	300	[1-2147483647]	
ACS URL			
ACS User Name	admin		
ACS Password	•••••		
WAN Interface used by TR-069 client	Any_WAN 🐱		
Display SOAP messages on serial console	O Enable	Disable	
Connection Request Authentication			
Connection Request User Name	admin		
Connection Request Password			
Connection Request URL	http://10.0.10.11	14:30005/	
Apply GetRPCMethods			

**Inform:** select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

**Inform Interval:** Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

**ACS URL:** Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

**ACS password:** Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

**Display SOAP message on serial console:** select whether to display SOAP message on serial console.

**Connection Request Authentication:** Check to enable connection request authentication feature.

**Connection Request User Name:** Enter the username for ACS server to make connection request.

**Connection Request User Password:** Enter the password for ACS server to make connection request.

**Connection Request URL:** Automatically match the URL for ACS server to make connection request.

**GetRPCMethods:** Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

## HTTP Port

The device equips user to change the embedded web server accessing port. Default is 80.

Advanced Setup		
▼HTTP Port		
Parameters		
HTTP Port	80 (Default: 80)	
Apply Cancel		

#### **Remote Access**

It is to allow remote access to the router to view or configure.

Advanced Setup				
*Remote Access				
Parameters				
Remote Access	Enable			
Enable Service				
Apply				
Allowed Access IP Address Range				
Valid				
IP Version	IPv4 💌 IP Address Range ~			
Add Edit / Delete				

**Remote Access:** Select "Enable" to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

**Enable Service:** Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"Allowed Access IP Address Range" was used to restrict which IP address could login to access system web GUI.

Valid: Enable/Disable Allowed Access IP Address Range

**IP Address Range:** Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click Add to add an IP Range to allow remote access.

Note: 1. If user wants to grant remote access to IPs, first enable Remote Access.

#### 2. Remote Access enabled:

1) Enable *Valid* for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.

2) Disable Valid for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.

3) No listing of IP range is to allow any IP(s) to remote access the router.

### **Mobile Network**

User can press **Scan** to discover available 3G/LTE mobile network.

Configuration		
▼Mobile Networks		
Parameters		
Select Network	Auto Scan	
Apply Cancel		

# 3G/4G LTE Usage Allowance

3G/4G LTE usage allowance is designated for users to monitor and control the 3G/4G LTE flow usage. 8700AX(L)-1600's 3G/4G LTE usage allowance offers exact control settings for each SIM card.

Advanced Setup	
▼ 3G/4G LTE Usage Allowance	
Parameters	
3G/4G LTE Usage Allowance	Enable
Mode	Volume-based     Only Download     10     MB data volume per month included     Time-based     hours per month included
The billing period begins on	day 1 of a month.
Over usage allowance action	E-mail Alert
E-mail alert at percentage of bandwidth	80 %
Save the statistics to ROM	Every one hours 💌
Apply Cancel	

3G/4G LTE Usage Allowance: Enable to monitor 3G/4G LTE usage.

Mode: include Volume-based and Time-based control.

- (i) **Volume-based** include "only Download", "only Upload" and "Download and Upload" to limit the flow.
- ① **Time-based** control the flow by providing specific hours per month.

The billing period begins on: The beginning day of billing each month.

**Over usage allowance action:** What to do when the flow is over usage allowance, the available methods are "E-mail Alert", "Email Alert and Disconnect" and "Disconnect".

**E-mail alert at percentage of bandwidth:** When the used bandwidth exceeds the set proportion, the system will send email to alert.

Save the statistics to ROM: To save the statistics to ROM system.

# **Power Management**

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.

Power Management					
Parameters					
MIPS CPU Clock divider when Idle	Enable	Status	Enabled		
Wait instruction when Idle	Enable	Status	Enabled		
DRAM Self Refresh	🗹 Enable	Status	Enabled		
Energy Efficient Ethernet	Enable	Status	Enabled		
Ethernet Auto Power Down and Sleep	🗹 Enable	Status	Enabled	Number of ethernet interfaces in: Powered up: 1 Powered down: 4	
Adaptive Voltage Scaling	Enable	Status	Enabled		

# Time Schedule

The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to <u>Internet Time</u> for details. You router time should synchronize with NTP server.

Management				
Time Schedule				1
Parameters				
Name		Day in a week	Sun Mon Tue Wed Thu Fri Sat	
Start Time	00 💙 : 00 💙	End Time	00 🔽 : 00 🖌	
Add Edit / D	elete			

For example, user can add a timeslot named "timeslot1" features a period of 9:00-19:00 on every weekday.

Advan	ced Setup												
Time	Schedule												
Parame	eters												
Name					Day in a	a week		Su	n 🗖 Mor	n 🗖 Tue 🗖 We	ed 🗌 Thu 🔲 F	ri 🔲 Sat	
Start Tir	me	00 💉 : 00 💊	*		End Tin	ne		00 🗸	: 00 🗸				
Add	Edit / Delete	]											
Edit	Name		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Delete	
0	timeslot1			х	x	х	X	x		09:00	19:00		

# Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.

Advanced Setup		
▼Auto Reboot		
Parameters		
Schedule	1. Enable Sun Mon Tue Wed Thu Fri Sat Time 00 v: 00 v 2. Enable Sun Mon Tue Wed Thu Fri Sat Time 00 v: 00 v	
Apply		

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:

Advanced Setup		
▼ Auto Reboot		
Parameters		
Schedule	1. ☑ Enable   Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri   Sat Time 22   : 00 2. ☑ Enable ☑ Sun   Mon   Tue   Wed   Thu   Fri ☑ Sat Time 09   : 00	
Apply		

# Diagnostics

# **Diagnostics Tools**

BiPAC 8700AX(L)-1600 offers diagnostics tools including "Ping" and "Trace route test" tools to check for problems associated with network connections.

Advanced Setup		
<ul> <li>Diagnostics Tools</li> </ul>		
Ping Test		
Destination Host		
Source Address	Interface	
Ping Test		
Trace route Test		
Destination Host		
Source Address	O IP Address     O IP Address     O     I	
Max TTL value	16 [2-30]	
Waittime	3 seconds [2-999]	
Trace route Test		

**Ping Test:** to verify the connectivity between source and destination.

**Destination Host:** Enter the destination host (IP, domain name) to be checked for connectivity. **Source Address:** Select or set the source address to test the connectivity from the source to the destination.

Ping Test: Press this button to proceed ping test.

**Trace route Test:** to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

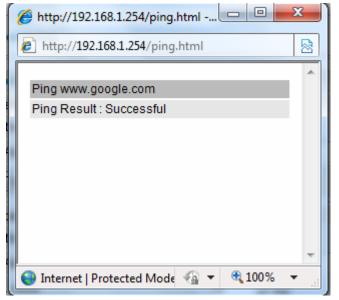
Destination Host: Set the destination host (IP, domain name) to be traced.

**Source Address:** Select or set the source address to trace the route from the source to the destination.

Max TTL value: Set the max Time to live (TTL) value.

Wait time: Set waiting time for each response in seconds.

Advanced Setup			
<ul> <li>Diagnostics Tools</li> </ul>			
Ping Test			
Destination Host	www.	oogle.com	
Source Address	In	erface pppoe_0_8_35/ppp0.1 👻 🔘 IP Ad	ddress
Ping Test			
Trace route Test			
Destination Host			
Source Address	In	erface 🔍 🗸 🔘 IP Ad	ddress
Max TTL value	16	[2-30]	
Wait time	3	seconds [2-999]	
Trace route Test			



Interfa	ce	▼
www.goog	gle.com	
Interfa	ce pppoe_0_8_35/ppp0.1	O IP Address
16 [2	2-30]	
3 s	econds [2-999]	
	www.goog Interfa	16 [2-30]

🏉 http:/	//192.168.1.254/tracert.html - Win	dows Intern 😐 😐 📈	J
🦲 http	://192.168.1.254/tracert.html		]
		*	1
Trace	www.google.com		
No.	Route Address	Time	
1	112.86.208.1	22.229 ms	
2	221.6.9.93	20.352 ms	
3	221.6.2.169	24.345 ms	
4	219.158.24.41	52.837 ms	
5	219.158.23.18	54.696 ms	
6	219.158.19.190	54.904 ms	
7	219.158.3.238	57.824 ms	
8	72.14.215.130	58.851 ms	
9	209.85.248.60	57.644 ms	
10	209.85.250.122	81.242 ms	
11	209.85.250.103	81.351 ms	
12	*	* *	
13	173.194.72.147	79.753 ms	

# **Push Service**

With push service, the system can send email messages with consumption data and system information.

Advanced Setup		
▼Push Service		
Parameters		
Recipient's E-mail	(Must be xxx@yyy.zzz)	
Push Now		

**Recipient's E-mail:** Enter the destination mail address. The email is used to receive *system log*, *system configuration*, *security log* sent by the device when the **Push Now** button is pressed (information sent only when pressing the button ), but the mail address is not remembered.

Note: Please first set correct the SMTP server parameters in Mail Alert.

# Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection. Click *Help* link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

Advanced Setup			
Test the connection to your local network p	ppoe_0_8_35		
Test LAN Connection ( P3 )	FAIL		Help
Test LAN Connection ( P2 )	FAIL		Help
Test LAN Connection (P1)	FAIL		Help
Test LAN Connection ( P4 )	FAIL		Help
Test your Wireless Connection	PASSPASS		Help
Test the connection to your DSL service provide	ler		
Test xDSL Synchronization	FAIL	Help	
Test ATM OAM F5 segment ping	DISABLED	Help	
Test ATM OAM F5 end-to-end ping	DISABLED	Help	
Test the connection to your Internet service pr	ovider		
Test PPP server connection	FAILFAIL	Help	
Test authentication with ISP	FAILFAIL	Help	
Test the assigned IP address	FAILFAIL	Help	
Ping default gateway	PASS	Help	
Ping primary Domain Name Server	PASS	Help	

# Ethernet OAM

8700AX(L)-1600 offers industry standard OAM capabilities to enable network providers to provision and operate their networks with full visibility and control, simply and efficiently to minimize ongoing OPEX.

Both peers should be Ethernet-OAM-enabled.

There are two phases of how Ethernet OAM is usually realized:

1.) **Ethernet Link OAM:** Ethernet in the First Mile (EFM) Link OAM as defined in IEEE 802.3ah, Designed for testing and maintaining access links between EFM-OAM-enabled devices on L2. It includes a set of discovery, link monitoring, remote failure detection and remote loop-back protocols.

2). Ethernet Service OAM (802.1ag/Y1.1731): designed to detect and isolate connectivity faults within the customer service path and ensure a health service end to end.

**802/1ag/CFM** enable Ethernet services to be partitioned into maintenance domains with maintenance endpoints (MEP) and intermediate points (MIP) across which continuity check, link trace and loopback tests can be performed as needed to validate connection integrity.

**Y1.1731** extends beyond CFM (802.1ag) to support performance monitoring and testing of key Ethernet service attributes including frame loss, frame delay, and frame delay variation, which are necessary for ensuring conformance to SLAs and verifying end to end service quality.

Advanced Setup		
▼ Ethernet OAM		
Parameters		
Ethernet Link OAM (802.3ah)	Enable	
Ethernet Service OAM (802.1ag / Y.1731)	□ Enable ④ 802.1ag ○ Y.1731	
Apply Send Loopback Send Linktrace		

**Ethernet Link OAM(802.3ah):** Enable to activate Ethernet in the First Mile (EFM) Link OAM to do link fault management.

**Ethernet Service OAM (802.1ag/Y1.1731):** Enable to activate Ethernet Service OAM check mechanism, including connectivity fault management and performance monitoring..

**Linktrace:** Operators trigger linktrace protocol to perform path discovery and fault isolation in their networks.Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

**Loopback:** Loopback protocol is used to verify and isolate connectivity faults. Loop-back messages otherwise known as Mac ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loop-back to successive MIPs can determine the location of a fault. Sending a high volume of Loop-back Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loop-back to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

# Restart

This section lets you restart your router if necessary. Click  $\[Phi]^{Restart}$  in the low right corner of each configuration page.

Configuration		
▼ Restart		
After restarting. Please wait for sev	eral seconds to let the system come up.	
Restart device with	C Factory Default Settings	
	Ourrent Settings	
Restart		

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.

progress	
progress	
Do not switch off d	evice during flash update or rebooting.
total :	8%

# **Chapter 5: Troubleshooting**

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

# **Problems with the router**

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

### **Problems with WAN interface**

Problem	Suggested Action
Frequent loss of ADSL line sync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

# **Problem with LAN interface**

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

# **Appendix: Product Support & Contact**

If you come across any problems please contact the dealer from where you purchased your product.

**Contact Billion** 

Worldwide:

http://www.billion.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10 are registered Trademarks of Microsoft Corporation.

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

### FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device and its antenna(s) must not be colocated or operating in conjunction with any other antenna or transmitter.

#### **Co-location statement**

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

# FCC Radiation Exposure Statement

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