



BiPAC 8700AX-1600

**Triple-WAN Wireless 1600Mbps VPN
VDSL2/ADSL2+ Firewall Router**

User Manual

Version Released: 2.52.d1

Last revised date: March 20, 2018

Table of Contents

Chapter 1: Introduction	1
Introduction to your Router.....	1
Features	3
VDSL2/ADSL2+ Compliance.....	3
Network Protocols and Features.....	4
Firewall.....	4
Quality of Service Control	5
ATM and PPP Protocols	5
IPTV Applications.....	5
Wireless LAN.....	5
Virtual Private Network (VPN)	5
USB Application Server	6
Management.....	6
Hardware Specifications	7
Physical Interface.....	7
Chapter 2: Installing the Router.....	8
Package Contents.....	8
Important note for using this router	9
Device Description	10
The Front LEDs	10
The Rear Ports	11
Cabling.....	13
Chapter 3: Basic Installation	14
Connecting Your Router.....	15
Network Configuration	16
Configuring a PC in Windows 7/ 8/ 10	16
Configuring a PC in Windows Vista.....	19
Configuring a PC in Windows XP	22
Factory Default Settings.....	24
Information from your ISP	26
Easy Sign On (EZSO)	27
Chapter 4: Configuration	32
Configuration via Web Interface.....	32
Status	34
Summary	35
WAN.....	36
Statistics	37
LAN.....	37
WAN Service.....	38
xTM	38
xDSL.....	39
Bandwidth Usage.....	42
LAN	42
WAN Service.....	44
Route.....	46
ARP	47
DHCP	48
VPN	49
IPSec	49
PPTP	50

L2TP.....	51
OpenVPN.....	52
GRE.....	53
Log.....	54
System Log	54
Security Log.....	55
Quick Start.....	56
Quick Start.....	56
Configuration	61
LAN - Local Area Network	62
Ethernet	62
IPv6 Autoconfig	65
Interface Grouping	69
LAN VLAN Setting.....	72
Eth Port Control.....	73
Wireless 5G(wl0) & 2.4G(Wl1).....	74
Basic	75
Security	77
MAC Filter	88
Wireless Bridge	89
Advanced.....	106
Station Info.....	111
Schedule Control	112
WAN-Wide Area Network	113
WAN Service.....	113
DSL.....	113
Ethernet	125
Failover.....	132
DSL.....	133
SNR	134
System	135
Internet Time	135
Firmware Upgrade	136
Backup / Update	137
Access Control.....	138
Mail Alert	139
SMS Alert.....	140
Configure Log	141
USB.....	142
Storage Device Info	142
User Account.....	143
Print Server	148
DLNA	153
IPTunnel.....	155
IPv6inIPv4.....	155
IPv4inIPv6.....	157
Security.....	158
IP Filtering Outgoing	158
IP Filtering Incoming	161
MAC Filtering	163
Blocking WAN PING	164
Time Restriction.....	165
URL Filter.....	167
Parental Control Provider.....	170

QoS - Quality of Service	171
Quality of Service	171
QoS Port Shaping	176
NAT	177
Exceptional Rule Group.....	177
Virtual Servers.....	178
DMZ Host	182
One-to-One NAT.....	183
Port Triggering.....	184
ALG	187
Wake On LAN.....	188
VPN.....	189
IPSec.....	189
VPN Account.....	199
Exceptional Rule Group.....	200
PPTP	202
PPTP Server	202
PPTP Client	203
L2TP	215
L2TP Server	215
L2TP Client	217
OpenVPN.....	232
OpenVPN Server	232
OpenVPN CA	234
OpenVPN Client	235
GRE.....	242
Advanced Setup	243
Routing.....	244
Default Gateway.....	244
Static Route	245
Policy Routing.....	247
RIP	248
DNS.....	249
DNS.....	249
Dynamic DNS.....	251
DNS Proxy.....	254
Static DNS.....	255
Static ARP	256
UPnP.....	257
Certificate	263
Trusted CA	263
Multicast.....	266
Management.....	269
SNMP Agent	269
TR- 069 Client	270
HTTP Port	272
Remote Access	273
Power Management.....	274
Time Schedule.....	275
Auto Reboot	276
Diagnostics.....	277
Diagnostics Tools	277
Push Service	280
Diagnostics	281

Ethernet OAM	282
Restart.....	283
Chapter 5: Troubleshooting	284
Appendix: Product Support & Contact	286

Chapter 1: Introduction

Introduction to your Router

The Billion BiPAC 8700AX-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, and NAS (Network Attached Storage) in one unit. As well as being IPv6-capable, the BiPAC 8700AX-1600 VDSL2 router supports super-fast 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. With an array of advanced features, the Billion BiPAC 8700AX-1600 delivers a future-proof solution for VDSL2 connections, super-fast FTTC and ultra-speed FTTH (Fiber-To-The-Home) network deployment and services.

Flexible Deployment Options

The BiPAC 8700AX-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-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. 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-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-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.

Experience Gigabit WAN

The BiPAC 8700AX-1600 has one Gigabit WAN port. This WAN offers broadband connectivity option for connecting to a cable, DSL, fibre modem. The BiPAC 8700AX-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 indispensable addressing system for the savvy cloud computing users. Equipped with IPv6, the BiPAC 8700AX-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)
 - WAN approach – VDSL2/ADSL2+, 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
 - 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^{*2}
 - 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-1600 A model only) -

ITU-T G.992.3 (G.dmt.bis, Annex M, ADSL2

Annex M, available for BiPAC 8700AX-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^{*2}

- 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

- 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

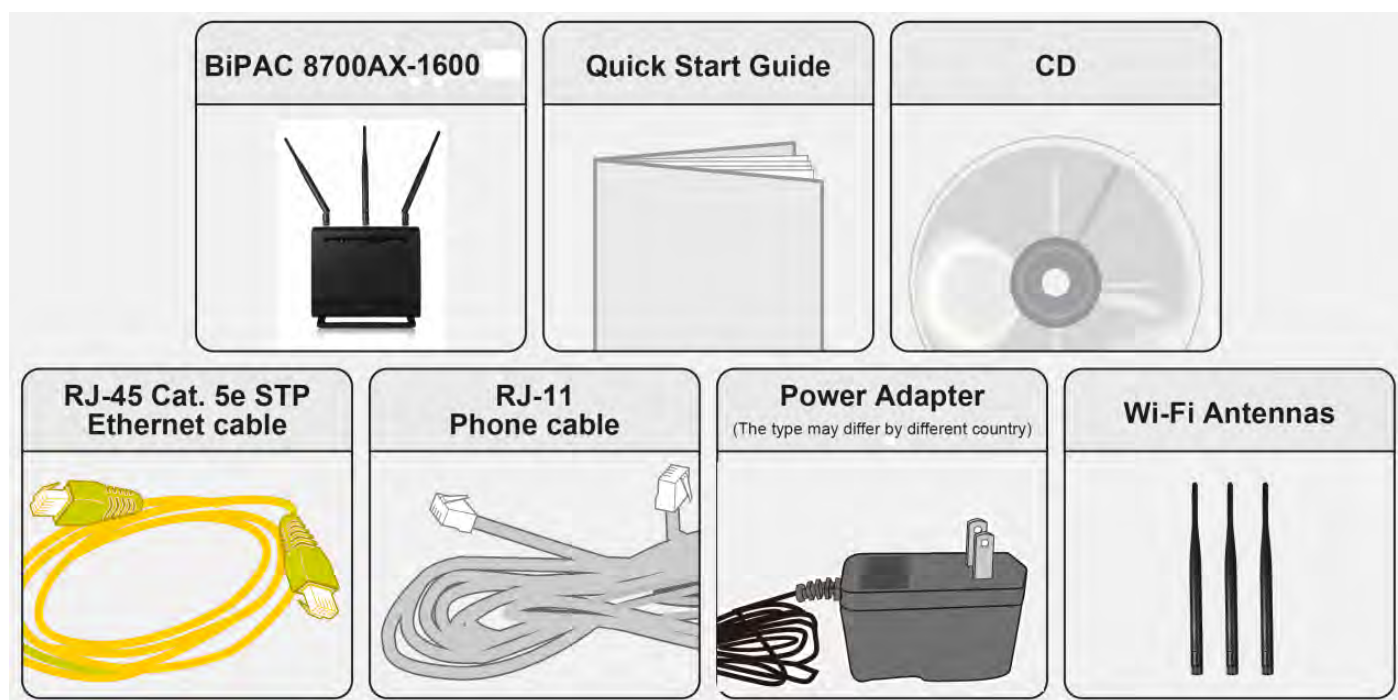
Physical Interface

- 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
- Wireless on/off and WPS push button
- Power jack
- Power switch
- Factory default reset button

Chapter 2: Installing the Router

Package Contents

- BiPAC 8700AX-1600 Triple-WAN Wireless 1600Mbps (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



Warning

1. Do not use the router in high humidity or high temperatures.
2. Do not use the same power source for the router as other equipment.
3. 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.
4. Avoid using this product and all accessories outdoors.

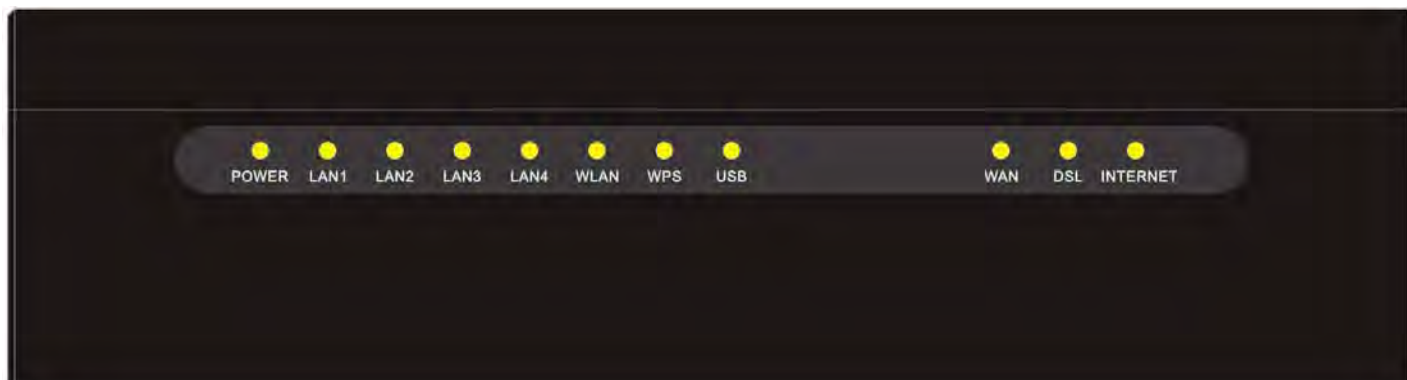


Attention

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

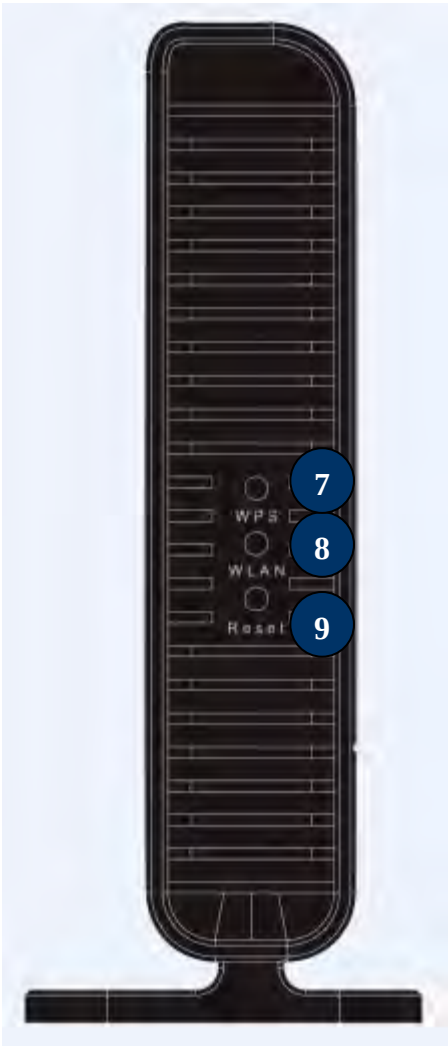
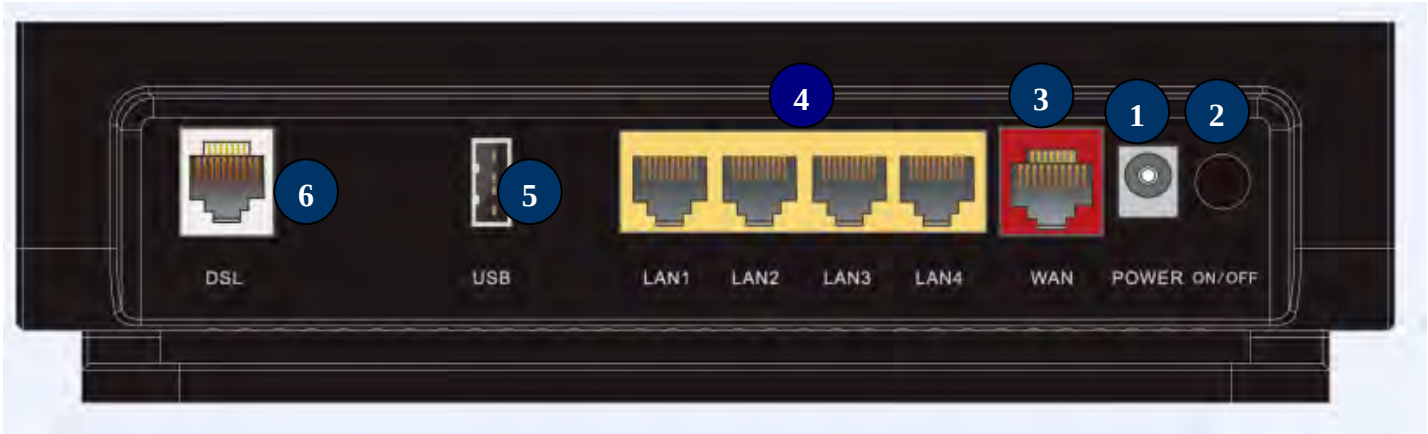
Device Description

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
	Off	Data being transmitted / received
WLAN(2.4G / 5G)	Green	Wireless enabled (either 2.4G or 5G wireless).
	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.
USB	Green	Successfully connected to a USB device (Printer, USB 2.0 storage.)
WAN	Green	Successfully connected to an Ethernet device or to a broadband device.
	Blinking	Data being transmitted / received
DSL	Green	Successfully connected to an xDSL DSLAM (Line Synced)
	Green Blinking	xDSL synchronizing or waiting for DSL synchronizing
	Off	xDSL cable unplugged
Internet	Green	IP connected and traffic is passing through the device
	Blinking	Data being transmitted / received
	Red	The router fails to obtain an 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) to this port.
6	DSL	Connect to the xDSL/ telephone network with RJ-11 cable(telephone)
7	WPS	Press & hold the button for 2 seconds to trigger WPS function * For WPS configuration, please refer to the WPS section in the User Manual.
8	WLAN	Press & hold the button for more than 6 seconds 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.

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.

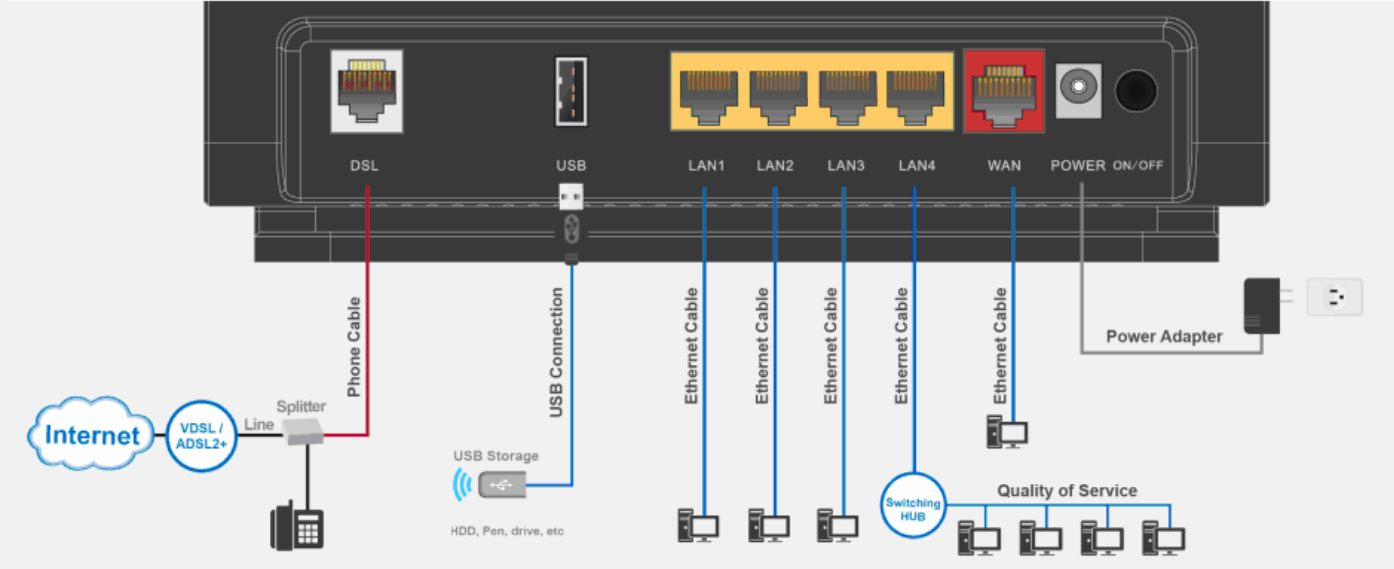


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

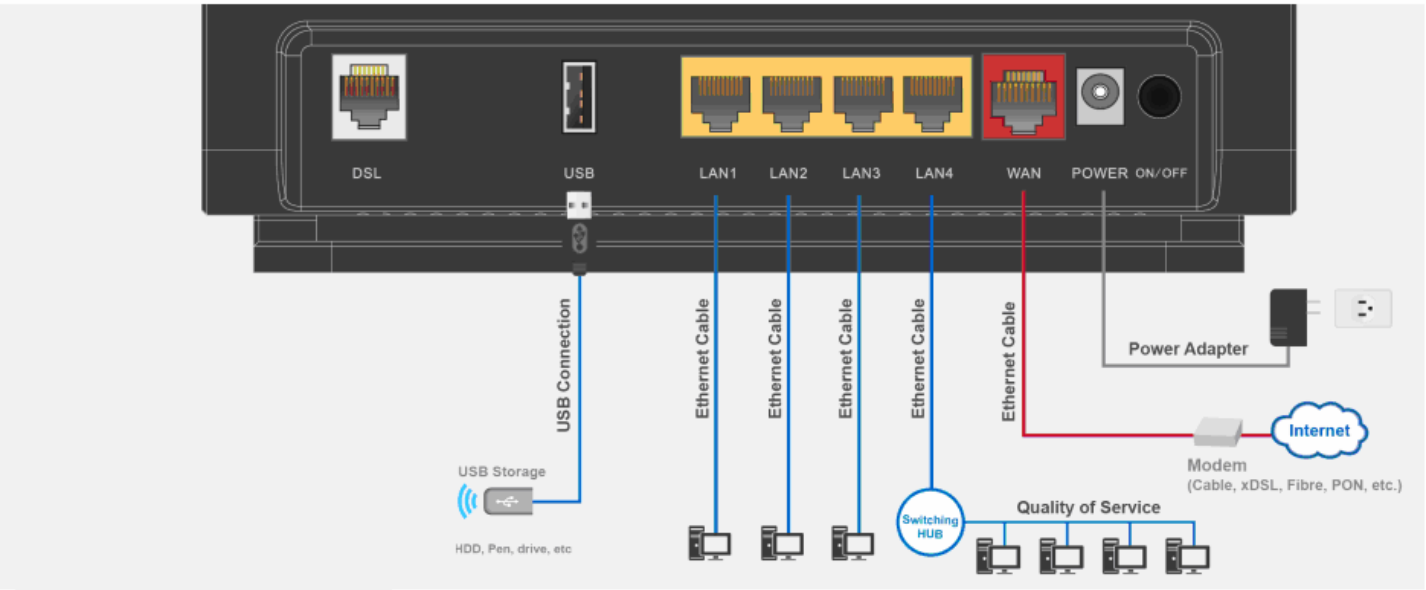
Connecting Your Router

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

DSL mode



Broadband mode

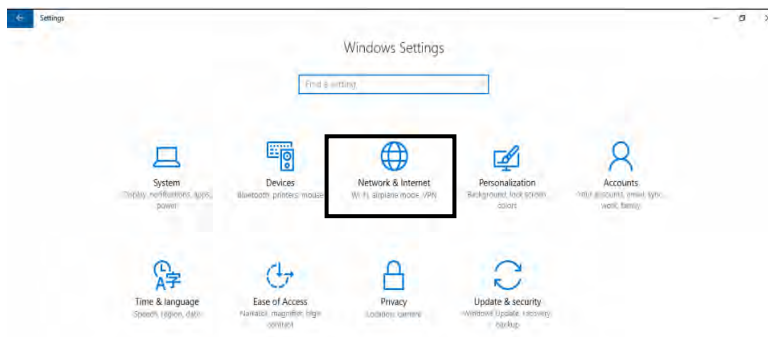


Network Configuration

Configuring a PC in Windows 7/ 8/ 10

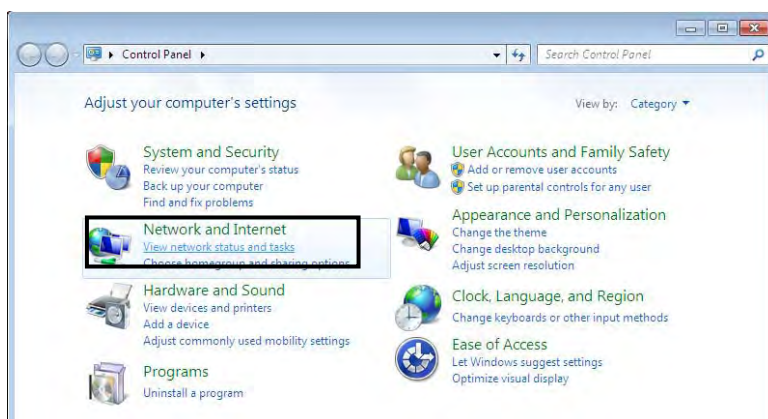
1. For Windows 7/8, go to **Start**. Click on **Control Panel**.

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**.



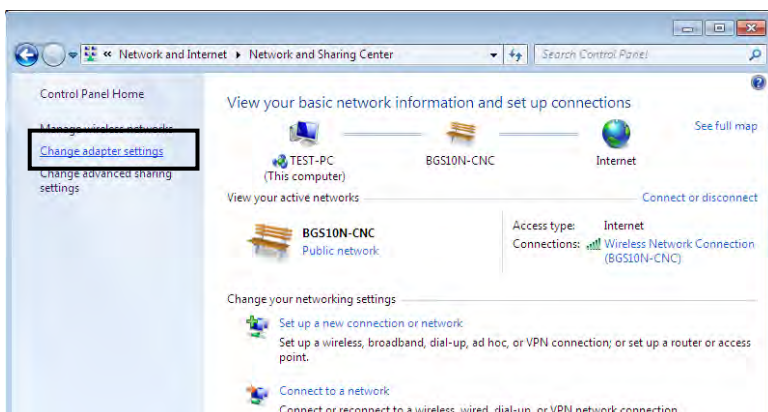
Settings of Windows 10

3. Click on **Network and Internet**.

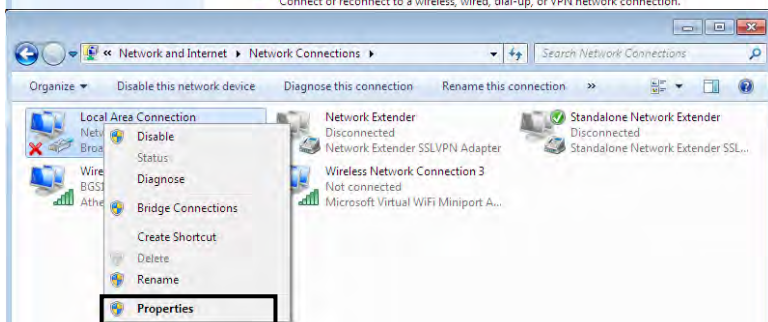


Control Panel

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

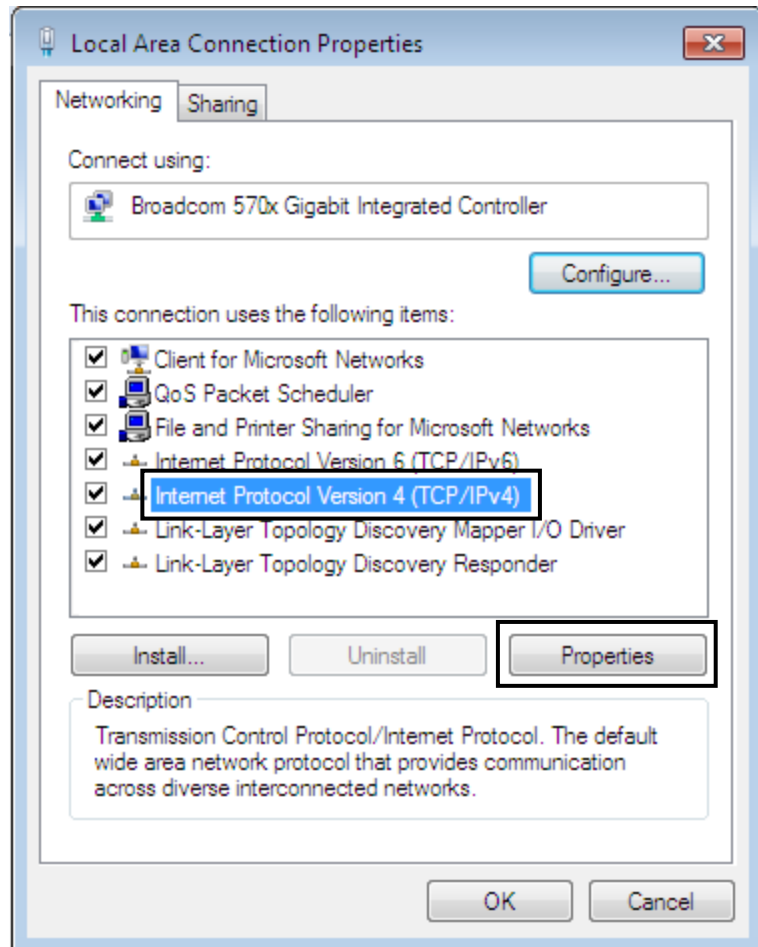


5. Select the **Local Area Connection**, and right click the icon to select **Properties**.

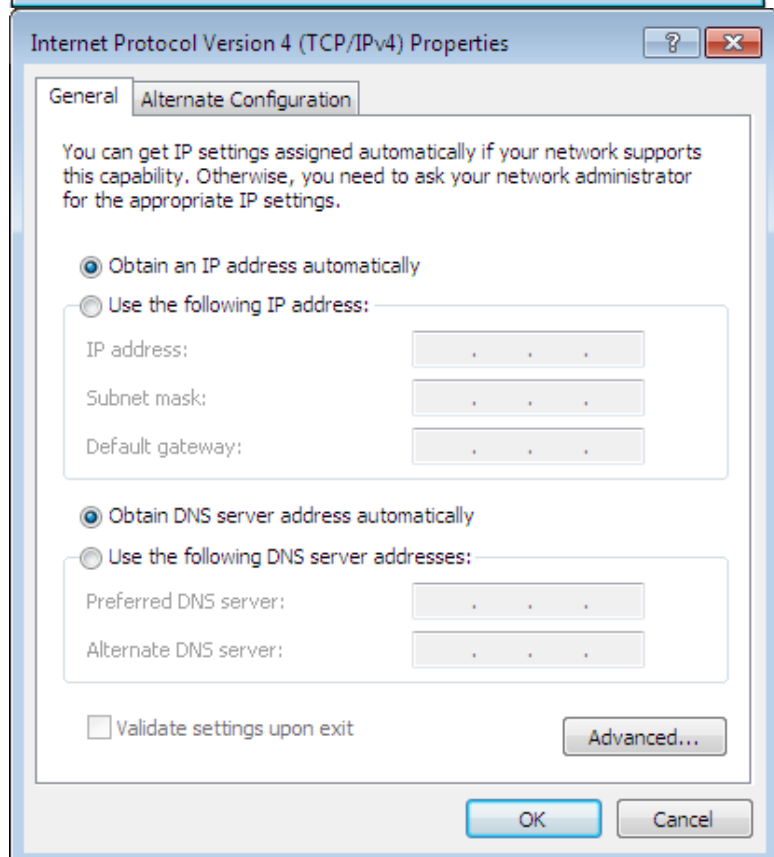


IPv4:

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

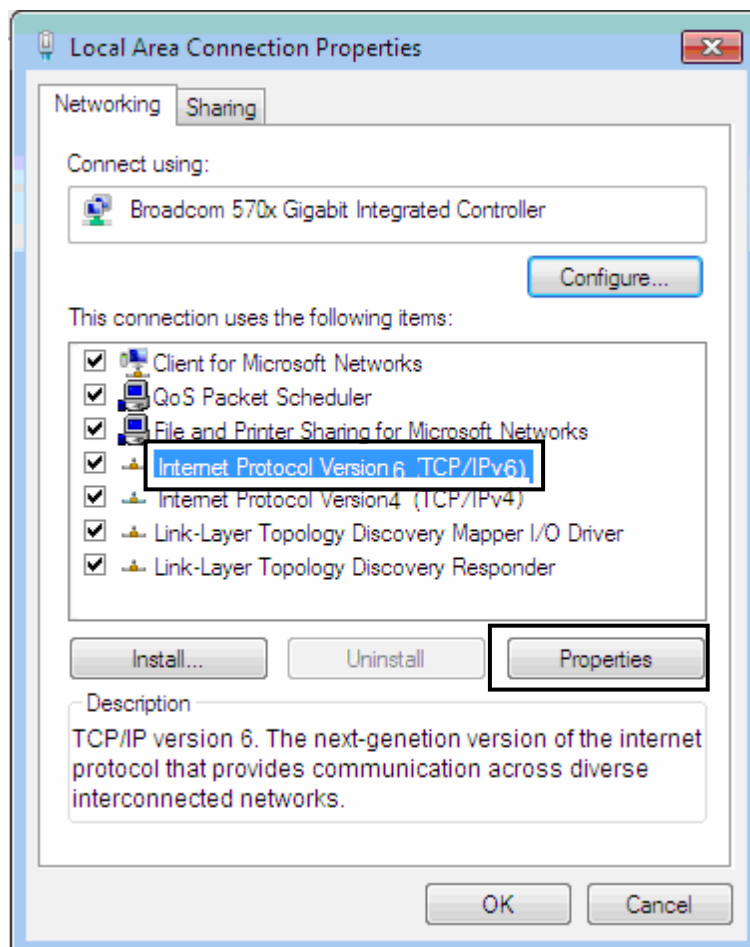


7. In the **TCP/IPv4** properties window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
8. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

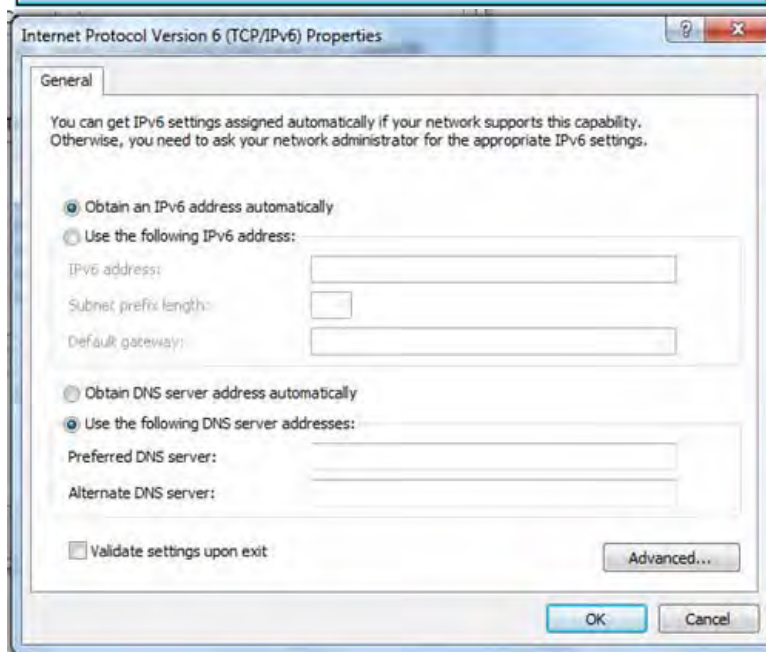


IPv6:

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



7. 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.



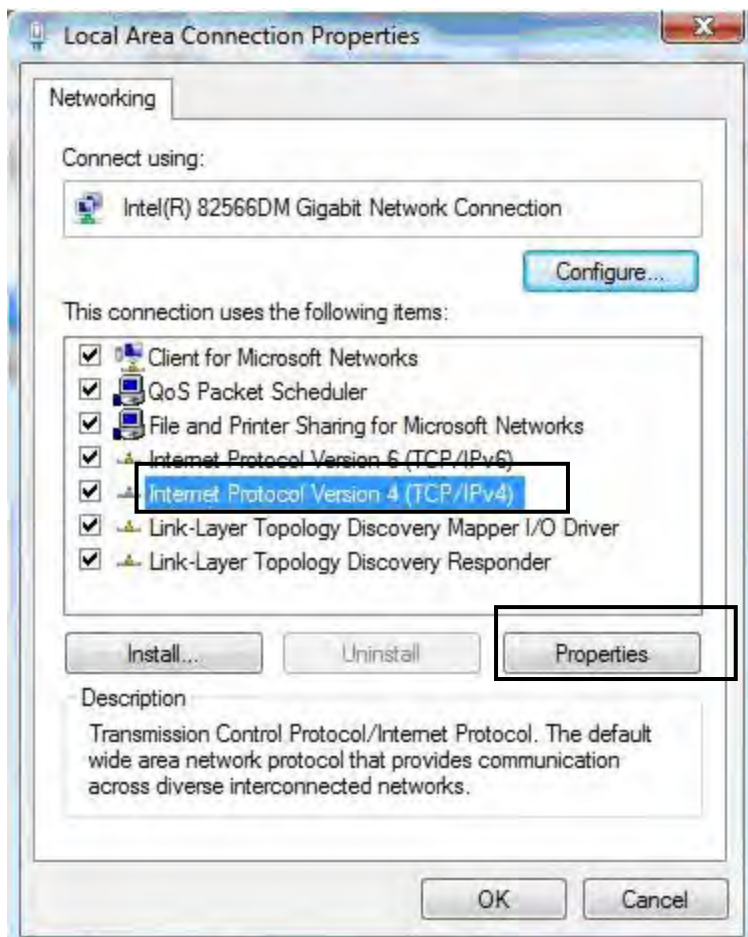
Configuring a PC in Windows Vista

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**.

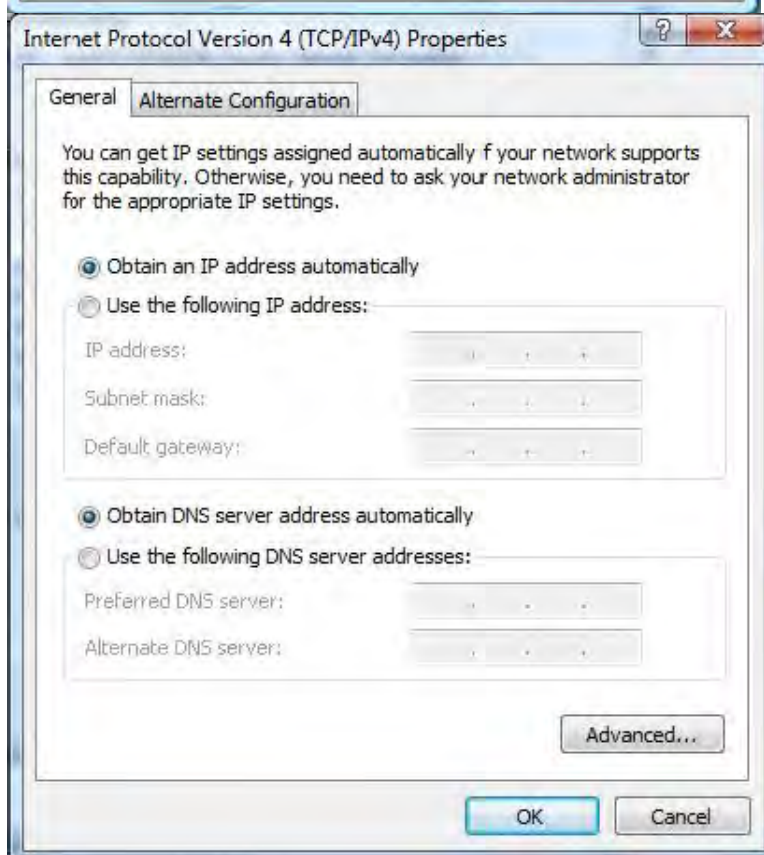


IPv4:

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

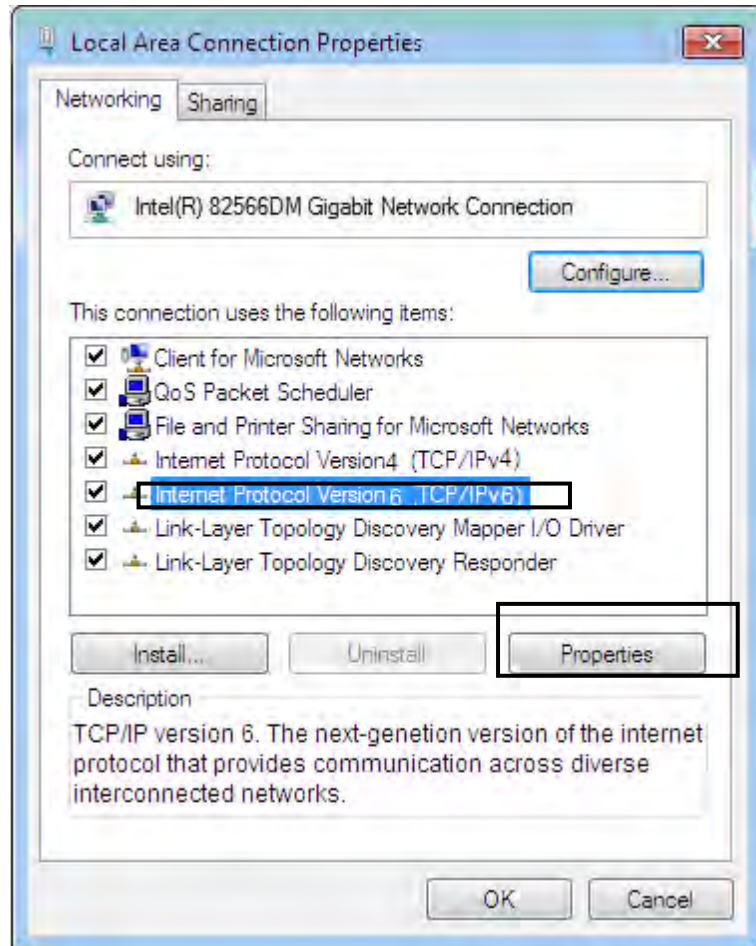


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

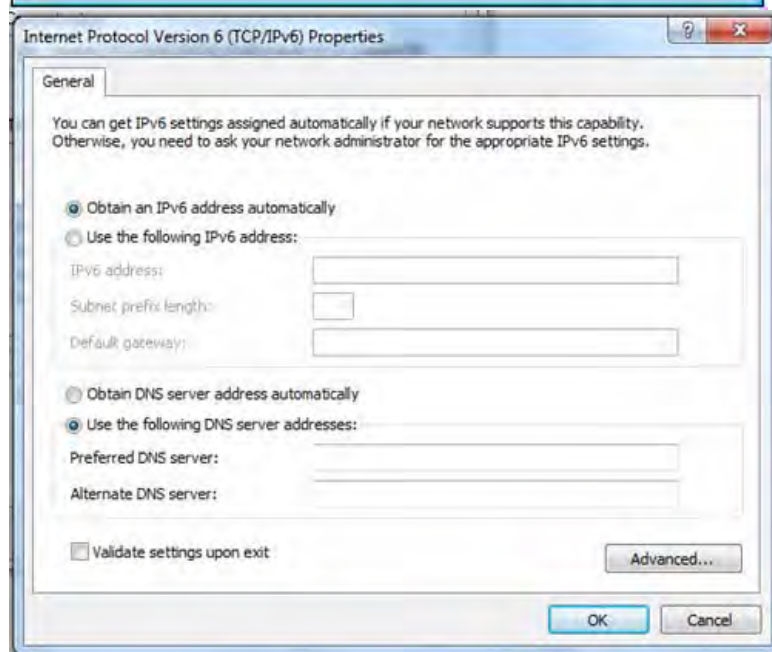


IPv6:

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



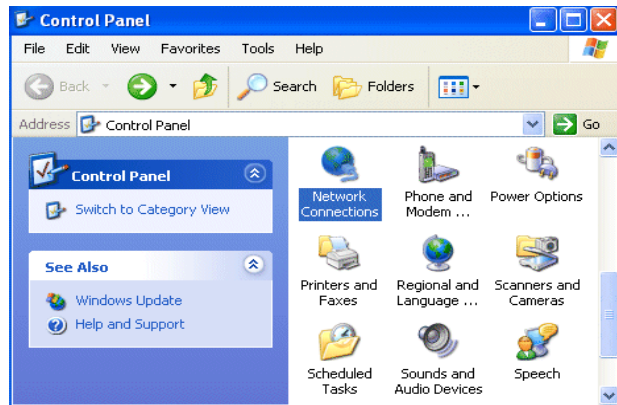
6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring a PC in Windows XP

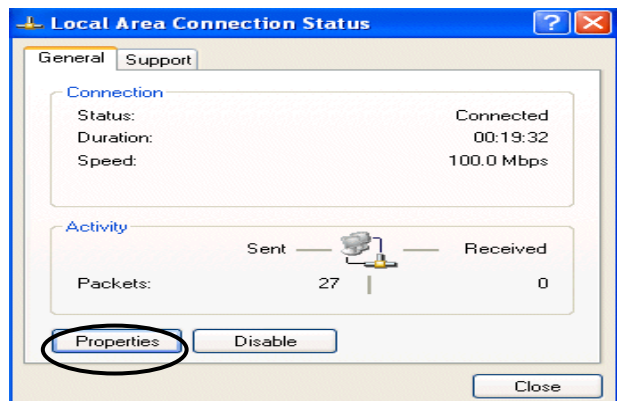
IPv4:

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

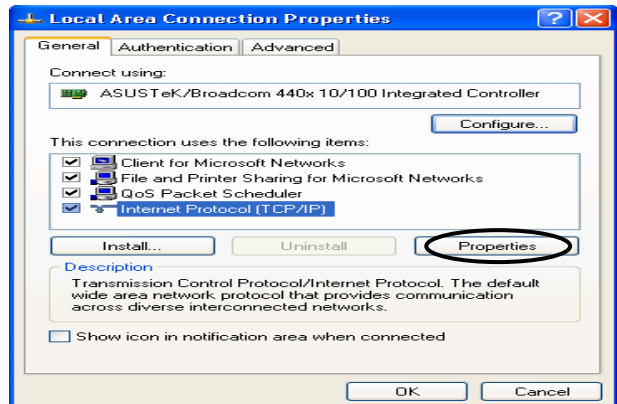


2. Double-click **Local Area Connection**.

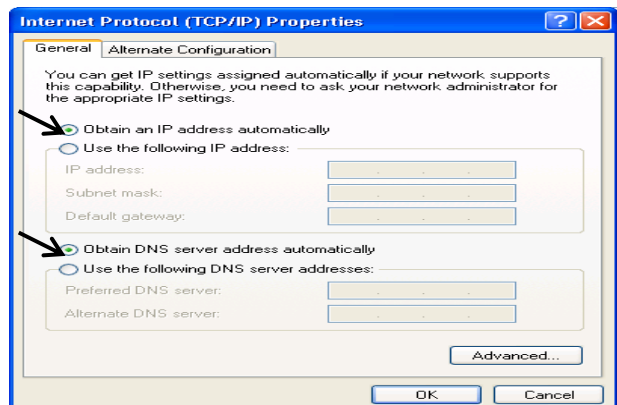
3. In the **Local Area Connection Status** window, click **Properties**.



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.



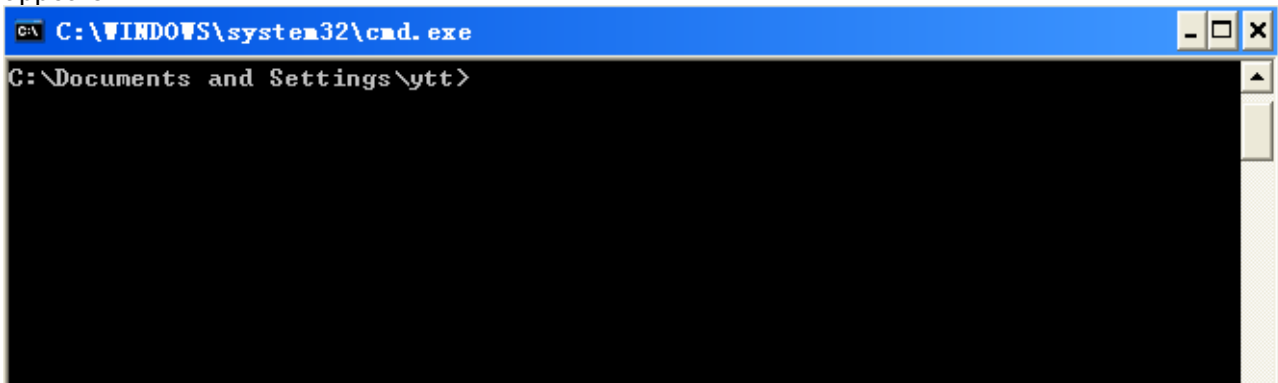
6. Click **OK** to finish the configuration.

IPv6:

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

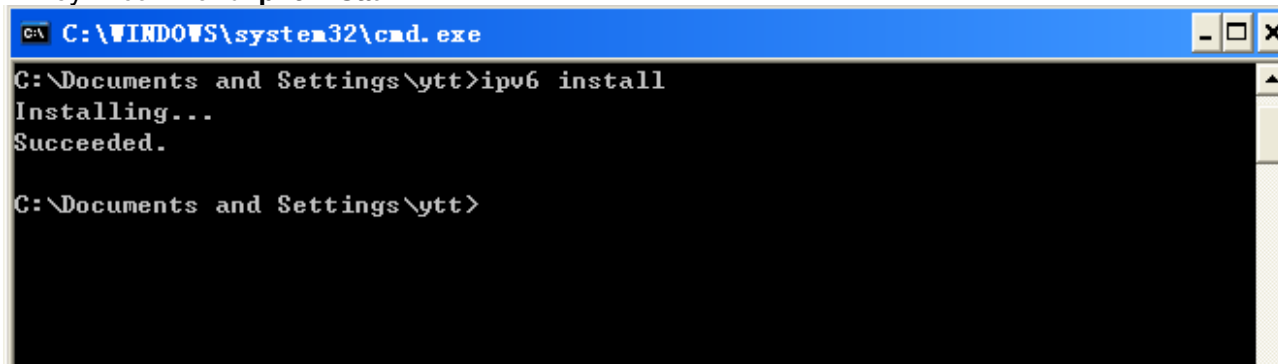
Act as shown below:

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



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

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 [Access Control](#) .

Administrator

- ▶ Username: admin
- ▶ Password: admin

Local

- ▶ Username: user
- ▶ Password: user

Remote

- ▶ Username: support
- ▶ Password: support



Attention

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: fe80:0000:0000:0000:0204: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	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

IPv6

LAN Port		WAN Port
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::204:edff:fe01:1/64, the prefix initiates by fe80::	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
DHCP server function	Enabled	

Information from your ISP

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

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.

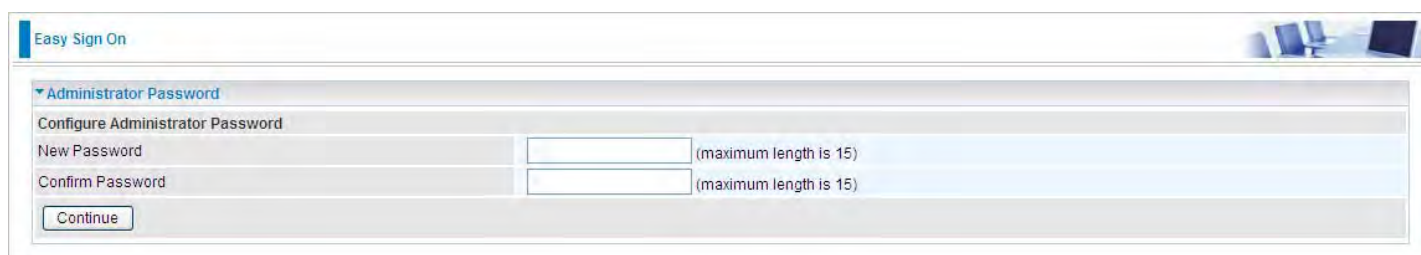
Easy Sign On (EZSO)

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.



The screenshot shows the 'Easy Sign On' window with the 'Administrator Password' section expanded. It contains two input fields: 'New Password' and 'Confirm Password', both with a note '(maximum length is 15)'. A 'Continue' button is at the bottom left.

Step 2: Set the Time Zone.



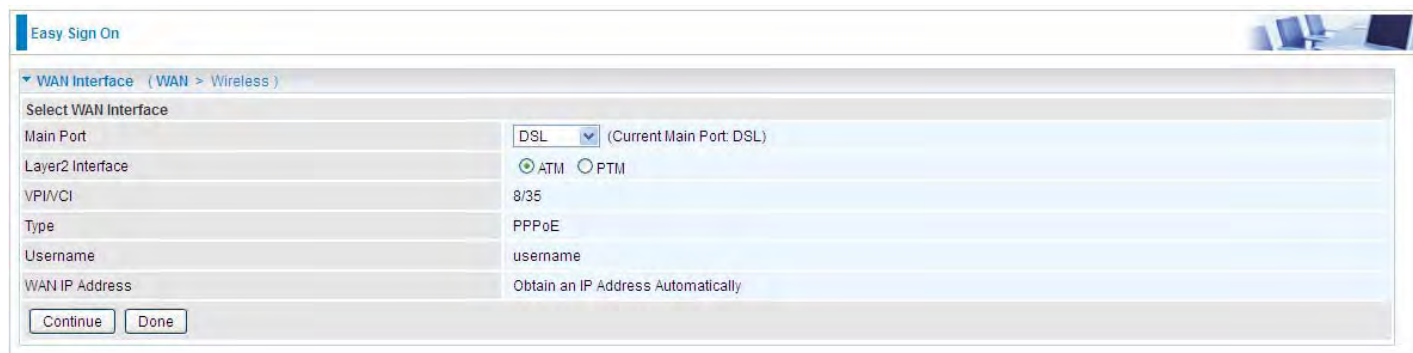
The screenshot shows the 'Easy Sign On' window with the 'Time Zone' section expanded. It contains a dropdown menu for 'Time zone offset' with the selected value '(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. A 'Continue' button is at the bottom left.

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.



The screenshot shows the 'Easy Sign On' window with the 'WAN Interface' section expanded. It contains several fields: 'Main Port' (DSL), 'Layer2 Interface' (ATM selected, PTM unselected), 'VPI/VCI' (8/35), 'Type' (PPPoE), 'Username' (username), and 'WAN IP Address' (Obtain an IP Address Automatically). 'Continue' and 'Done' buttons are at the bottom left.

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

▼ WAN Interface (WAN > Wireless)

WAN Service

Type	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	
MTU	1492

Continue

If the DSL 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**.

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-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)

Parameters

Band

5GHz (w/o)

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)

Parameters

Band

2.4GHz (w/1)

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.

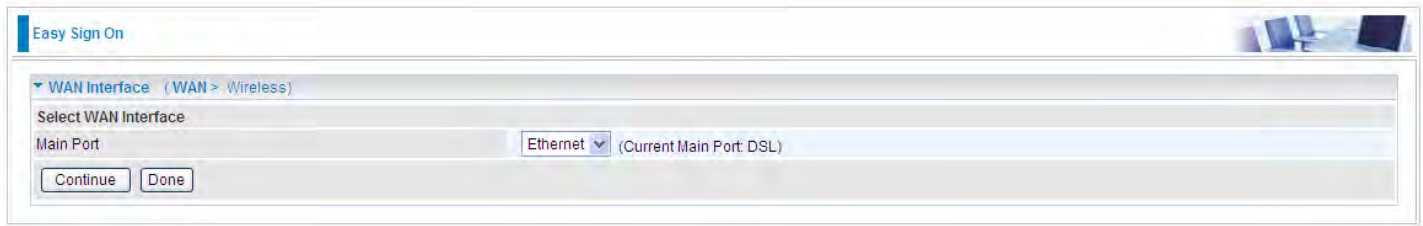
You can now:

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

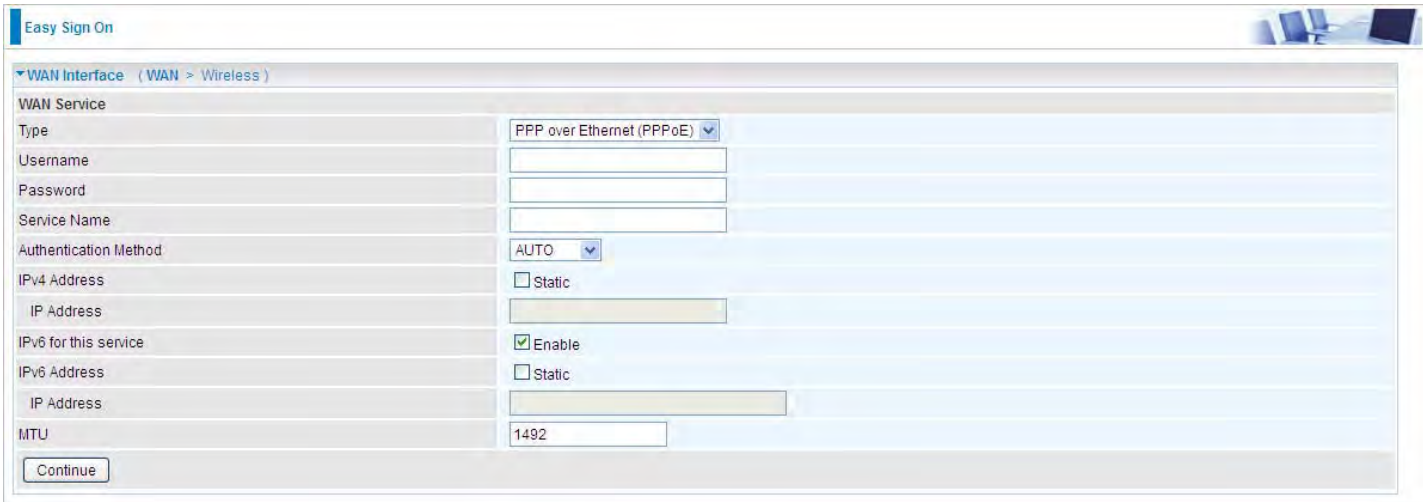
▼ WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port 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

▼ WAN Interface (WAN > Wireless)

WAN Service

Type 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

MTU 1492

Continue

3. Wait while the device is configured.

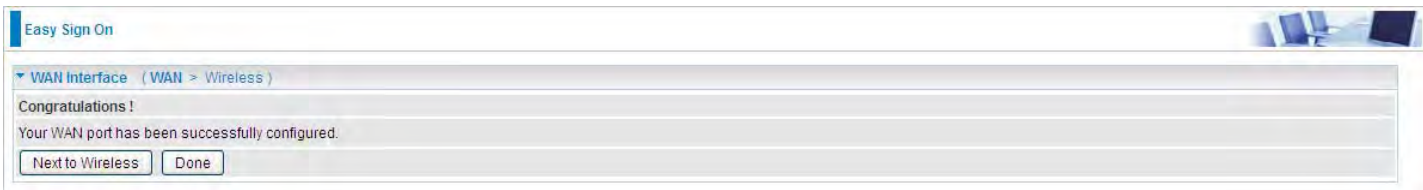


Easy Sign On

▼ 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.



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-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)

Parameters

Band	5GHz (w10)
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)

Parameters

Band	2.4GHz (w11)
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](#)

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.



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

Once you have logged on to your BiPAC 8700AX-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, 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)

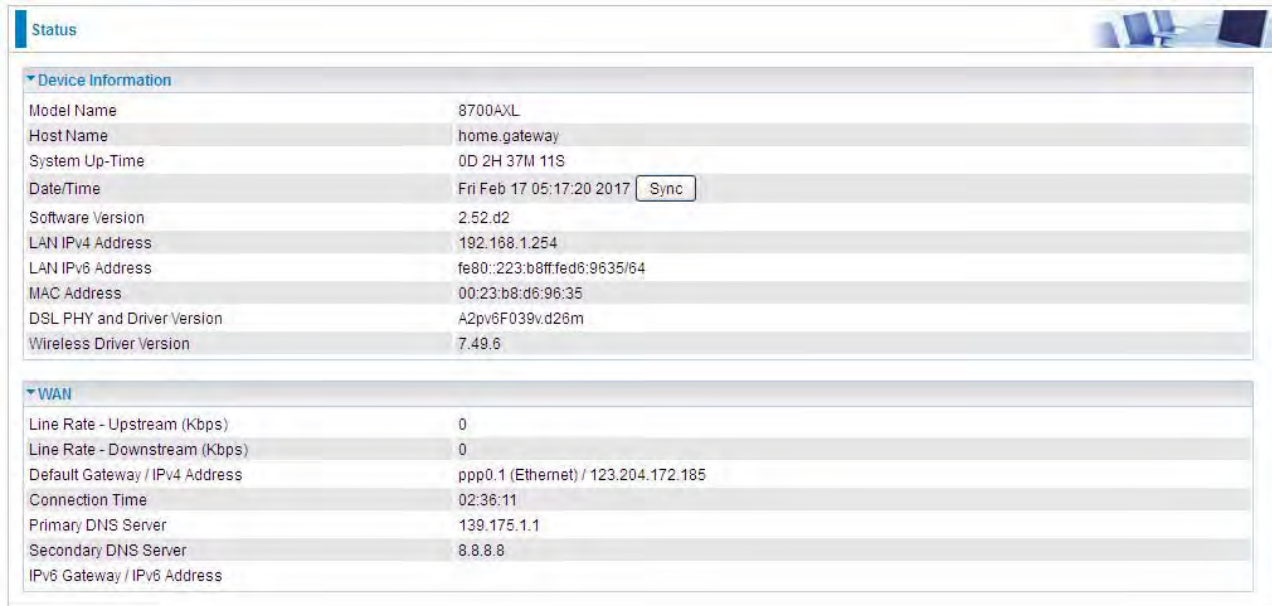
Status

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](#), [Route](#), [ARP](#), [DHCP](#), [VPN](#) and [Log](#) subsections are included.

▼ Status
▪ Summary
▪ WAN
▶ Statistics
▶ Bandwidth Usage
▪ 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).



The screenshot shows the 'Status' page of a router. It has two main sections: 'Device Information' and 'WAN'. The 'Device Information' section includes fields for Model Name, Host Name, System Up-Time, Date/Time (with a 'Sync' button), Software Version, LAN IPv4 Address, LAN IPv6 Address, MAC Address, DSL PHY and Driver Version, and Wireless Driver Version. The 'WAN' section includes fields for Line Rate - Upstream (Kbps), Line Rate - Downstream (Kbps), Default Gateway / IPv4 Address, Connection Time, Primary DNS Server, Secondary DNS Server, and IPv6 Gateway / IPv6 Address.

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:fe6:9635/64
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.

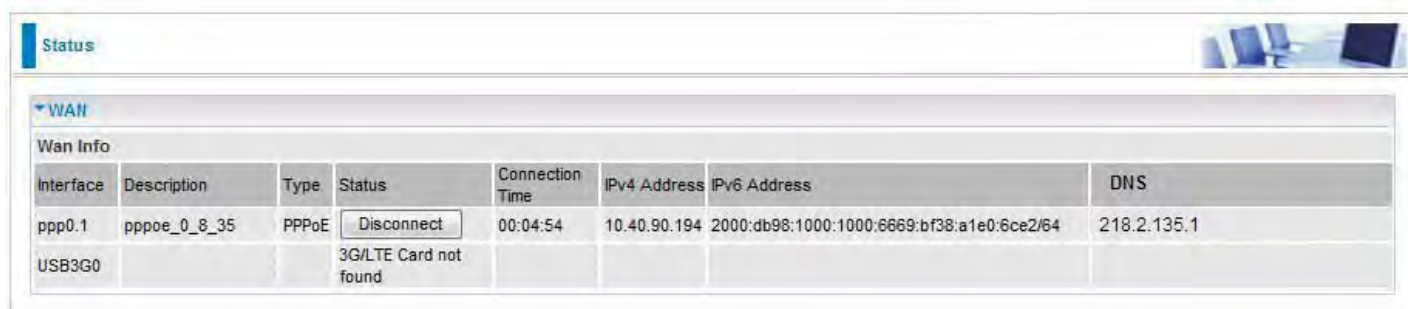
Primary DNS Server: Displays IPV4 address of Primary DNS Server.

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.



The screenshot shows a web interface with a 'Status' tab selected. Under the 'WAN' section, there is a table titled 'Wan Info'.

Interface	Description	Type	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.

Status														
LAN Statistics														
Interface	Received							Transmitted						
	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
wl0	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
Reset														

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.

Interface		Received				Transmitted			
Interface	Description	Total				Total			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
ppp0.1	pppoe_0_0_33	209804	2671	0	0	593212	2133	0	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.

xTM

The Statistics-xTM screen displays all the xTM statistics

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
1	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

Status		
xDSL		
Mode	ADSL_2plus	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	
	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
xDSL BER Test Reset		

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.

ADSL BER Test -- Start

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

Start

Close

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

ADSL BER Test -- Running

The xDSL BER test is in 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 -- Result

The ADSL BER test completed successfully.

Test Time

20 seconds

Total Transferred Bits

0x000000001DA1F500

Error Ratio

0.00e+00

Close

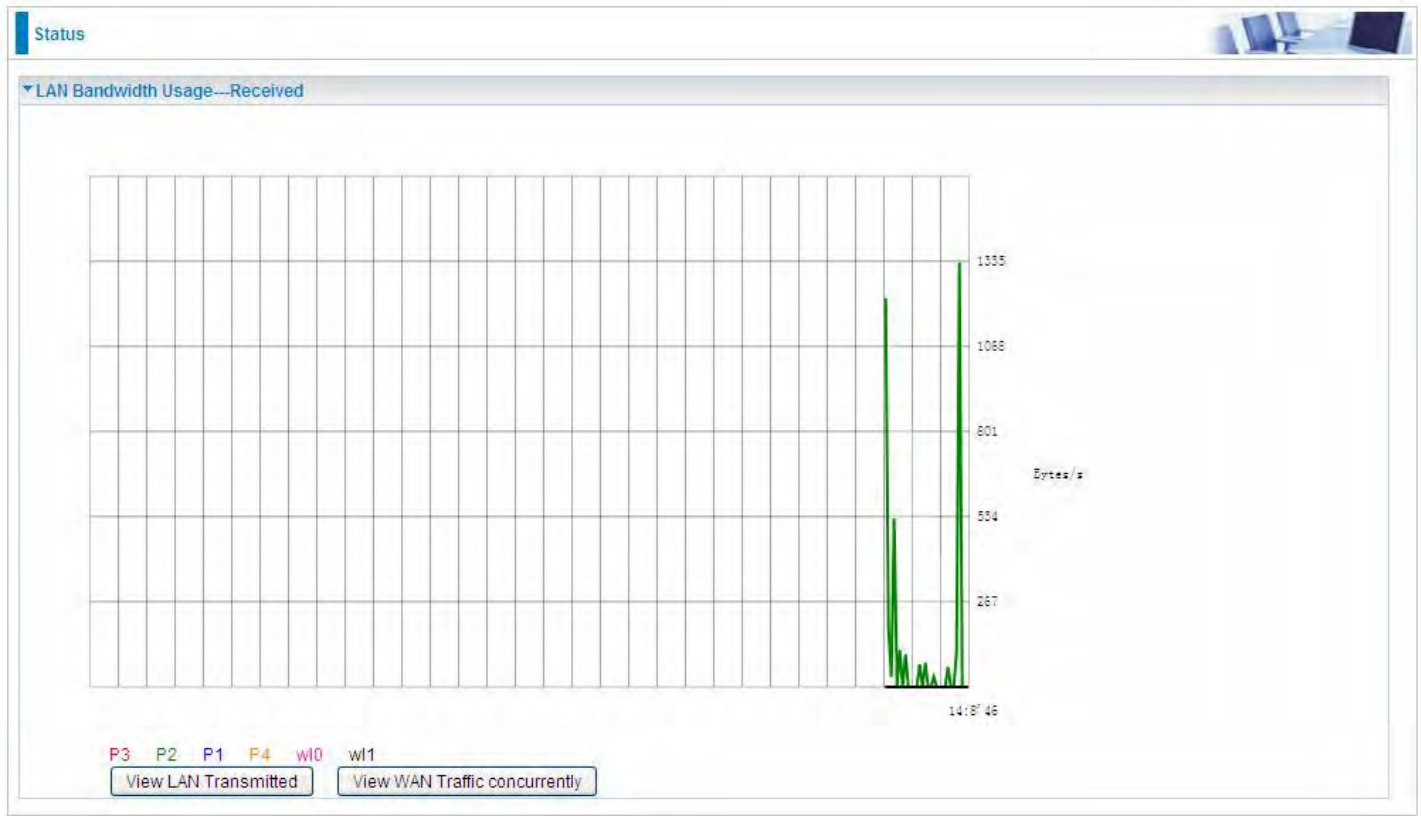
Reset: Click this button to reset the statistics.

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).

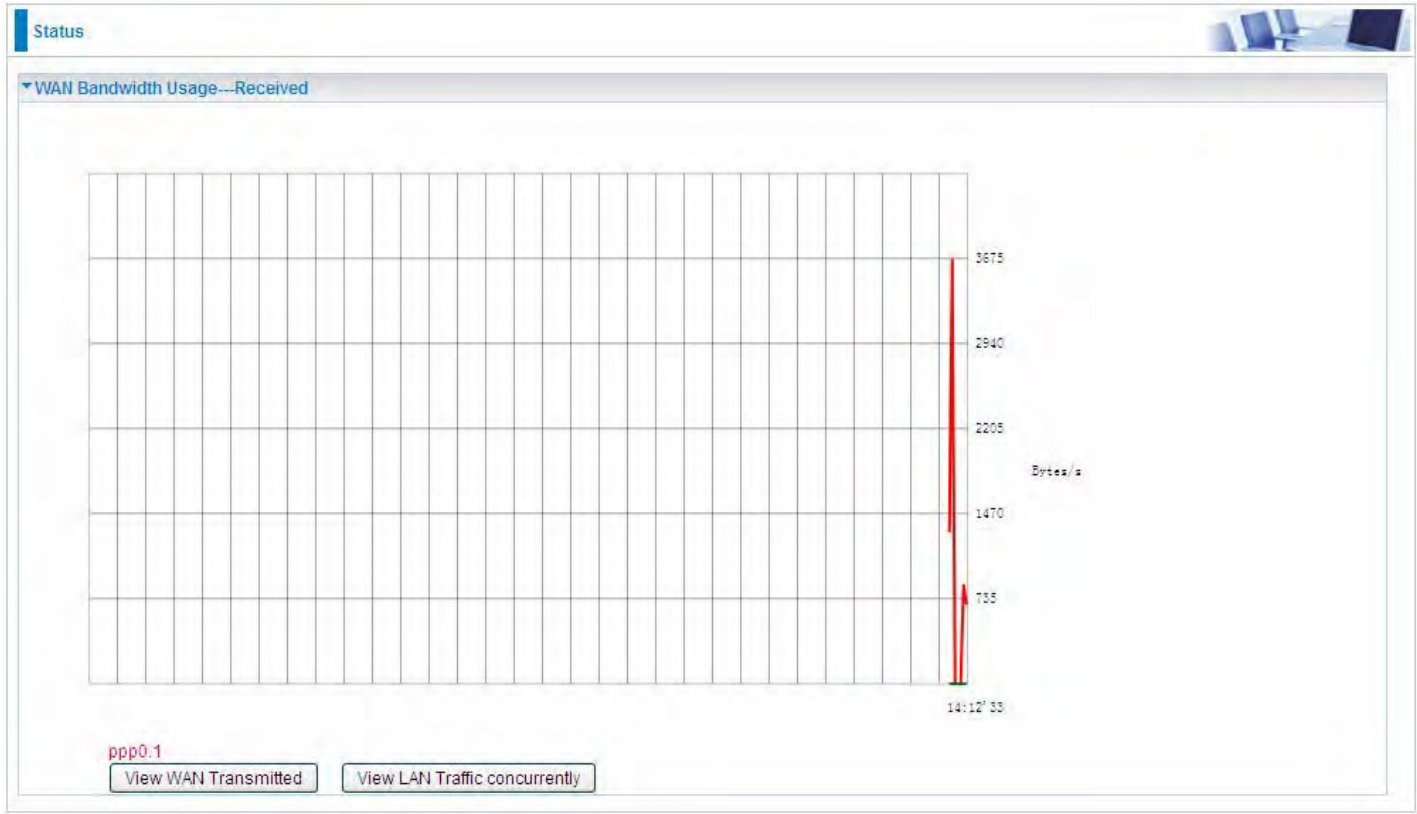


Press **View LAN Transmitted** button to change the diagram to the statistics of the LAN Transmitted Bytes. (**Note:** P2 means Ethernet port #2, and the traffic information of the port #2 is identified with blue, the same color with port#2 in the diagram; other ports all take the same mechanism.)

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

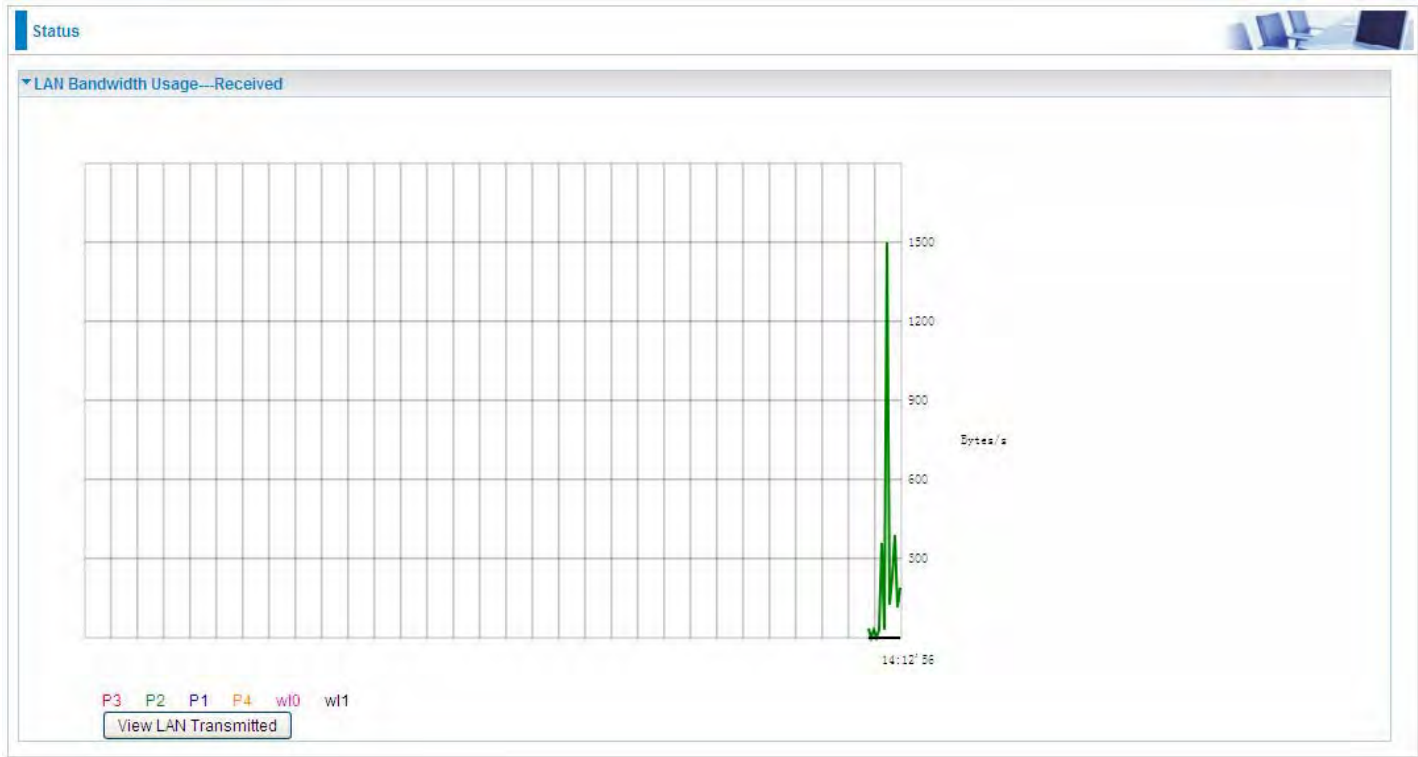


WAN Service



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.



Route

Status						
Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.46	0.0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_8_35	ppp0.1

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.
- ① **H (host):** destination is host not the subnet.
- ① **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.

Status				
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:9009:87ae		00:22:64:1b:6ffd	br0	
2000:1211:1002:4f0b:bd94: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	
ytt-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



The screenshot shows a web interface titled "Status" with a sub-section "IPSec Status". Below this is a table labeled "VPN Tunnels". The table has six columns: Name, Active, Local Subnet, Remote Subnet, Remote Gateway, and SA. There is one row with the name "11". The "Active" column for this row contains a red "X" icon, indicating the tunnel is inactive. The "Local Subnet" is "192.168.1.0 -- 255.255.255.0", the "Remote Subnet" is "192.168.0.0 -- 255.255.255.0", and the "Remote Gateway" is "172.16.1.235". The "SA" column is empty. Below the table is a "Refresh" button.

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.

Refresh: Click this button to refresh the tunnel status.

PPTP

Status						
▼ PPTP Status						
PPTP Server ▼						
Name ▼	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test	✓	Connected	Remote Access		172.16.1.207	Drop
PPTP Client ▼						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action
Refresh						

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.

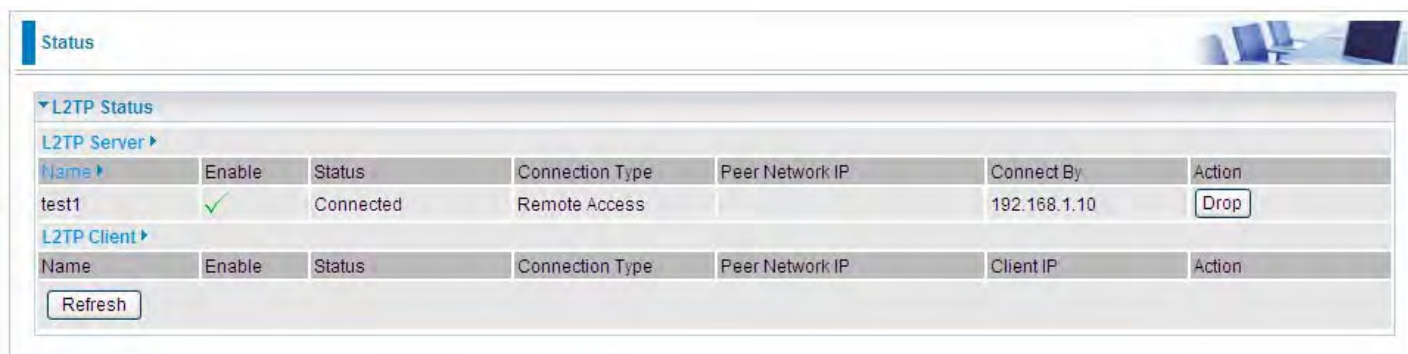
Peer Network IP: Display the remote (server side) network and subnet mask.

Client: Assigned IP by PPTP server.

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

Refresh: Click this button to refresh the connection status.

L2TP



Status						
L2TP Status						
L2TP Server						
Name	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.1.10	Drop
L2TP Client						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action

Refresh

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.

Refresh: Click this button to refresh the connection status.

OpenVPN

Status

▼ OpenVPN Status

OpenVPN Server ▶

Name ▶	Enable	Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.15.1	192.168.15.22	Drop

OpenVPN Client ▶

Name	Enable	Status	Peer Network IP	Client IP	Action
test1	✓	Connected	192.168.15.1 (192.168.200.131)	192.168.15.22	Disconnect

Refresh

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.

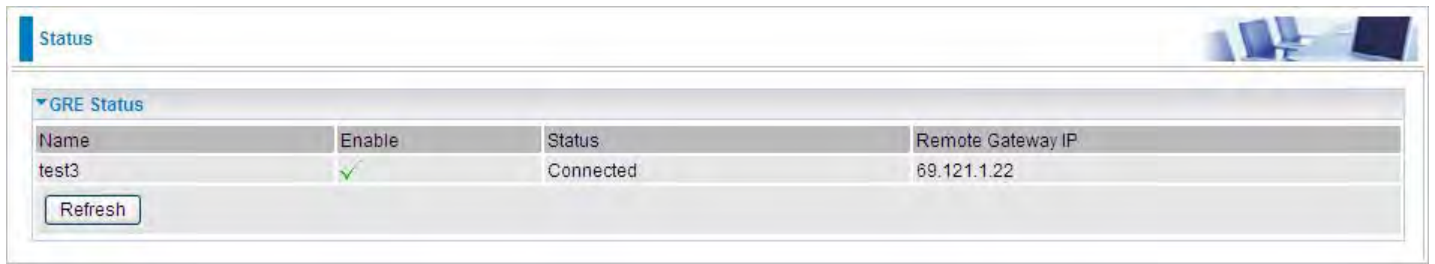
Peer Network IP: Display the tunnel virtual address (WAN address) of server side.

Client: Assigned tunnel virtual IP by OpenVPN server.

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

Refresh: Click this button to refresh the connection status.

GRE



The screenshot shows a window titled 'Status' with a 'GRE Status' section. It contains a table with four columns: Name, Enable, Status, and Remote Gateway IP. There is one row with the name 'test3', which is enabled (indicated by a green checkmark) and has a status of 'Connected' to a remote gateway at IP '69.121.1.22'. A 'Refresh' button is located below the table.

Name	Enable	Status	Remote Gateway IP
test3	✓	Connected	69.121.1.22

Refresh

Name: The GRE connection name.

Enable: Display the connection status with icons.

Status: The connection status, connected or disable.

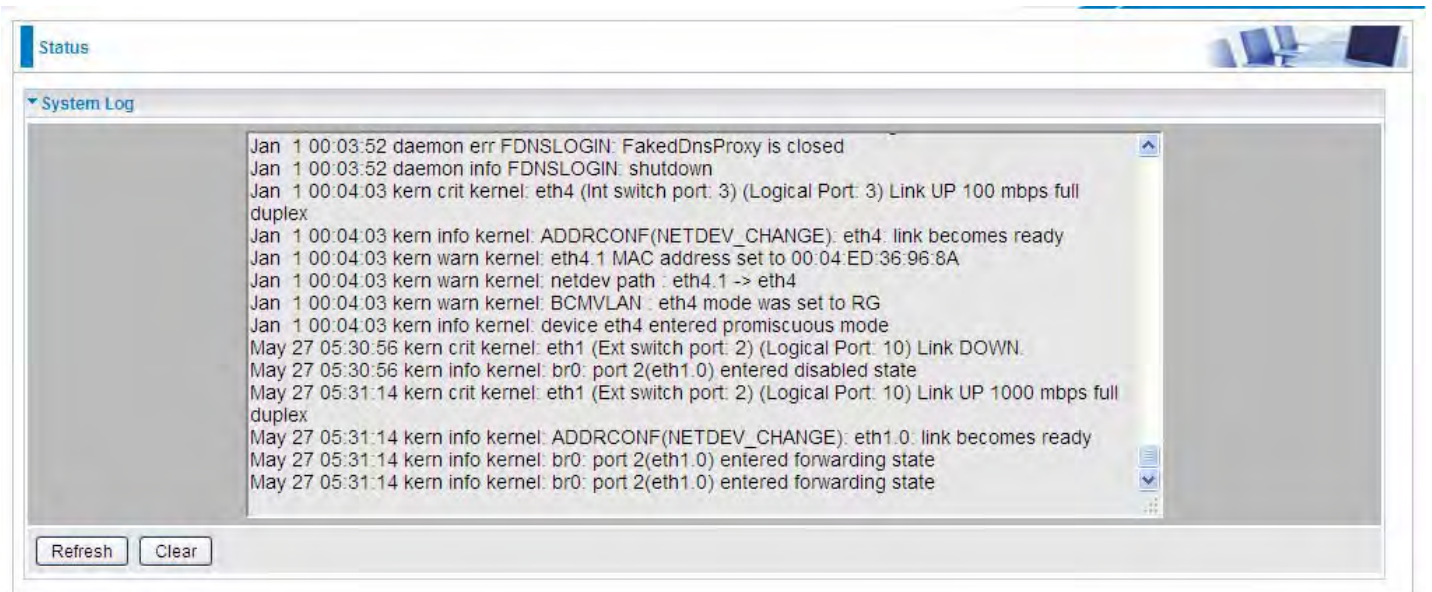
Remote Gateway: The IP of remote gateway.

Refresh: Click this button to refresh the connection status.

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 [Configure Log](#) section.

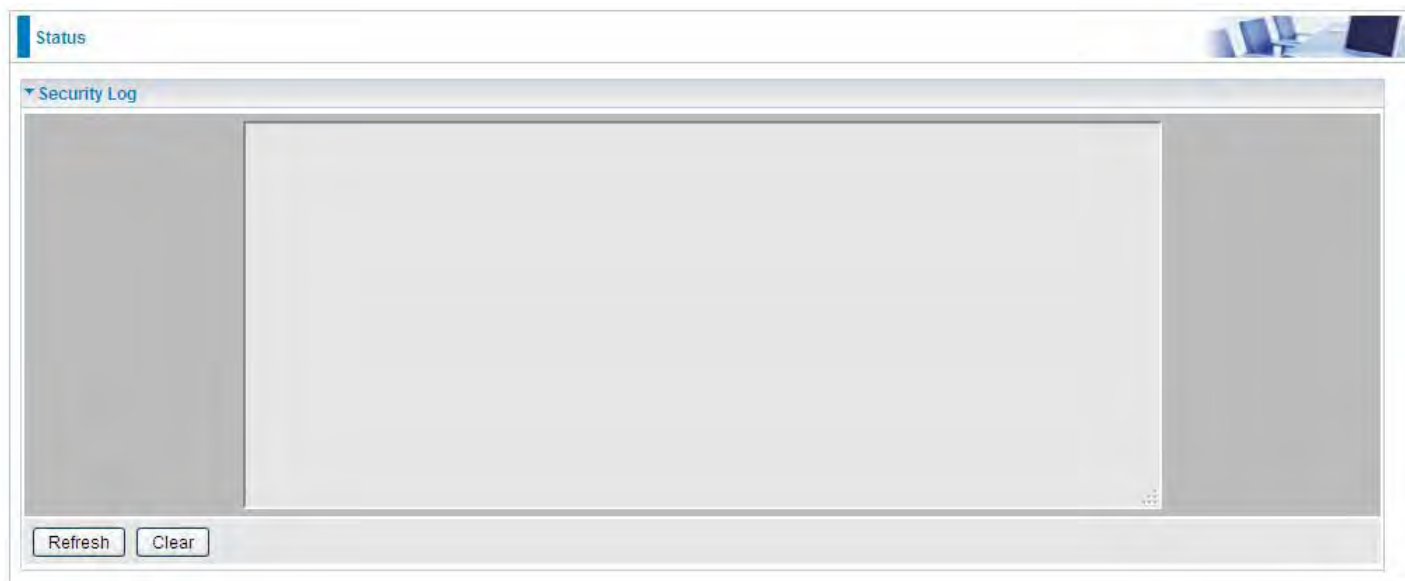


Refresh: Click to update the system log.

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 [IP Filtering Outgoing](#), [IP Filtering Incoming](#), [URL Filter](#) 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.



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

Type

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

WAN Interface (WAN > Wireless)

WAN Service

Type

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

Static

IPv6 Address

Static

IP Address

MTU

1492

Continue

If the DSL 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-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)

Parameters

Band

5GHz (w10)

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)

Parameters

Band

2.4GHz (w11)

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.

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

WAN Interface (WAN > Wireless)

WAN Service

Type

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

MTU

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)

Parameters

Band

5GHz (w/0)

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)

Parameters

Band

2.4GHz (w/1)

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

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
▾ 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

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

The screenshot displays the 'Configuration' window for the LAN settings. The 'LAN' section is expanded, showing a list of parameters. The 'Group Name' is set to 'Default'. The 'IP Address' is 192.168.1.254, and the 'Subnet Mask' is 255.255.255.0. 'IGMP Snooping' is enabled, with 'Blocking Mode' selected. 'IGMP LAN to LAN Multicast' is disabled. 'LAN side firewall' is disabled. The 'DHCP Server' is enabled, with a start IP of 192.168.1.100 and an end IP of 192.168.1.199. The 'Leased Time' is 24 hours. 'Option 66' is disabled. 'Use Router's setting as DNS Server' is enabled. The 'Static IP Lease List' table is empty. The 'IP Alias' section is also visible, with 'Enable' unchecked.

Host Label	MAC Address	IP Address	Remove	Edit
<button>Add</button>				

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:

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **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 [IP Filtering Incoming](#) 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.

Disable

DHCP Server	
DHCP Server	Disable

Disable the DHCP Server function.

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.

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

IP Address

Subnet Mask

☐ Enable

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.

IPv6 Autoconfig

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 auto-configuration 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 COMPRESSION "::". Please enter the complete information.
For example: Please enter "0:0:0:2" instead of "::2".

Group Name: Default

Static LAN IPv6 Address Configuration
Interface Address / Prefix Length:

IPv6 LAN Applications

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

ULA Prefix Advertisement: ☐ Enable

RADVD Type: ☒ Randomly Generate ☐ Statically Configure

Prefix:

Preferred Life Time: -1

Valid Life Time: -1

MLD Snooping: ☒ Enable

MLD Snooping Mode: ☐ 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.

- ① 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.

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **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 and Stateful IPv6 address Configuration

Stateless: Two methods can be carried.

① With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	☐ Enable
Issue 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.

② 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.

① 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.

① 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

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.)

Configuration

Interface Grouping

Groups Isolation

Enable

Apply

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	P1	
			P2	
			P3	
			P4	
			P5/EWAN	
			wlan-ap-2.4g	
		wlan-ap-5g		

Add

Remove

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 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.
IMPORTANT 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.

Group Name

Grouped WAN Interfaces

Available WAN Interfaces

pppoe_0_8_35/ppp0.1

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.

70

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 can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P1	
			P3	
			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 can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P1	
			P3	
			P4	
			P5/EWAN	
			wlan-ap-2.4g	
			wlan-ap-5g	
test	☒	ppp0.1	P2	

Add

Remove

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.

LAN VLAN Setting

When LAN VLAN is opened on a LAN port, outgoing packets from the port will be tagged with the specific VLAN ID user set.



Configuration

LAN VLAN Setting

Parameters

Note: Change VLAN parameter may affect interface grouping which grouped with this vlan interface. Therefore, please check your settings on interface grouping after modification done here.

LAN Port: P1

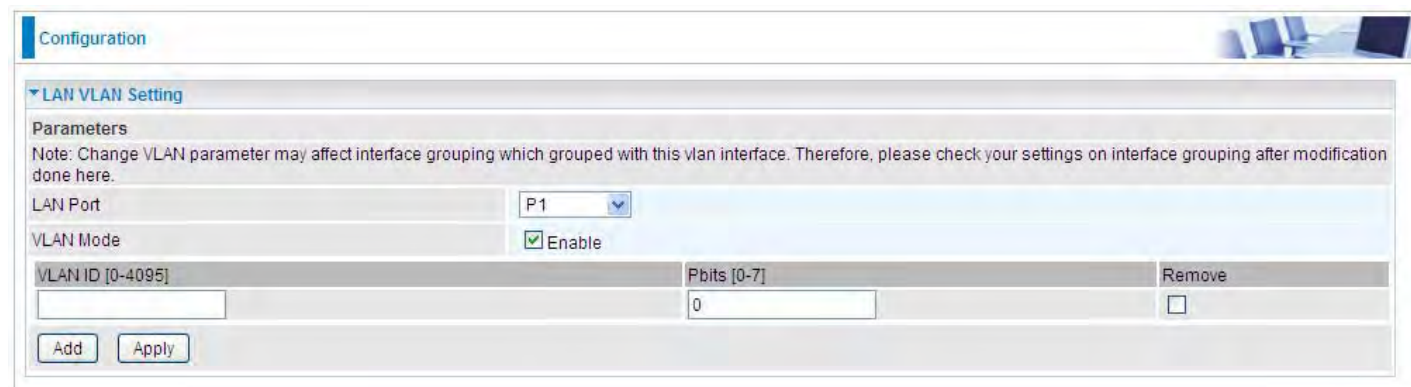
VLAN Mode: ☐ Enable

VLAN ID [1-4094]	Pbits [0-7]	Remove
------------------	-------------	--------

Add Apply

LAN Port: Select the LAN port users want to set LAN VLAN.

VLAN Mode: Check if to enable LAN VLAN for the selected port.



Configuration

LAN VLAN Setting

Parameters

Note: Change VLAN parameter may affect interface grouping which grouped with this vlan interface. Therefore, please check your settings on interface grouping after modification done here.

LAN Port: P1

VLAN Mode: ☒ Enable

VLAN ID [0-4095]	Pbits [0-7]	Remove
	0	☐

Add Apply

Click Add to set the VLAN ID, Pbits for the port.

VLAN ID: a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 1-4094

Pbits: 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).

Eth Port Control

Eth port control features the control of Ethernet port working patterns like Max Bit Rate and Duplex Mode.

Configuration

Eth Port Control

Parameters

Eth Port

Max Bit Rate

Duplex Mode

Apply

Edit	Eth Port	Status	Max Bit Rate	Duplex Mode
☐	P1	Down	Auto	Auto
☐	P2	Down	Auto	Auto
☐	P3	Down	Auto	Auto
☐	P4	Down	Auto	Auto
☐	P5/EWAN	Down	Auto	Auto

Select to change the port working patterns in the Edit vertical column.

Eth Port: Select the port, P1-P5/EWAN (P5 can server as a EWAN port.)

Max Bit Rate: Manually specify the max bit rate for the Ethernet port, 10 or 100Mbps.

Duplex Mode: Manually specify the duplex mode for the Ethernet port, half or full duplex.

Press **Apply** to save the changes to the port.

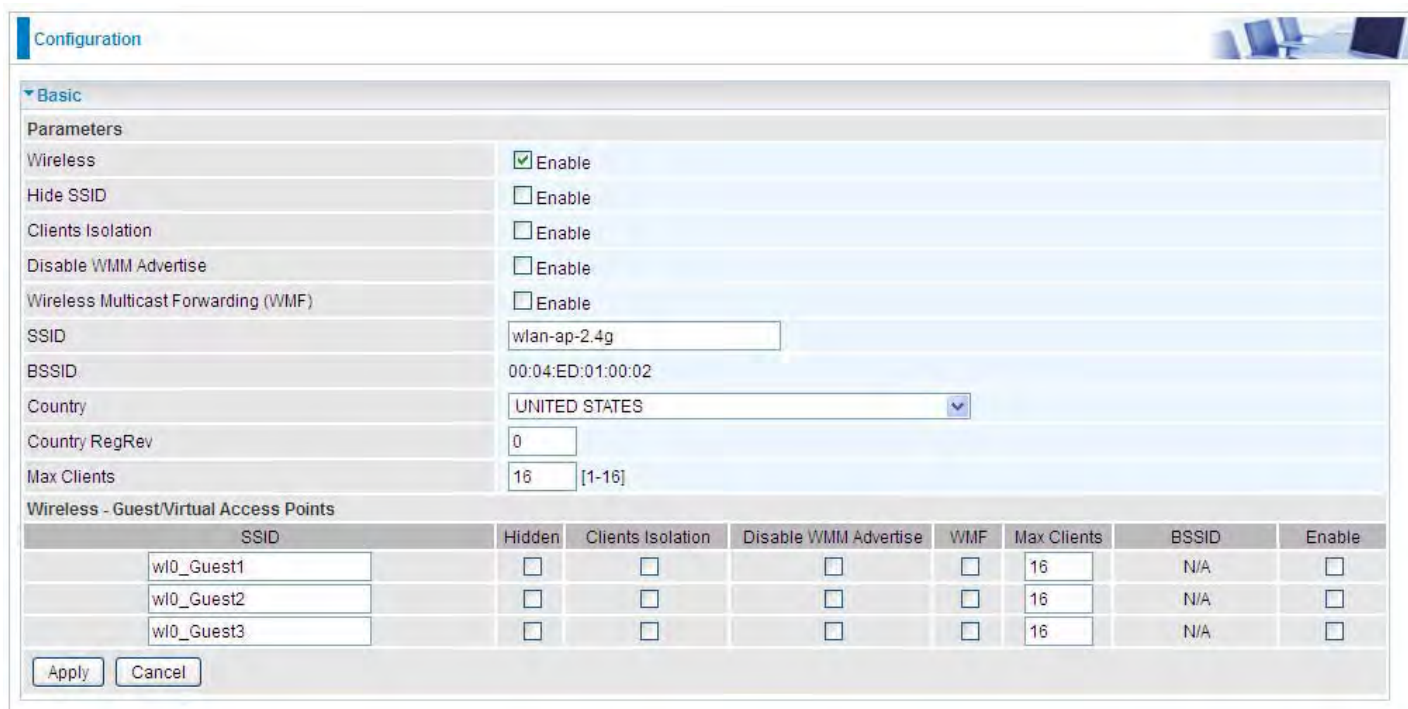
Wireless 5G(wl0) & 2.4G(Wl1)

BiPAC 8700AX-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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_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 built-in to the router's wireless interface. It is case sensitive and must not exceed 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

ApplyCancel

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

① 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.

① Shared

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

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.

① 802.1x

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.

① WPA2

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	0.0.0.0
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.

① 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

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.

① 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	0.0.0.0
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.

① 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

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.

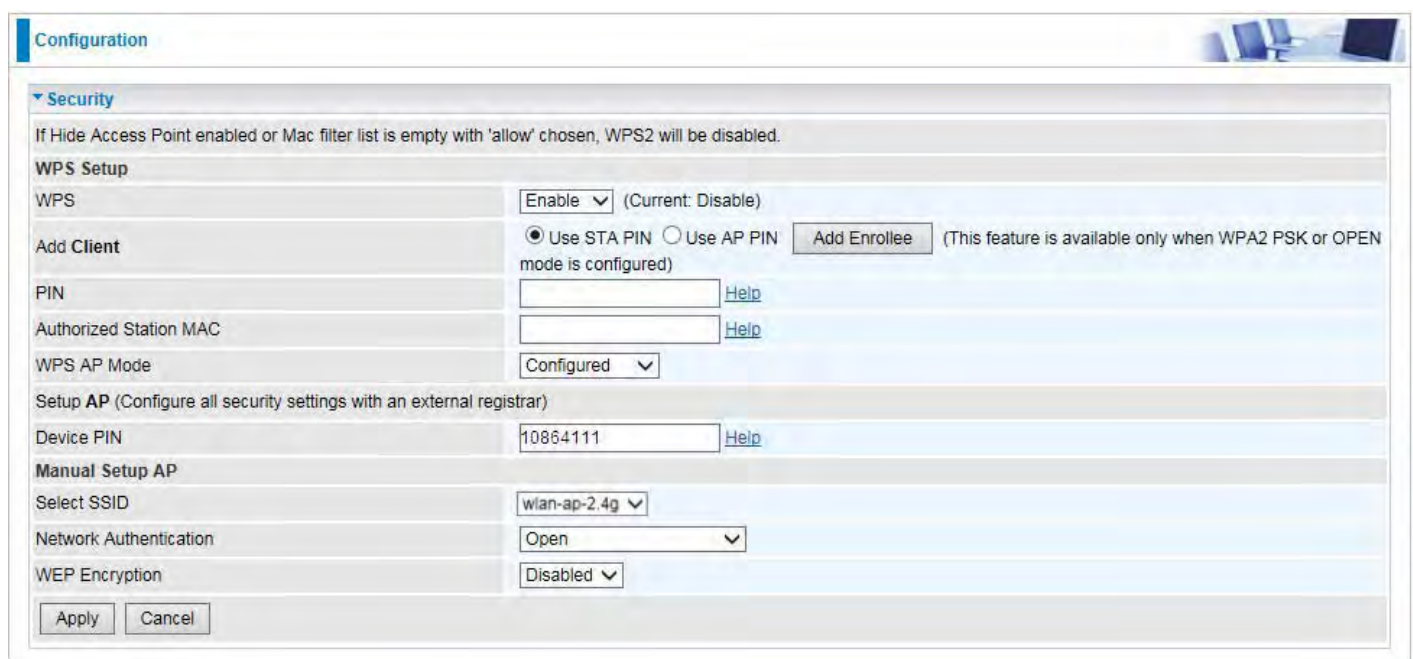
WPS Setup

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:

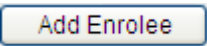
- 1) WPS feature is only available when in WPA2 PSK or OPEN mode in security settings.
- 2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select “Configured” in the WPS AP Mode below, and default WPS AP Mode is “Configured”. When AP is configured as Enrollee, the WPS AP Mode below should be changed to “Unconfigured”. Follow the following steps.

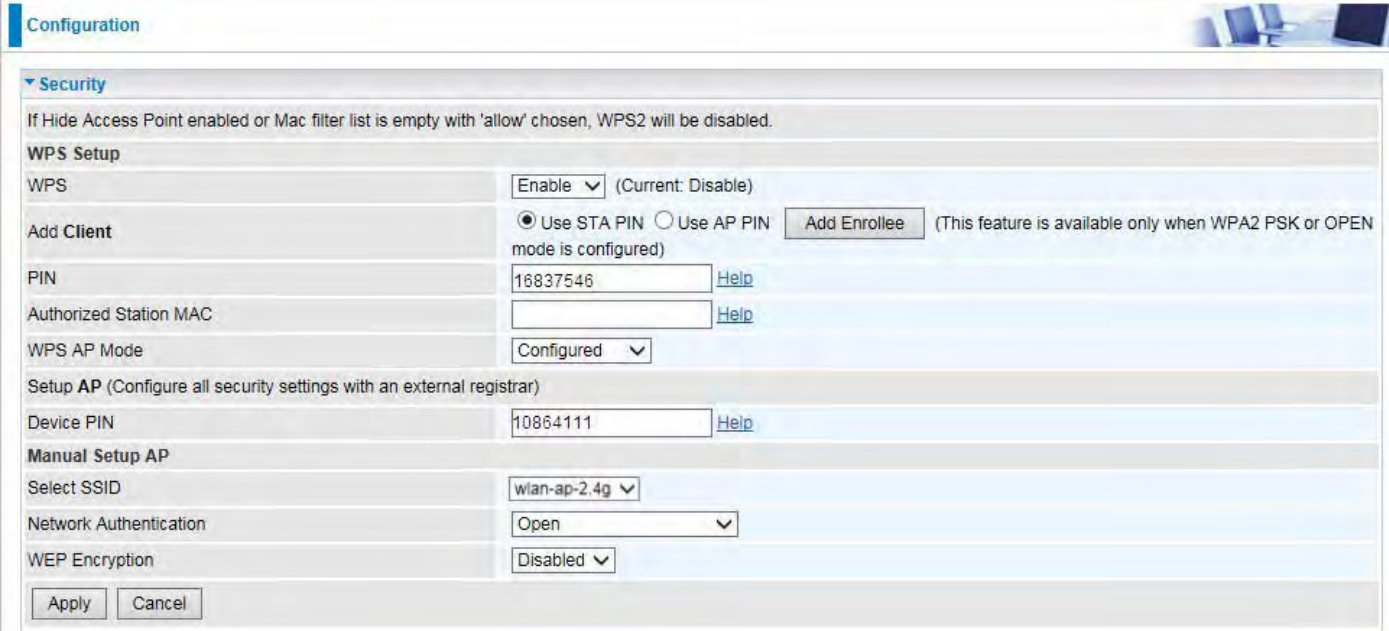


The screenshot shows a web-based configuration interface for WPS (Wi-Fi Protected Setup). The page is titled "Configuration" and has a "Security" tab selected. A warning message states: "If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled." The "WPS Setup" section includes a "WPS" dropdown menu set to "Enable" (Current: Disable). Below this are radio buttons for "Use STA PIN" (selected) and "Use AP PIN", with an "Add Enrollee" button and a note: "(This feature is available only when WPA2 PSK or OPEN mode is configured)". There are input fields for "PIN" and "Authorized Station MAC", each with a "Help" link. The "WPS AP Mode" dropdown is set to "Configured". The "Setup AP (Configure all security settings with an external registrar)" section includes a "Device PIN" input field with the value "10864111" and a "Help" link. The "Manual Setup AP" section includes a "Select SSID" dropdown set to "wlan-ap-2.4g", a "Network Authentication" dropdown set to "Open", and a "WEP Encryption" dropdown set to "Disabled". At the bottom are "Apply" and "Cancel" buttons.

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.
3. Click .



Configuration

Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS Enable (Current: Disable)

Add Client Use STA PIN Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN 16837546 [Help](#)

Authorized Station MAC [Help](#)

WPS AP Mode Configured

Setup AP (Configure all security settings with an external registrar)

Device PIN 10864111 [Help](#)

Manual Setup AP

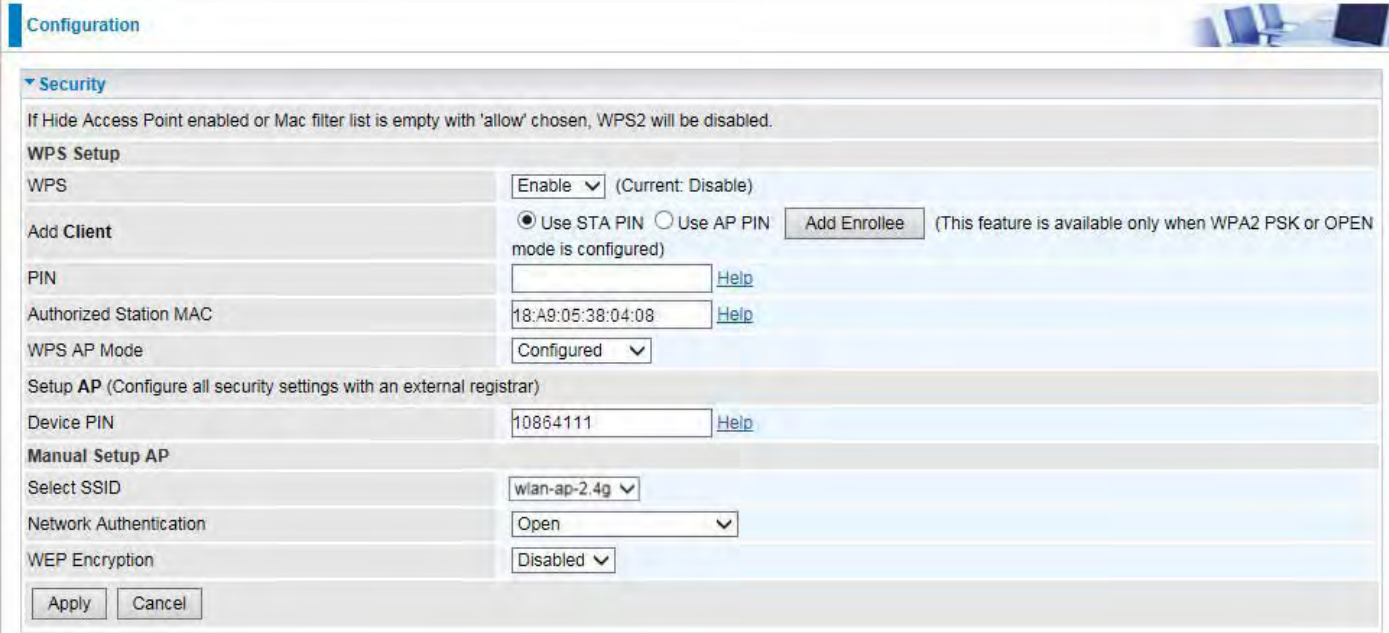
Select SSID wlan-ap-2.4g

Network Authentication Open

WEP Encryption Disabled

Apply Cancel

(Station PIN)



Configuration

Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS Enable (Current: Disable)

Add Client Use STA PIN Use 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 [Help](#)

WPS AP Mode Configured

Setup AP (Configure all security settings with an external registrar)

Device PIN 10864111 [Help](#)

Manual Setup AP

Select SSID wlan-ap-2.4g

Network Authentication Open

WEP Encryption Disabled

Apply Cancel

(Station MAC)

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

- 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.

The screenshot displays the Ralink WPS utility interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main area is divided into several sections:

- WPS AP List:** A table showing available APs. The selected AP is "wlan-ap-2.4g" with ID "00-04-ED-00-00-01".
- WPS Profile List:** A section for managing WPS profiles.
- WPS Configuration:** Includes checkboxes for "WPS Associate IE" and "WPS Probe IE", and a "Progress" bar showing 0%.
- Buttons:** A vertical column of buttons on the right side, including Rescan, Information, Pin Code (with a text field showing "16837546" and a Renew button), Config Mode (set to Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.
- Status and Link Quality:** A section showing "Status >> Disconnected", "Link Quality >> 0%", "Signal Strength 1 >> 0%", "Signal Strength 2 >> 0%", and "Noise Strength >> 0%".
- Transmit and Receive Performance:** A section showing "Transmit" and "Receive" metrics, including Link Speed (Max) and Throughput (0.000 Kbps).
- HT (High Throughput) Section:** A section showing HT-related metrics, including BW (n/a), SNR0 (n/a), GI (n/a), MCS (n/a), and SNR1 (n/a).

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

Profile

Network

Advanced

Statistics

WMM

WPS

Radio On/Off

About

WPS AP List

ID :	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

WPS Profile List

wlan-ap

PIN

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Rescan

Information

Pin Code

16837546

Renew

Config Mode

Enrollee

Detail

Connect

Rotate

Disconnect

Export Profile

Delete

Status >> wlan-ap-2.4g <--> 00-04-ED-01-00-01

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel 3

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 192.168.1.1

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

HT

BW >> 40

GI >> long

MCS >> 15

SNR0 >> 19

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 64%

Signal Strength 2 >> 34%

Noise Strength >> 26%

Transmit

Link Speed >> 270.0 Mbps

Throughput >> 5.600 Kbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 81.608 Kbps

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 list is empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Enable (Current: Disable)

Add Client

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

Setup AP (Configure all security settings with an external registrar)

Device PIN

10864111

Help

Manual Setup AP

Select SSID

wlan-ap-2.4g

Network Authentication

Open

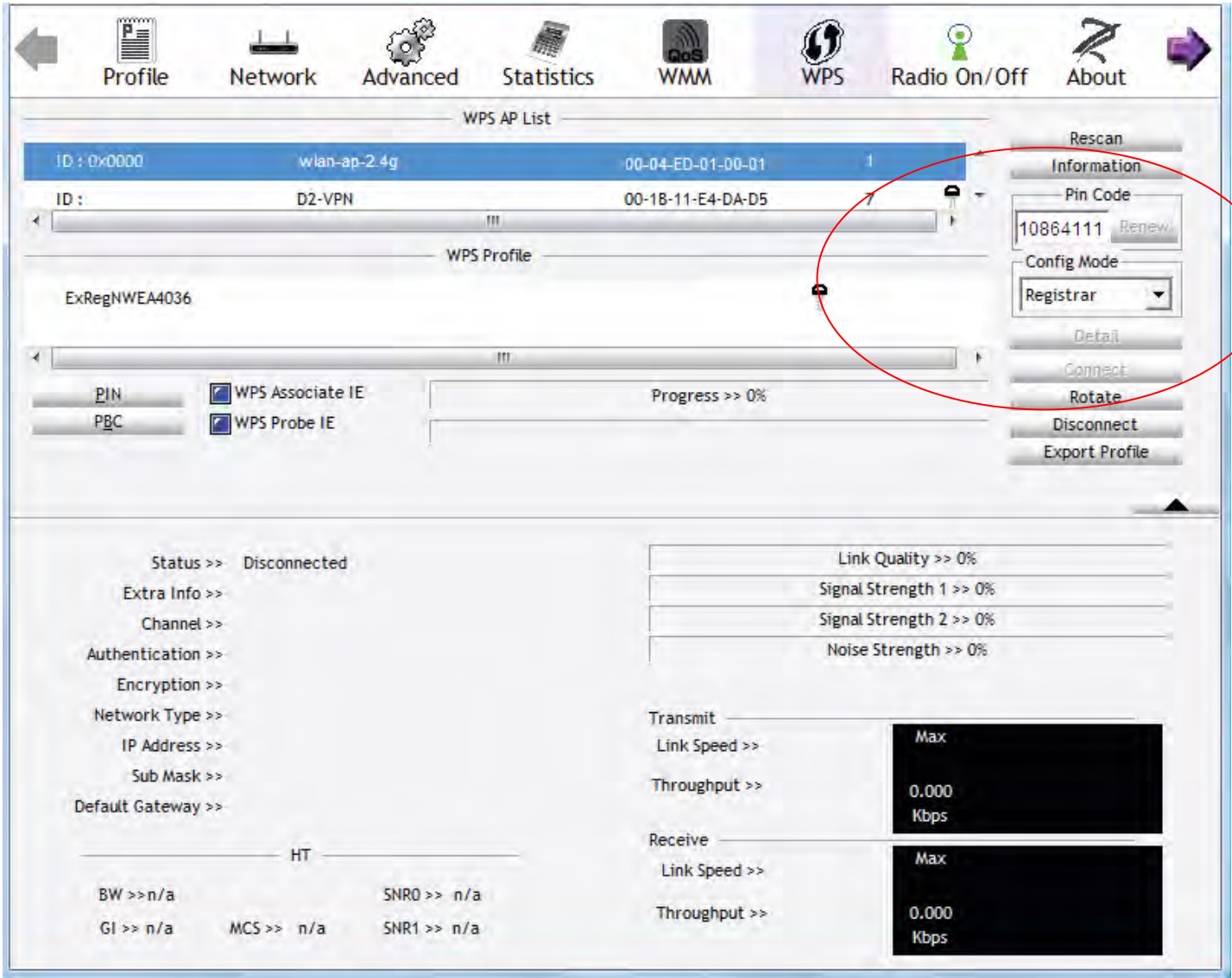
WEP Encryption

Disabled

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.



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

Profile

Network

Advanced

Statistics

WMM

WPS

Radio On/Off

About

WPS AP List

ID :	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

WPS Profile List

ExRegNWEA4036

6229909

PIN

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress 100%

PIN - Get WPS profile successfully.

Rescan

Information

Pin Code

10864111

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

Status >> wlan-ap-2.4g <-> 00-04-ED-01-00-01

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <-> 2412 MHz; central channel : 3

Authentication >> WPA2-PSK

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.1.1

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

HT

BW >> 40

GI >> long

MCS >> 14

SNR0 >> 20

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 65%

Signal Strength 2 >> 39%

Noise Strength >> 26%

Transmit

Link Speed >> 243.0 Mbps

Throughput >> 0.000 Kbps

Receive

Link Speed >> 40.5 Mbps

Throughput >> 98.612 Kbps

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 empty, WPS will be disabled.

MAC Address	Remove	Edit
-------------	--------	------

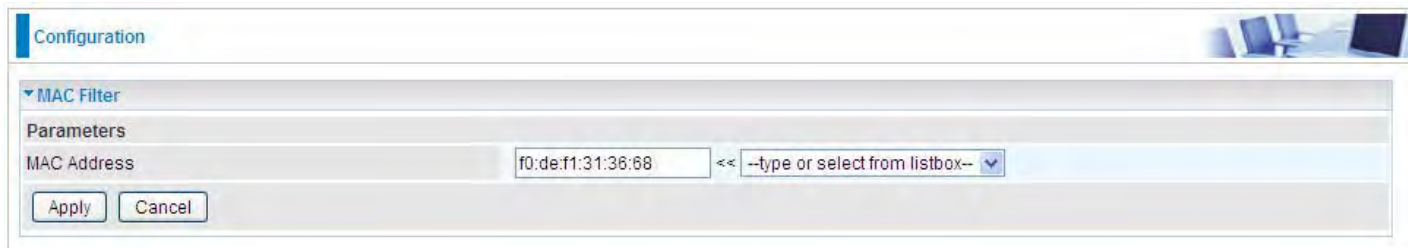
Add Remove

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

MAC Restrict Mode:

- ❶ **Disable:** disable the MAC Filter function.
- ❶ **Allow:** allow the hosts with the following listed MACs to access the wireless network.
- ❶ **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 or select from listbox--

Apply Cancel

MAC Address: enter the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

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 *: ☐ Disable ☒ Allow ☐ 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 wireless bridge restriction.
Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction.
Only those bridges selected in Remote Bridges will be granted access.

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	BSSID
☐	wlan-ap	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

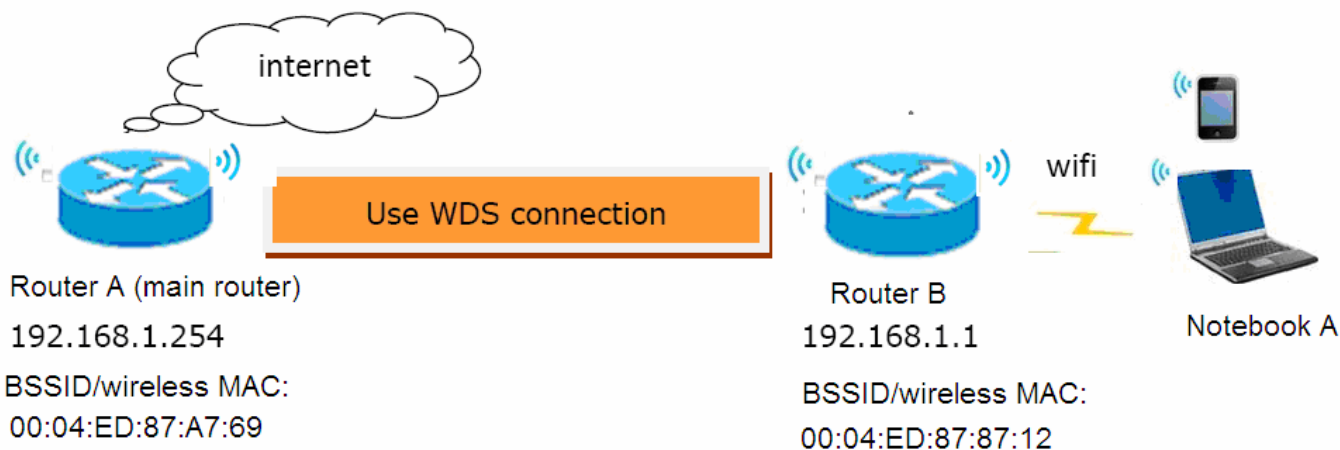
Before setting up WDS:

- 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.

The screenshot shows the 'Configuration' page of Router A, specifically the 'LAN' section. The 'Parameters' tab is selected. The 'DHCP Server' is enabled. The 'Start IP Address' is 192.168.1.100 and the 'End IP Address' is 192.168.1.199. The 'Leased Time (hour)' is 24. The 'Option 66' is disabled. The 'Use Router's setting as DNS Server' is checked. The 'Primary DNS server' and 'Secondary DNS server' fields are empty. The 'Static IP Lease List' table is empty. The 'IP Alias' section is also empty. The 'Apply' and 'Cancel' buttons are at the bottom.

Host Label	MAC Address	IP Address	Remove	Edit
------------	-------------	------------	--------	------

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

Status

WAN

Wan Info

Interface	Description	Type	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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

00:04:ED:87:A7:69

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

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 empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Disable

(Current: Disable)

Manual Setup AP

Select SSID

test-ap-2.4g

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

Apply

Cancel

91

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	
Channel	1	Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15	minutes
802.11n/EWC	Auto	
Bandwidth	20MHz / 40MHz	Current: 40MHz
Control Sideband	Lower	Current: Lower
802.11n Rate	Auto	
802.11n Protection	Auto	
Support 802.11n Client Only	Off	
RIFS Advertisement	Auto	
OBSS Coexistence	Disable	
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	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	
Transmit Power	100%	
WMM(Wi-Fi Multimedia)	Enable	
WMM No Acknowledgement	Disable	
WMM APSD	Enable	

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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

(Router B's wireless basic configuration)

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enabled

Remote Bridges MAC Address

Apply

Refresh

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enabled

Remote Bridges MAC Address

00:04:ED:87:87:12

Apply

Refresh

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

IP Address

192.168.1.1

Subnet Mask

255.255.255.0

IGMP Snooping

☒ Enable

IGMP Snooping Mode

☐ 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

Disable

DHCP Server

Disable

IP Alias

☐ Enable

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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advartise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

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 Advartise	WMF	Max Clients	BSSID	Enable
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

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 empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Disable

(Current: Disable)

Manual Setup AP

Select SSID

test-ap-2.4g

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

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

Current: 1 (interference: acceptable)

Scan Used Channel

Auto Channel Timer

15

minutes

802.11n/EWC

Auto

Bandwidth

20MHz / 40MHz

Current: 40MHz

Control Sideband

Lower

Current: Lower

802.11n Rate

Auto

802.11n Protection

Auto

Support 802.11n Client Only

Off

RIFS Advertisement

Auto

OBSS Coexistence

Disable

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

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

Transmit Power

100%

WMM(Wi-Fi Multimedia)

Enable

WMM No Acknowledgement

Disable

WMM APSD

Enable

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

Basic

Parameters

Wireless

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

00:04:ED:87:A7:69

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

(Router A's wireless basic configuration)

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction.
Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction.
Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable
Enabled(Scan)
Disable

Remote Bridges MAC Address

Apply

Refresh

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction.
Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction.
Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable

Remote Bridges MAC Address

00:04:ED:87:A7:69

x

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

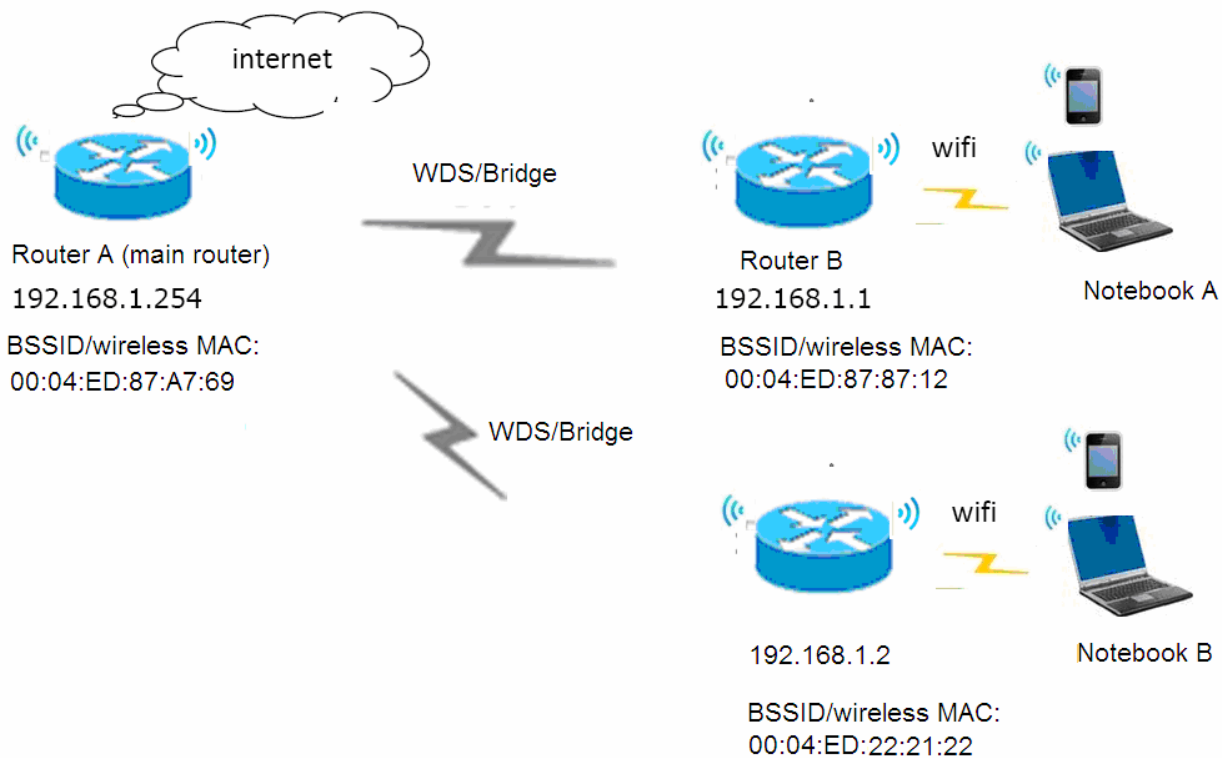
MAC Address	Associated	Authorized	SSID	Interface
00:0C:43:32:46:93	Yes	Yes	test-ap-2.4g	wl0

Refresh

■ 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

LAN

Parameters

Group Name

Default

IP Address

192.168.1.254

Subnet Mask

255.255.255.0

IGMP Snooping

☒ Enable

IGMP Snooping Mode

☐ 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

Enable

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

☐ Enable

IP Alias

☐ Enable

IP Address

Subnet Mask

Apply

Cancel

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

Status

WAN

Wan Info

Interface	Description	Type	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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

00:04:ED:87:A7:69

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

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 empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Disable

(Current: Disable)

Manual Setup AP

Select SSID

test-ap-2.4g

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

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	
Channel	1	Current: 1 (interference: acceptable) Scan Used Channel
Auto Channel Timer	15	minutes
802.11n/EWC	Auto	
Bandwidth	20MHz / 40MHz	Current: 40MHz
Control Sideband	Lower	Current: Lower
802.11n Rate	Auto	
802.11n Protection	Auto	
Support 802.11n Client Only	Off	
RIFS Advertisement	Auto	
OBSS Coexistence	Disable	
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	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	
Transmit Power	100%	
WMM(Wi-Fi Multimedia)	Enable	
WMM No Acknowledgement	Disable	
WMM APSD	Enable	

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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

(Router B's wireless basic configuration)

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable

Remote Bridges MAC Address

Apply

Refresh

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable

Remote Bridges MAC Address

00:04:ED:87:87:12

00:04:ED:22:21:22

Apply

Refresh

WDS Configuration finished for Router A.

101

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

IP Address

192.168.1.1

Subnet Mask

255.255.255.0

IGMP Snooping

☒ Enable

IGMP Snooping Mode

☐ 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

Disable

IP Alias

☐ Enable

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

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advetise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

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 Advetise	WMF	Max Clients	BSSID	Enable
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

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 empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Manual Setup AP

Select SSID

test-ap-2.4g

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

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

Current: 1 (interference: acceptable)

Scan Used Channel

Auto Channel Timer

15

minutes

802.11n/EWC

Auto

Bandwidth

20MHz / 40MHz

Current: 40MHz

Control Sideband

Lower

Current: Lower

802.11n Rate

Auto

802.11n Protection

Auto

Support 802.11n Client Only

Off

RIFS Advertisement

Auto

OBSS Coexistence

Disable

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

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

Transmit Power

100%

WMM(Wi-Fi Multimedia)

Enable

WMM No Acknowledgement

Disable

WMM APSD

Enable

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

Basic

Parameters

Wireless

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

test-ap-2.4g

BSSID

00:04:ED:87:A7:69

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
wl0_Guest1	☐	☐	☐	☐	16	N/A	☐
wl0_Guest2	☐	☐	☐	☐	16	N/A	☐
wl0_Guest3	☐	☐	☐	☐	16	N/A	☐

Apply

Cancel

(Router A's wireless basic configuration)

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction.
Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction.
Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable

Remote Bridges MAC Address

Apply

Refresh

Configuration

Wireless Bridge

Parameters

Select Disabled in Bridge Restrict which disables wireless bridge restriction.
Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction.
Only those bridges selected in Remote Bridges will be granted access.

Bridge Restrict

Enable

Remote Bridges MAC Address

00:04:ED:87:A7:69 x

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
00:0C:43:32:46:93	Yes	Yes	test-ap-2.4g	wl0

Refresh

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 ▼
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	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 ▼
Transmit Power	100% ▼
WMM(Wi-Fi Multimedia)	Enable ▼
WMM No Acknowledgement	Disable ▼
WMM APSD	Enable ▼

Apply Cancel

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™ 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.

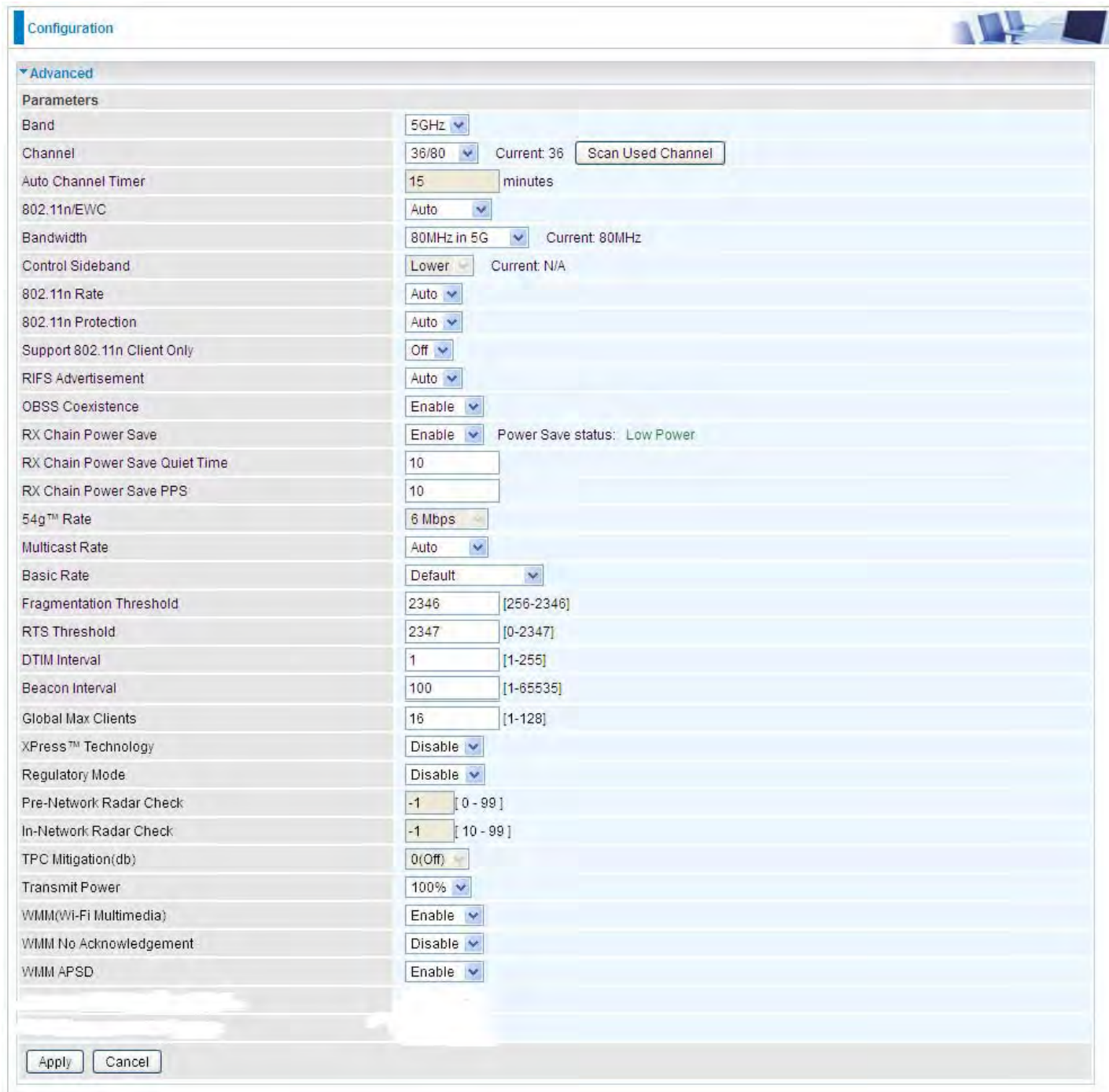
Transmit Power: select the transmitting power of your wireless signal.

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.

– 5GHz Wireless



The screenshot shows a 'Configuration' window with a '5GHz Wireless' section. The 'Advanced' tab is selected, displaying a list of parameters and their current settings. The parameters include Band, Channel, Auto Channel Timer, 802.11n/EWC, Bandwidth, Control Sideband, 802.11n Rate, 802.11n Protection, Support 802.11n Client Only, RIFS Advertisement, OBSS Coexistence, RX Chain Power Save, RX Chain Power Save Quiet Time, RX Chain Power Save PPS, 54g™ Rate, Multicast Rate, Basic Rate, Fragmentation Threshold, RTS Threshold, DTIM Interval, Beacon Interval, Global Max Clients, XPress™ Technology, Regulatory Mode, Pre-Network Radar Check, In-Network Radar Check, TPC Mitigation(db), Transmit Power, WMM(Wi-Fi Multimedia), WMM No Acknowledgement, and WMM APSD. Each parameter has a dropdown menu or input field to select or enter a value. Some parameters also show the current status or value. For example, 'Band' is set to '5GHz', 'Channel' is '36/80', 'Auto Channel Timer' is '15 minutes', '802.11n/EWC' is 'Auto', 'Bandwidth' is '80MHz in 5G', 'Control Sideband' is 'Lower', '802.11n Rate' is 'Auto', '802.11n Protection' is 'Auto', 'Support 802.11n Client Only' is 'Off', 'RIFS Advertisement' is 'Auto', 'OBSS Coexistence' is 'Enable', 'RX Chain Power Save' is 'Enable', 'RX Chain Power Save Quiet Time' is '10', 'RX Chain Power Save PPS' is '10', '54g™ Rate' is '6 Mbps', 'Multicast Rate' is 'Auto', 'Basic Rate' is 'Default', 'Fragmentation Threshold' is '2346', 'RTS Threshold' is '2347', 'DTIM Interval' is '1', 'Beacon Interval' is '100', 'Global Max Clients' is '16', 'XPress™ Technology' is 'Disable', 'Regulatory Mode' is 'Disable', 'Pre-Network Radar Check' is '-1', 'In-Network Radar Check' is '-1', 'TPC Mitigation(db)' is '0(Off)', 'Transmit Power' is '100%', 'WMM(Wi-Fi Multimedia)' is 'Enable', 'WMM No Acknowledgement' is 'Disable', and 'WMM APSD' is 'Enable'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Parameter	Setting	Current
Band	5GHz	
Channel	36/80	36
Auto Channel Timer	15	minutes
802.11n/EWC	Auto	
Bandwidth	80MHz in 5G	80MHz
Control Sideband	Lower	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	

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™ 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.

Station Info

Here you can view information about the wireless clients.

The screenshot shows a web interface for configuring wireless clients. At the top, there is a 'Configuration' tab. Below it, the 'Station Info' section is expanded, showing a table titled 'Associated Stations'. The table has five columns: 'MAC Address', 'Associated', 'Authorized', 'SSID', and 'Interface'. A 'Refresh' button is located below the table.

MAC Address	Associated	Authorized	SSID	Interface
-------------	------------	------------	------	-----------

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](#) .

The screenshot shows the 'Configuration' page with a 'Schedule Control' section. It includes instructions: 'The Wireless schedule only functions whilst Wireless is enabled.' and 'The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.' Below this, there are settings for 'wlan-ap-5g' (Enabled) and three 'Wireless - Guest/Virtual Access Points' (w10_Guest1, w10_Guest2, w10_Guest3, all Disabled). Each has a 'Time Schedule' section with two options: '1. Always On' and '2. check or select from listbox'. Each option includes checkboxes for days of the week and time slots (From and To). An 'Apply' button is at the bottom.

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-1600 offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals.)

This screenshot shows the 'Time Schedule' settings for 'wlan-ap-5g' which is 'Enable'. It shows two intervals: Interval 1 is set to 'check or select from listbox' with days Mon, Tue, Thu, Fri selected and time slots 00:00 to 23:59. Interval 2 is also set to 'check or select from listbox' with days Thu, Fri selected and time slots 00:00 to 23:59. The 'Sun' checkbox is unchecked in both intervals.

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.



The screenshot shows the 'Configuration' page with the 'WAN Service' tab selected. Under the '3G/4G LTE Interface' section, there is a table with the following data:

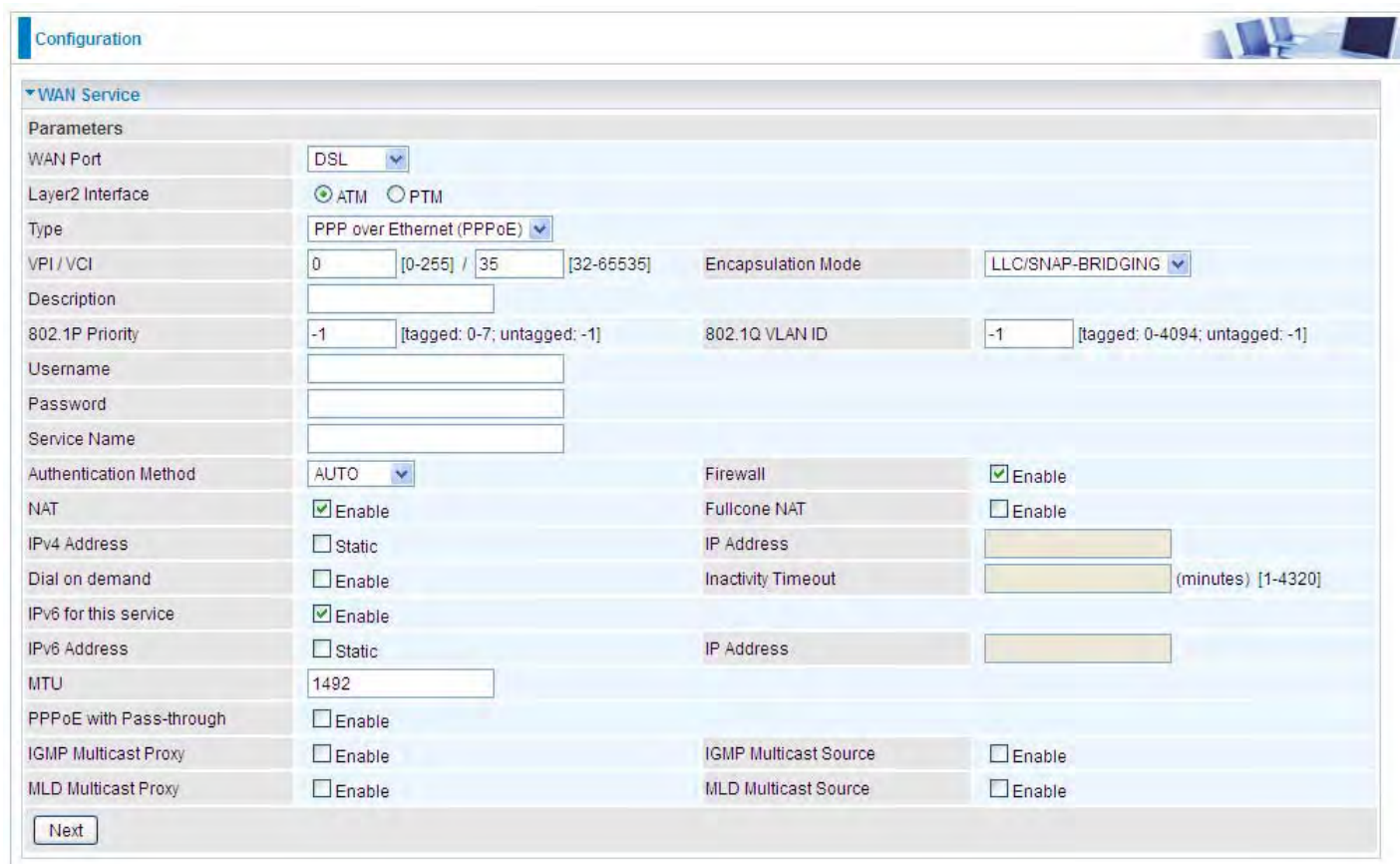
Interface	Description	TEL No.	APN	Username	NAT	Firewall	Dial on demand	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Below the table are 'Add' and 'Remove' buttons.

Click **Add** to add new WAN connections.

① 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.



The screenshot shows the 'Configuration' page with the 'WAN Service' tab selected. The 'Parameters' section is expanded, showing the following configuration options:

- WAN Port: DSL
- Layer2 Interface: ☒ ATM ☐ PTM
- Type: PPP over Ethernet (PPPoE)
- 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]
- 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

At the bottom, there is a 'Next' button.

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

● PPPoE

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

Type: PPP over Ethernet (PPPoE)

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]

Username:

Password:

Service Name:

Authentication Method: AUTO

NAT: ☒ Enable

IPv4 Address: ☐ Static

Dial on demand: ☐ Enable

IPv6 for this service: ☒ Enable

IPv6 Address: ☐ Static

MTU: 1492

PPPoE with Pass-through: ☐ Enable

IGMP Multicast Proxy: ☐ Enable

MLD Multicast Proxy: ☐ Enable

Firewall: ☒ Enable

Fullcone NAT: ☐ Enable

IP Address:

Inactivity Timeout: (minutes) [1-4320]

IP Address:

IGMP Multicast Source: ☐ Enable

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.

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 [IP Filtering Incoming](#) 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 (**I**nternet **G**roup **M**anagement **P**rotocol) 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 (**M**ulticast **L**istener **D**iscovery 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.

The screenshot shows a 'Configuration' window with a 'Default Gateway / DNS' section. It is divided into two main parts: 'Default Gateway' and 'DNS'.
Default Gateway: It has two columns: 'Selected Default Gateway Interfaces' (containing 'ppp0.1') and 'Available Routed WAN Interfaces' (containing '3G0/USB3G0'). Between them are arrows for moving items. Below, 'Selected WAN Interface As The System Default IPv6 Gateway' is set to 'pppoe_0_8_35/ppp0.1'.
DNS: It has two columns: 'Selected DNS Server Interfaces' (containing 'ppp0.1') and 'Available WAN Interfaces' (containing '3G0/USB3G0'). Below these are radio buttons for 'Available WAN Interfaces' (selected), 'Static DNS Address', and 'Parent Controls'. Under 'Available WAN Interfaces', 'WAN Interface selected' is 'pppoe_0_8_35/ppp0.1'. At the bottom, there are fields for 'Primary DNS server' and 'Secondary DNS server'. A note states: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.' Below this, there are radio buttons for 'Available WAN Interfaces' (selected) and 'Static DNS IPv6 Address', followed by fields for 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server'. A 'Next' button is at the bottom left.

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.
- ① **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 [Parental Control Provider](#)).

➤ 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.

Configuration

WAN Service

ATM Interface

Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Mld	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 demand	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Add Remove

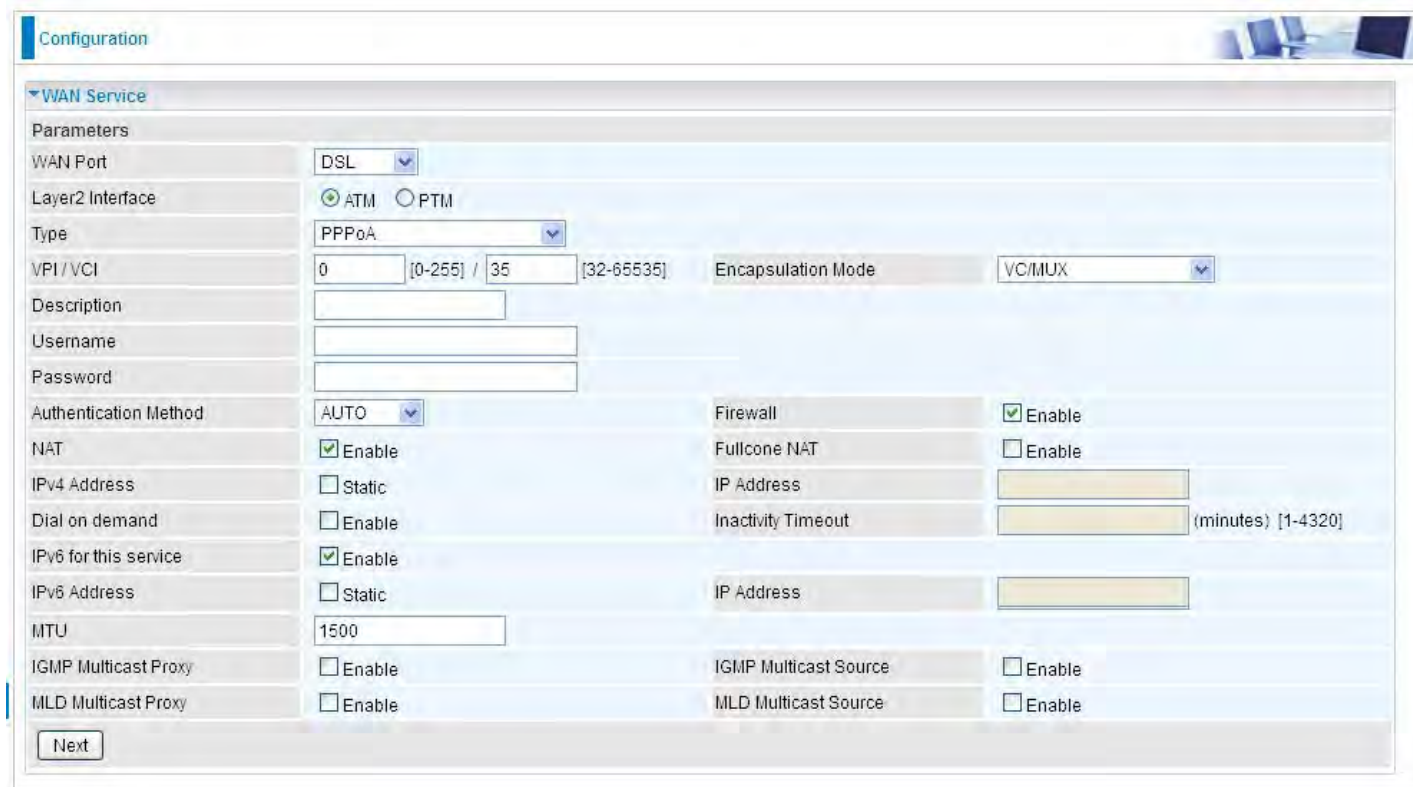
Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).
(IPv4 or IPv6)

Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_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				



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 [IP Filtering Incoming](#) 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.

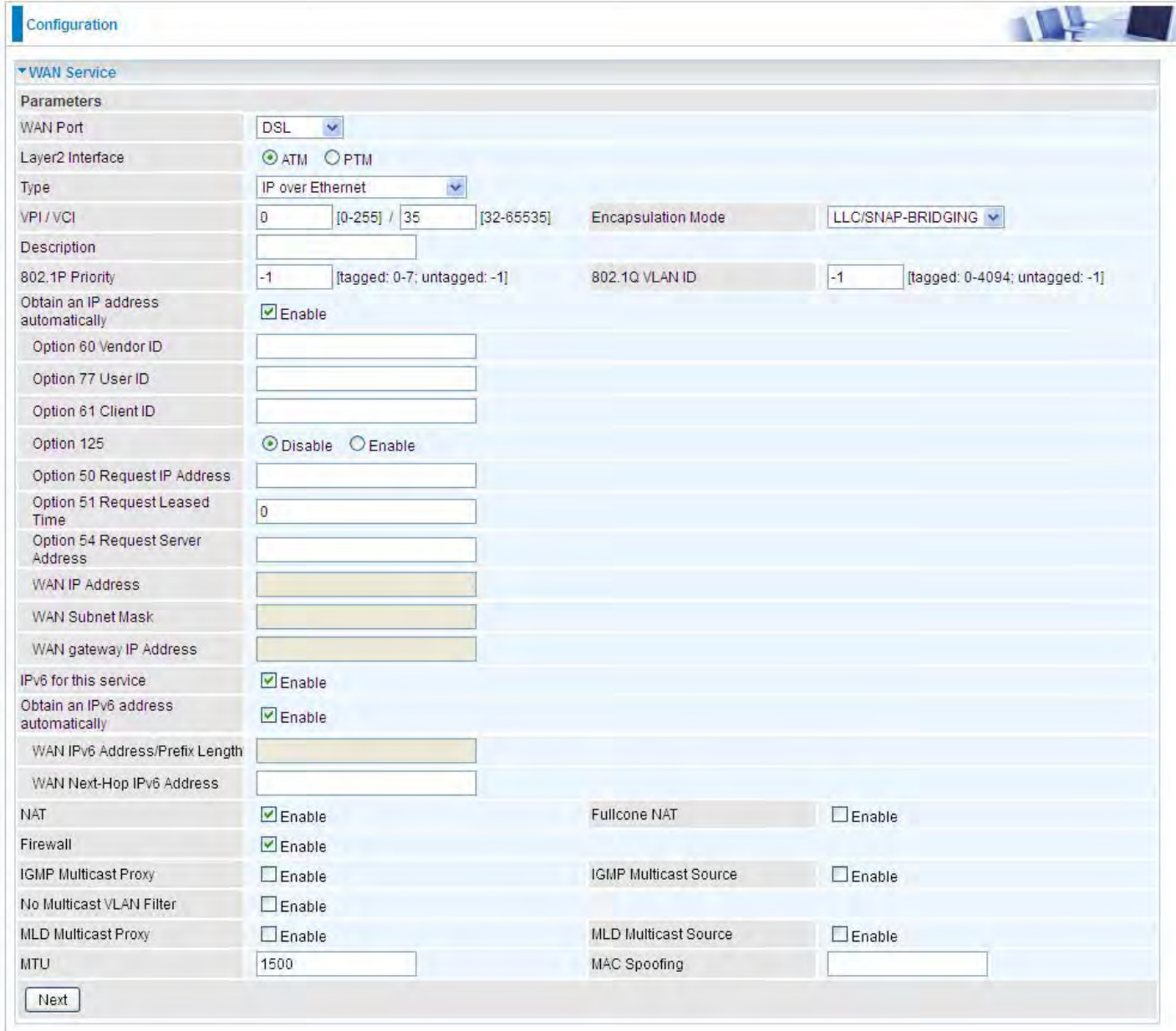
IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

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 (**M**ulticast **L**istener **D**iscovery **P**rotocol) 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

WAN Service

Parameters

WAN Port: DSL

Layer2 Interface: ☒ ATM ☐ PTM

Type: IP over Ethernet

VPI / VCI: 0 [0-255] / 35 [32-85535] 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]

Obtain an IP address automatically: ☒ Enable

Option 60 Vendor ID:

Option 77 User ID:

Option 61 Client ID:

Option 125: ☒ Disable ☐ 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

Firewall: ☒ Enable

IGMP Multicast Proxy: ☐ Enable IGMP Multicast Source: ☐ Enable

No Multicast VLAN Filter: ☐ Enable

MLD Multicast Proxy: ☐ Enable MLD Multicast Source: ☐ Enable

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 [IP Filtering Incoming](#) 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.

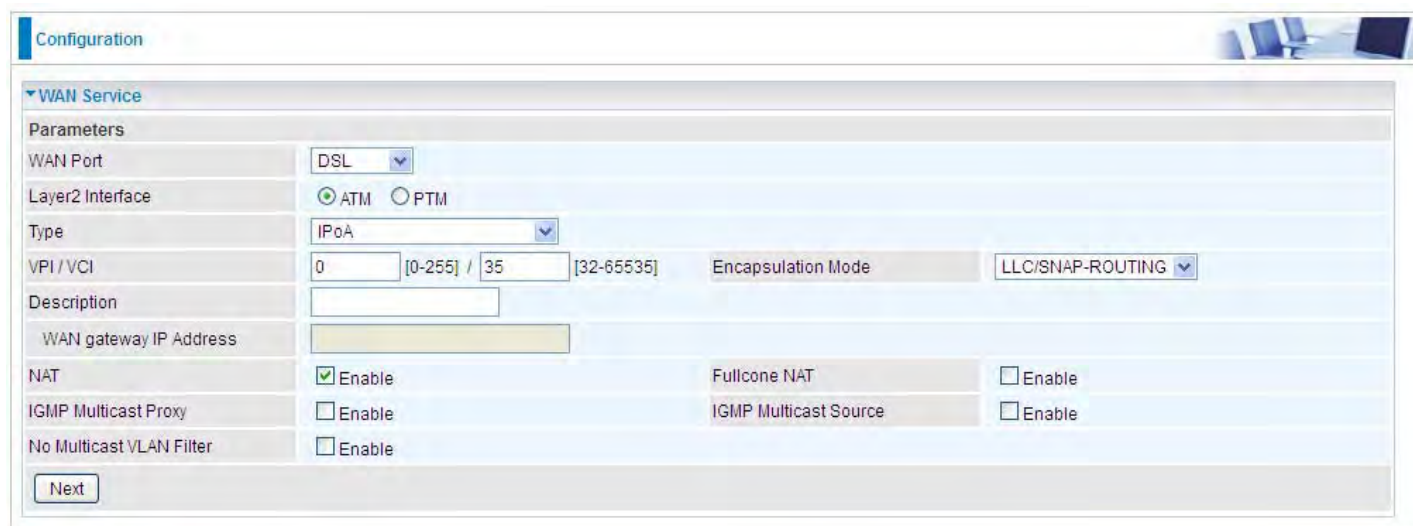
MLD Multicast Proxy: check whether to enable this function. MLD (Multicast Listener Discovery Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1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



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.

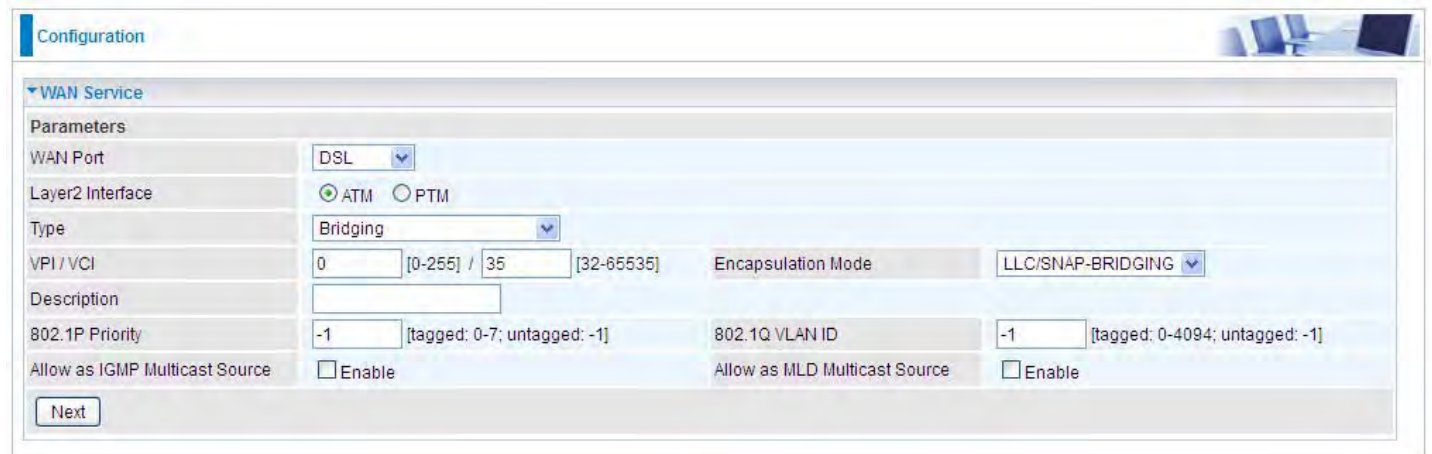
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter 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.



The image shows a 'Configuration' window for a 'WAN Service'. The 'Parameters' section includes the following fields:

- WAN Port:** A dropdown menu set to 'DSL'.
- Layer2 Interface:** Radio buttons for 'ATM' (selected) and 'PTM'.
- Type:** A dropdown menu set to 'Bridging'.
- VPI / VCI:** Two input fields. The first is '0' with a range '[0-255]' and a slash. The second is '35' with a range '[32-65535]'.
- Encapsulation Mode:** A dropdown menu set to 'LLC/SNAP-BRIDGING'.
- Description:** An empty text input field.
- 802.1P Priority:** An input field with '-1' and a range '[tagged: 0-7; untagged: -1]'.
- 802.1Q VLAN ID:** An input field with '-1' and a range '[tagged: 0-4094; untagged: -1]'.
- Allow as IGMP Multicast Source:** A checkbox labeled 'Enable'.
- Allow as MLD Multicast Source:** A checkbox labeled 'Enable'.

A 'Next' button is located at the bottom left of the configuration area.

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.

① Ethernet

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

Configuration

WAN Service

Parameters

WAN Port: Ethernet

Type: 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

NAT: ☒ Enable

IPv4 Address: ☐ Static

Dial on demand: ☐ Enable

IPv6 for this service: ☒ Enable

IPv6 Address: ☐ Static

MTU: 1492

PPPoE with Pass-through: ☐ Enable

IGMP Multicast Proxy: ☐ Enable

MLD Multicast Proxy: ☐ Enable

Firewall: ☒ Enable

Fullcone NAT: ☐ Enable

IP Address:

Inactivity Timeout: (minutes) [1-4320]

IGMP Multicast Source: ☐ Enable

MLD Multicast Source: ☐ Enable

Next

● PPPoE

Configuration

WAN Service

Parameters

WAN Port: Ethernet

Type: 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

NAT: ☒ Enable

IPv4 Address: ☐ Static

Dial on demand: ☐ Enable

IPv6 for this service: ☒ Enable

IPv6 Address: ☐ Static

MTU: 1492

PPPoE with Pass-through: ☐ Enable

IGMP Multicast Proxy: ☐ Enable

MLD Multicast Proxy: ☐ Enable

Firewall: ☒ Enable

Fullcone NAT: ☐ Enable

IP Address:

Inactivity Timeout: (minutes) [1-4320]

IGMP Multicast Source: ☐ Enable

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.

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 [IP Filtering Incoming](#) 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 (**I**nternet **G**roup **M**anagement **P**rotocol) 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 (**M**ulticast **L**istener **D**iscovery **P**rotocol) 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.

The screenshot shows a 'Configuration' window with a 'Default Gateway / DNS' section. It is divided into two main parts: 'Default Gateway' and 'DNS'.

Default Gateway:

- Selected Default Gateway Interfaces:** A list box containing 'ppp0.1'.
- Available Routed WAN Interfaces:** A list box containing '3G0/USB3G0'.
- Between the two list boxes are two buttons: '->' and '<-'.
- Selected WAN Interface As The System Default IPv6 Gateway:** A dropdown menu showing 'pppoe_eth0/ppp0.1'.

DNS:

- DNS Server Interface:** A section with three radio buttons: 'Available WAN Interfaces' (selected), 'Static DNS Address', and 'Parent Controls'.
- Selected DNS Server Interfaces:** A list box containing 'ppp0.1'.
- Available WAN Interfaces:** A list box containing '3G0/USB3G0'.
- Between the two list boxes are two buttons: '->' and '<-'.
- Primary DNS server:** An empty text input field.
- Secondary DNS server:** An empty text input field.
- A note: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.'
- DNS Server Interface:** A section with two radio buttons: 'Available WAN Interfaces' (selected) and 'Static DNS IPv6 Address'.
- WAN Interface selected:** A dropdown menu showing 'pppoe_eth0/ppp0.1'.
- Primary IPv6 DNS server:** An empty text input field.
- Secondary IPv6 DNS server:** An empty text input field.
- At the bottom left is a 'Next' button.

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.
- ① **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 [Parental Control Provider](#)).

➤ 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.

Configuration

WAN Service

ETH Interface

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	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 demand	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Add

Remove

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).

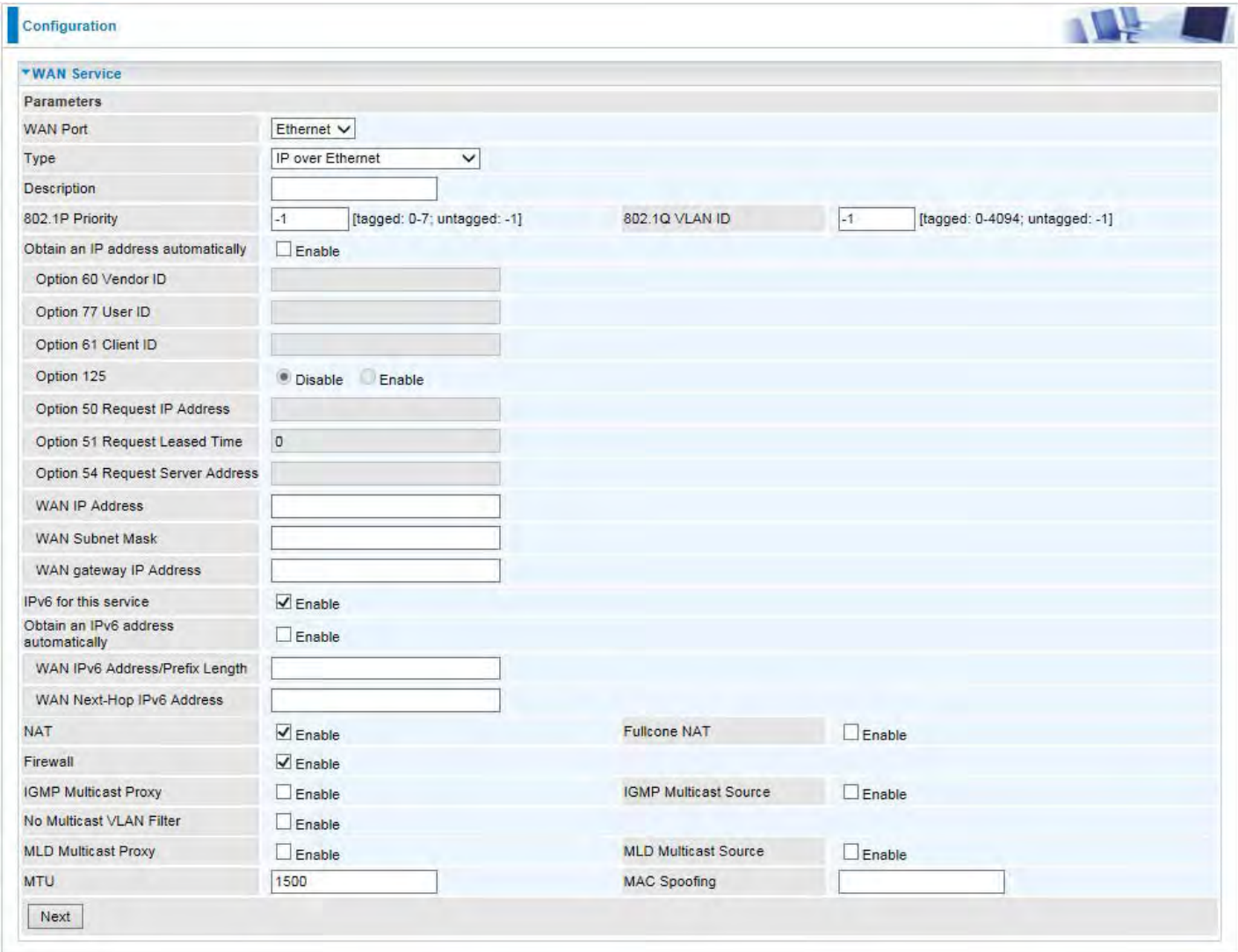
(IPv4 or IPv6)

Status

WAN

Wan Info

Interface	Description	Type	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				



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 [IP Filtering Incoming](#) 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.



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.

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.



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 interface's connectivity.

- ① **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.
- ① **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 interface's connectivity.

- ① **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.



The image shows a 'Configuration' window with a 'DSL' section expanded. It contains a table of parameters with checkboxes for various DSL modes and profiles. A warning message at the bottom states: '*** If DSL line is not ready, related configuration cannot successfully set.' An 'Apply' button is located at the bottom left of the configuration area.

Parameters	
Modulation	☒ G.Dmt ☒ G.lite ☒ T1.413 ☒ ADSL2 ☒ AnnexL ☒ ADSL2+ ☐ AnnexM ☒ VDSL2
Profile	☒ 8a ☒ 8b ☒ 8c ☒ 8d ☒ 12a ☒ 12b ☒ 17a
US0	☒ Enable
Phone line pair	☒ Inner pair ☐ Outer pair
Capability	☒ Bitswap ☐ SRA
PhyR	☐ Upstream ☒ Downstream

*** If DSL line is not ready, related configuration cannot successfully set.

Apply

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.

① Bitswap Enable: Allows bitswaping function.

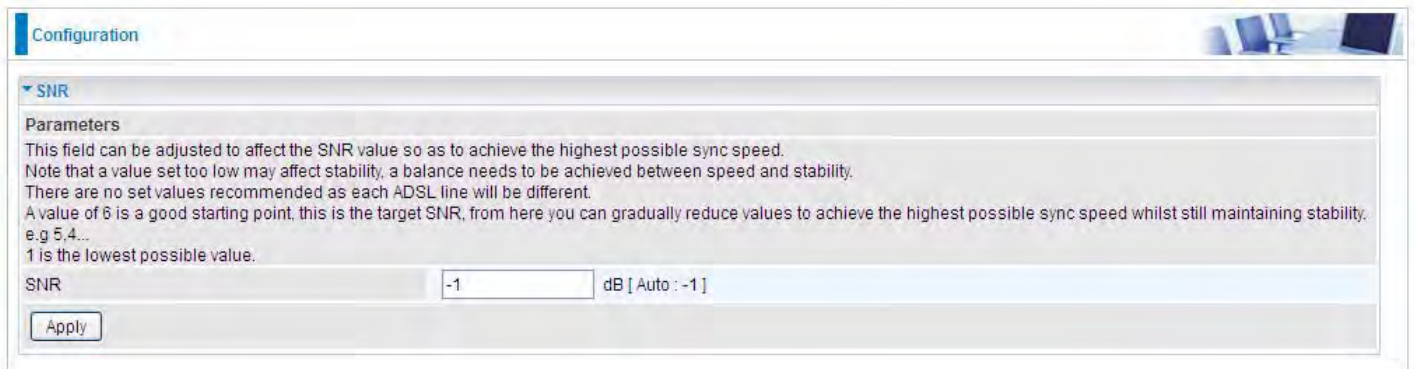
① SRA Enable: Allows seamless rate adaptation.

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.



The screenshot shows a 'Configuration' window with a tab labeled 'SNR'. Under the 'Parameters' section, there is explanatory text: 'This field can be adjusted to affect the SNR value so as to achieve the highest possible sync speed. Note that a value set too low may affect stability, a balance needs to be achieved between speed and stability. There are no set values recommended as each ADSL line will be different. A value of 6 is a good starting point, this is the target SNR, from here you can gradually reduce values to achieve the highest possible sync speed whilst still maintaining stability. e.g 5,4... 1 is the lowest possible value.' Below this text is a text input field labeled 'SNR' containing the value '-1', followed by the unit 'dB [Auto : -1]'. An 'Apply' button is located at the bottom left of the configuration area.

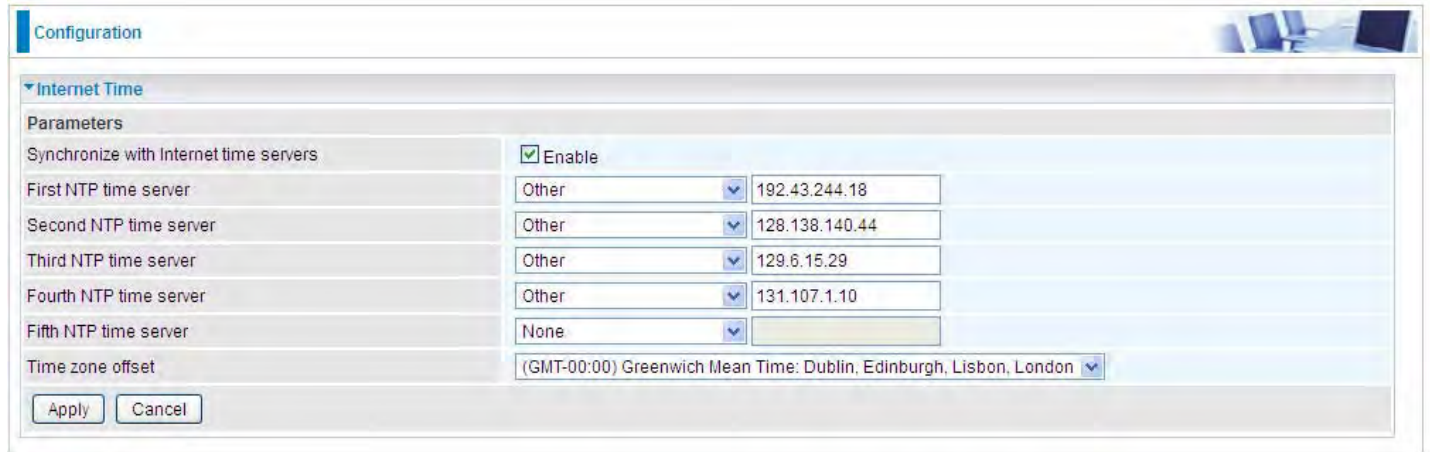
SNR: Change the value to adjust the DSL link rate, more suitable for an advanced user.

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.



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) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Apply Cancel

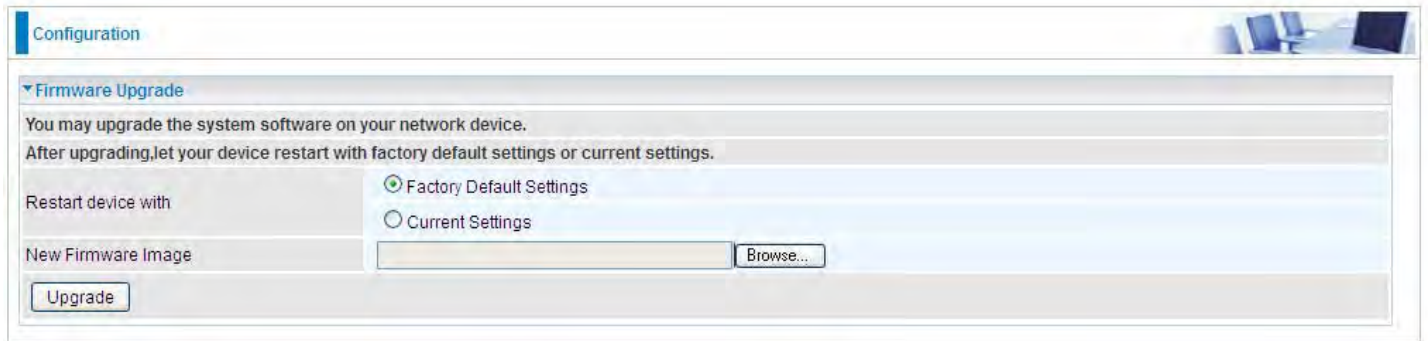
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Firmware Upgrade' section is expanded. The text reads: 'You may upgrade the system software on your network device. After upgrading, let your device restart with factory default settings or current settings.' There are two radio buttons: 'Factory Default Settings' (which is selected) and 'Current Settings'. Below these, there is a field for 'New Firmware Image' with a 'Browse...' button next to it. At the bottom left of the section is an 'Upgrade' button.

Restart device with:

- ① **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- ① **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.



Warning

DO NOT power down the router or interrupt the firmware upgrading 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 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

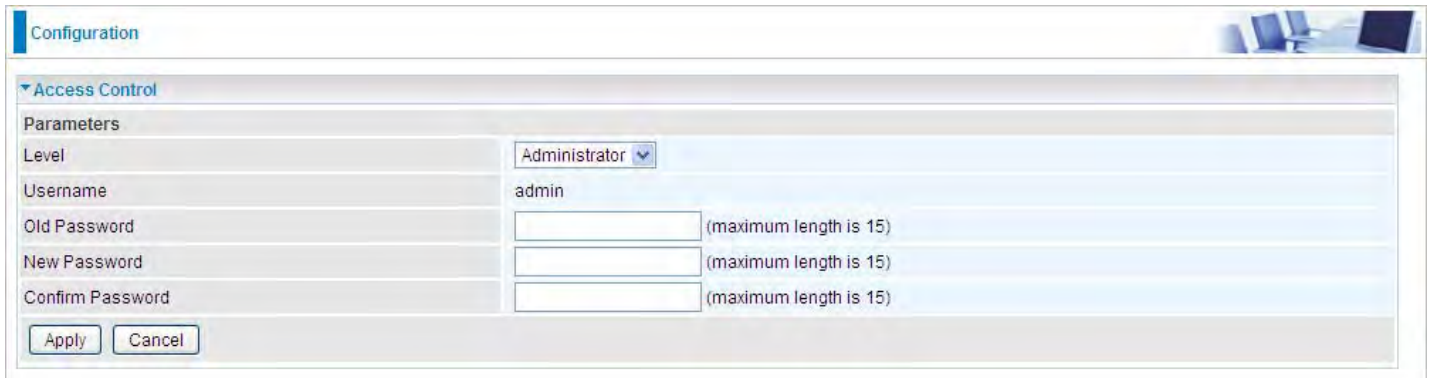
progress...

Do not switch off device during flash update or rebooting.

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.



The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Administrator'. The 'Username' is 'admin'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom are 'Apply' and 'Cancel' buttons.

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.
- ① **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.

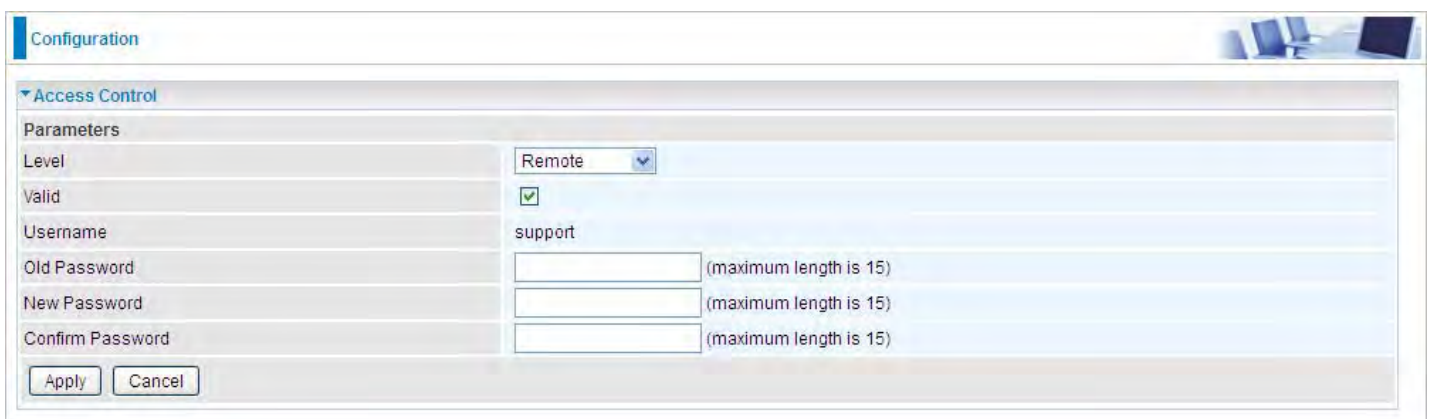
Username: The default username for each user level.

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.



The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Remote'. The 'Valid' checkbox is checked. The 'Username' is 'support'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom are 'Apply' and 'Cancel' buttons.

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

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. 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 (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-1600 offers SMS alert sending clients alert messages when a WAN IP change is detected.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'SMS Alert' is expanded. Inside this section, there is a label 'WAN IP Change Alert' followed by a text input field. Below the input field is an 'Apply' button. The interface has a light blue and white color scheme.

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



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:

- ① **Emergency** = system is unusable
- ① **Alert** = action must be taken immediately
- ① **Critical** = critical conditions
- ① **Error** = error conditions
- ① **Warning** = warning conditions
- ① **Notice** = normal but significant conditions
- ① **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.
- ① **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.
- ① **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-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.



- 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 configured: 16

Username	Home Directory	Remove	Edit
admin	/		

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

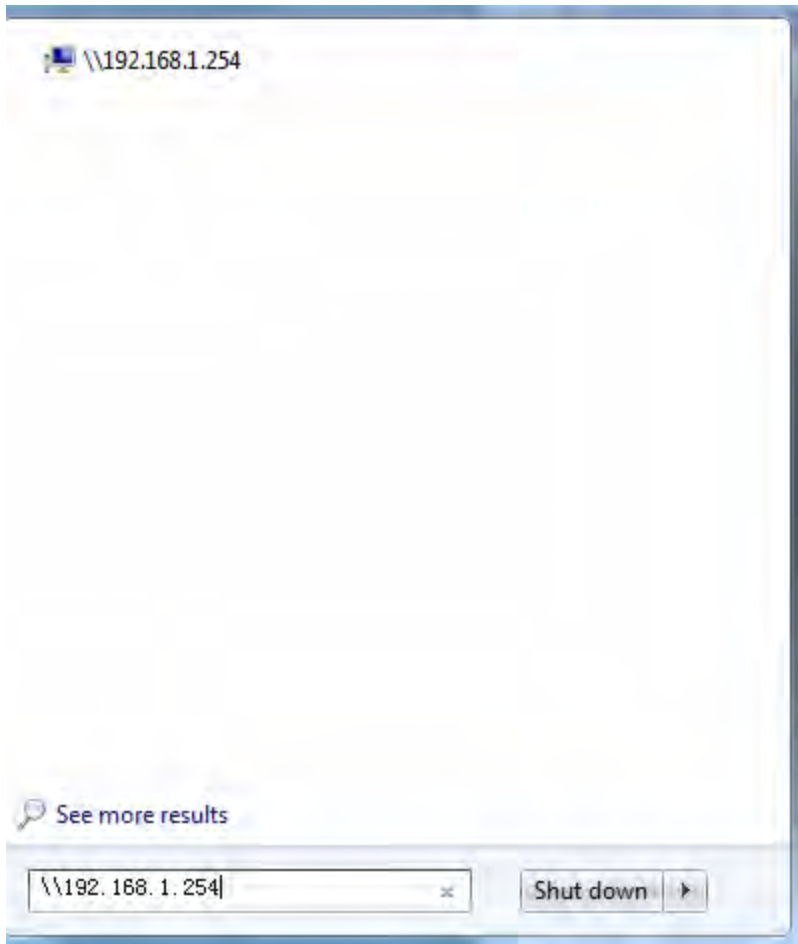
Username	Home Directory	Remove	Edit
admin	/		
test	disk1_1/test	☐	Edit

Add

Remove

Accessing mechanism of Storage:

In your computer, Click **Start** > **Run**, enter [\\192.168.1.254](http://192.168.1.254)

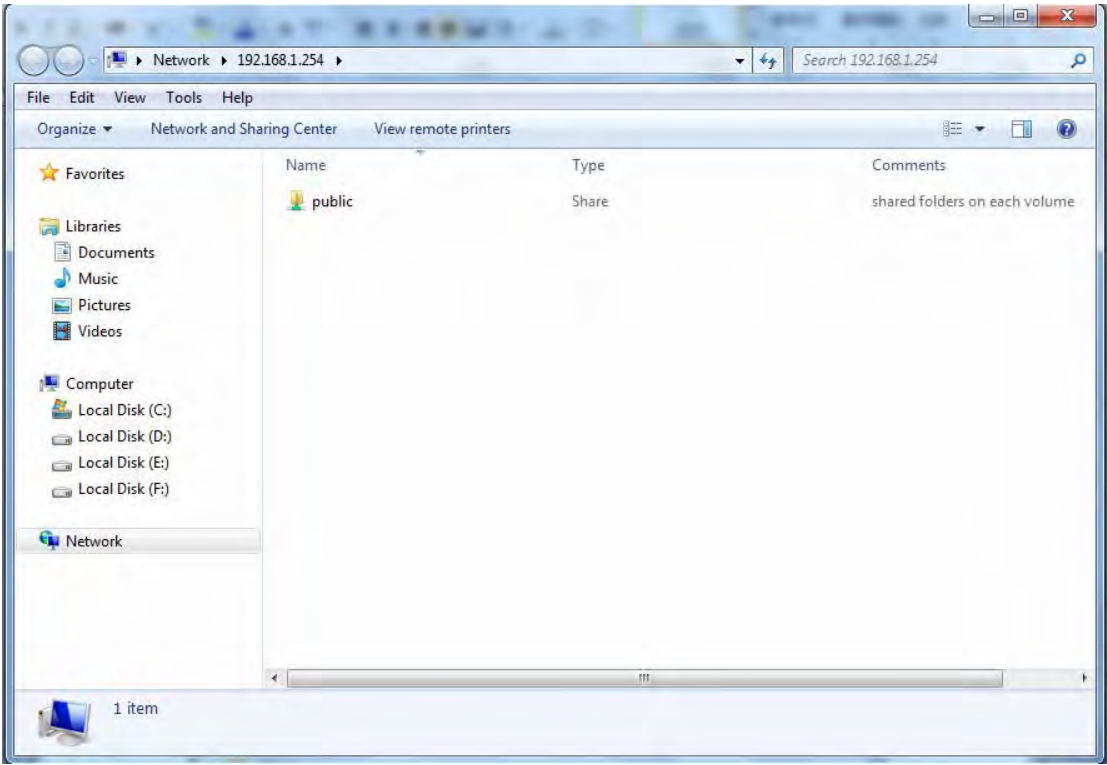


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

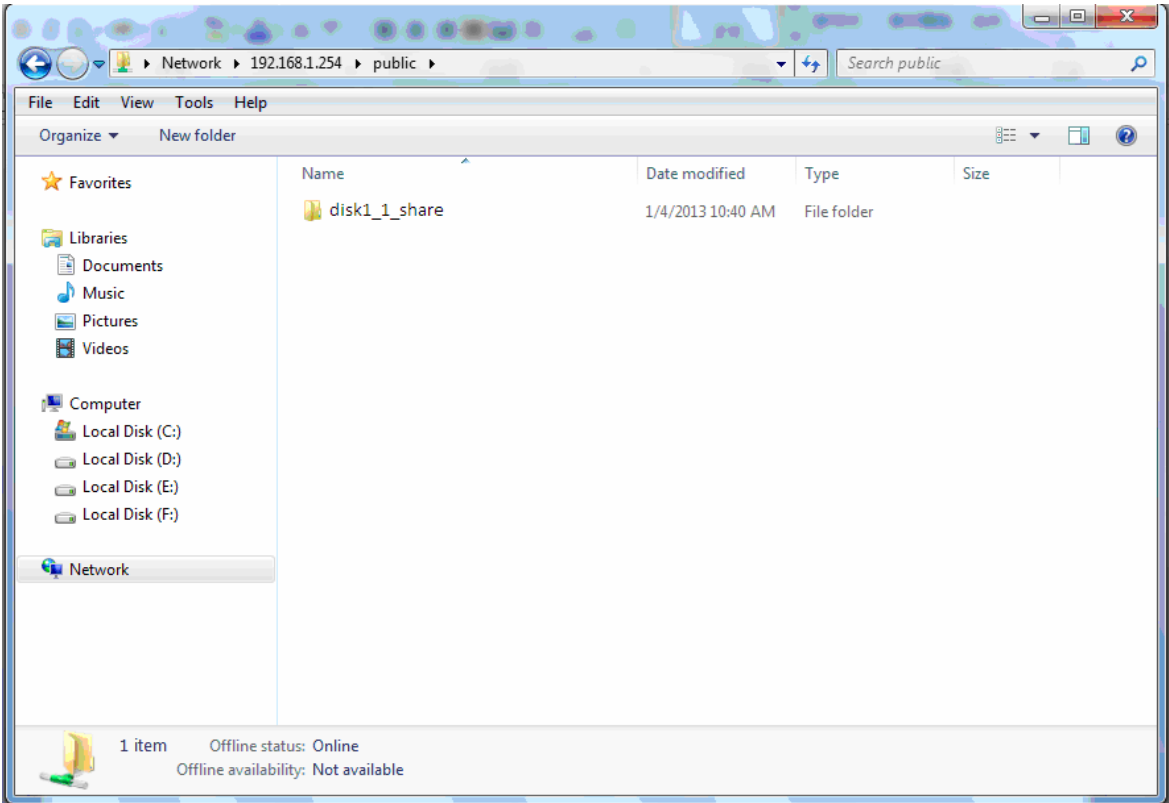
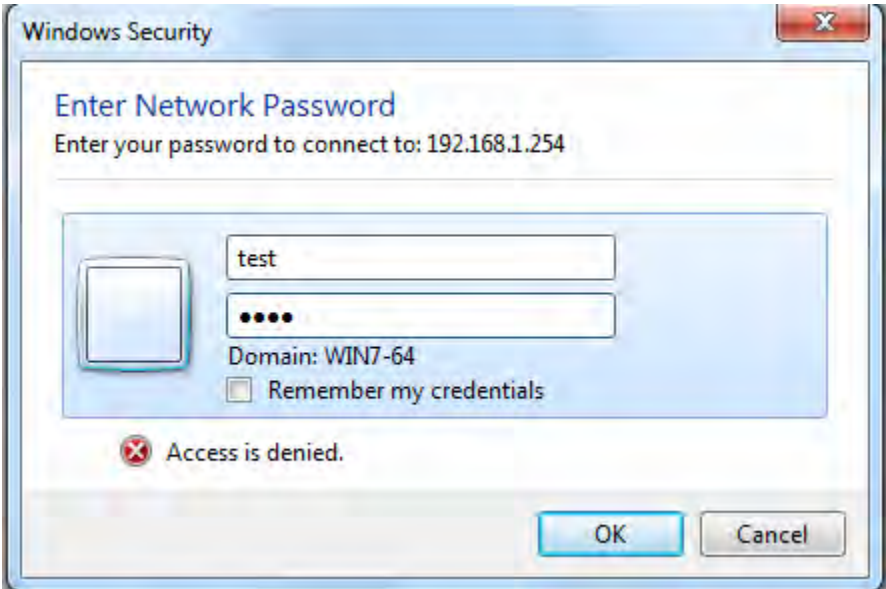
When first logged on to the network folder, you will see the “**public**” folder.

Public: The public sharing space for each user in the USB Storage.

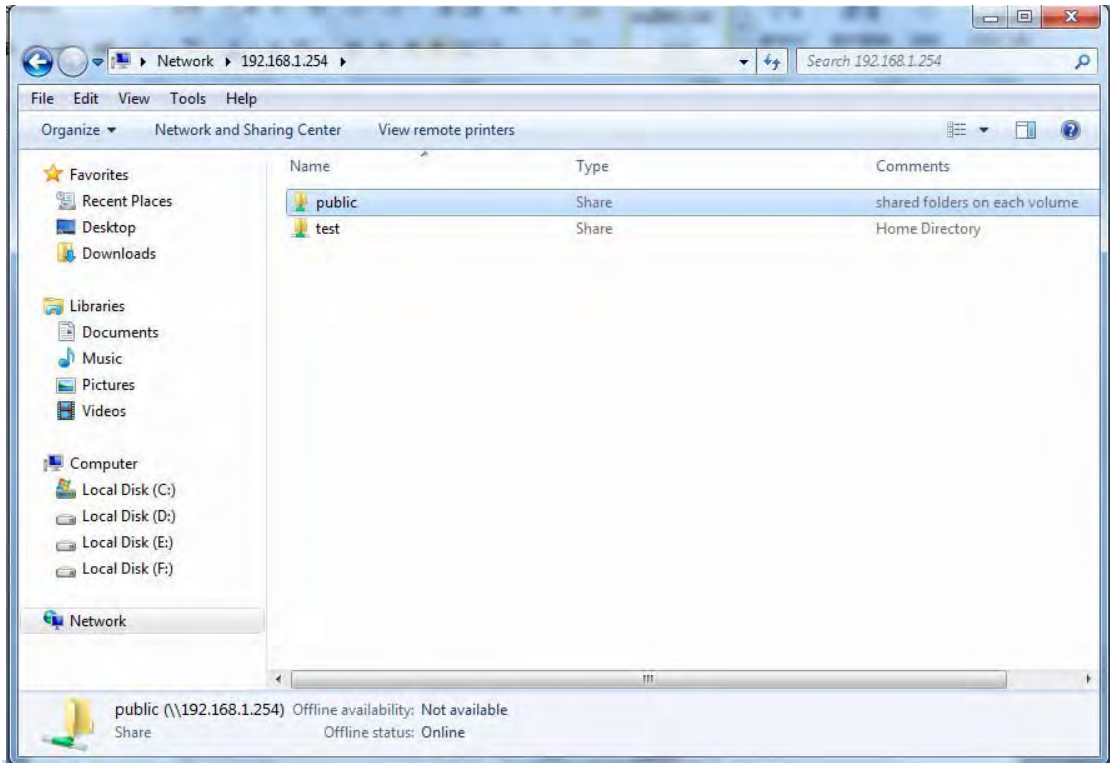
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



Access the folder *public*.



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.



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-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



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*

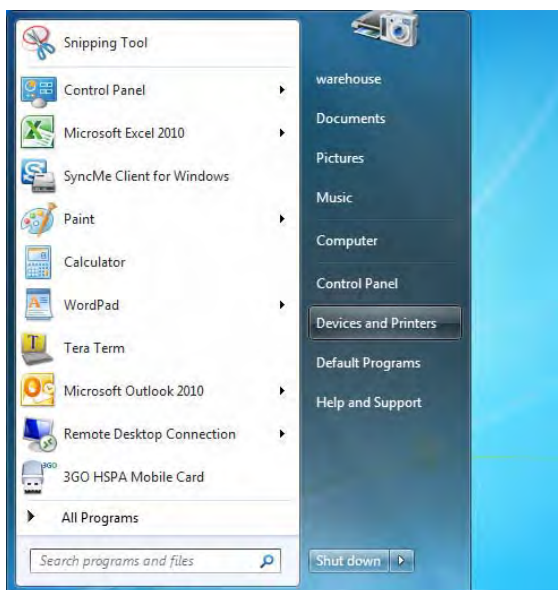
Note:

The **Printer name** can be any text string up to **40** characters. It cannot contain spaces.

The **Make and Model** can be any text string up to **128** characters.

Setup of Printer client (Windows 7)

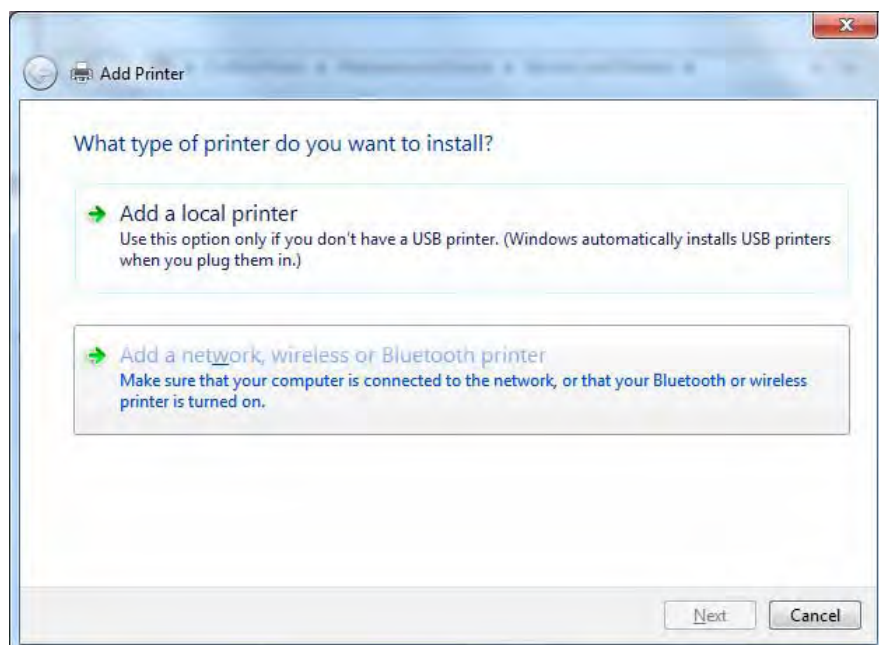
Step 1: Click **Start** and select "Devices and Printers"



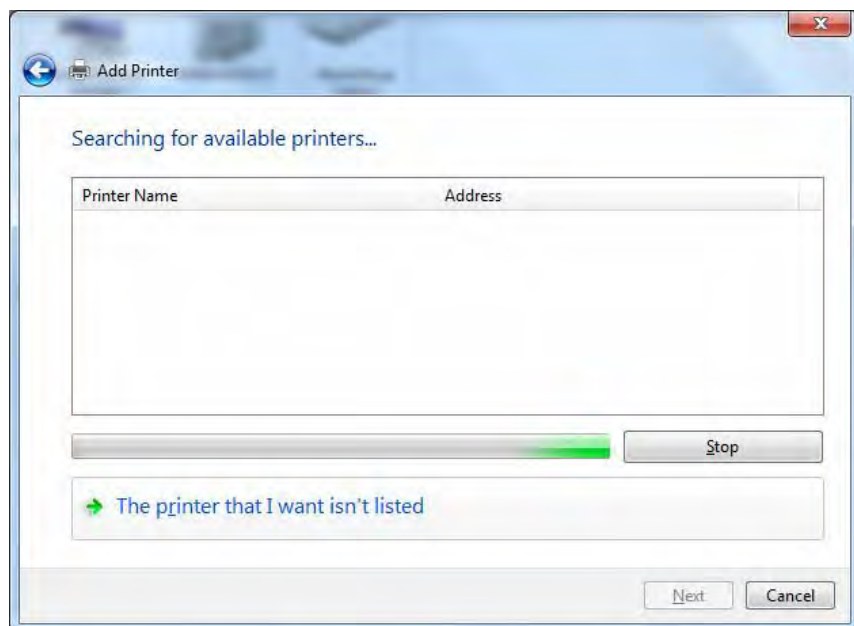
Step 2: Click "Add a Printer".



Step 3: Click "Add a network, wireless or Bluetooth printer



Step 4: Click “The printer that I want isn’t listed”

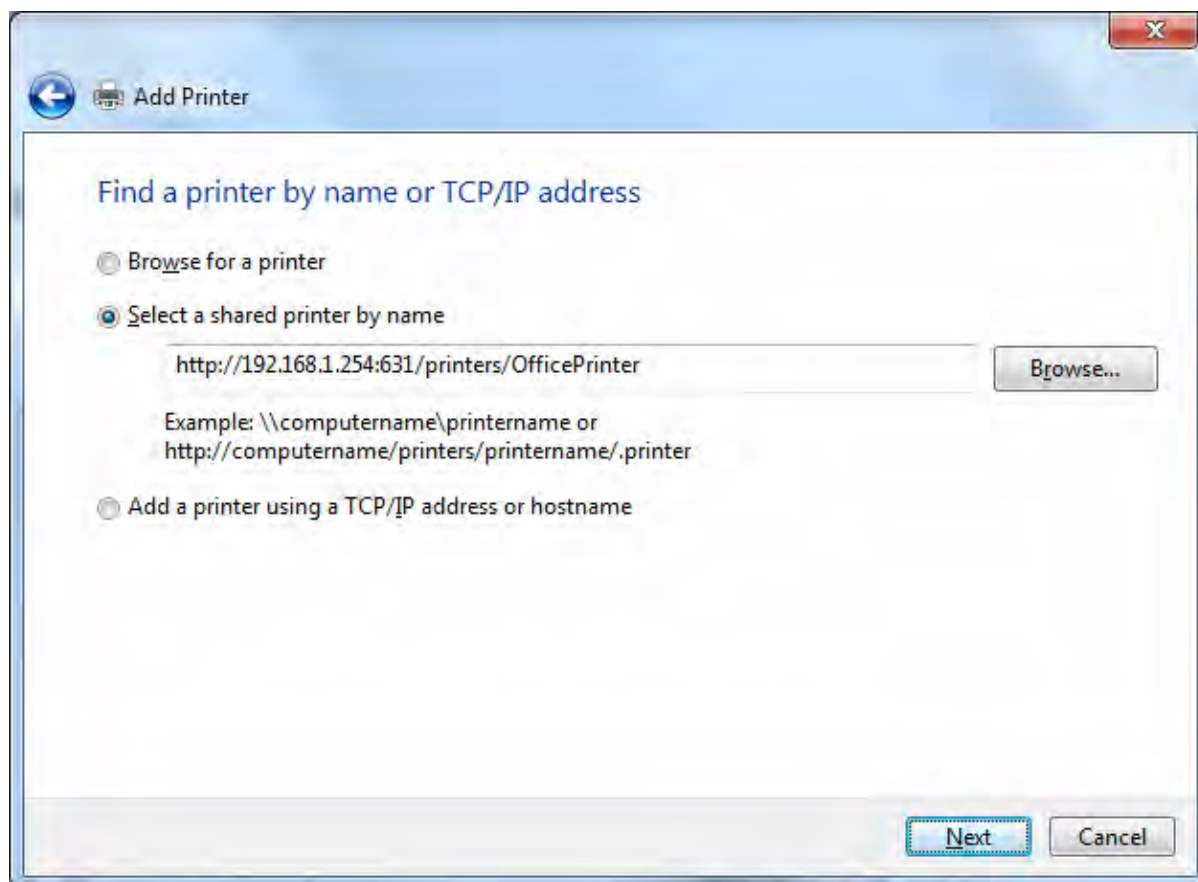


Step 5: Select “Select a shared printer by name”

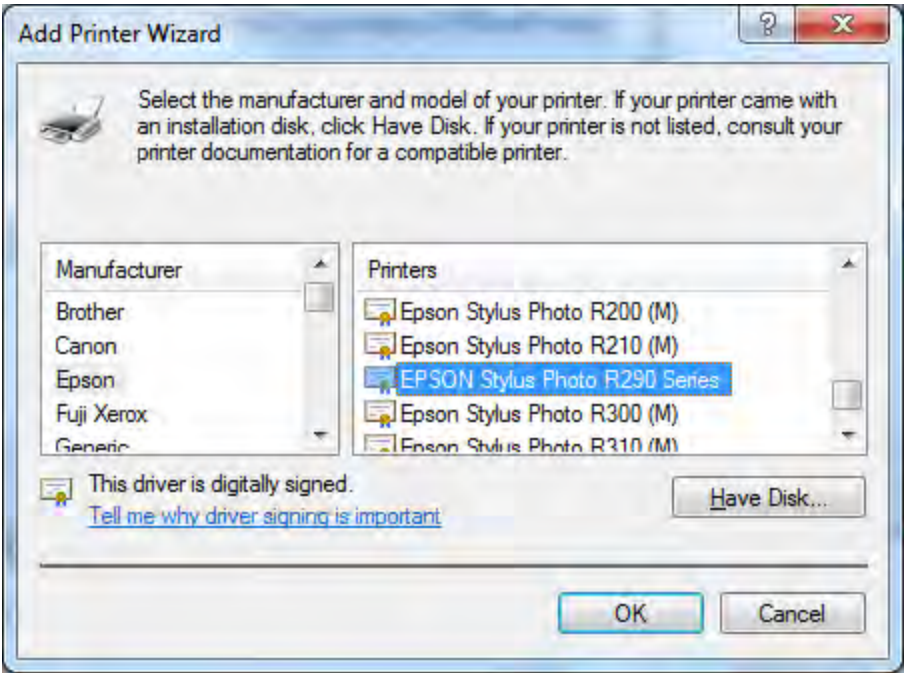
Enter <http://8700AX-1600> - LAN-IP:631/printers/printer-name or. Make sure printer’s name is the same as what you set in the 8700AX earlier

For Example: *http://192.168.1.254:631/printers/OfficePrinter*

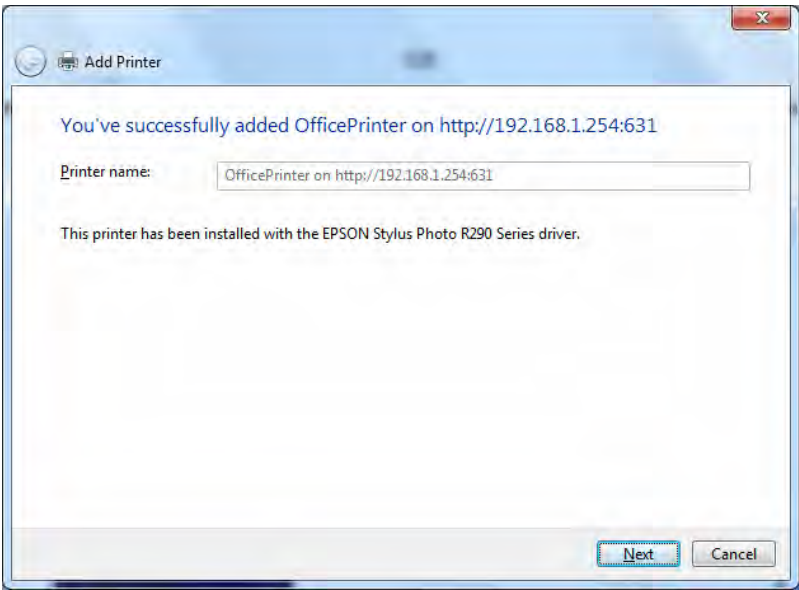
OfficePrinter is the Printer Name we set up earlier



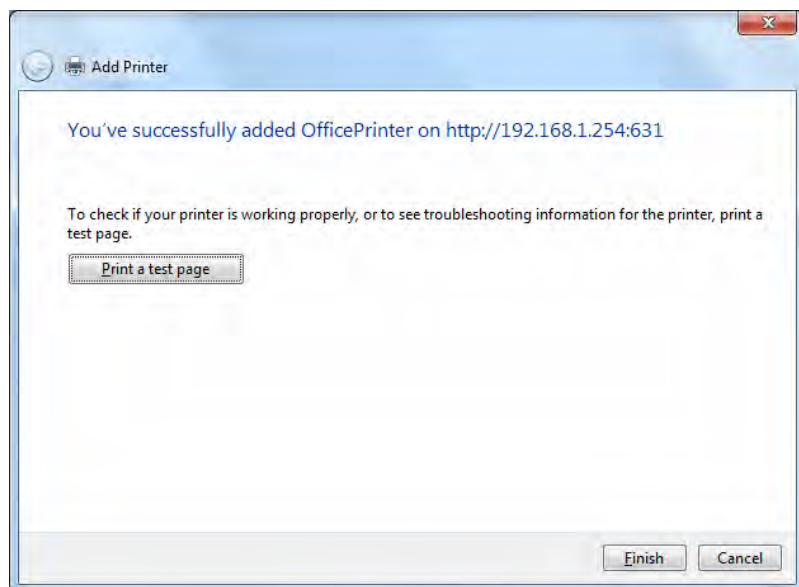
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



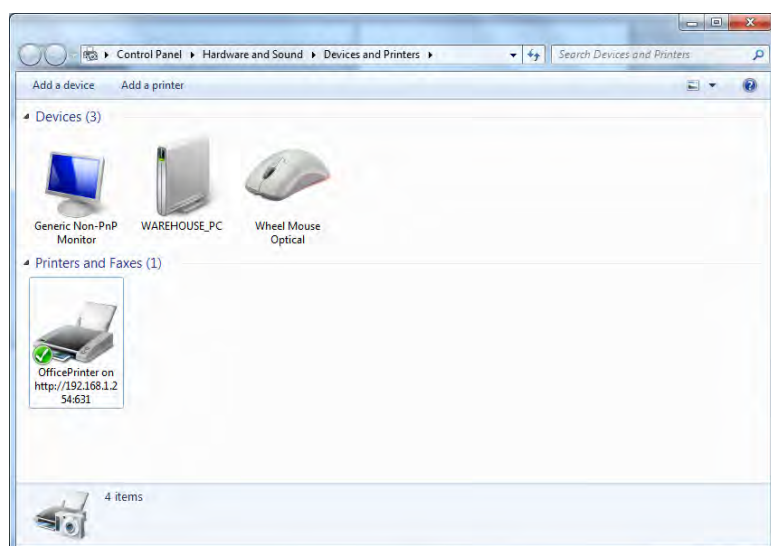
Step 7: Click “Next”



Step 8: Click “Next” and you are done



You will now be able to see your printer on the Devices and Printers Page



DLNA

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-1600 can serve as a DLNA server.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Digital Media Server settings' is expanded. Under this section, there is a 'Parameters' table with three rows: 'On-board digital media server' with a checked 'Enable' checkbox, 'Interface' with a 'Default' dropdown menu, and 'Media Library Path' with a 'disk1_1' dropdown menu. At the bottom of the settings section, there are 'Apply' and 'Cancel' buttons.

Parameters	
On-board digital media server	☒ Enable
Interface	Default
Media Library Path	disk1_1

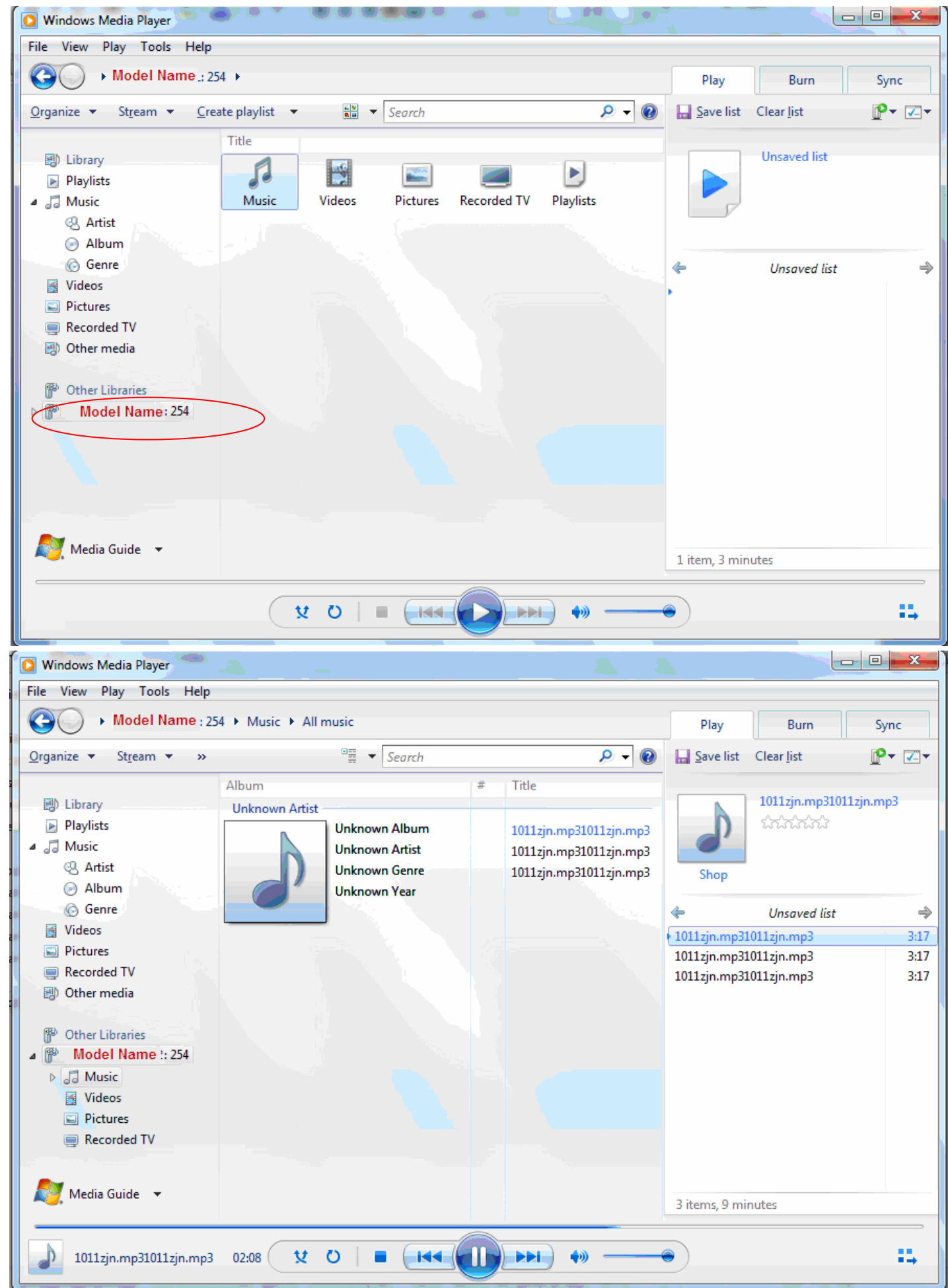
Apply Cancel

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.

Configuration

IPv6inIPv4

6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	V4 Common Bit Length	6rd Prefix with Prefix Length	Border Relay Address	Remove

Add

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	☒ Manual ☐ Automatic
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

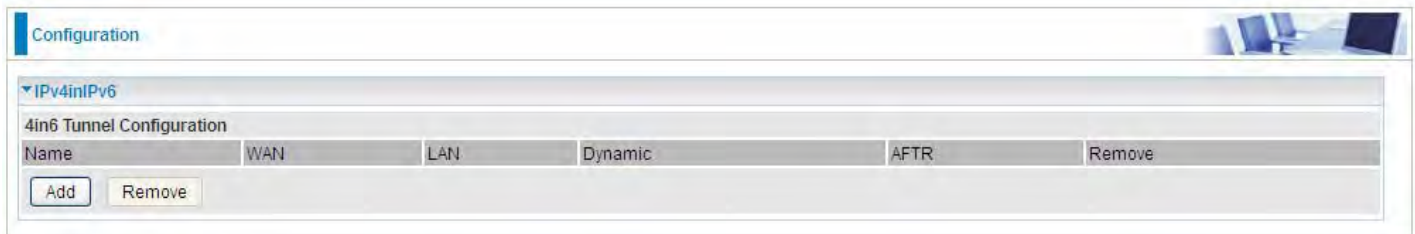
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

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).

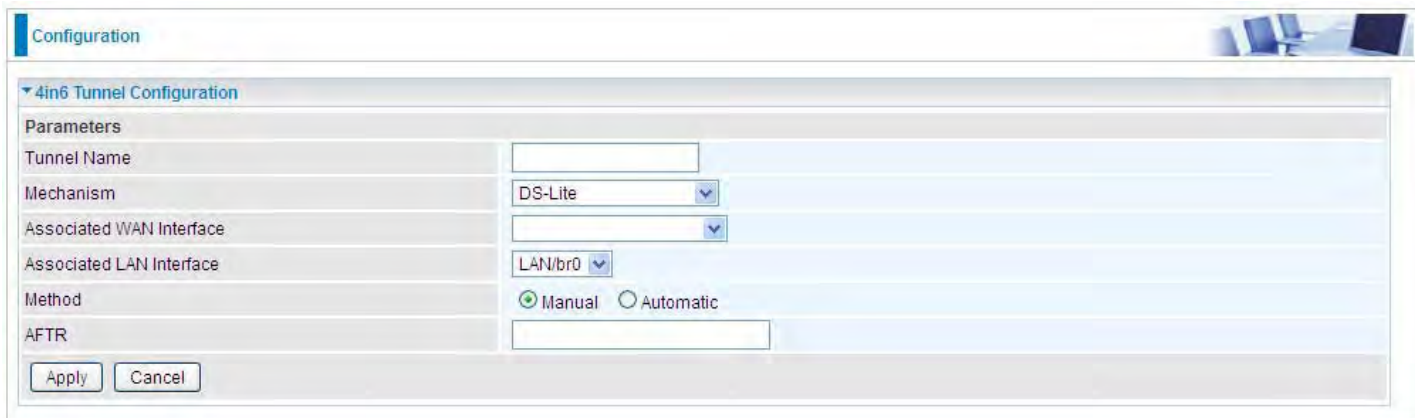
The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



The screenshot shows a web-based configuration interface for IPv4inIPv6. At the top, there's a 'Configuration' tab. Below it, a section titled 'IPv4inIPv6' contains a '4in6 Tunnel Configuration' table. The table has columns for Name, WAN, LAN, Dynamic, AFTR, and Remove. There is one row with the name 'WAN' and 'Dynamic' checked. Below the table are 'Add' and 'Remove' buttons.

Name	WAN	LAN	Dynamic	AFTR	Remove
WAN			☒		

Click **Add** button to manually add the 4in6 rules.



The screenshot shows a detailed configuration window for a 4in6 tunnel. It has a 'Configuration' tab and a section titled '4in6 Tunnel Configuration'. Under 'Parameters', there are fields for Tunnel Name, Mechanism (set to DS-Lite), Associated WAN Interface, Associated LAN Interface (set to LAN/br0), Method (with radio buttons for Manual and Automatic, Manual is selected), and AFTR. At the bottom are 'Apply' and 'Cancel' buttons.

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.

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
				Destination IP address	Destination Port					

Add

Remove

Reorder

Click **Add** button to enter the exact rule setting page.

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name

<< --type or select from 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

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

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.

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 [Time Schedule](#).

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 Setup

Parameters

Filter Name

FTP

<< --type or select from listbox--

IP Version

IPv4

Protocol

TCP/UDP

Source IP address

~

Destination IP address

~

Time Schedule

Always On

Sun

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

00

To

00

:

00

Action

forward

Protocol Number

[0 - 254]

Source Port

[port or port:port]

Destination Port

21

[port or port:port]

Log

☒

Apply

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
	FTP	4	TCP	Any	Any	forward	Disable	☐		Edit
				Any	21					

Add

Remove

Reorder

(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.

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
	FTP	4	TCP	Any	Any	forward	Disable	☐		Edit
				Any	21					
	HTTP	4	TCP	Any	Any	drop	Disable	☐		Edit
				Any	80					

Add

Remove

Reorder

How to disable set rule.

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name

FTP

<< --type or select from listbox--

IP Version

IPv4

Protocol

TCP

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

Disable

Sun

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

00

To

00

:

00

Action

forward

Log

Apply

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
	FTP	4	TCP	Any	Any	forward	Disable	☒	☐	Edit
				Any	21					

Add

Remove

Reorder

(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.

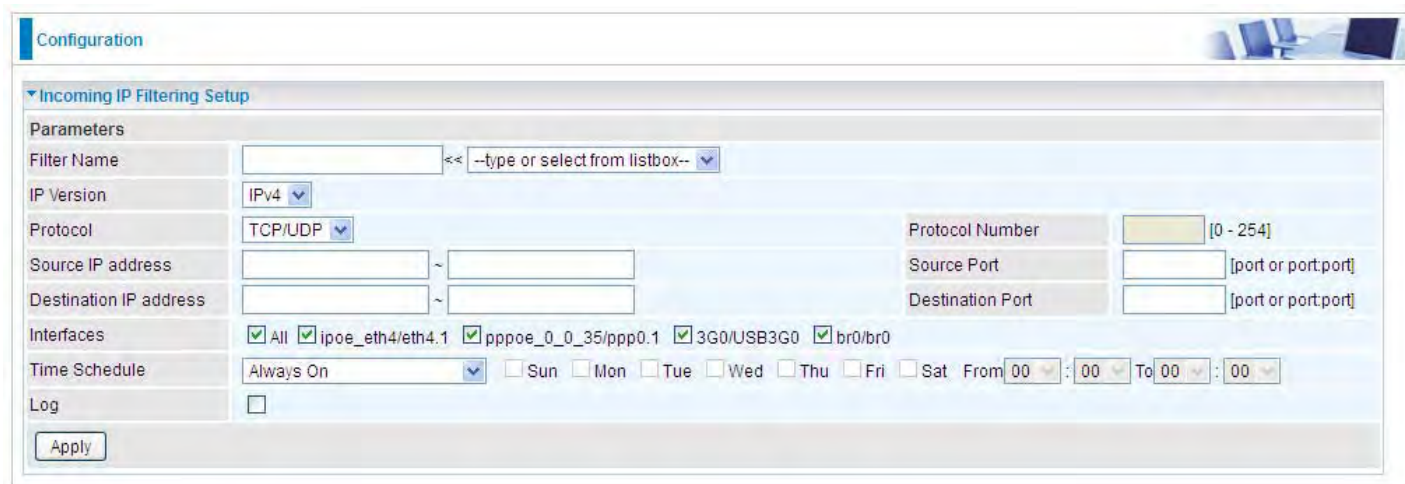
Note:

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.



Filter Name	Interfaces	IP Version	Protocol	Source IP address	Source Port	Destination IP address	Destination Port	Log	Disable	Remove	Edit
-------------	------------	------------	----------	-------------------	-------------	------------------------	------------------	-----	---------	--------	------

Click **Add** button to enter the exact rule setting page.



Parameters

Filter Name: << --type or select from listbox--

IP Version:

Protocol: Protocol Number:

Source IP address: ~ Source Port:

Destination IP address: ~ Destination Port:

Interfaces: ☒ All ☒ ipoe_eth4/eth4.1 ☒ pppoe_0_0_35/ppp0.1 ☒ 3G0/USB3G0 ☒ br0/lbr0

Time Schedule: ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From : To :

Log: ☐

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 [Time Schedule](#).

Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

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 Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge 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.

MAC Filtering Policy For Each Interface

Interface	Policy	Change
atm0.1	FORWARD	☒

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Change Policy

MAC filtering rules

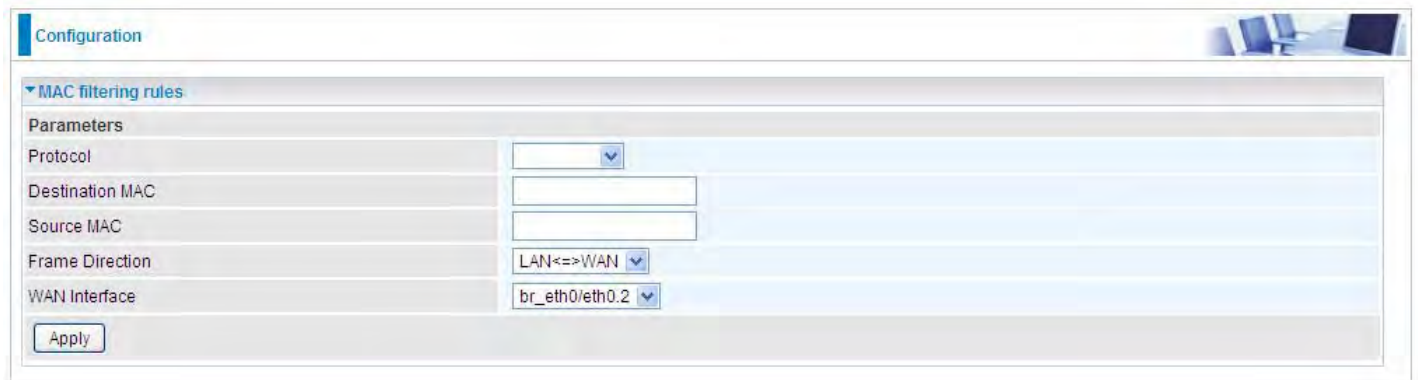
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Add Remove

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

Block WAN PING

Parameters

Block WAN PING

☐ Enable ☒ Disable

Block WAN (IPv6) PING

☐ Enable ☒ Disable

Apply

Cancel

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.

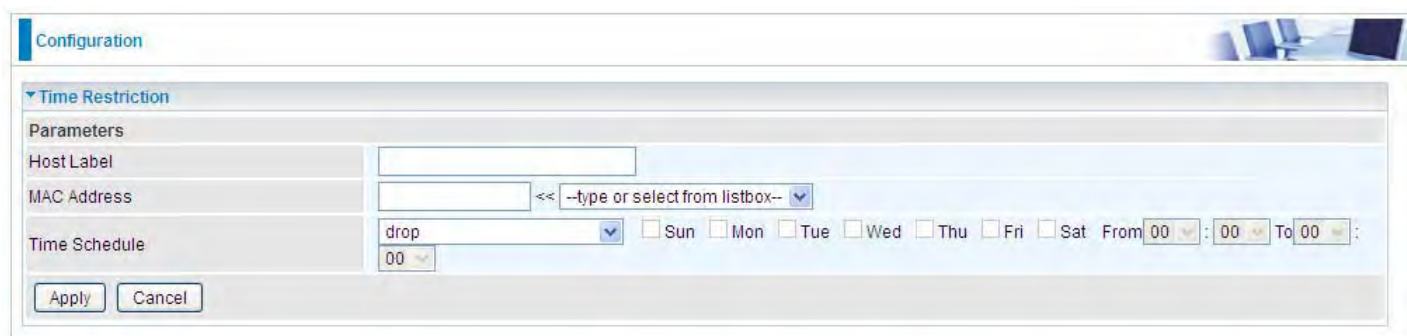
To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



The screenshot shows the 'Configuration' page with the 'Time Restriction' section expanded. It displays a table of existing rules with columns: Host Label, MAC Address, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, Remove, and Edit. Below the table are 'Add' and 'Remove' buttons. A note above the table states: 'A maximum entries can be configured: 32'.

Click **Add** to add the rules.



The screenshot shows the 'Add' dialog box for Time Restriction. It contains fields for 'Host Label', 'MAC Address' (with a dropdown menu labeled '--type or select from listbox--'), and 'Time Schedule'. The 'Time Schedule' section includes a dropdown menu (currently set to 'drop'), checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat), and time selection fields for 'From' and 'To' (both set to 00:00). 'Apply' and 'Cancel' buttons are at the bottom.

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:xx or xx-xx-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.
- ① **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 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	forward									☐	Edit
child-use	18:a9:05:04:12:23		x	x	x	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.

Configuration

URL 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 To 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 [Time Schedule](#).

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 [Security Log](#).

Keywords Filtering

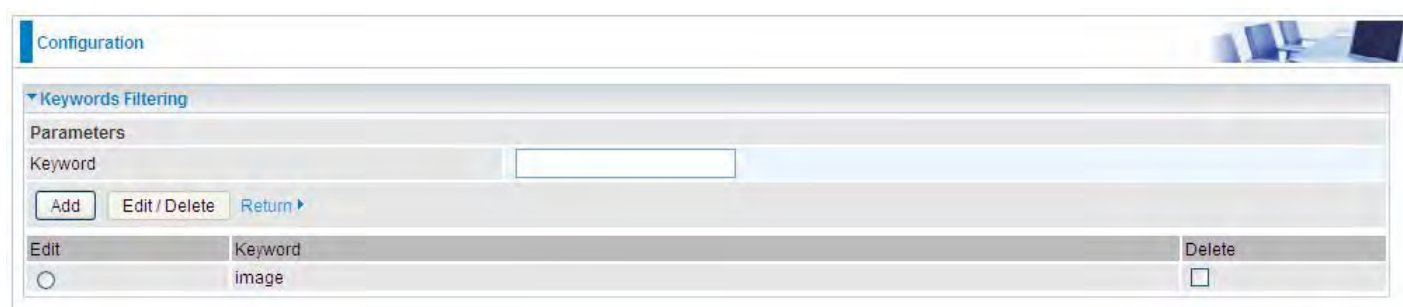
Note: Maximum number of entries: 32.

Click [Detail ▶](#) to add the keywords.



The screenshot shows the 'Configuration' window with the 'Keywords Filtering' section expanded. Under 'Parameters', there is a 'Keyword' text input field. Below the input field are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'. The 'Return' button is highlighted in blue.

Enter the Keyword, for example image, and then click **Add**.



This screenshot shows the 'Keywords Filtering' section after adding a keyword. The 'Parameters' section is still at the top. Below it, a table lists the added keywords. The first entry is 'image'. To the left of the keyword is an 'Edit' radio button (which is selected). To the right is a 'Delete' checkbox (which is unchecked).

Edit	Keyword	Delete
☐	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.



The screenshot shows the 'Configuration' window with the 'Domains Filtering' section expanded. Under 'Parameters', there are two input fields: 'Domains Filtering' and 'Type'. The 'Type' field is a dropdown menu currently set to 'Forbidden Domain'. Below the input fields are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'. The 'Return' button is highlighted in blue.

Domains Filtering: enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

- ① **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.



The screenshot shows a web interface for configuring network settings. The main heading is 'Configuration'. Below it, there's a section titled 'Except IP Address'. Under this section, there's a 'Parameters' area. The 'IP Version' is set to 'IPv4' via a dropdown menu. Below that, the 'Internal IP Address' field is empty, followed by a tilde '~' and another empty field. At the bottom of the form are three buttons: 'Add', 'Edit / Delete', and '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](#)).



The screenshot shows a web-based configuration interface. At the top, there is a blue header bar with the word "Configuration" on the left and a small graphic of a desk with a monitor and keyboard on the right. Below the header, the main content area is titled "Parental Control Provider" with a dropdown arrow. Under this title, there is a section labeled "Parameters" which contains a descriptive paragraph: "Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance." Below the text, there are four input fields arranged in a table-like structure. The first row has the label "Provider" and the value "www.opendns.com". The second row has the label "Host Name" and an empty text box. The third row has the label "Username" and an empty text box. The fourth row has the label "Password" and an empty text box. At the bottom left of the form, there are two buttons: "Apply" and "Cancel".

Parameters	
Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.	
Provider	www.opendns.com
Host Name	
Username	
Password	

Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website www.opendns.com.

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..

The screenshot shows the 'Configuration' tab with the 'QoS Classification Setup' section expanded. It includes a section for 'EWAN Line Speed' with input fields for 'Upstream / Downstream' rates in kbps, a note that 0 means 'Disable', and an 'Apply' button. Below this is a table header for QoS rules with columns: Class Name, IP Version, Direction, Internal IP Address, Internal Port, Protocol, External IP Address, External Port, DSCP Mark, Rate Type, Disabled, Remove, and Edit. There are 'Add' and 'Remove' buttons at the bottom of the table area.

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.

The screenshot shows the 'Configuration' tab with the 'Quality of Service' section expanded. It displays 'Non-Assigned Bandwidth Ratio' for Upstream (100%) and Downstream (100%). The configuration fields include: IP Version (IPv4), Application (with a search icon and a dropdown), 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, and Time Schedule (Always On with checkboxes for days of the week and time range). An 'Apply' button is at the bottom.

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.
- ① **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

Mapping 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**.

- ① **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximum rate 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.
- ① **Set DSCP Marking:** When select **Set DSCP Marking**, the packets matching the rule will be 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 $20\% \times 256 \times 0.9 = 46\text{kbps}$. (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.

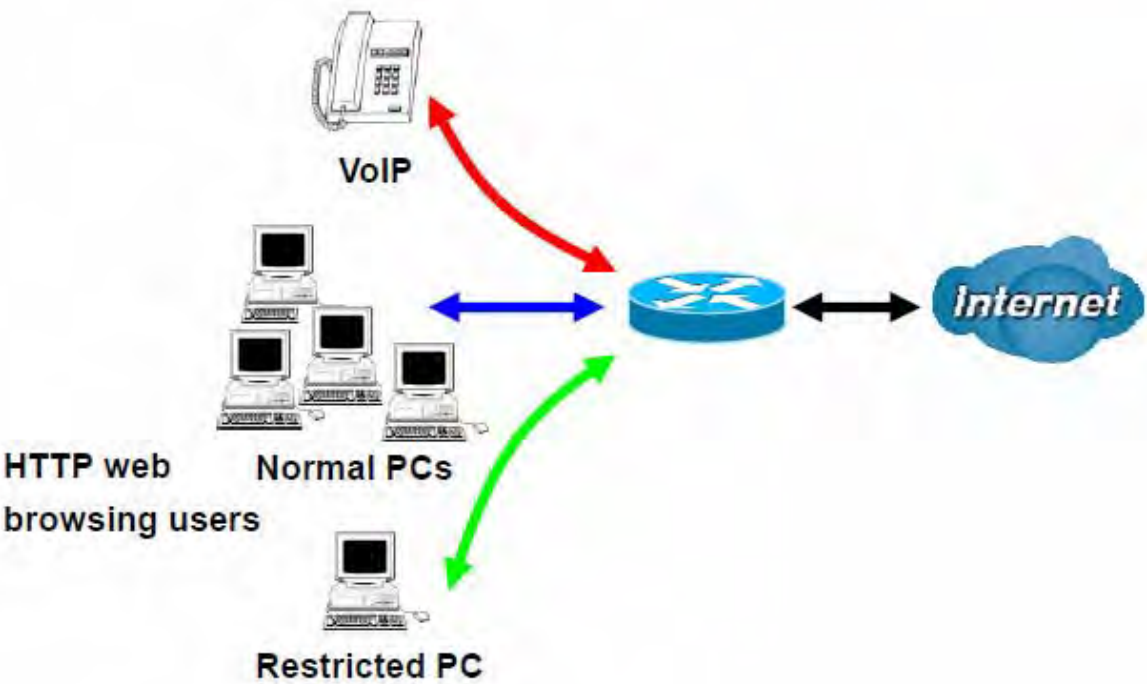
External IP Address: The IP address on remote / WAN side.

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](#).

Examples: Common usage



- 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 Ratio => 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	
Rate Type	Prioritization	Ratio	%	
Internal IP Address			DSCP Marking	EF(101110)
External IP Address			Priority	High
Time Schedule	timeslot1 ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat From 00 : 00 To 09 : 19			

Apply

- 2. Give regular web http access a limited rate

Configuration

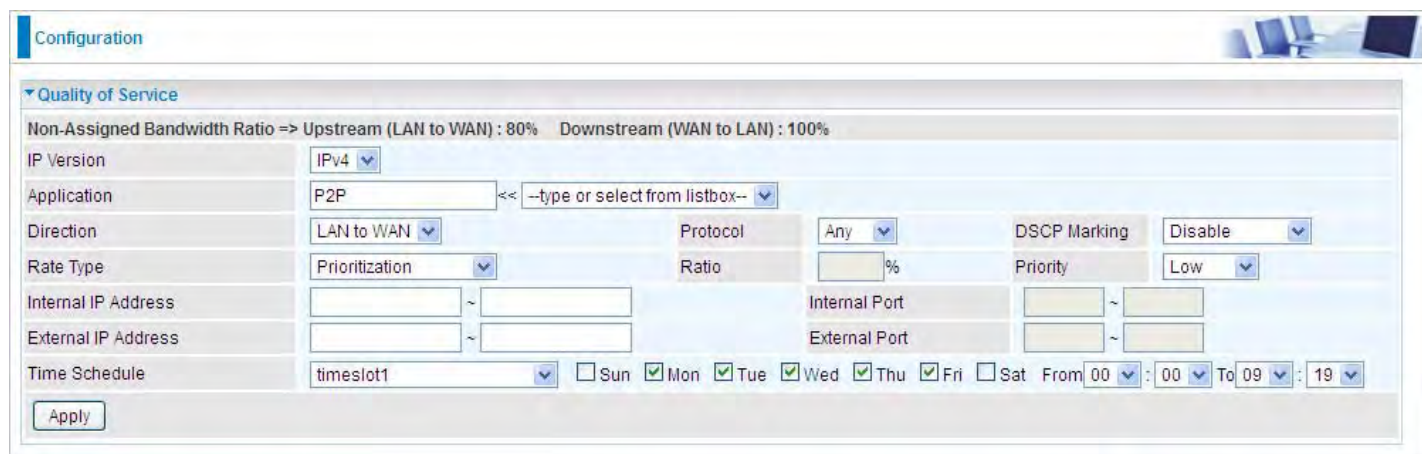
Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

IP Version	IPv4			
Application	HTTP << HTTP(TCP 80)			
Direction	LAN to WAN	Protocol	TCP	
Rate Type	Limited (Maximum)	Ratio	20 %	
Internal IP Address			DSCP Marking	Disable
External IP Address			Priority	Normal
Time Schedule	timeslot1 ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ 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.



The screenshot displays a network configuration window titled "Configuration". Under the "Quality of Service" section, the "Non-Assigned Bandwidth Ratio" is set to "Upstream (LAN to WAN) : 80%" and "Downstream (WAN to LAN) : 100%". The "IP Version" is set to "IPv4". The "Application" is set to "P2P". The "Direction" is set to "LAN to WAN". The "Rate Type" is set to "Prioritization". The "Protocol" is set to "Any". The "DSCP Marking" is set to "Disable". The "Ratio" is set to "%". The "Priority" is set to "Low". The "Internal IP Address" and "External IP Address" fields are empty. The "Internal Port" and "External Port" fields are empty. The "Time Schedule" is set to "timeslot1". The "Time Schedule" section includes checkboxes for "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", and "Sat", with "Mon", "Tue", "Wed", "Thu", and "Fri" checked. The "Time Schedule" section also includes a "From" field set to "00:00" and a "To" field set to "09:19". An "Apply" button is located at the bottom left of the configuration section.

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.

Configuration

QoS Port Shaping

Parameters

QoS port shaping supports traffic shaping of Ethernet interface. If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	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

Apply

Cancel

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

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

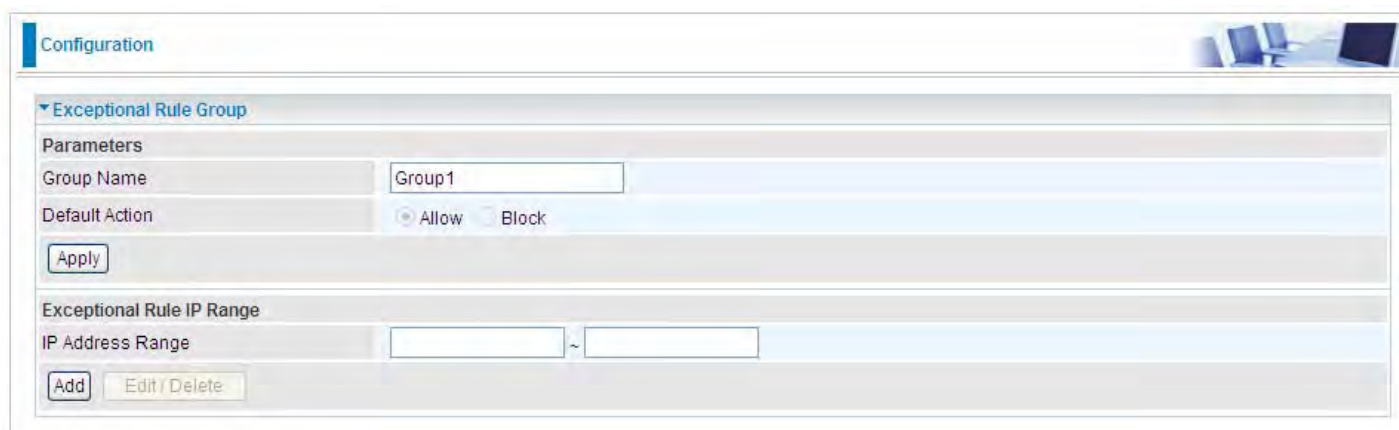
Exceptional Rule is dedicated to giving or blocking NAT/DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a table with the following columns: Group Index, Group Name, Default Action, Exceptional Rule IP Range, and Edit. There are 8 rows, each representing a group from Group1 to Group8, all with a Default Action of 'Allow'. Each row has an 'Edit' button in the last column.

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).



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a form for editing a group. The form has two main sections: 'Parameters' and 'Exceptional Rule IP Range'. The 'Parameters' section includes a 'Group Name' field (set to 'Group1') and a 'Default Action' section with radio buttons for 'Allow' (selected) and 'Block'. There is an 'Apply' button below the 'Default Action' section. The 'Exceptional Rule IP Range' section includes an 'IP Address Range' field with a tilde (~) separator and two input boxes. Below this field are 'Add', 'Edit', and 'Delete' buttons.

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.

Configuration

▼ **Exceptional Rule Group**

Parameters

Group Name:

Default Action: ☐ Allow ☒ Block

Exceptional Rule IP Range

IP Address Range: ~

Edit	Action	IP Address Range	Delete
☐	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.

Configuration

▼ **Virtual Servers**

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					

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 Servers

Parameters

Interface: pppoe_0_8_35/ppp0.1 WAN IP:

Server Name: Custom Service

Custom Service:

Server IP Address: << --type or select from listbox--

Time Schedule: Always On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

Exceptional Rule Group: None

External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Apply Cancel

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-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 user-defined 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

- ① **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

- ① **Start:** Enter a port number as the internal starting number.
- ① **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  in the list table indicating the rule is disabled. See [Time Schedule](#).

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block Virtual Server

Set up

- Virtual Servers

Parameters

Interface

pppoe_0_8_35/ppp0.1

WAN IP

Server Name

Custom Service

Custom Service

Server IP Address

<< --type or select from listbox--

Time Schedule

Always On

☐ Sun
☐ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat

From

00

:

00

To

00

Exceptional Rule Group

None

External Port

Start	End	Protocol	Protocol Number	Internal Port	Start	End
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				
		TCP				

Apply

Cancel

- [illegible]

Configuration

Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
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

Add
Remove

( 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.

Configuration

Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
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

Add
Remove

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.

Configuration

DMZ Host

Parameters

DMZ Host IP Address

<< --type or select from listbox--

Time Schedule

Always On

☐Sun☐Mon☐Tue☐Wed☐Thu☐Fri☐Sat

From00:00To00:00

Exceptional Rule Group

None

Apply

Cancel

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 [Time Schedule](#).

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.

NOTE:

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

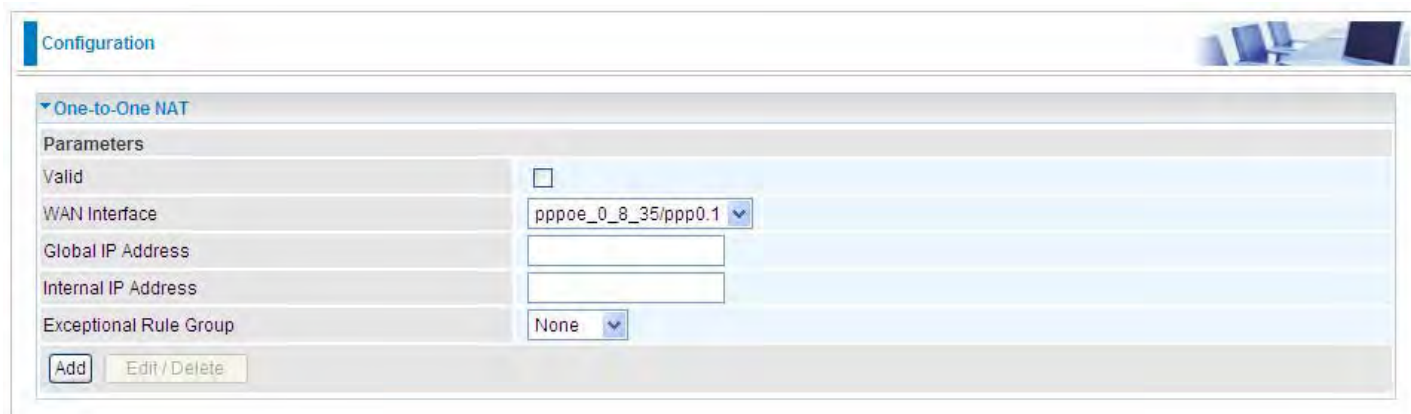
Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

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.



The screenshot shows a web-based configuration interface for "One-to-One NAT". At the top, there is a "Configuration" tab and a small graphic of a network setup. Below the tab, the "One-to-One NAT" section is expanded, showing a "Parameters" table. The table has five rows: "Valid" with a checkbox, "WAN Interface" with a dropdown menu showing "pppoe_0_8_35/ppp0.1", "Global IP Address" with an empty text box, "Internal IP Address" with an empty text box, and "Exceptional Rule Group" with a dropdown menu showing "None". At the bottom of the table, there are two buttons: "Add" and "Edit/Delete".

Parameters	
Valid	☐
WAN Interface	pppoe_0_8_35/ppp0.1
Global IP Address	
Internal IP Address	
Exceptional Rule Group	None

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.

Configuration

Port Triggering

Port Triggering Setup

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range	Port Range			
		StartEnd		StartEnd				
AddRemove								

Click **Add** to add a port triggering rule.

Configuration

Port Triggering

Parameters

Interfacepppoe_0_8_35/ppp0.1

ApplicationCustom Application

Custom Application

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply

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

- Start: Enter a port number as the open port staring number.
- 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/ppp0.1

Application

Aim Talk

Custom Application

Trigger Port

Start	End	Trigger Protocol	Open Port	Start	End	Open Protocol
4099	4099	TCP	5191	5191	5191	TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP
		TCP				TCP

Apply

2. Press **Apply** to conform, and the items will be list in the **Port TriggeringSetup** table.

Configuration

Port Triggering

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☐	Edit

Add Remove

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

Port Triggering

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit			
	Protocol	Port Range		Protocol	Port Range							
		Start	End		Start	End						
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☒	Edit			

ALG

The ALG Controls enable or disable protocols over application layer.



The screenshot shows a 'Configuration' window with a tab labeled 'ALG'. Under the 'Parameters' section, there are three rows: 'SIP', 'H.323', and 'IPSec'. Each row has two radio buttons: 'Enable' (which is selected for all three) and 'Disable'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Parameter	Enable	Disable
SIP	☒	☐
H.323	☒	☐
IPSec	☒	☐

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.

Configuration

Wake On LAN

Parameters

Host Label

MAC Address

<< --select--

(type or select from listbox)

Wake by Schedule

☐ Enable

Schedule ▶

Add

Edit / Delete

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 [Schedule](#) to enter time schedule configuring page to set the exact timeline.

Configuration

Wake up Time Schedule

Parameters

Name

Day in a week

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time

00 : 00

Add

Edit / Delete

Edit	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Delete
☐	11		x	x	x	x	x		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.

Configuration

Wake On LAN

Parameters

Host Label

MAC Address

<< --select--

(type or select from listbox)

Wake by Schedule

☐ Enable

Schedule ▶

Add

Edit / Delete

Edit	Action	Host Label	MAC Address	Ready	Delete
☐	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.

The screenshot shows a VPN configuration window. At the top, there's a 'VPN' tab. Below it, the 'IPSec' section is expanded. Under 'NAT Traversal', there's a checkbox for 'Enable' which is currently unchecked. To its right is a 'Keep Alive' field set to '60' with the unit 'Second(s) [1-60]'. An 'Apply' button is below these settings. Below the NAT Traversal section is a 'Tunnel Mode Connections' table. The table has columns for 'Active', 'L2TP', 'Connection Name', 'Local Network', 'Remote Network', 'Remote Security Gateway', 'Remove', and 'Edit'. There are 'Add' and 'Remove' buttons below the table.

Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
--------	------	-----------------	---------------	----------------	-------------------------	--------	------

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.

Click **Add** to create IPSec connections.

The screenshot shows the 'IPSec Settings' tab in a VPN configuration window. The 'L2TP over IPsec' checkbox is unchecked. The 'Connection Name' field is empty. The 'WAN Interface' is set to 'Default' and 'IP Version' is 'IPv4'. The 'Local Network' is set to 'Single Address' with an empty 'IP Address' and 'Netmask' field. The 'Remote Security Gateway' is empty, and the 'Anonymous' checkbox is unchecked. The 'Remote Network' is also set to 'Single Address' with empty 'IP Address' and 'Netmask' fields. The 'Key Exchange Method' is 'IKE' and the 'IPsec Protocol' is 'ESP'. The 'Pre-Shared Key' field is empty. The 'Local ID Type' and 'Remote ID Type' are both set to 'Default', with empty 'ID Content' fields. The 'Phase 1' section has 'Mode' set to 'Main', 'Encryption Algorithm' set to '3DES', 'Integrity Algorithm' set to 'MD5', 'DH Group' set to 'MODP1024(DH2)', and 'SA Lifetime' set to '480 Minute(s) [60-1440]'. The 'Phase 2' section has 'Encryption Algorithm' set to '3DES', 'Integrity Algorithm' set to 'MD5', 'DH Group' set to 'None', 'IPsec Lifetime' set to '60 Minute(s) [60-1440]', 'Keep Alive' set to 'None', and 'MTU' set to '0 (0 : Default)'. An 'Apply' button is located at the bottom left.

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.

- ① **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- ① **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.

- ① **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.
- ① **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.
- ① **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.
- ① **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	Second(s) [180-86400]	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.

- ① **Ping:** This mode will detect whether the remote IPSec peer has lost or not by pinging specify IP address.

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

The screenshot shows the 'IPSec' configuration window. Under 'IPSec Settings', the 'L2TP over IPSec' checkbox is checked. The 'Connection Name' field is empty. The 'WAN Interface' is set to 'Default' and 'IP Version' is 'IPv4'. The 'Remote Security Gateway' field is empty, and the 'Anonymous' checkbox is unchecked. The 'Key Exchange Method' is 'IKE' and the 'IPsec Protocol' is 'ESP'. The 'Pre-Shared Key' field is empty. The 'Encryption Algorithm' is '3DES' and the 'Integrity Algorithm' is 'MD5'. The 'DH Group' is 'None' and the 'IPsec Lifetime' is '60' minutes. An 'Apply' button is at the bottom left.

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.
- ① **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.
- ① **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.

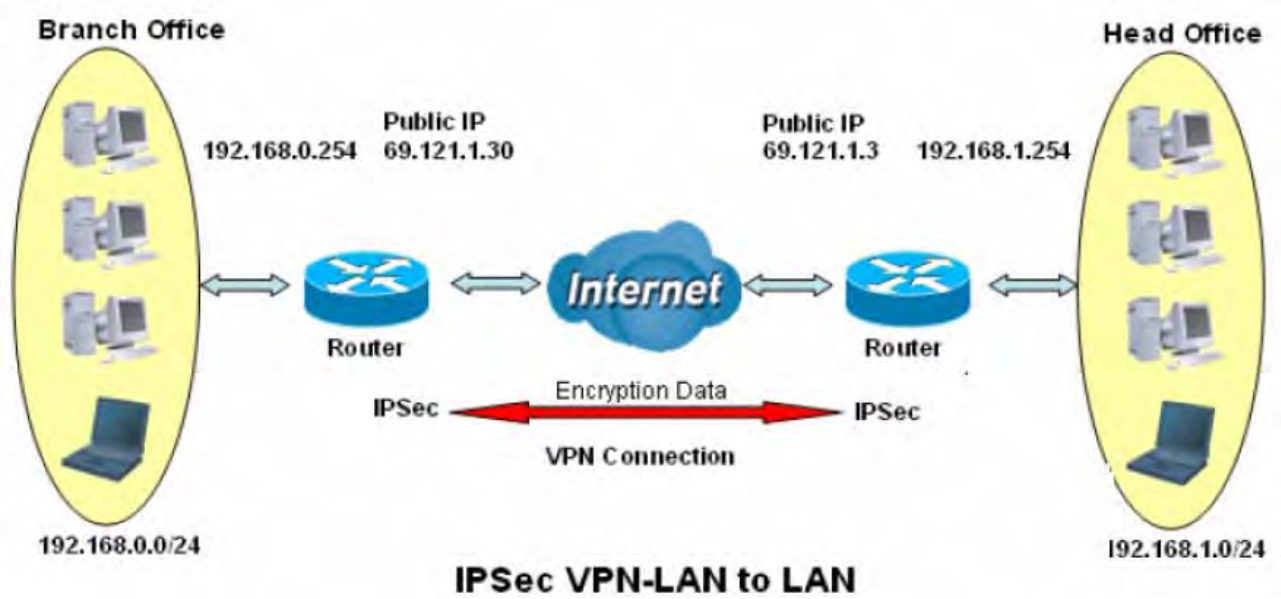
IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to 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 details:

Item	Function		Description
1	Connection Name	H-to-B	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Secure Gateway Address(Hostname)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



▼ 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	☐ Anonymous			
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)		