

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

The screenshot displays the WPS configuration interface. At the top, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** A table with columns for ID, SSID, MAC address, and a lock icon. Two entries are visible: 'wlan-ap-2.4g' (MAC: 00-04-ED-01-00-01) and 'wlan-ap' (MAC: 00-04-ED-38-F7-2E).
- WPS Profile List:** Shows a profile named 'ExRegNWEA4036' with a lock icon and the number '6229909'.
- Configuration Options:** Includes checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. There are also buttons for 'PIN' and 'PBC'.
- Progress Bar:** A blue progress bar indicates 'Progress >> 100%' with the message 'PIN - Get WPS profile successfully.'
- Right-Hand Panel:** Contains buttons for 'Rescan', 'Information', 'Pin Code' (with input '10864111' and a 'Renew' button), 'Config Mode' (set to 'Registrar'), 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.
- Status and Link Quality:**
 - 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 >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- Link Quality Metrics:**
 - Link Quality >> 100%
 - Signal Strength 1 >> 65%
 - Signal Strength 2 >> 39%
 - Noise Strength >> 26%
- Transmit/Receive Performance:**
 - Transmit:** Link Speed >> 243.0 Mbps, Throughput >> 0.000 Kbps. A bar chart shows a peak of 5.392 Kbps.
 - Receive:** Link Speed >> 40.5 Mbps, Throughput >> 98.612 Kbps. A bar chart shows a peak of 118.432 Kbps.
- HT (High Throughput) Parameters:**
 - BW >> 40
 - GI >> long
 - MCS >> 14
 - SNRO >> 20
 - SNR1 >> n/a

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

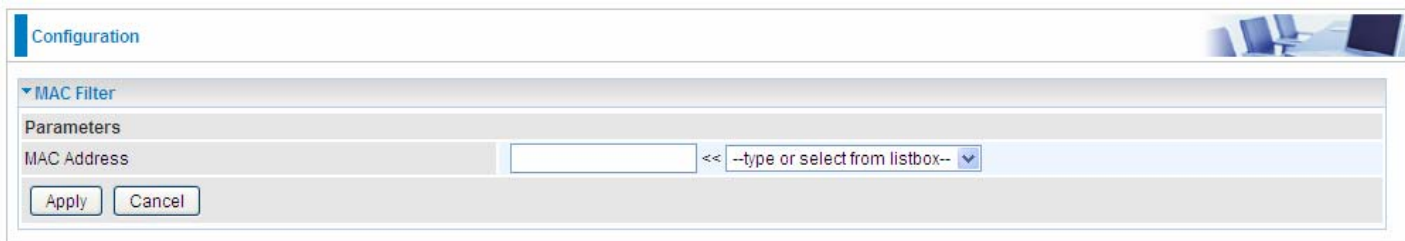
Add Remove

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

MAC Restrict Mode:

- ① **Disable:** disable the MAC Filter function.
- ① **Allow:** allow the hosts with the following listed MACs to access the wireless network.
- ① **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: << --type or select from listbox-- >>

Apply Cancel

MAC Address: Enter the MAC address(es) or select 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
E0:63:E5:C5:B2:B6	<input type="checkbox"/>	Edit

Add Remove

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other 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.

Here you can select what role the AP server has, AP or wireless bridge (WDS).

Configuration

Wireless Bridge

Parameters
You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. 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.

AP Mode: Access Point

Bridge Restrict: Enable

Remote Bridges MAC Address

Apply Refresh

AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- ① **Access Point:** the gateway communicates with both clients and bridges.
- ① **Wireless Bridge:** the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this 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
<input checked="" type="checkbox"/>	wlan-ap	00:04:ED:14:27:13

Apply Refresh

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

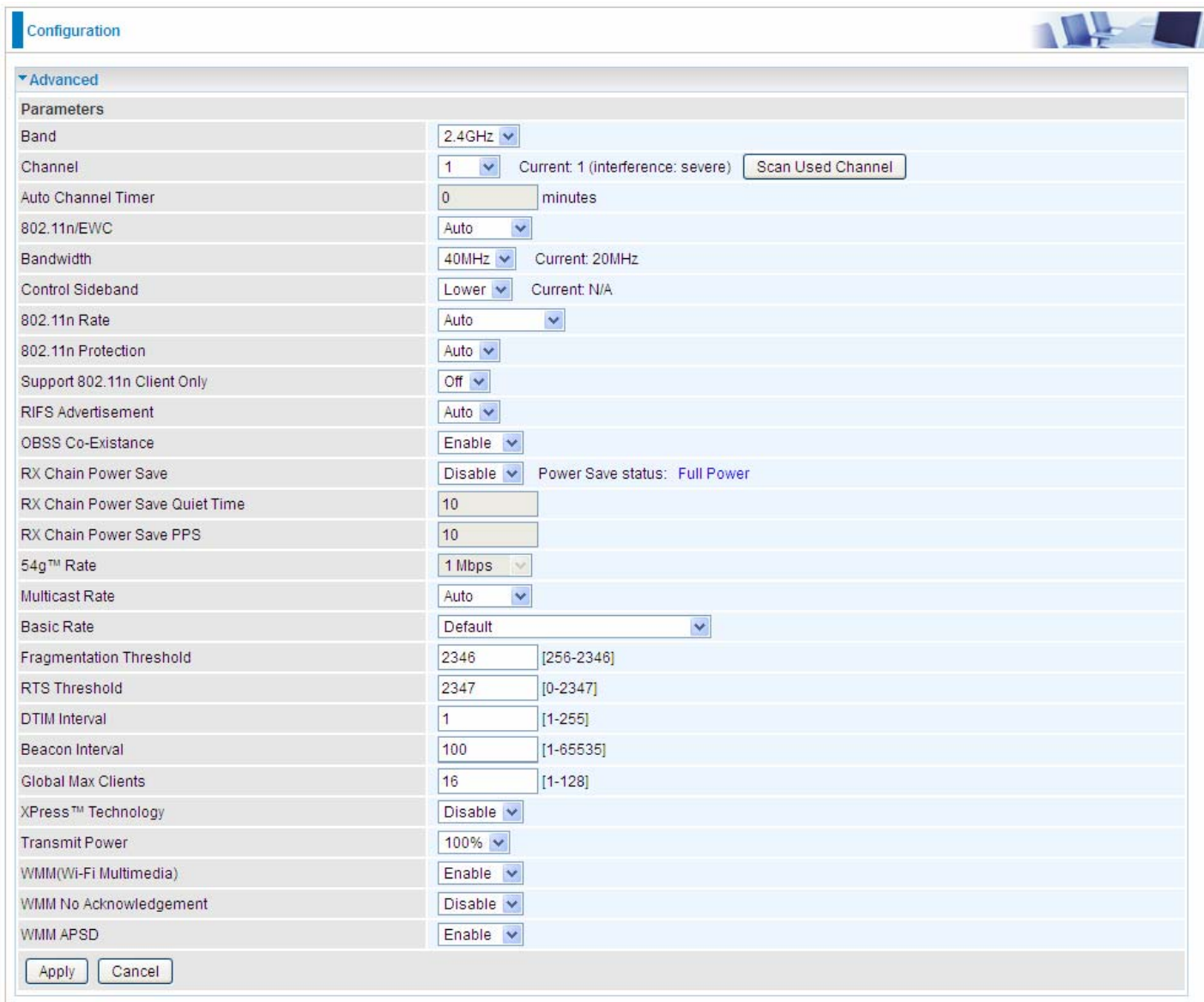
- ① **Disable:** Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.

Bridge Restrict	Disable
<input type="button" value="Apply"/>	<input type="button" value="Refresh"/>

Click **Apply** to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.



The screenshot shows a web-based configuration interface for wireless settings. The page is titled "Configuration" and has a sub-section for "Advanced". The "Parameters" section is expanded, showing a list of settings. Each setting has a label, a value field (either a dropdown menu or a text input), and sometimes a "Current" status or a "Scan Used Channel" button. The settings are as follows:

Parameter	Value	Current / Notes
Band	2.4GHz	
Channel	1	Current: 1 (interference: severe) [Scan Used Channel]
Auto Channel Timer	0	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 Co-Existence	Enable	
RX Chain Power Save	Disable	Power Save status: Full 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	

At the bottom of the configuration area, there are "Apply" and "Cancel" buttons.

Band: select frequency band. Here 2.4GHz.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

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

Auto Channel Timer (min): The auto channel times length it takes to scan in minutes. Only available for auto channel mode.

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

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

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. Auto for greater security.

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 a 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 a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

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.

Station Info

Here you can view information about the wireless clients.



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](#) .

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.

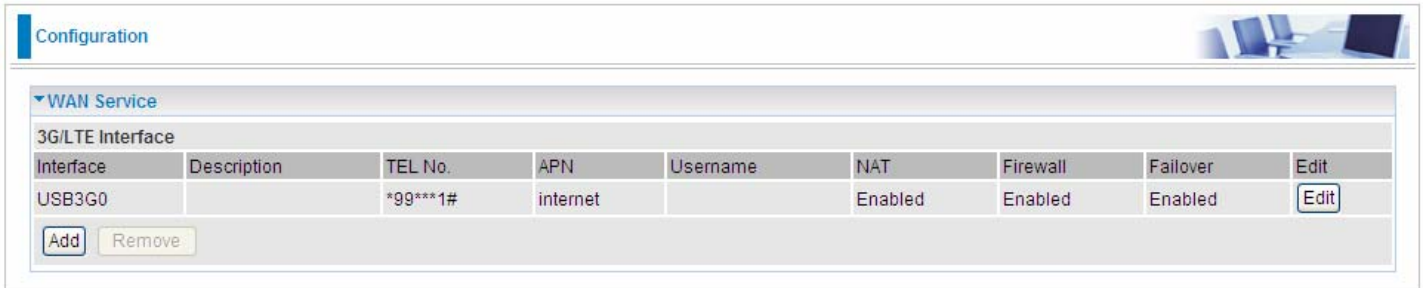
For example: user wants the SSID “*wlan-ap-2.4g*” to work on weekdays except for Wednesday, under this circumstance, user can set as shown below. (7820NZ offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals.)

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

Two WAN interfaces are provided for WAN connection: DSL and Ethernet.



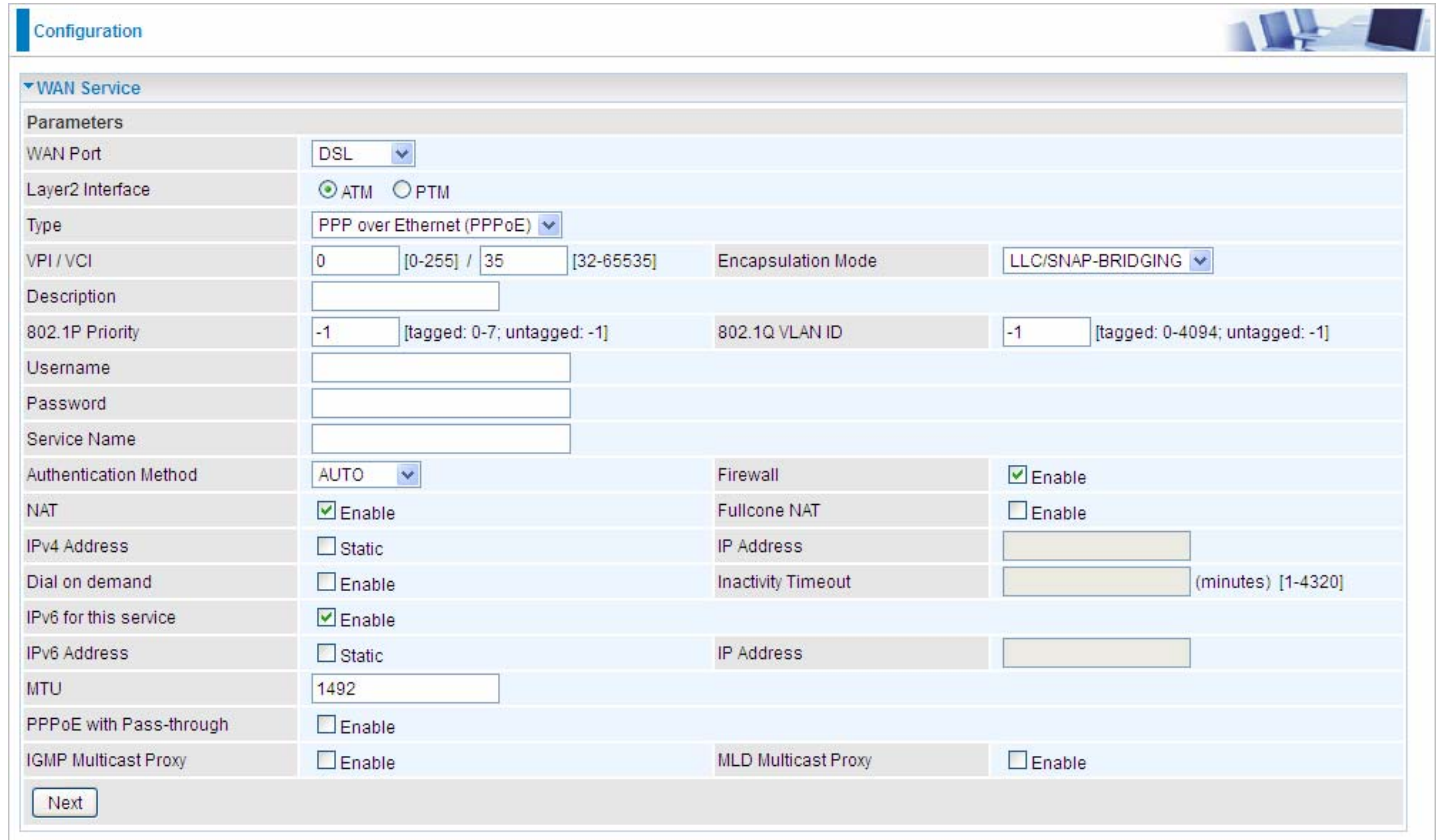
The screenshot shows a configuration page for WAN Service. At the top, there is a 'Configuration' header. Below it, a section titled 'WAN Service' contains a table for '3G/LTE Interface'. The table has columns for Interface, Description, TEL No., APN, Username, NAT, Firewall, Failover, and Edit. One entry is visible for 'USB3G0' with TEL No. '*99***1#' and APN 'internet'. Below the table are 'Add' and 'Remove' buttons.

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

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 and PTM, configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.



The screenshot shows a detailed configuration form for WAN Service. The 'WAN Port' is set to 'DSL'. Under 'Layer2 Interface', 'ATM' is selected. The 'Type' is 'PPP over Ethernet (PPPoE)'. 'VPI / VCI' is set to '0 / 35'. 'Encapsulation Mode' is 'LLC/SNAP-BRIDGING'. '802.1P Priority' is '-1' and '802.1Q VLAN ID' is '-1'. 'Authentication Method' is 'AUTO'. 'NAT' is checked 'Enable'. 'Firewall' is checked 'Enable'. 'Fullcone NAT' is unchecked. 'IPv4 Address' is unchecked 'Static'. 'IPv6 for this service' is checked 'Enable'. 'IPv6 Address' is unchecked 'Static'. 'MTU' is '1492'. 'PPPoE with Pass-through' is unchecked. 'IGMP Multicast Proxy' is unchecked. 'MLD Multicast Proxy' is unchecked. A 'Next' button is at the bottom.

Layer2 Interface: 2 transfer mode, ATM or PTM.

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

VCP/VPI: Enter the VCI/VPI 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 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 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.

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.

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

Configuration

▼ Default Gateway / DNS

Default Gateway

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
pppoe_0_8_35/ppp0.1	USB3G0
<input type="button" value="->"/> <input type="button" value="<-"/>	

Selected WAN Interface As The System Default IPv6 Gateway: pppoe_0_8_35/ppp0.1

DNS

DNS Server Interface: Available WAN Interfaces Static DNS Address Parent Controls

Selected DNS Server Interfaces	Available WAN Interfaces
pppoe_0_8_35/ppp0.1	USB3G0
<input type="button" value="->"/> <input type="button" value="<-"/>	

Primary DNS server:

Secondary DNS server:

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

DNS Server Interface: Available WAN Interfaces Static DNS IPv6 Address

WAN Interface selected: pppoe_0_8_35/ppp0.1

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

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	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	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	<input type="button" value="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				

Status

▼ Device Information

Model Name	BIPAC 7820NZ
Host Name	home.gateway
System Up-Time	0D 0H 4M 11S
Date/Time	Thu May 8 06:26:53 2014 <input type="button" value="Sync"/>
Software Version	2.32d.dr1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

▼ WAN

Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

Parameters			
WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM		
Type	PPPoA		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	VC/MUX
Description	<input type="text"/>		
Username	<input type="text"/>		
Password	<input type="text"/>		
Authentication Method	AUTO	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	<input type="text"/>
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	<input type="text"/> (minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable	IP Address	<input type="text"/>
IPv6 Address	<input type="checkbox"/> Static	IP Address	<input type="text"/>
MTU	1500		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> Enable

Next

VCP/VPI: Enter the VCI/VPI 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.

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.

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

WAN Service			
Parameters			
WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM		
Type	IP over Ethernet		
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]
Obtain an IP address automatically	<input checked="" type="checkbox"/> Enable		
Option 60 Vendor ID			
Option 61 Client ID			
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable		
MTU	1500	MAC Spoofing	
<input type="button" value="Next"/>			

VCP/VPI: Enter the VCI/VPI 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 61 Client ID: Enter the associated information provided by your ISP.

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**.

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 (**I**nternet **G**roup **M**embership 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.

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.

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 connecting in 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.

The screenshot shows a configuration window for WAN Service. Under the 'Parameters' section, the following settings are visible:

- WAN Port:** DSL
- Layer2 Interface:** ATM (selected), PTM
- Type:** IPoA
- VPI / VCI:** 0 [0-255] / 35 [32-65535]
- Encapsulation Mode:** LLC/SNAP-ROUTING
- Description:** (empty text box)
- WAN IP Address:** (empty text box)
- WAN Subnet Mask:** (empty text box)
- NAT:** Enable
- Fullcone NAT:** Enable
- Firewall:** Enable
- IGMP Multicast:** Enable

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

VCP/VPI: Enter the VCI/VPI 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 IP: Enter the WAN IP from the ISP.


WAN Subnet Mask: Enter the WAN Subnet Mask from the 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.

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 (**I**nternet **G**roup **M**embership 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.

Configuration 

▼ WAN Service

Parameters

WAN Port	DSL			Encapsulation Mode	LLC/SNAP-BRIDGING
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM				
Type	Bridging				
VPI / VCI	0	[0-255] /	35	[32-65535]	
Description					
802.1P Priority	-1	[tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1	[tagged: 0-4094; untagged: -1]

VCP/VPI: Enter the VCI/VPI 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.

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	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> 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	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> 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.

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.

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

The screenshot shows a configuration interface with two main sections: 'Default Gateway' and 'DNS'.
Default Gateway / DNS:
- **Default Gateway:** 'Selected Default Gateway Interfaces' contains 'ppp0.1'. 'Available Routed WAN Interfaces' contains '3G0/USB3G0'. A 'Selected WAN Interface As The System Default IPv6 Gateway' dropdown is set to 'pppoe_eth0/ppp0.1'.
- **DNS:** Radio buttons are set to 'Available WAN Interfaces'. 'Selected DNS Server Interfaces' contains 'ppp0.1'. 'Available WAN Interfaces' contains '3G0/USB3G0'.
- **IPv6 DNS:** Radio buttons are set to 'Available WAN Interfaces'. 'WAN Interface selected' dropdown is 'pppoe_eth0/ppp0.1'.
- There are input fields for 'Primary DNS server', 'Secondary DNS server', '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 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_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	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				

The device summary information

Status

▼ Device Information

Model Name	BiPAC 7820NZ
Host Name	home.gateway
System Up-Time	0D 0H 9M 34S
Date/Time	Thu May 8 08:32:16 2014 Sync
Software Version	2.32d.dr1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

▼ WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp0.1(Ethernet) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (Ethernet) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

WAN Service			
Parameters			
WAN Port	Ethernet		
Type	IP over Ethernet		
Description	<input type="text"/>		
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	<input checked="" type="checkbox"/> Enable		
Option 60 Vendor ID	<input type="text"/>		
Option 61 Client ID	<input type="text"/>		
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
WAN IP Address	<input type="text"/>		
WAN Subnet Mask	<input type="text"/>		
WAN gateway IP Address	<input type="text"/>		
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable		
WAN IPv6 Address/Prefix Length	<input type="text"/>		
WAN Next-Hop IPv6 Address	<input type="text"/>		
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable		
MTU	1500	MAC Spoofing	<input type="text"/>
<input type="button" value="Next"/>			

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

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

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

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

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

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 Client ID: Enter the associated information provided by your ISP.

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 pre-stored 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**.

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 (**I**nternet **G**roup **M**embership 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.

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.

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.

The screenshot shows a configuration page for 'WAN Service'. Under the 'Parameters' section, the following fields are visible:

WAN Port	Ethernet
Type	Bridging
Description	
802.1P Priority	-1 [tagged: 0-7; untagged: -1]
802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]

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

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.

① 3G/LTE

Select 3G/LTE to configure the route to enjoy the mobility. Given that BiPAC 7820NZ supports dual - SIM mobile connectivity, please determine which SIM you are gonna use or both (3G/LTE failover), and set the exact required connecting information for each SIM (SIM1 and SIM2). By default the 3G/LTE interface is on, user can edit the parameters to meet your own requirements.

Configuration

WAN Service

ATM Interface

Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/LTE Interface

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

[Add](#) [Remove](#)

Click **Edit** button to enter the 3G/LTE configuration page.

Configuration

WAN Service

Parameters

Failover Enable

SIM 1 (Current)

Mode: UMTS 3G preferred

TEL No.: *99***1# APN: internet

Username: Password:

Authentication Method: AUTO PIN:

Dial on demand Enable

Keep Alive Enable 7 seconds [1-86400]

IP Address: 8.8.8.8

MTU: 1500

SIM 2

Mode: UMTS 3G preferred

TEL No.: *99***1# APN: internet

Username: Password:

Authentication Method: AUTO PIN:

Dial on demand Enable

Keep Alive Enable 7 seconds [1-86400]

IP Address: 8.8.8.8

MTU: 1500

NAT Enable Firewall Enable

Selected Default Gateway Interfaces: USB3G0

Available Routed WAN Interfaces: ppp0.1, eth3.1

Obtain DNS: Use WAN Interface Use Static DNS Parent Controls

Selected DNS Server Interfaces: USB3G0

Available WAN Interfaces: ppp0.1, eth3.1

Primary DNS: Secondary DNS:

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply Cancel

Failover: If enabled, the 3G/LTE will work in failover mode and be brought up only when there is no active default route. In this mode, 3G/LTE work as a backup for the WAN connectivity. While if disabled, 3G/LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

SIM 1 & SIM 2

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

TEL No.: The dial string to make a 3G/LTE user internetworking call. It may provide by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The

service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

- ① **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 600 seconds.

Dial on demand	<input checked="" type="checkbox"/> Enable
Idle Timeout	<input type="text" value="600"/> seconds [10-86400]

- ① **Keep Alive:** Check Enable to allow the router to check the mobile connectivity every 7 (can be changed based on need) seconds by ping the IP address set below the keep the 3G/LTE link active.

IP Address: The IP address is used to "ping", and router will ping the IP to find whether the connection is still on.

Dial on demand	<input type="checkbox"/> Enable
Keep Alive	<input checked="" type="checkbox"/> Enable <input type="text" value="7"/> seconds [1-86400]
IP Address	<input type="text" value="8.8.8.8"/>

NAT: Check to enable the NAT function.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to [IP Filtering Incoming](#) to add allowing rules.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.


Select default gateway interfaces: Select from the interfaces the default gateway, here commonly we select ppp3g0.

Selected DNS Server Interfaces: Three ways to set a DNS server.

- ① **Available WAN interfaces:** Select a desirable WAN interface as the 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](#)).

Click **Apply** to confirm the settings.

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (Here user can see the 3G/LTE failover).

Status 

▼ WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured				
ppp3g0	3G0	PPP	Failover / Connected	00:01:10	10.44.183.197		221.5.4.55

Status 

▼ Device Information

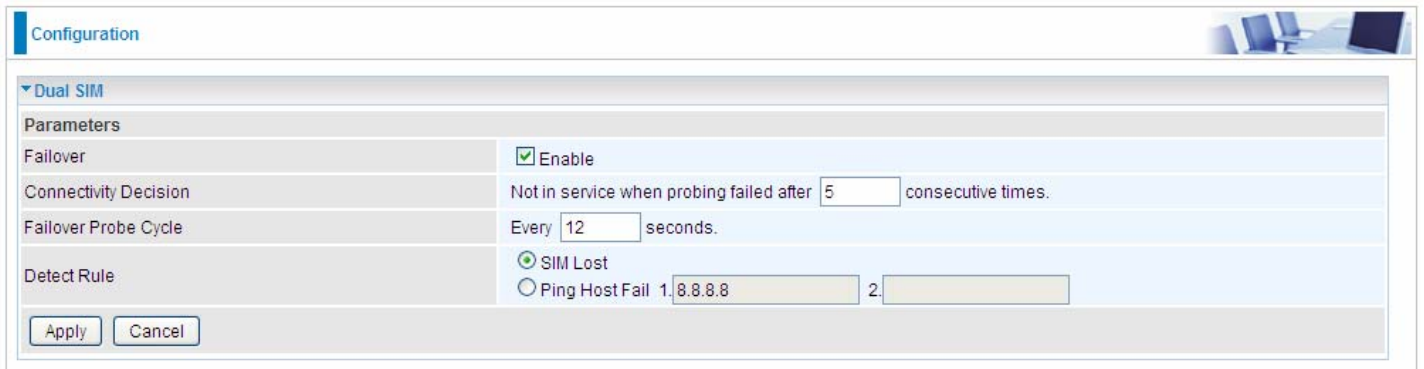
Model Name	BiPAC 7820NZ
Host Name	home.gateway
System Up-Time	0D 0H 12M 43S
Date/Time	Thu May 8 06:35:25 2014 <input type="button" value="Sync"/>
Software Version	2.32d.dr1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

▼ WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp3g0(3G/LTE) / 10.44.183.197
Connection Time	00:06:30
Primary DNS Server	221.5.4.55
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL)

Dual SIM

BiPAC 7820NZ offers dual-SIM slots for two mobile SIM cards. The SIM 1 will be in use when two SIM cards are both up. The current SIM connection will fail over to the other SIM connection when the situation below happens. But note when the failover is done, the connection cannot fail back to the previous SIM connection.



Configuration

▼ Dual SIM

Parameters

Failover	<input checked="" type="checkbox"/> Enable
Connectivity Decision	Not in service when probing failed after <input type="text" value="5"/> consecutive times.
Failover Probe Cycle	Every <input type="text" value="12"/> seconds.
Detect Rule	<input checked="" type="radio"/> SIM Lost <input type="radio"/> Ping Host Fail 1. <input type="text" value="8.8.8.8"/> 2. <input type="text"/>

Failover: Check Enable to activate failover feature.

Connectivity Decision: Set how many times of probing failure to switch to the other SIM.

Failover Probe Cycle: Set the time duration for the Probe Cycle to determine when the router will switch to the other SIM once the current SIM connection fails. For example, when set to 12 seconds, the probe will be conducted every 12 seconds.

Detect Rule: Choose the probe policy, to Ping Host or when SIM lost

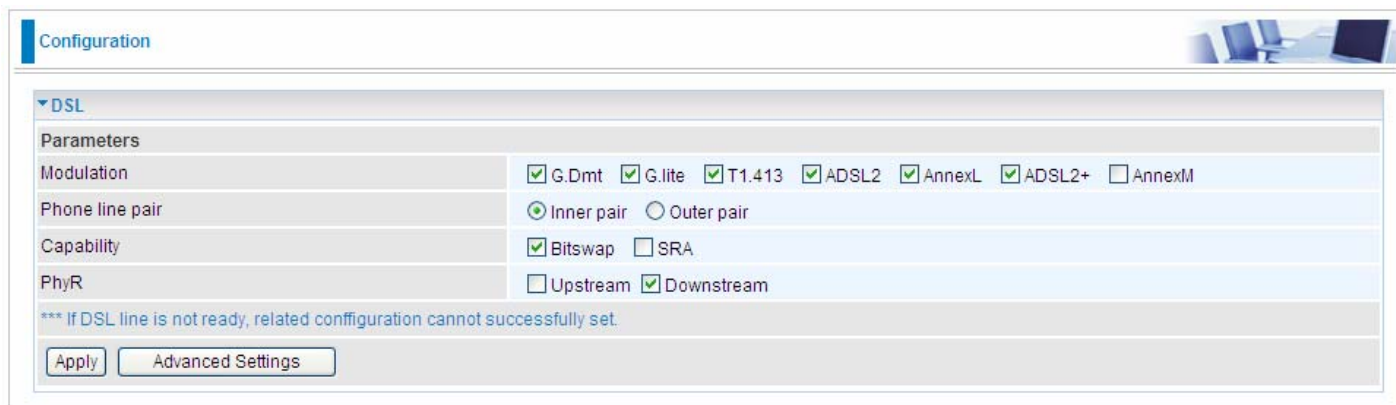
- ① **SIM Lost:** SIM card absent or not be able to establish connection.
- ① **Ping Host Fail:** It will send ping packets to host pre-set, and wait for response from it in every “Probe Cycle” to check the connectivity to the mail SIM.

Note:

The time set is for each probe cycle, but the decision to change to the other SIM is determined by Probe Cycle multiplied by connection Decision amount (e.g. From the image above it will be 12 seconds multiplied by 5 consecutive fails, the router will determine failover to another SIM).

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 screenshot shows a web interface titled "Configuration" with a sub-section for "DSL". Under "Parameters", there are four rows of settings:

Modulation	<input checked="" type="checkbox"/> G.Dmt <input checked="" type="checkbox"/> G.lite <input checked="" type="checkbox"/> T1.413 <input checked="" type="checkbox"/> ADSL2 <input checked="" type="checkbox"/> AnnexL <input checked="" type="checkbox"/> ADSL2+ <input type="checkbox"/> AnnexM
Phone line pair	<input checked="" type="radio"/> Inner pair <input type="radio"/> Outer pair
Capability	<input checked="" type="checkbox"/> Bitswap <input type="checkbox"/> SRA
PhyR	<input type="checkbox"/> Upstream <input checked="" type="checkbox"/> Downstream

Below the settings is a warning message: "*** If DSL line is not ready, related configuration cannot successfully set." At the bottom are two buttons: "Apply" and "Advanced Settings".

Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, “ADSL2+”, “AnnexM” that user can select for this connection.

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 bitswapping 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.

Click [Advanced Settings](#) to future configure DSL.



The screenshot shows the "DSL Advanced Settings" section of the configuration page. Under "Parameters", there is a "Test Mode" row with five radio button options: "Normal" (selected), "Reverb", "Medley", "No Retrain", and "L3". At the bottom are two buttons: "Apply" and "Tone Selection".

Select the Test Mode, or leave it as default.

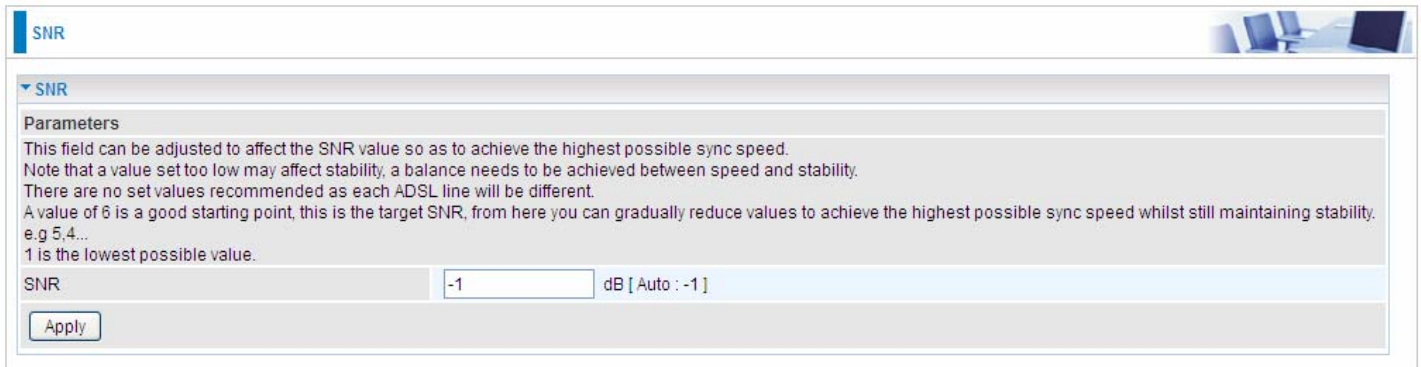
Tone Selection: This should be left as default or be configured by an advanced user.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream.

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 web-based configuration interface for SNR. At the top left, there is a blue header with the text "SNR". Below this, a dropdown menu is set to "SNR". Underneath, a section titled "Parameters" contains the following 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 the text is a form field labeled "SNR" with the value "-1" entered, followed by the unit "dB [Auto : -1]". At the bottom left of the form is an "Apply" button.

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	<input checked="" type="checkbox"/> Enable
First NTP time server	Other <input type="text" value="192.43.244.18"/>
Second NTP time server	Other <input type="text" value="128.138.140.44"/>
Third NTP time server	Other <input type="text" value="129.6.15.29"/>
Fourth NTP time server	Other <input type="text" value="131.107.1.10"/>
Fifth NTP time server	None <input type="text"/>
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Apply Cancel

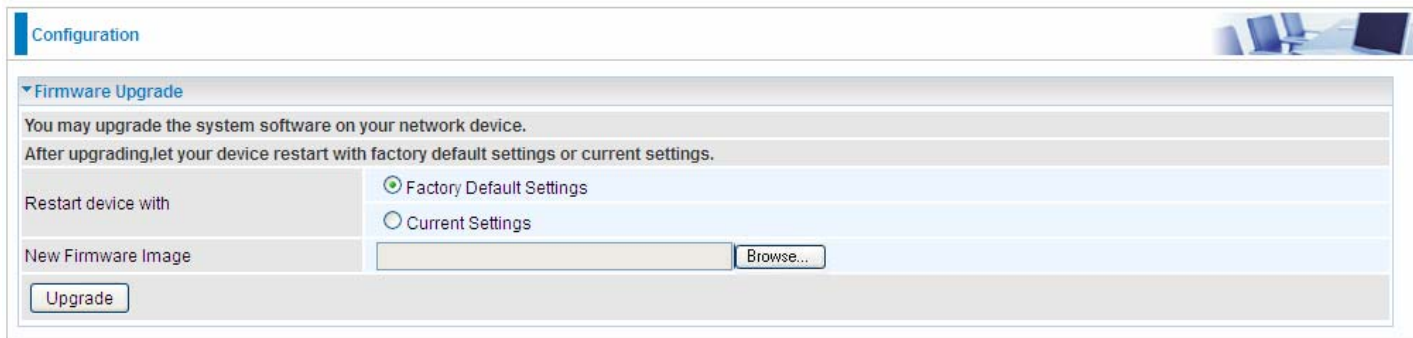
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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 the 'Configuration' page for a router, specifically the 'Firmware Upgrade' section. The page has a light blue header with 'Configuration' on the left and a small image of a router on the right. Below the header, the 'Firmware Upgrade' section is expanded, showing instructions: '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 for 'Restart device with': 'Factory Default Settings' (selected) and 'Current Settings'. Below this is a 'New Firmware Image' field with a 'Browse...' button. 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.

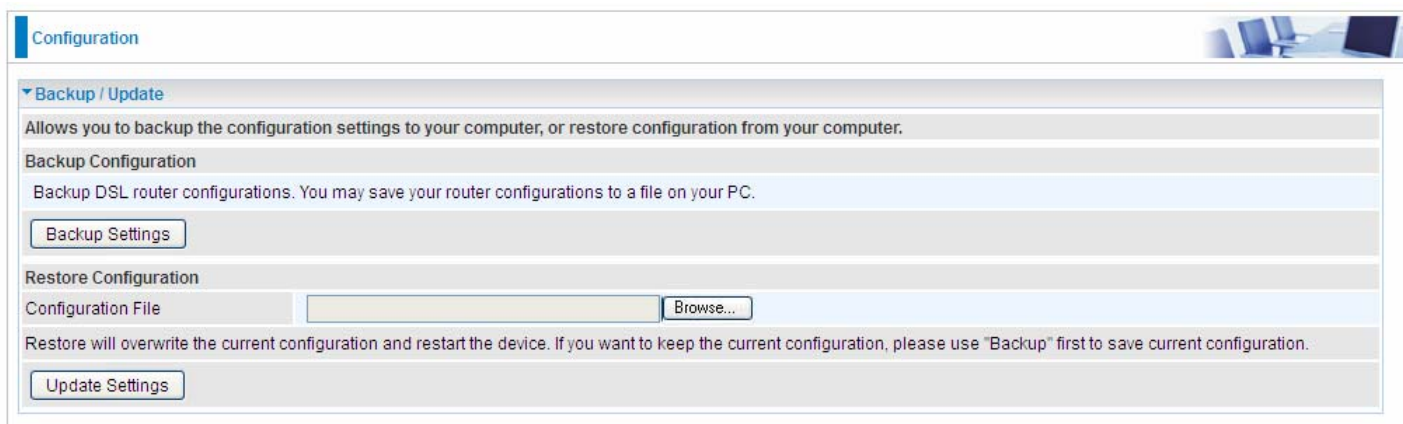


Warning

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.

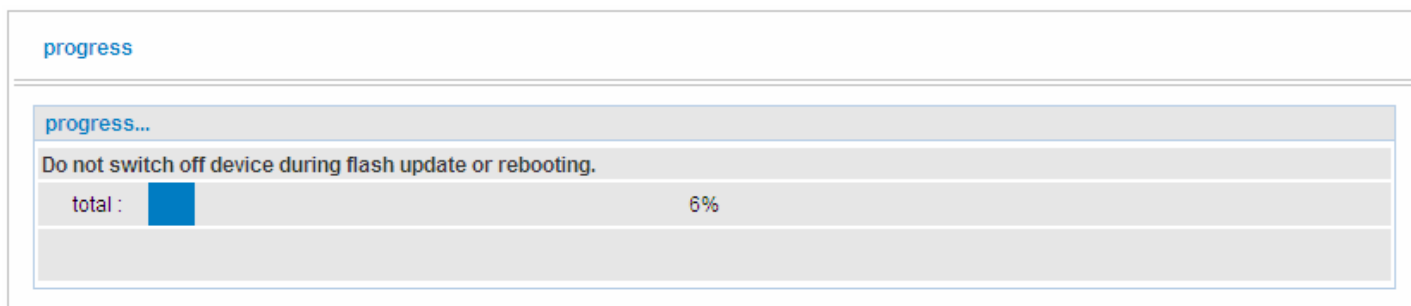


The screenshot shows the 'Configuration' page with a sub-section titled 'Backup / Update'. It contains the following elements:

- A header 'Configuration' with a small image of a laptop and chair.
- A dropdown menu 'Backup / Update'.
- A description: 'Allows you to backup the configuration settings to your computer, or restore configuration from your computer.'
- A section 'Backup Configuration' with the text: 'Backup DSL router configurations. You may save your router configurations to a file on your PC.'
- A button 'Backup Settings'.
- A section 'Restore Configuration'.
- A text input field for 'Configuration File' and a 'Browse...' button.
- A warning: '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.'
- A button '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.

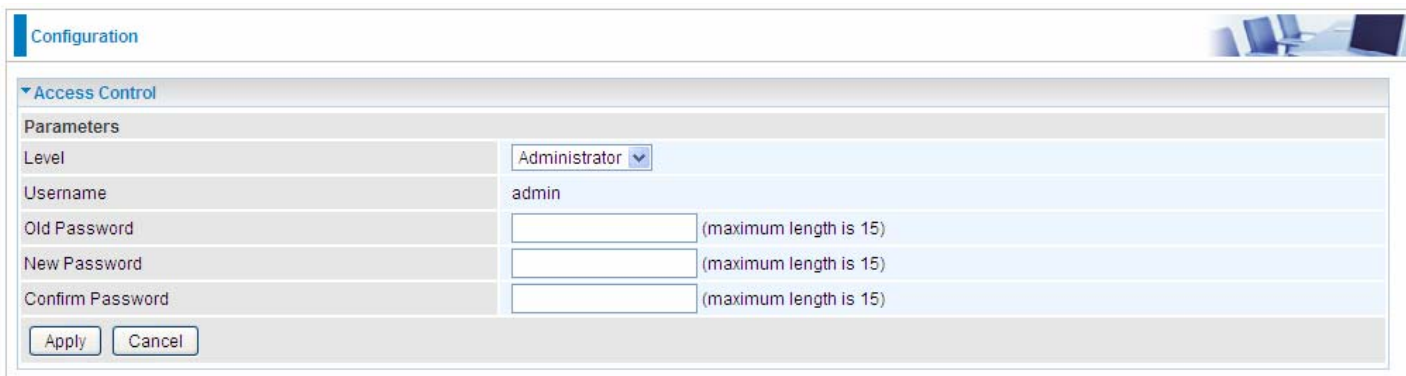


The screenshot shows a 'progress' screen with the following elements:

- A header 'progress'.
- A sub-header 'progress...'.
- A warning: 'Do not switch off device during flash update or rebooting.'
- A progress bar showing 'total :' followed by a blue bar and '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' dropdown is set to 'Administrator'. The 'Username' field contains 'admin'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom, there 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 lit items would be listed for common user, corresponding default username password are user and user respectively.

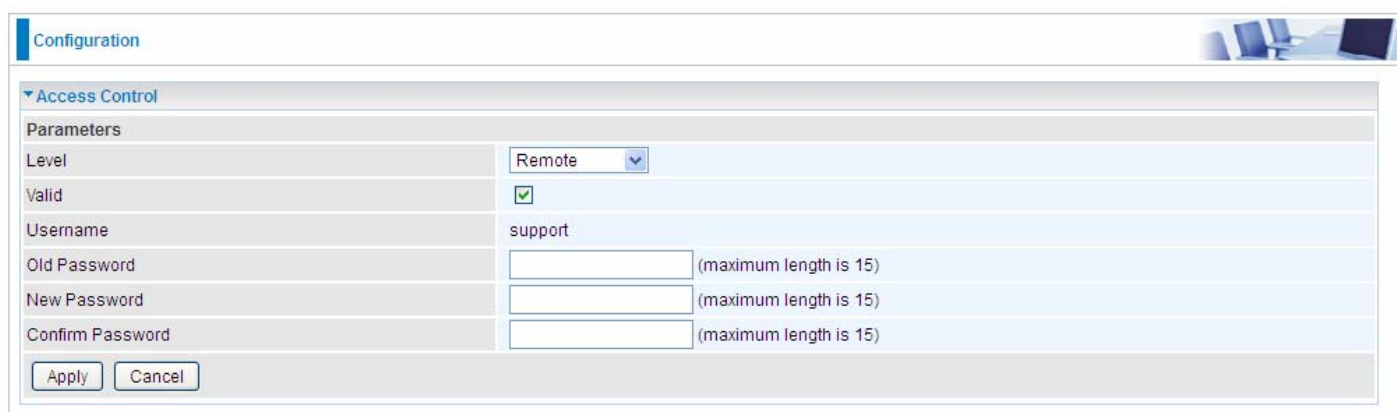
Username: the default username for each user level.

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' dropdown is set to 'Remote'. The 'Valid' checkbox is checked. The 'Username' field contains 'support'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom, there 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.

The screenshot shows a web-based configuration page for 'Mail Alert'. The page is titled 'Configuration' and has a 'Mail Alert' section expanded. The 'Server Information' section includes the following fields: WAN Port (set to DSL), Apply all the settings to (with checkboxes for Ethernet and 3G/LTE), SMTP Server, Username, Password, Sender's E-mail (with a validation note '(Must be xxx@yyy.zzz)'), SSL / TLS (with an 'Enable' checkbox), and Port (set to 25). There is an 'Account Test' button. Below this, under 'WAN IP Change Alert', there is a 'Recipient's E-mail' field (with validation note '(Must be xxx@yyy.zzz)'). Below that, under '3G/LTE Usage Allowance', there is another 'Recipient's E-mail' field (with validation note '(Must be xxx@yyy.zzz)'). At the bottom are 'Apply' and 'Cancel' buttons.

WAN Port: Mail Alert feature can be applicable to every WAN mode: Ethernet, DSL and 3G/LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

Apply all settings to: check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL: check to whether to enable SSL encryption feature.

Port: the port, default is 25.

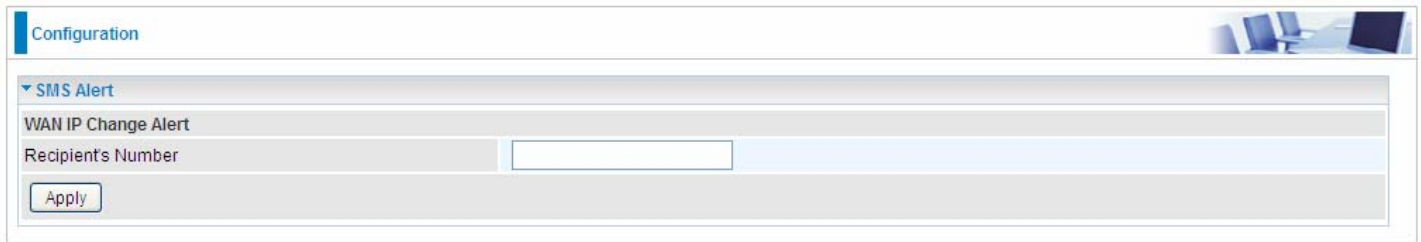
Account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

Recipient's Email (3G/LTE Usage Allowance): Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

SMS Alert

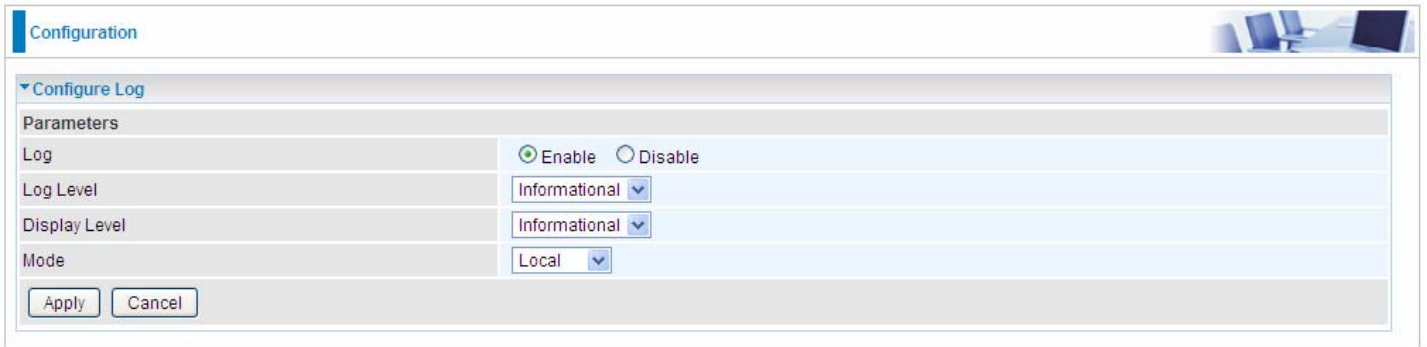
SMS, Short Message Service, is to inform clients the information clients subscribe. The BiPAC 7820NZ offers SMS alert sending clients alert messages when a WAN IP change is detected.



The screenshot shows a web interface for configuring SMS alerts. At the top, there is a 'Configuration' tab. Below it, a section titled 'SMS Alert' is expanded. Under this section, there is a 'WAN IP Change Alert' heading. Below the heading is a 'Recipient's Number' label followed by an empty text input field. At the bottom of this section is an 'Apply' button.

Recipient's Number (WAN IP Change Alert): Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

Configure Log



Configuration

Configure Log

Parameters

Log Enable Disable

Log Level Informational

Display Level Informational

Mode Local

Apply Cancel

Log: Enable or disable this function.

Log level: Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- 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.

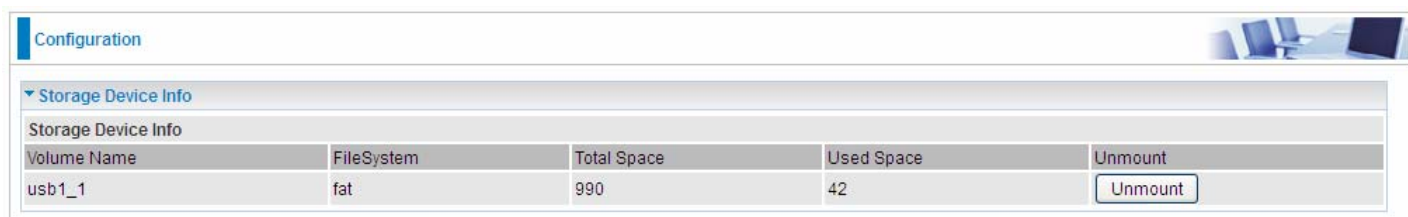
Click **Apply** to save your settings.

USB

Storage here refers to network sharing in the network environment, USB devices act as the storage carrier for **DLNA**, NAS (**Samba server**, **FTP server**).

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.



The screenshot shows a web interface with a 'Configuration' header. Below it is a section titled 'Storage Device Info' which contains a table with the following data:

Volume Name	FileSystem	Total Space	Used Space	Unmount
usb1_1	fat	990	42	<input type="button" value="Unmount"/>

Volume Name: Display the storage volume name

FileSystem: Display the storage device's file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

Used Space: Display the remaining space of each partition, unit MB.

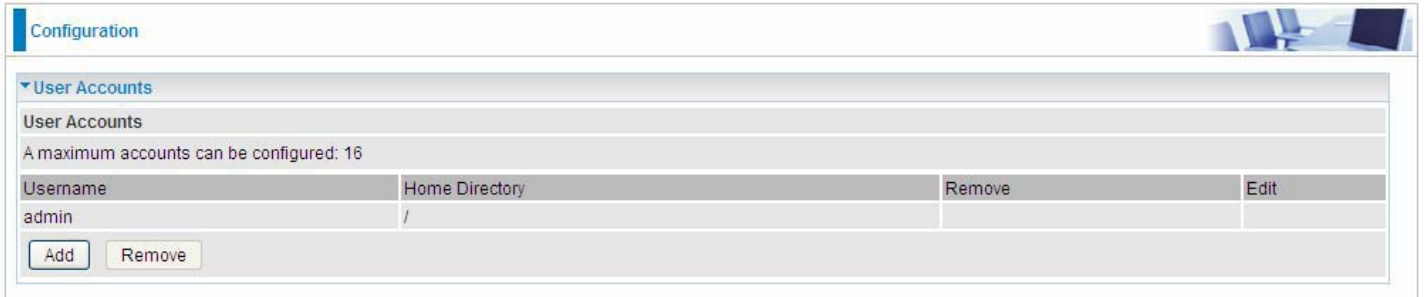
Unmount: Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

User Account

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Users added here are entitled to have access to both **Samba server** and **FTP server**.

Default user admin.



Configuration

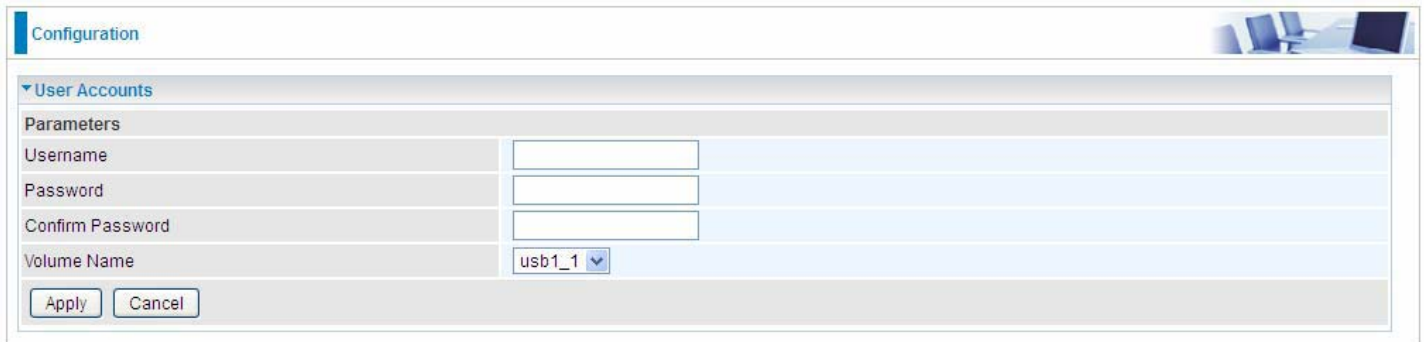
▼ User Accounts

User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		

Click **Add** button, enter the user account-adding page:



Configuration

▼ User Accounts

Parameters

Username

Password

Confirm Password

Volume Name

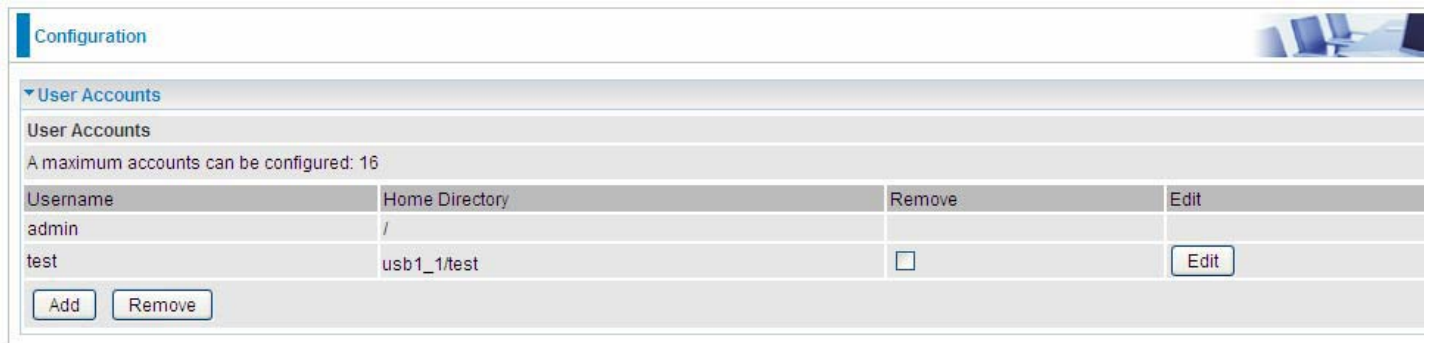
Username: user-defined name, but simpler and more convenient to remember would be favorable.

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 usb1_1.



Configuration

▼ User Accounts

User Accounts

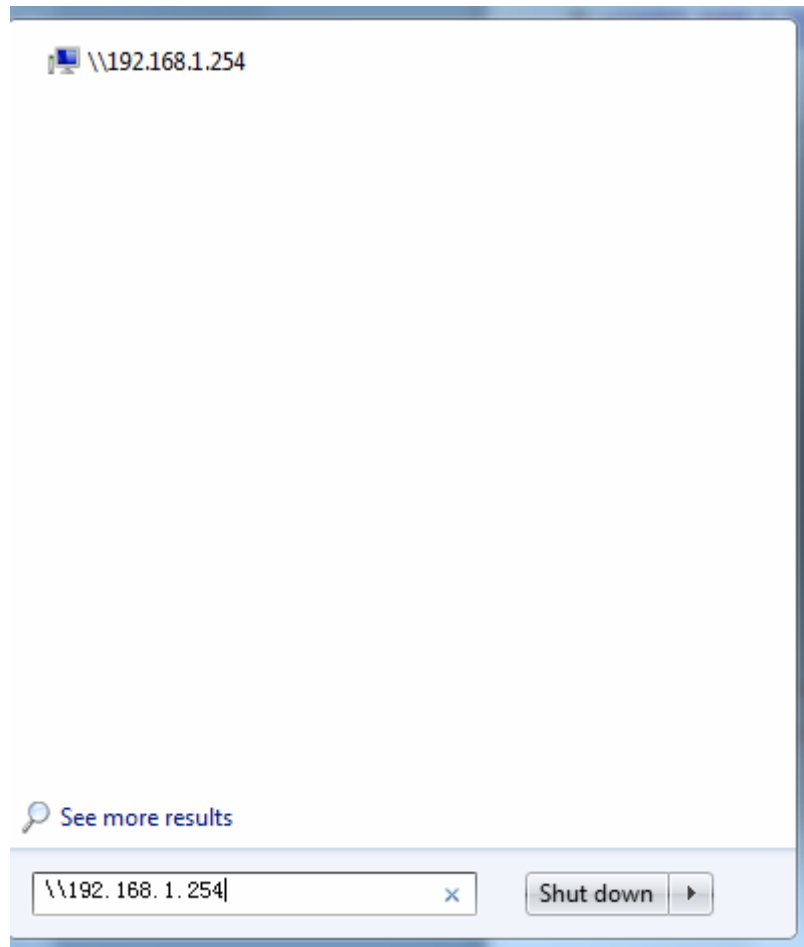
A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		
test	usb1_1/test	<input type="checkbox"/>	<input type="button" value="Edit"/>

The user “test” has the right to access both **Samba** and **FTP server**.

How to access Samba:

In your computer, Click **Start** > **Run**, enter [\\192.168.1.254](#) (LAN IP)

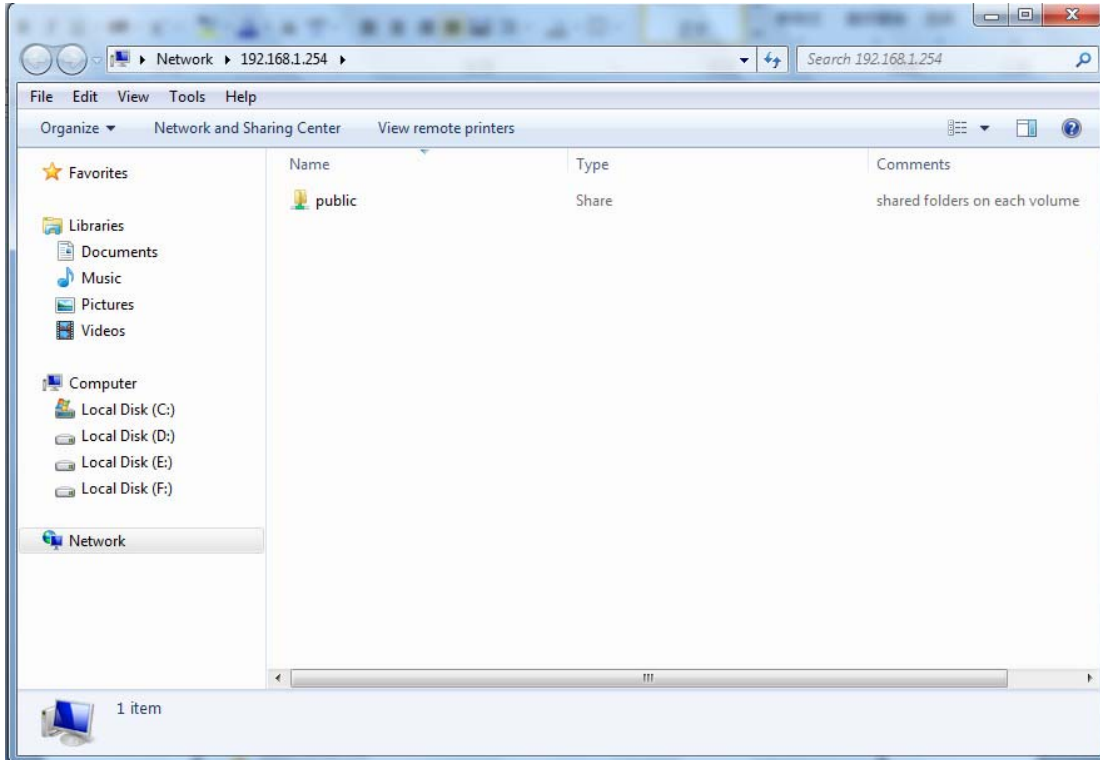


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

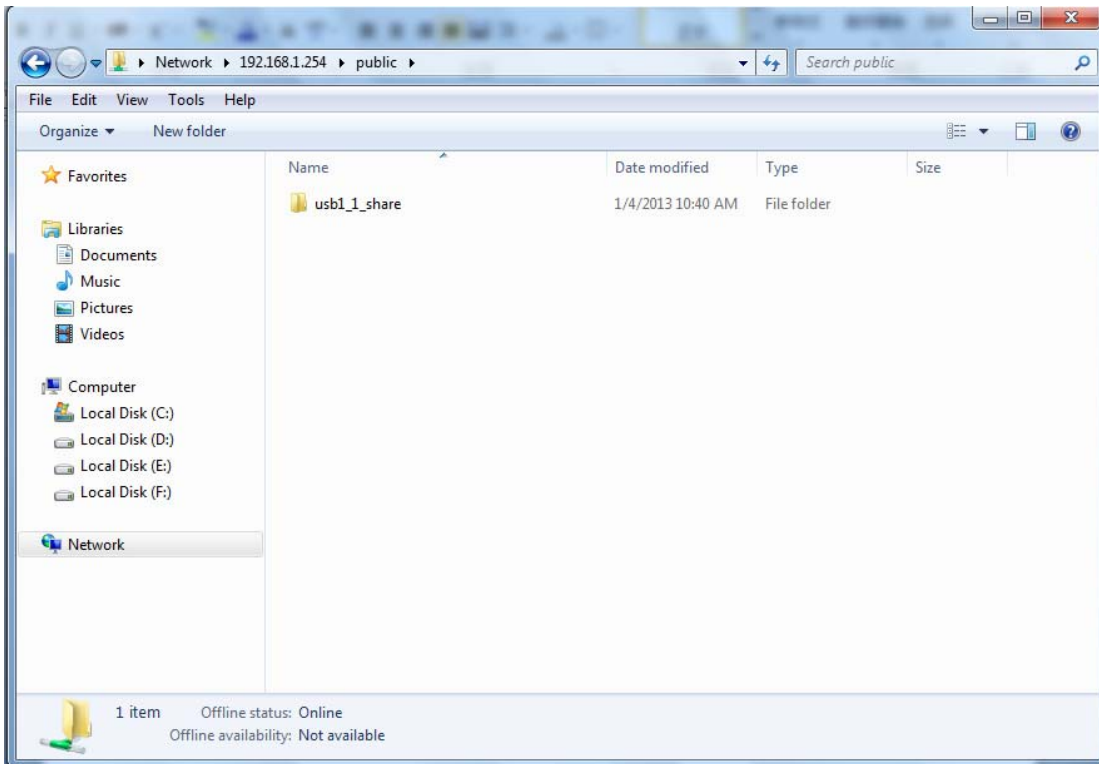
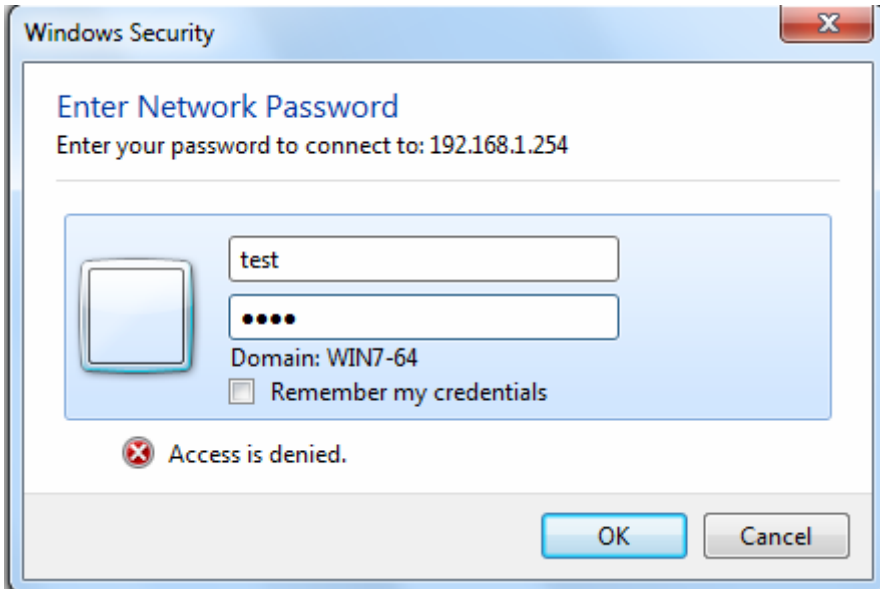
When first logged on to the network folder, you will see the “**public**” folder.

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

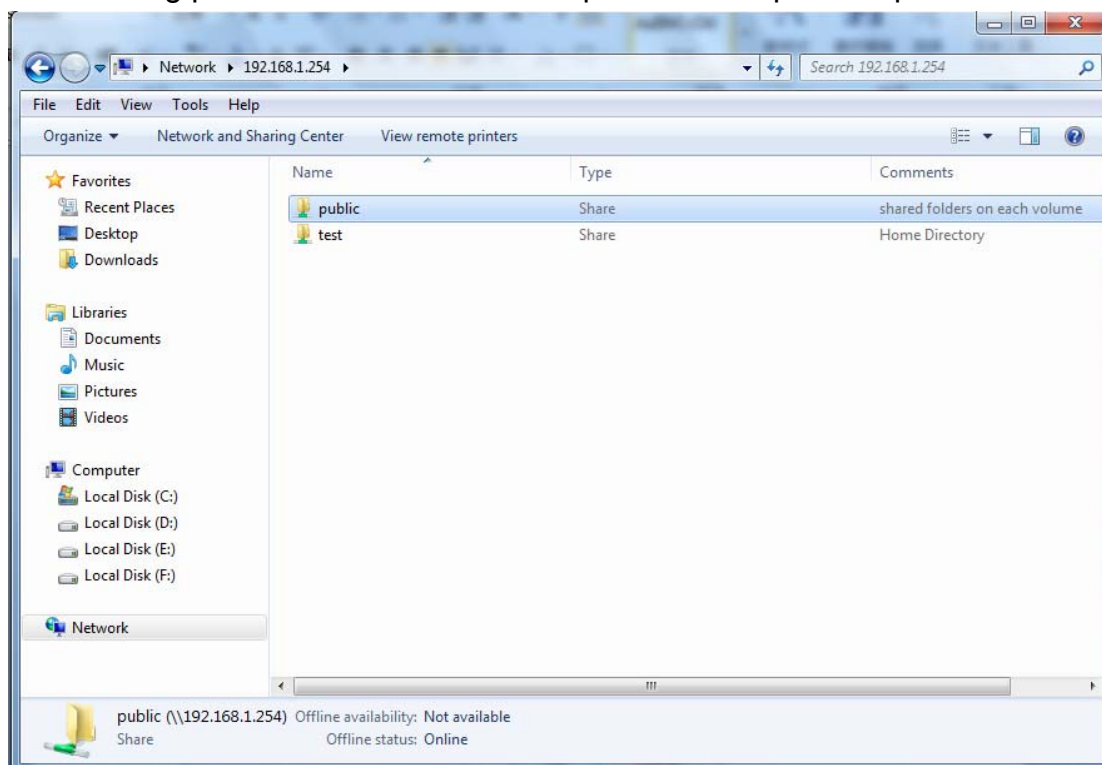
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



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.



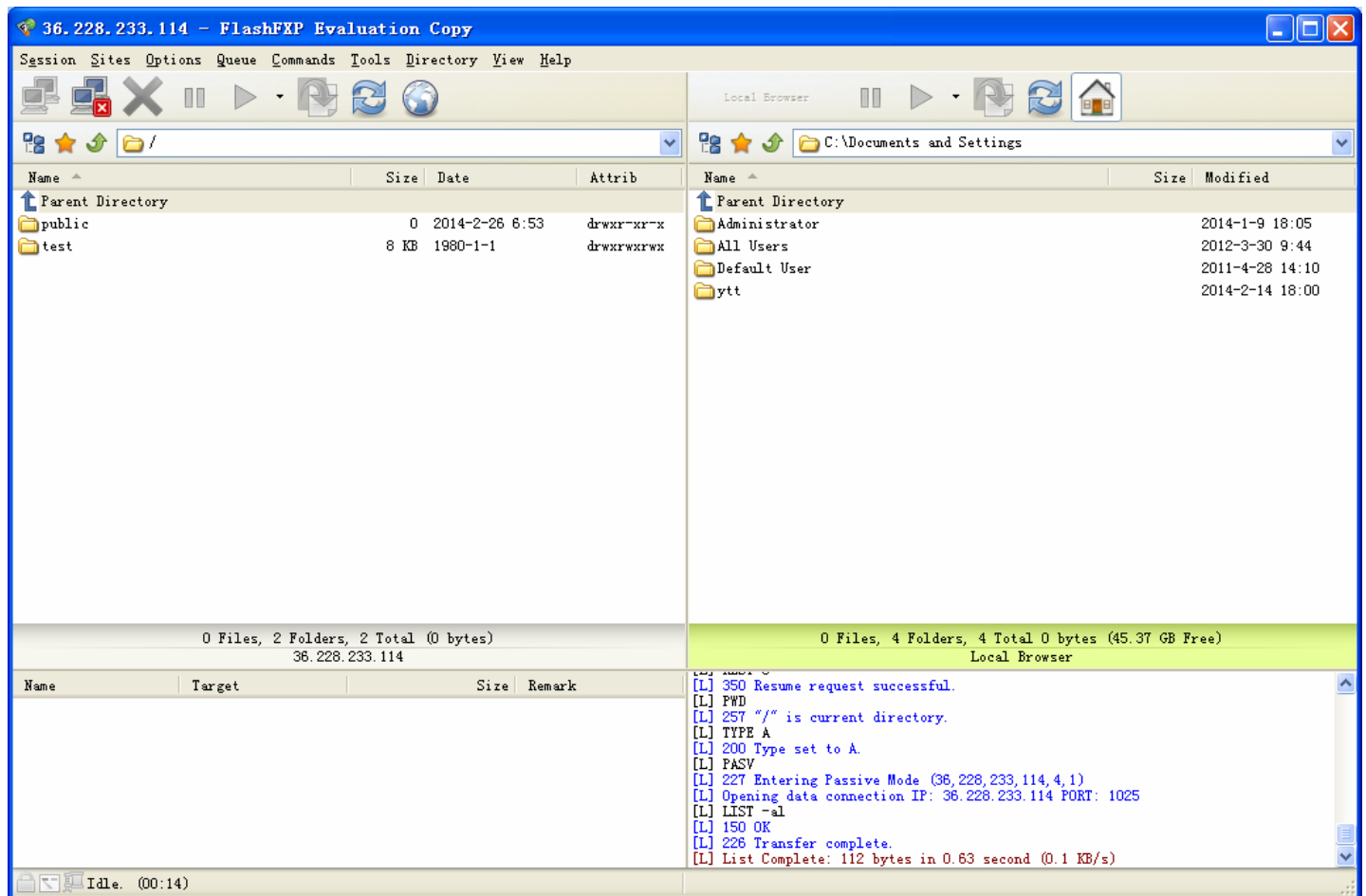
How to use FTP:

Please **note** to enable remote FTP access in [Remote Access](#).

1. Access via FTP tools

Take popular FTP tool of FlashFXP for example:

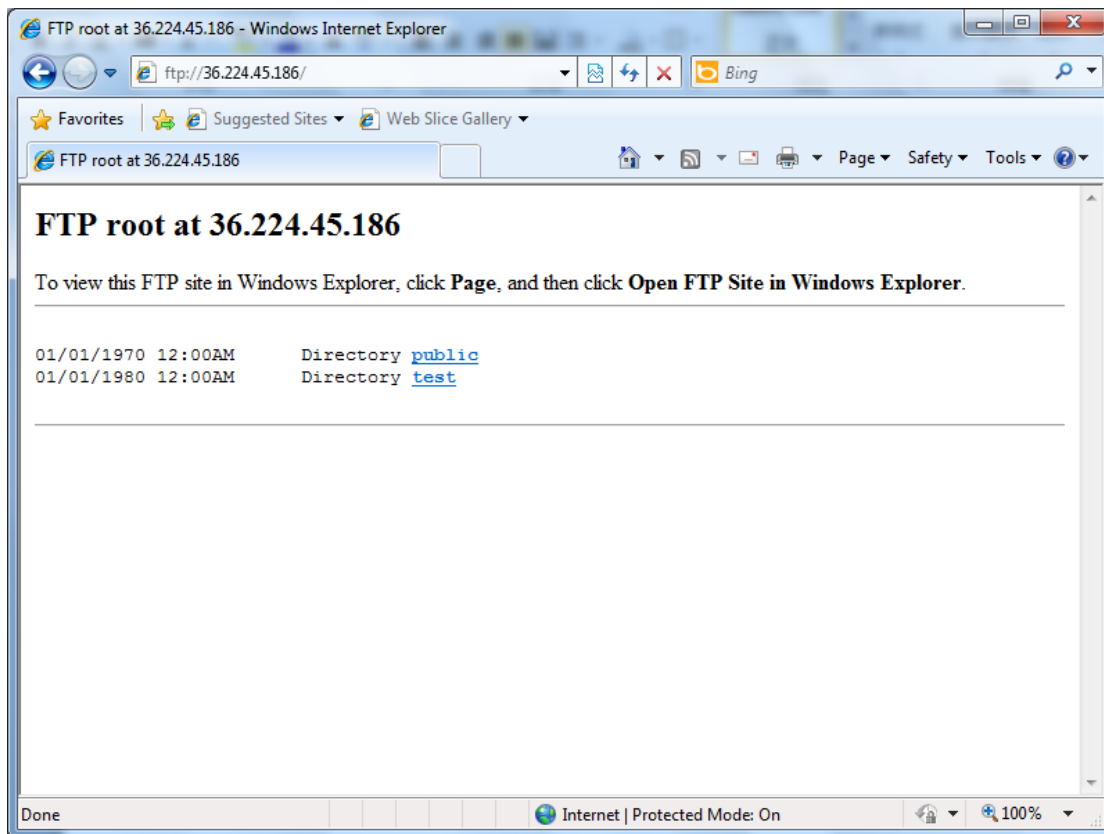
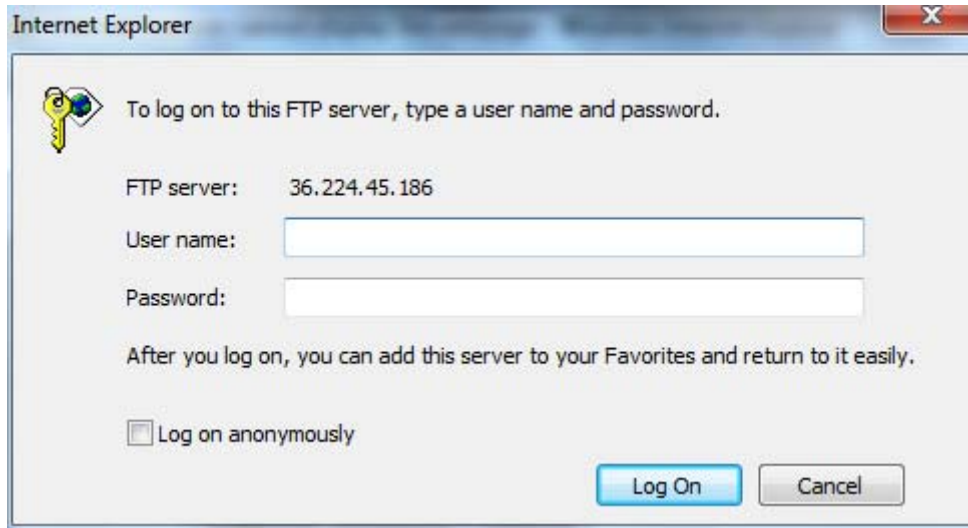
- 1) Open FlashFXP
- 2) Create ftp sites (LAN IP / WAN IP, and set the account, port).
- 3) Connect to the ftp site.



2. Web FTP access

1) Enter <ftp://admin@WAN-IP> or <ftp://admin@LAN-IP> at the address bar of the IE. In terms of other browsers, type <ftp://WAN-IP> or <ftp://LAN-IP> directly.

2) Enter the account's username and password.



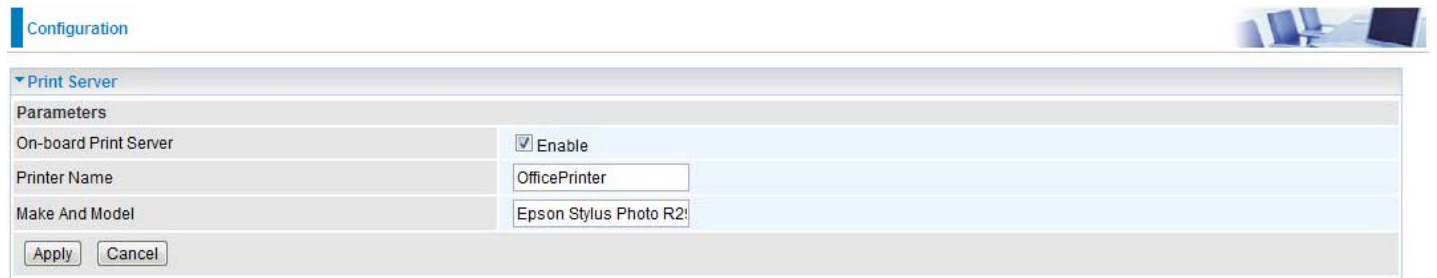
Print Server

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 7820NZ. 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 (7820NZ for example)

1. Connect the printer to the 7820NZ's USB port
2. Enable the print server on the 7820NZ
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*

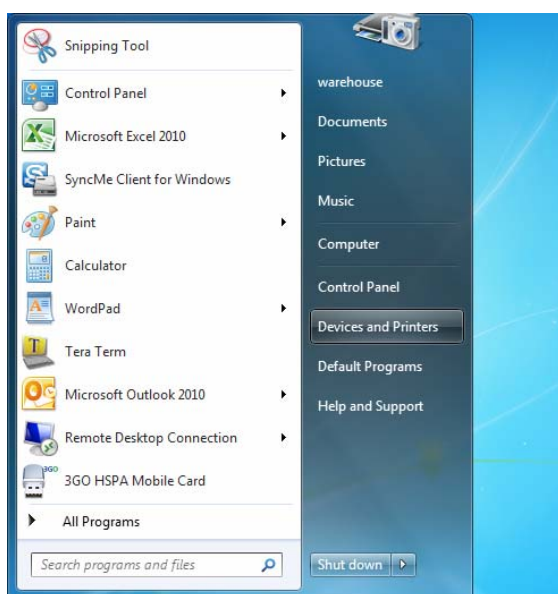
Note:

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.

Set up of Printer client (Windows 7)

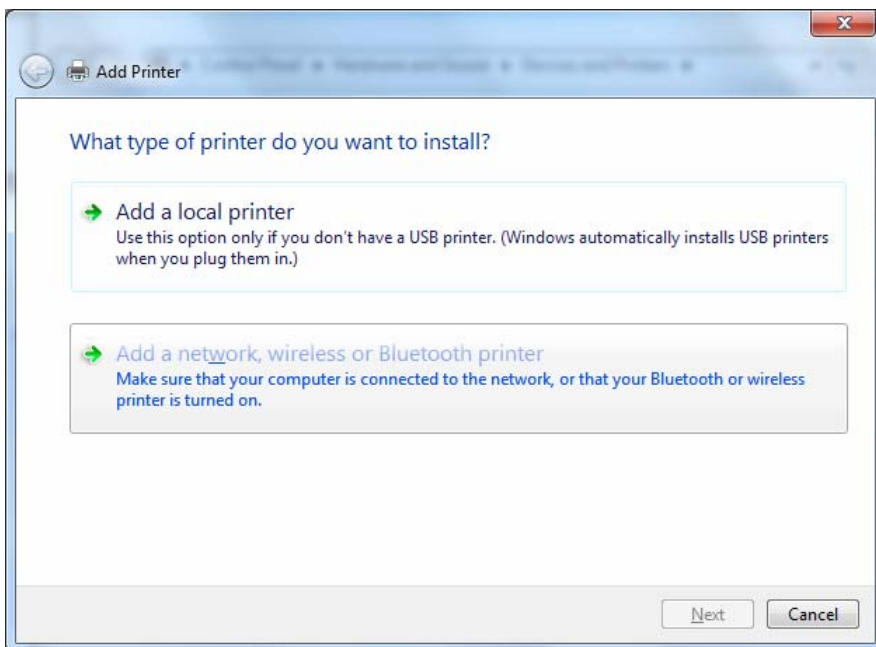
Step 1: Click **Start** and select "Devices and Printers"



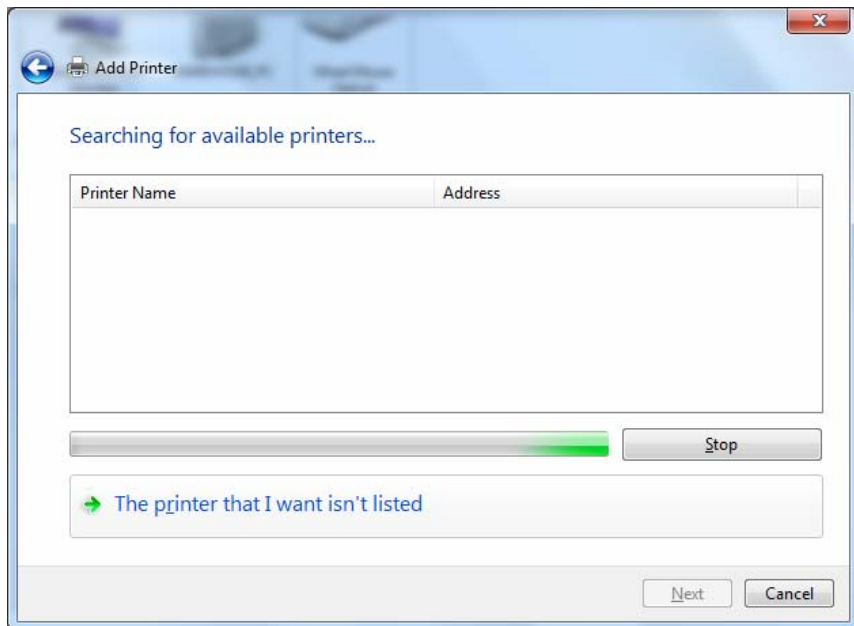
Step 2: Click "Add a Printer".



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



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

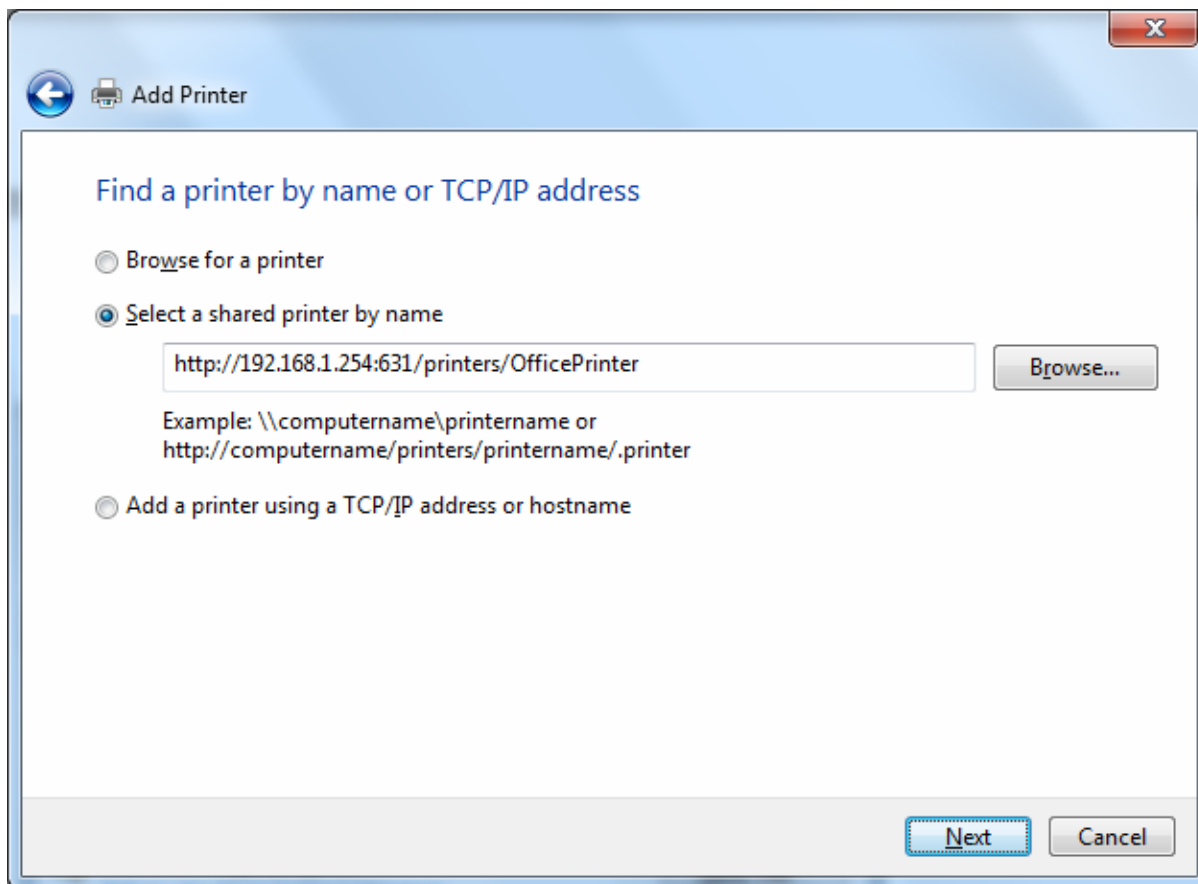


Step 5: Select “Select a shared printer by name”

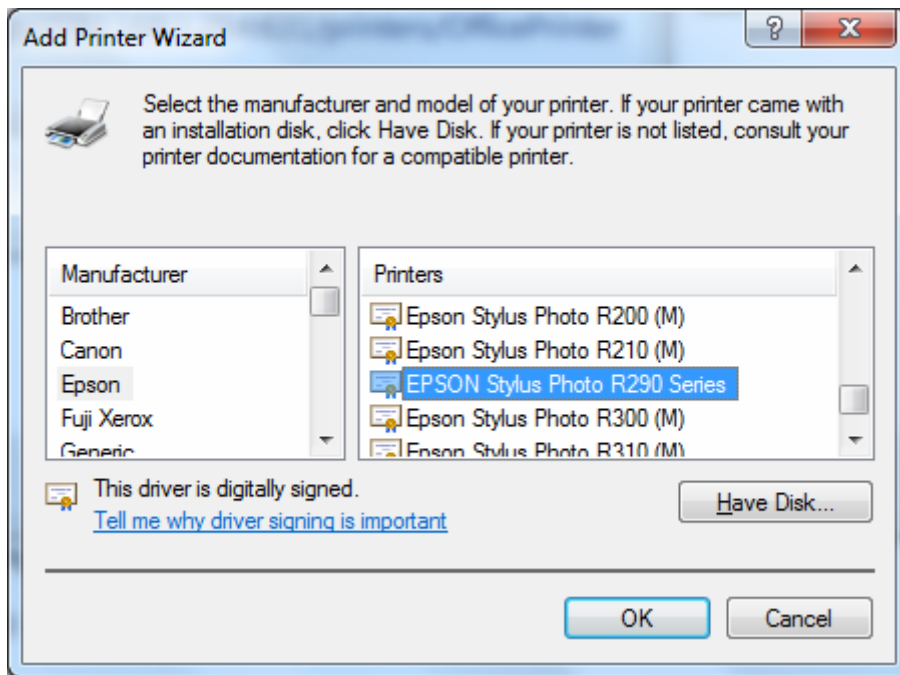
Enter `http://7820NZ- LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the 7820NZ earlier

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

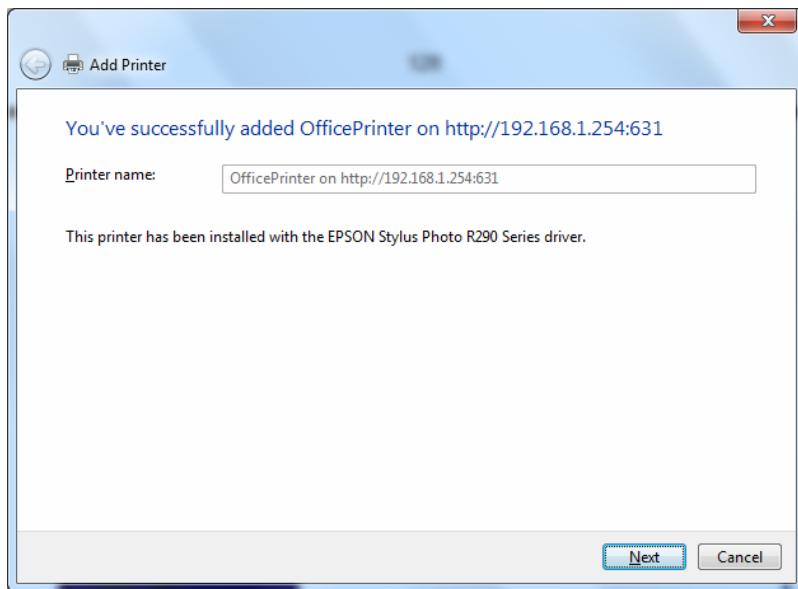
OfficePrinter is the Printer Name we setup earlier



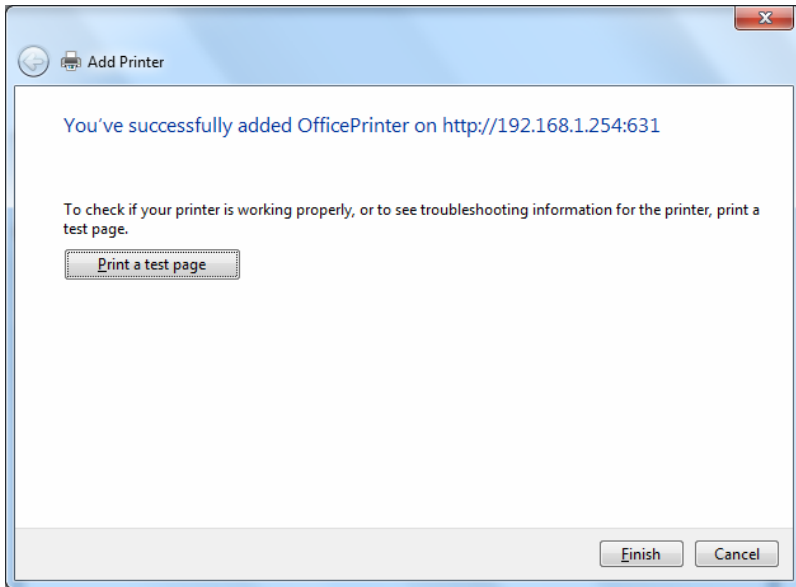
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



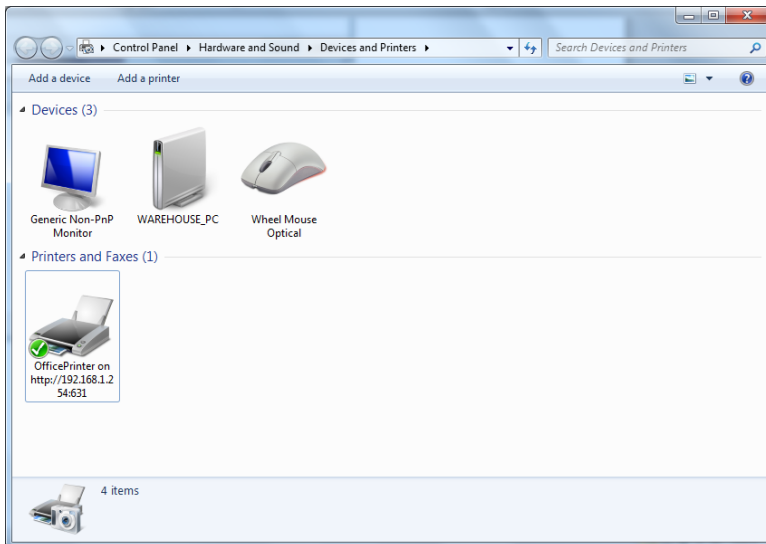
Step 7: Click “Next”



Step 8: Click “Next” and you are done



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



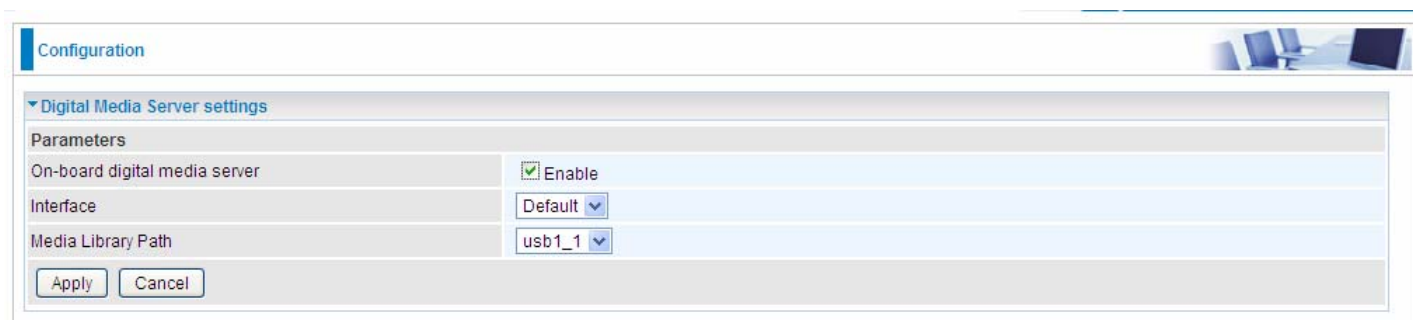
DLNA

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, 7820NZ can serve as a DLNA server.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Digital Media Server settings". Under "Parameters", there are three settings: "On-board digital media server" is checked and set to "Enable"; "Interface" is set to "Default"; and "Media Library Path" is set to "usb1_1". At the bottom of the settings area are "Apply" and "Cancel" buttons.

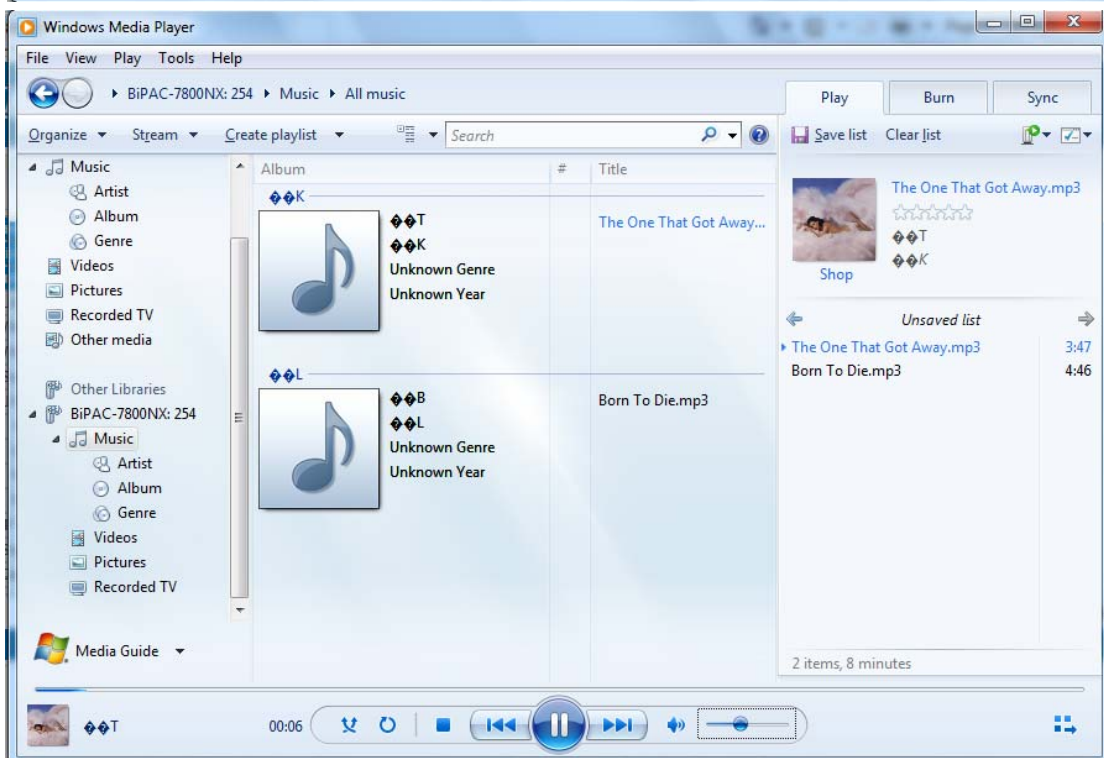
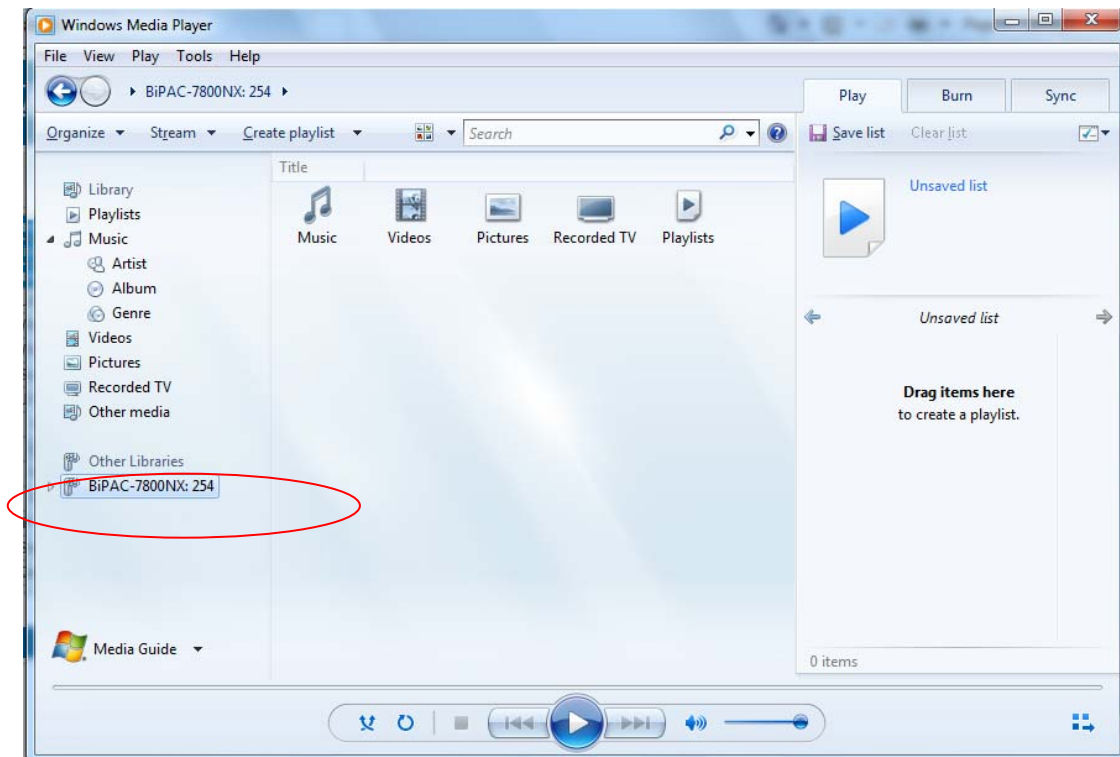
Parameters	
On-board digital media server	<input checked="" type="checkbox"/> Enable
Interface	Default
Media Library Path	usb1_1

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 usb1_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.

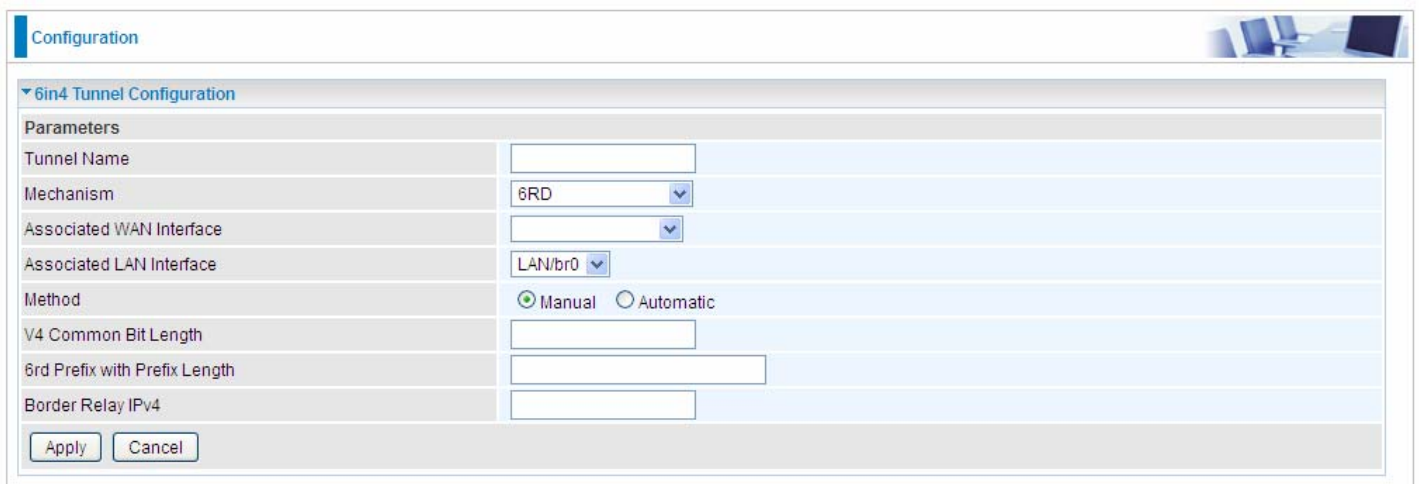
6RD:

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.



Click **Add** button to manually add the 6in4 rules.



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

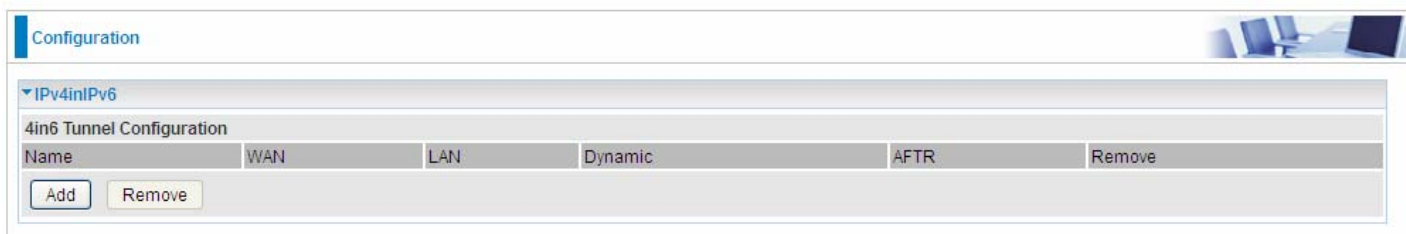
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

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

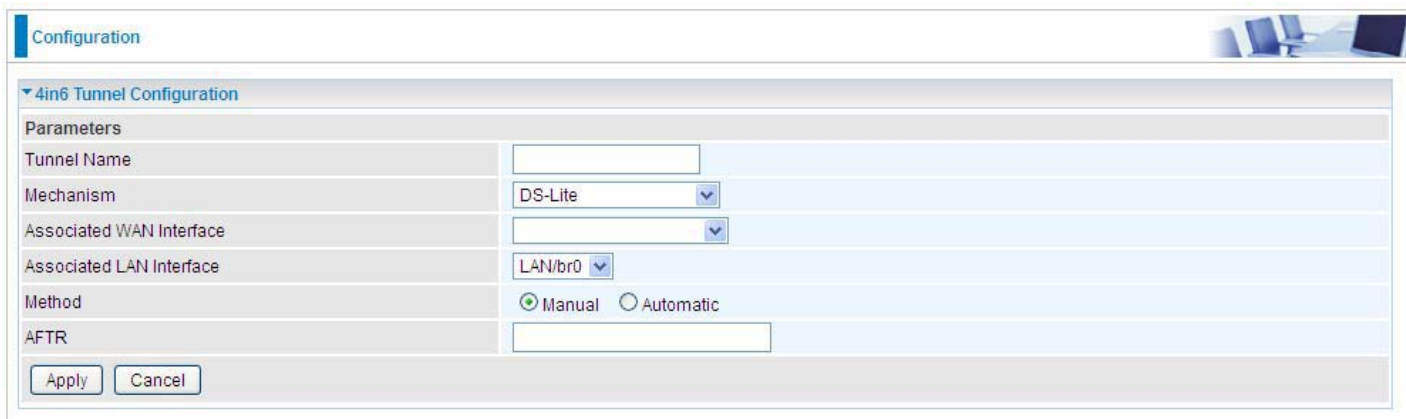
DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

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 interface for configuring IPv4inIPv6 tunnels. At the top, there is a 'Configuration' header. Below it, a section titled 'IPv4inIPv6' contains a table for '4in6 Tunnel Configuration'. The table has columns for Name, WAN, LAN, Dynamic, AFTR, and Remove. There is one entry with Name 'WAN', LAN 'LAN', Dynamic 'Dynamic', and AFTR 'AFTR'. Below the table are 'Add' and 'Remove' buttons.

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



The screenshot shows the '4in6 Tunnel Configuration' form. It includes 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), and AFTR. There are 'Apply' and 'Cancel' buttons at the bottom.

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.

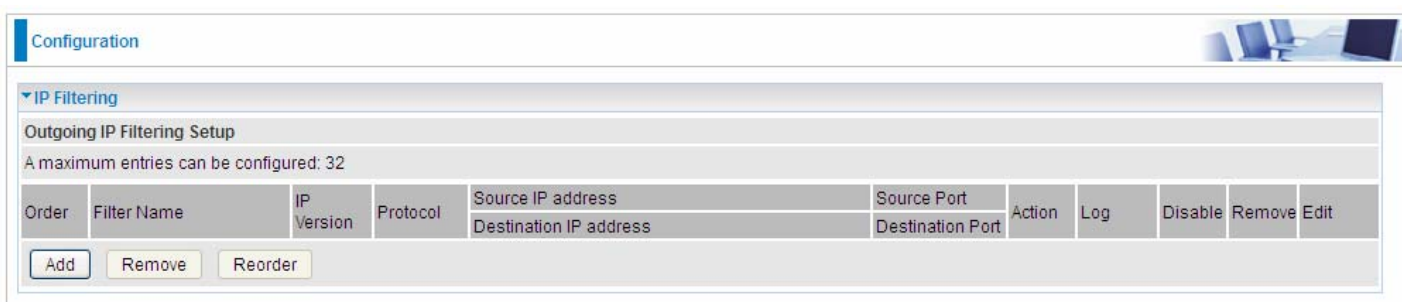
Security

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.

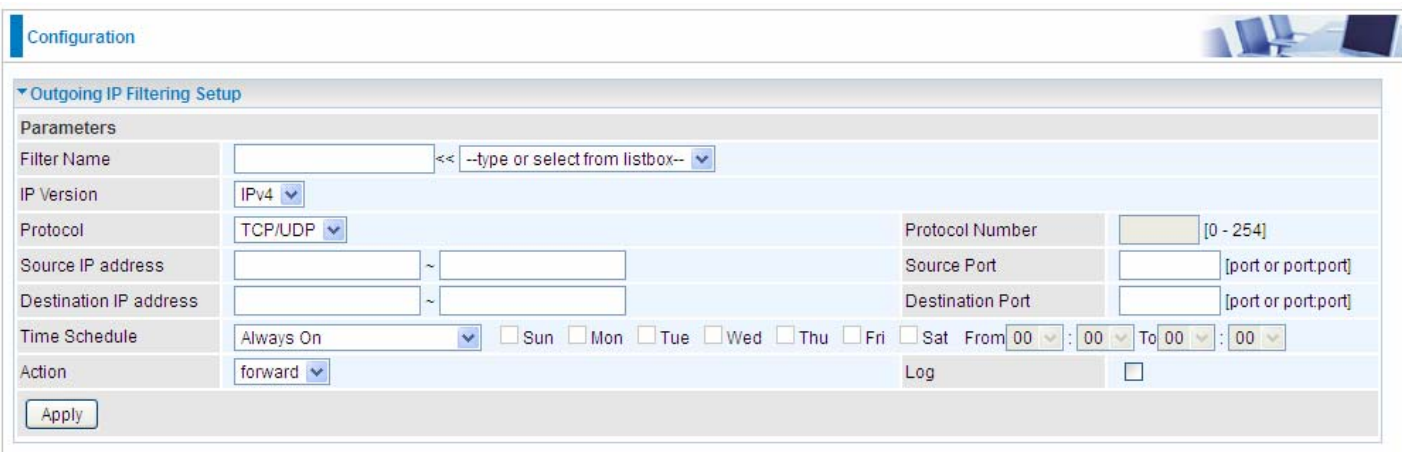
Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.



The screenshot shows the 'Configuration' page for 'IP Filtering'. Under 'Outgoing IP Filtering Setup', it states 'A maximum entries can be configured: 32'. Below this is a table with columns: Order, Filter Name, IP Version, Protocol, Source IP address, Destination IP address, Source Port, Destination Port, Action, Log, Disable, Remove, and Edit. At the bottom of the table are buttons for 'Add', 'Remove', and 'Reorder'.

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



The screenshot shows the 'Outgoing IP Filtering Setup' page. It includes a 'Parameters' section with the following fields: Filter Name (text input with a dropdown), IP Version (IPv4), Protocol (TCP/UDP), Protocol Number (0-254), Source IP address (range), Destination IP address (range), Source Port (range), Destination Port (range), Time Schedule (Always On, with checkboxes for days of the week and time range), Action (forward), and Log (checkbox). An 'Apply' button is at the bottom.

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) 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.

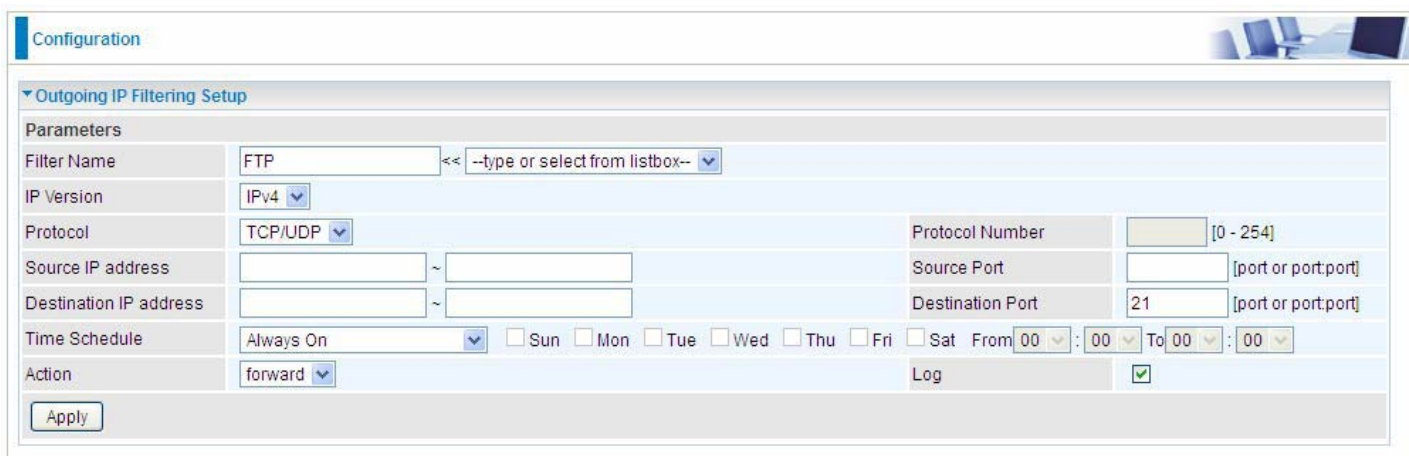
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule 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 Protocol Number: [0 - 254]

Source IP address: ~

Source Port: [port or port:port]

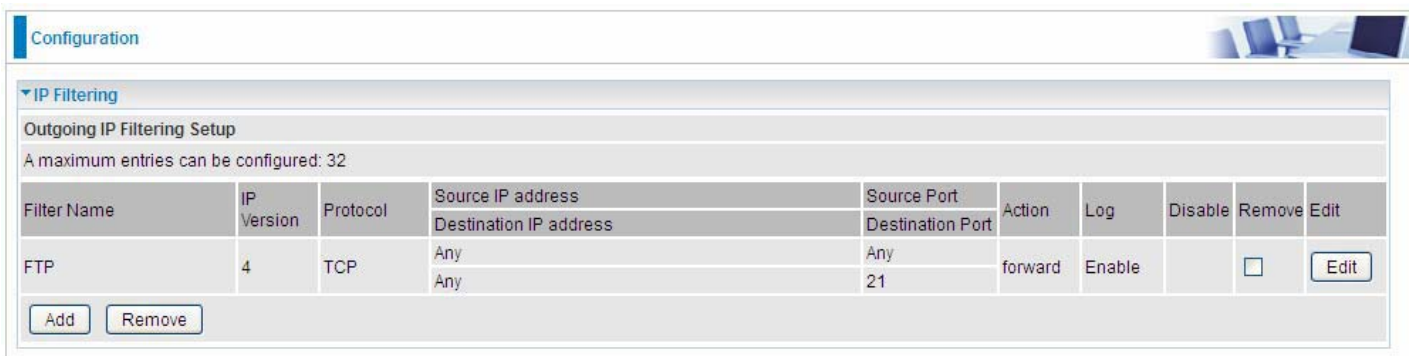
Destination IP address: ~

Destination Port: 21 [port or port:port]

Time Schedule: Always On Sun 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

Filter Name	IP Version	Protocol	Source IP address	Destination IP address	Source Port	Destination Port	Action	Log	Disable	Remove	Edit
FTP	4	TCP	Any	Any	Any	21	forward	Enable	<input type="checkbox"/>		Edit

Add Remove

(The rule is active; disable field shows the status of the rule, active or inactive)

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: ~ Destination IP address: ~

Source Port: [] [port or port:port] 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

Filter Name	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Action	Log	Disable	Remove	Edit
FTP	4	TCP	Any Any	Any 21	forward	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit

Add Remove

(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.

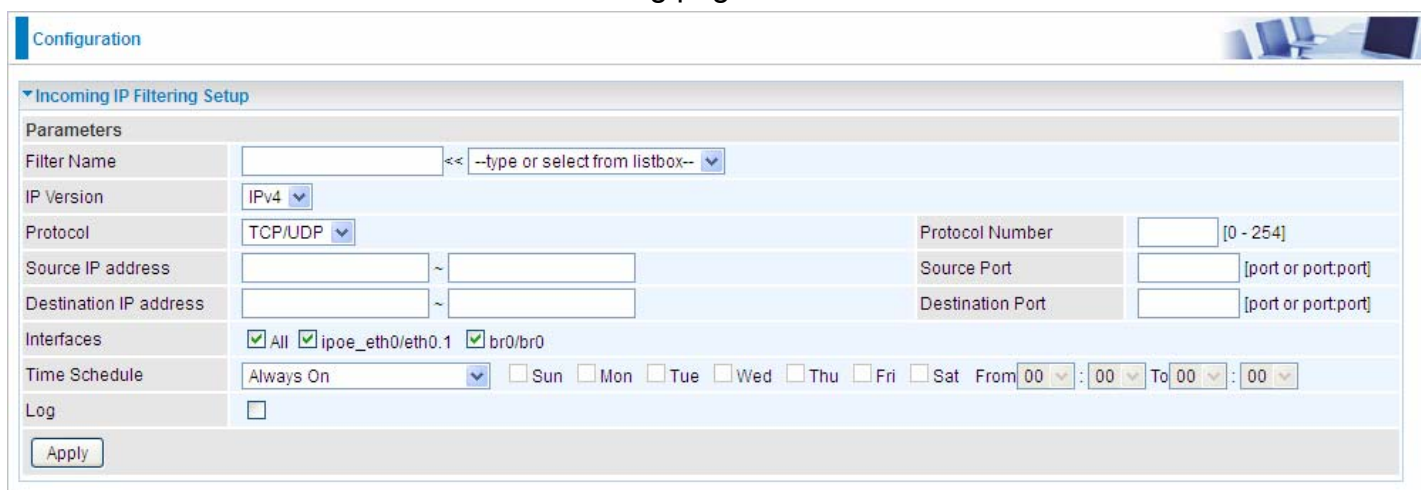
Note:

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.



The screenshot shows the 'Configuration' page for 'IP Filtering'. Under 'Incoming IP Filtering Setup', there is a note: 'A maximum entries can be configured: 32'. Below this is a table with columns: Filter Name, Interfaces, IP Version, Protocol, Source IP address, Destination IP address, Source Port, Destination Port, Log, Disable, Remove, and Edit. There are 'Add' and 'Remove' buttons at the bottom left of the table area.

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



The screenshot shows the 'Incoming IP Filtering Setup' configuration page. It includes fields for: Filter Name (with a dropdown), IP Version (IPv4), Protocol (TCP/UDP), Protocol Number (0-254), Source IP address, Destination IP address, Source Port, Destination Port, Interfaces (checkboxes for All, ipoe_eth0/eth0.1, br0/br0), Time Schedule (Always On, with checkboxes for days of the week and time range), and Log (checkbox). An 'Apply' button is at the bottom.

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) 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](#).

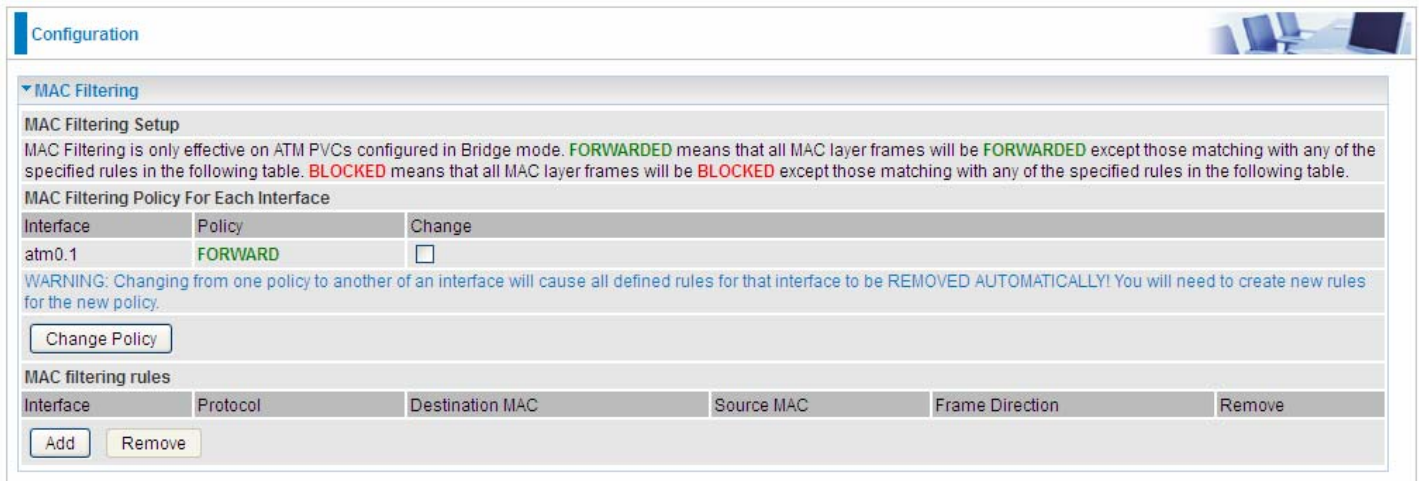
Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

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.



The screenshot shows the 'Configuration' page with the 'MAC Filtering' section expanded. It includes a 'MAC Filtering Setup' section with explanatory text and a 'MAC Filtering Policy For Each Interface' table. The table has columns for 'Interface', 'Policy', and 'Change'. The 'atm0.1' interface is currently set to 'FORWARD' with an unchecked 'Change' checkbox. A warning message states: '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.' Below the table is a 'Change Policy' button. At the bottom, there is a section for 'MAC filtering rules' with columns for 'Interface', 'Protocol', 'Destination MAC', 'Source MAC', 'Frame Direction', and 'Remove', along with 'Add' and 'Remove' buttons.

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.



The screenshot shows the 'Configuration' page with the 'MAC filtering rules' section expanded. It displays a 'Parameters' section with the following fields: 'Protocol' (a dropdown menu), 'Destination MAC' (a text input field), 'Source MAC' (a text input field), 'Frame Direction' (a dropdown menu with 'LAN<=>WAN' selected), and 'WAN Interface' (a dropdown menu with 'br_eth0/eth0.2' selected). An 'Apply' button is located at the bottom of the configuration area.

Protocol type: Select from the drop-down menu the protocol that applies to this rule.

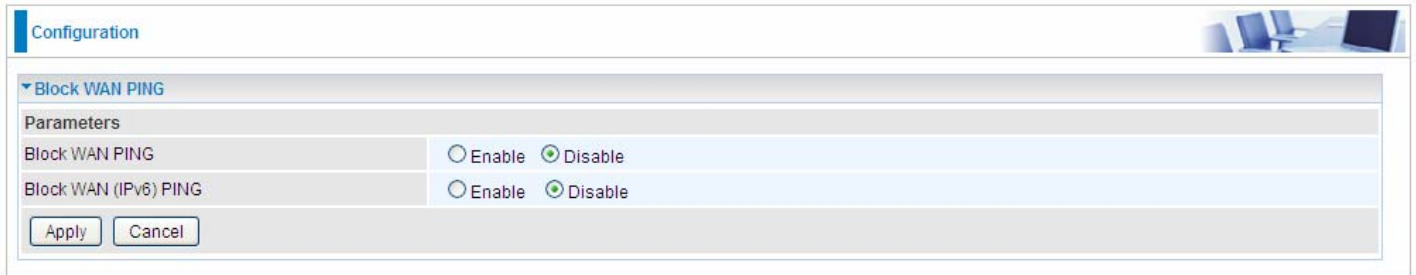
Destination /Source MAC Address: Enter the destination/source address.

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.



The screenshot shows a configuration window titled "Configuration" with a sub-section "Block WAN PING". Under "Parameters", there are two rows of radio button options. The first row is for "Block WAN PING" and the second is for "Block WAN (IPv6) PING". In both rows, the "Disable" option is selected. At the bottom of the configuration area are "Apply" and "Cancel" buttons.

Parameters	
Block WAN PING	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block WAN (IPv6) PING	<input type="radio"/> Enable <input checked="" type="radio"/> 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. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. 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.



Configuration

Time Restriction

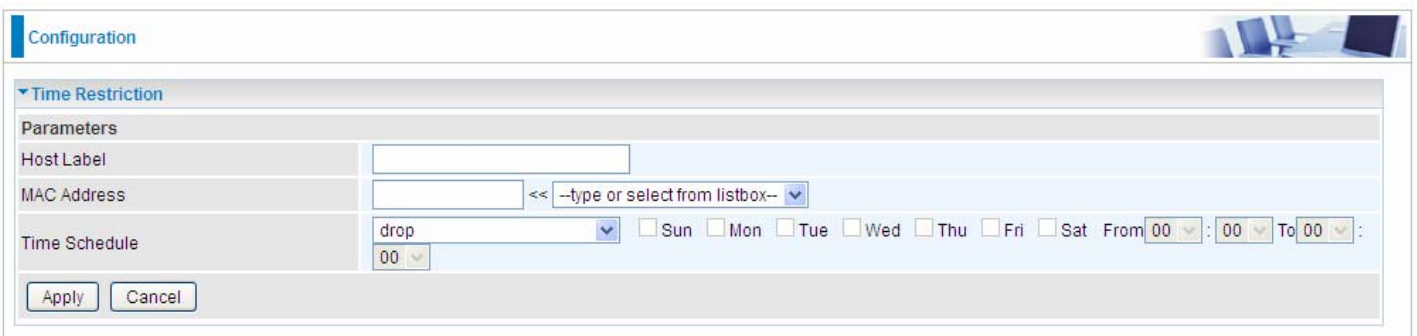
Access Time Restriction

A maximum entries can be configured: 32

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit
------------	-------------	-----	-----	-----	-----	-----	-----	-----	------------	----------	--------	------

Add Remove

Click **Add** to add the rules.



Configuration

Time Restriction

Parameters

Host Label:

MAC Address: << --type or select from listbox-- >>

Time Schedule: drop [Sun] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat] From 00:00 To 00:00

Apply Cancel

Host Label: User-defined name.

MAC Address: Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

Time Schedule: To determine when the rule works.

- 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										<input type="checkbox"/>	Edit
child-use	18:a9:05:04:12:23		x	x	x	x	x		00:00	23:59	<input type="checkbox"/>	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 **Exception IP Address** part, user can click [Detail ▶](#) to set the exception IP address(es) for IPv4 and IPv6 respectively.

Parameters	
Keywords Filtering	<input type="checkbox"/> Enable Detail ▶
Domains Filtering	<input type="checkbox"/> Enable Detail ▶
Restrict URL Features	BLOCK <input type="checkbox"/> Java Applet <input type="checkbox"/> ActiveX <input type="checkbox"/> Cookie <input type="checkbox"/> Proxy
Except IP Address	<input type="checkbox"/> Detail ▶
Log	<input type="checkbox"/>
Time Schedule	Always On <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat From <input type="text" value="00"/> : <input type="text" value="00"/> To <input type="text" value="00"/> : <input type="text" value="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.

Exception 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.



Configuration

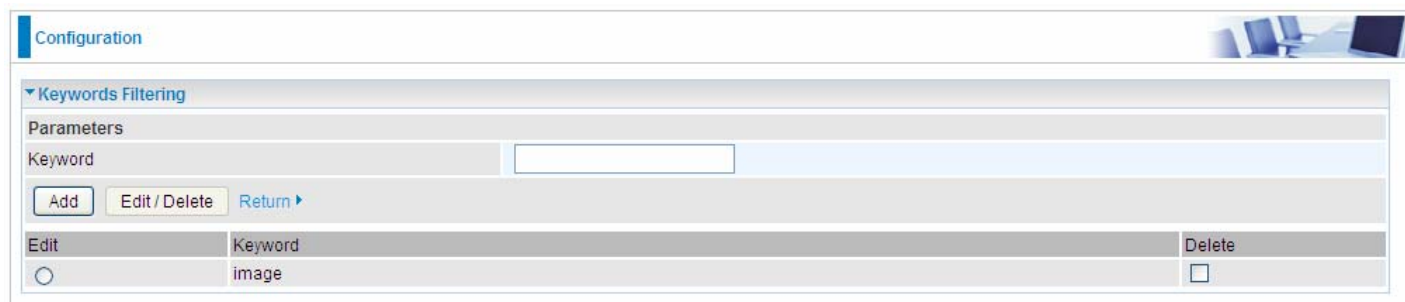
▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)

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



Configuration

▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)

Edit	Keyword	Delete
<input type="radio"/>	image	<input type="checkbox"/>

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.

Domain Filtering

Note: Maximum number of entries: 32.

Click [Detail ▶](#) to add Domains.



Configuration

▼ Domains Filtering

Parameters

Domains Filtering Type

[Return ▶](#)

Domain 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.

Exception 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 exception IP addresses. At the top, there is a 'Configuration' header. Below it, a section titled 'Except IP Address' is expanded. Under 'Parameters', the 'IP Version' is set to 'IPv4' via a dropdown menu. The 'Internal IP Address' field consists of two input boxes separated by a tilde (~). At the bottom of the configuration area, there are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

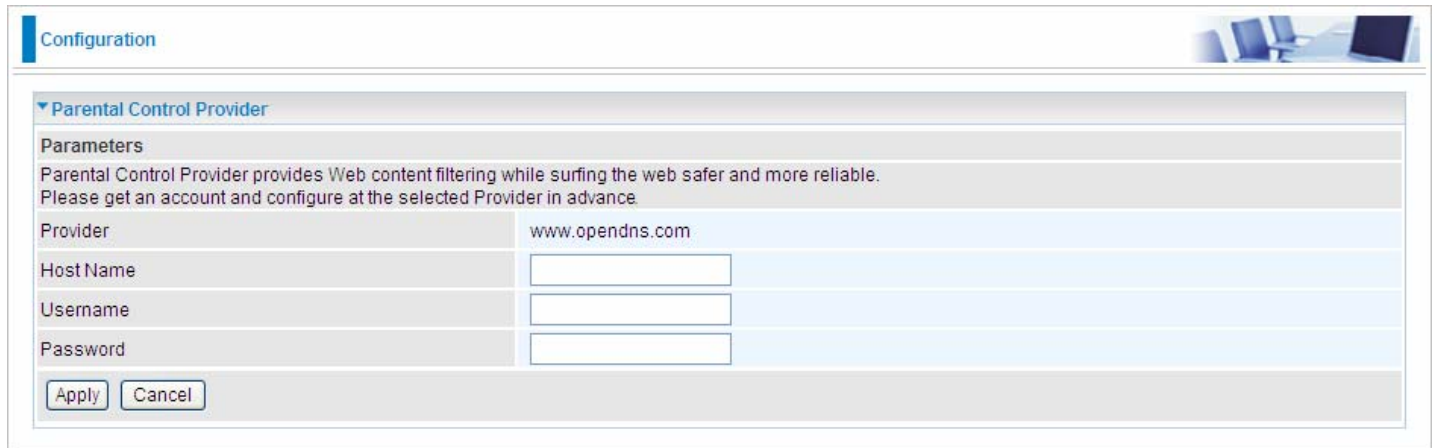
Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the **Exception List**, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords Filtering**.

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 configuration window titled "Configuration" with a sub-section for "Parental Control Provider". Under "Parameters", there is a descriptive text: "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 this, there are four input fields: "Provider" (pre-filled with "www.opendns.com"), "Host Name", "Username", and "Password". At the bottom left, there are "Apply" and "Cancel" buttons.

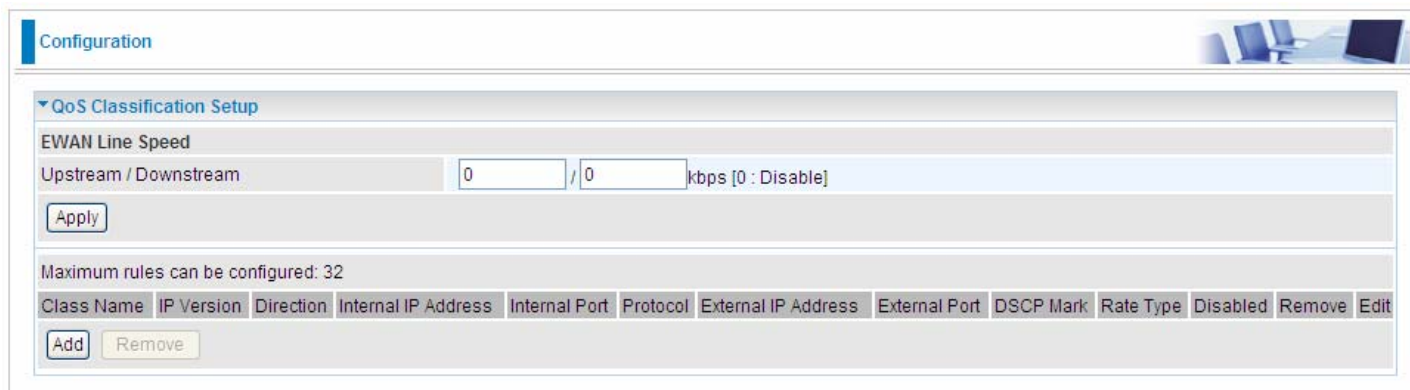
Parental Control Provider	
Parameters	
Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.	
Provider	www.opendns.com
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

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: ADSL line speed is based on the ADSL sync rate. But there is no QoS on 3G/LTE as the 3G/LTE line speed is various and can not be known exactly.

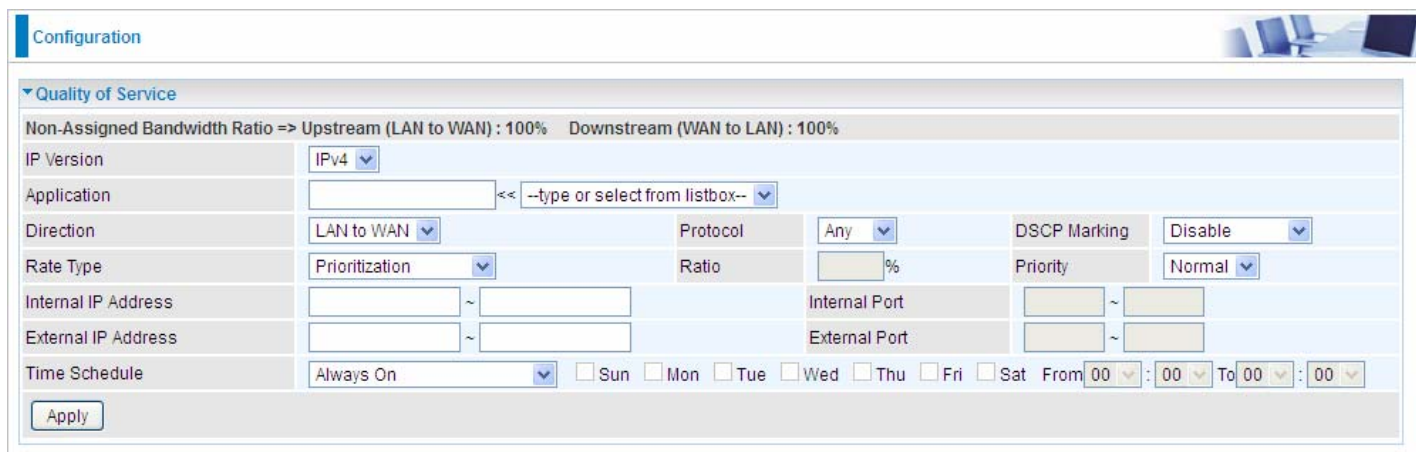


The screenshot shows the 'Configuration' page with a sub-section titled 'QoS Classification Setup'. It features a form for 'EWAN Line Speed' with input fields for 'Upstream / Downstream' rates, currently set to 0 / 0 kbps. Below the form is an 'Apply' button. A message states 'Maximum rules can be configured: 32'. At the bottom, there is a table header 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 below the table.

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' page with a sub-section titled 'Quality of Service'. It displays 'Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%'. The form includes fields for 'IP Version' (set to IPv4), 'Application' (with a dropdown for '--type or select from listbox--'), 'Direction' (set to LAN to WAN), 'Protocol' (set to Any), 'DSCP Marking' (set to Disable), 'Rate Type' (set to Prioritization), 'Ratio' (with a percentage input), and 'Priority' (set to Normal). It also has fields for 'Internal IP Address', 'Internal Port', 'External IP Address', and 'External Port'. A 'Time Schedule' section includes 'Always On' and checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and time ranges (From 00:00 To 00:00). 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 be 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 $20\% * 256 * 0.9 = 46\text{kbps}$. (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.

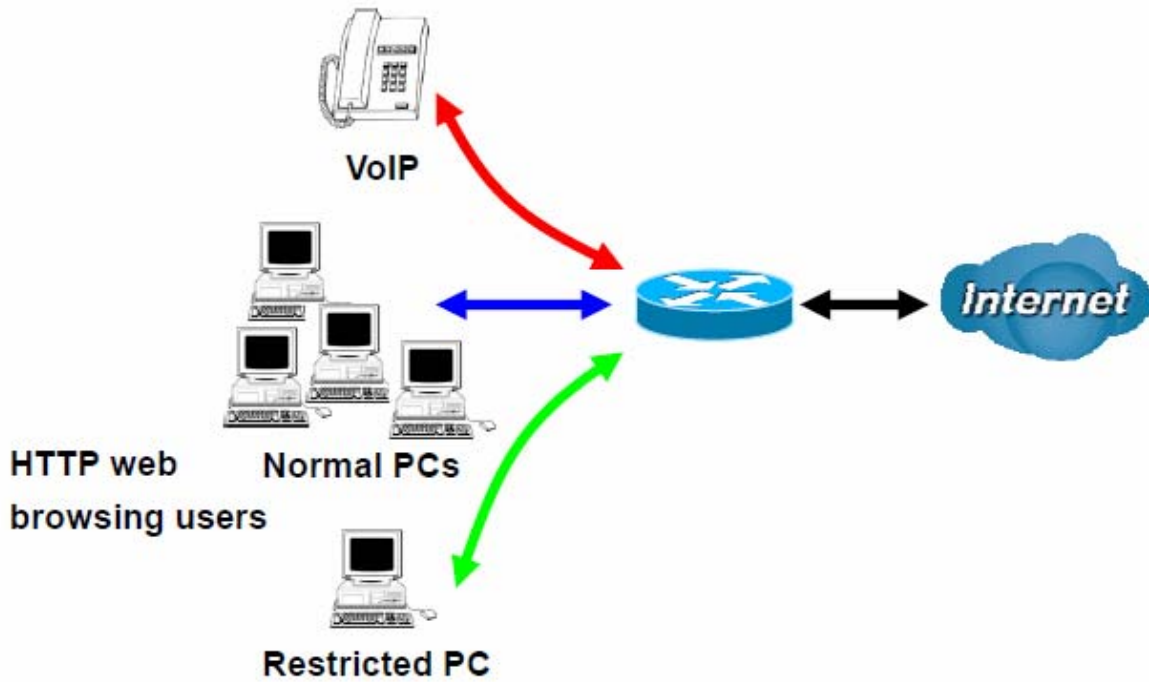
External IP Address: The IP address on remote / WAN side.

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	DSCP Marking	EF(101110)
Rate Type	Prioritization	Ratio	%	Priority	High
Internal IP Address		Internal Port			
External IP Address		External Port			
Time Schedule	timeslot1	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> 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	DSCP Marking	Disable
Rate Type	Limited (Maximum)	Ratio	20 %	Priority	Normal
Internal IP Address		Internal Port			
External IP Address		External Port	80 ~ 80		
Time Schedule	timeslot1	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat	From 00 : 00 To 09 : 19		

Apply

3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.

Configuration

Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80% Downstream (WAN to LAN) : 100%

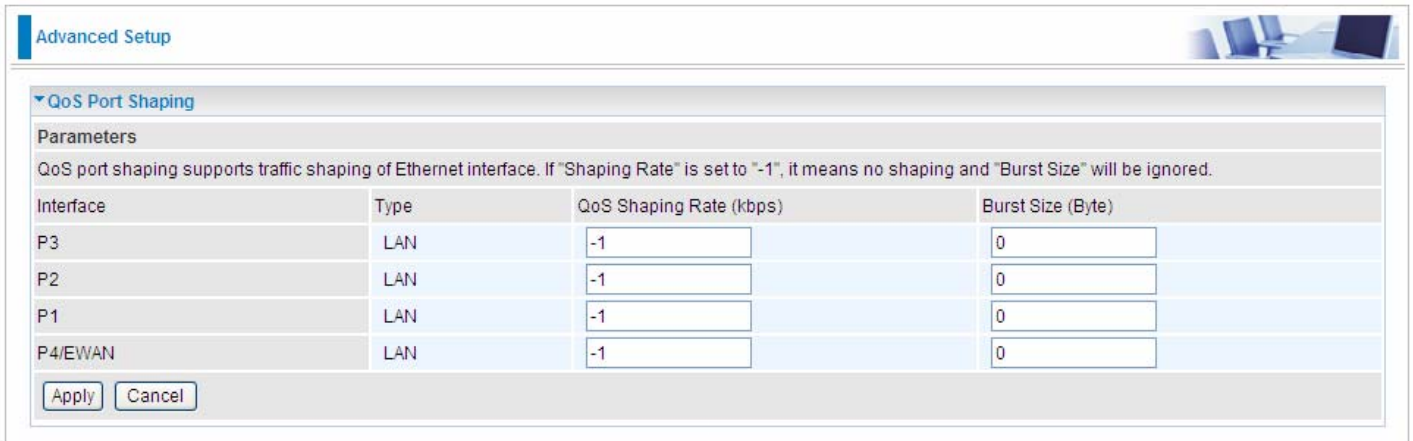
IP Version	IPv4				
Application	P2P << --type or select from listbox--				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	%	Priority	Low
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	timeslot1	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat	From 00 : 00 To 09 : 19		

Apply

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.



Advanced Setup

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)
P3	LAN	-1	0
P2	LAN	-1	0
P1	LAN	-1	0
P4/EWAN	LAN	-1	0

Apply Cancel

Interface: P1-P4. P4 used as EWAN also covered.

Type: All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

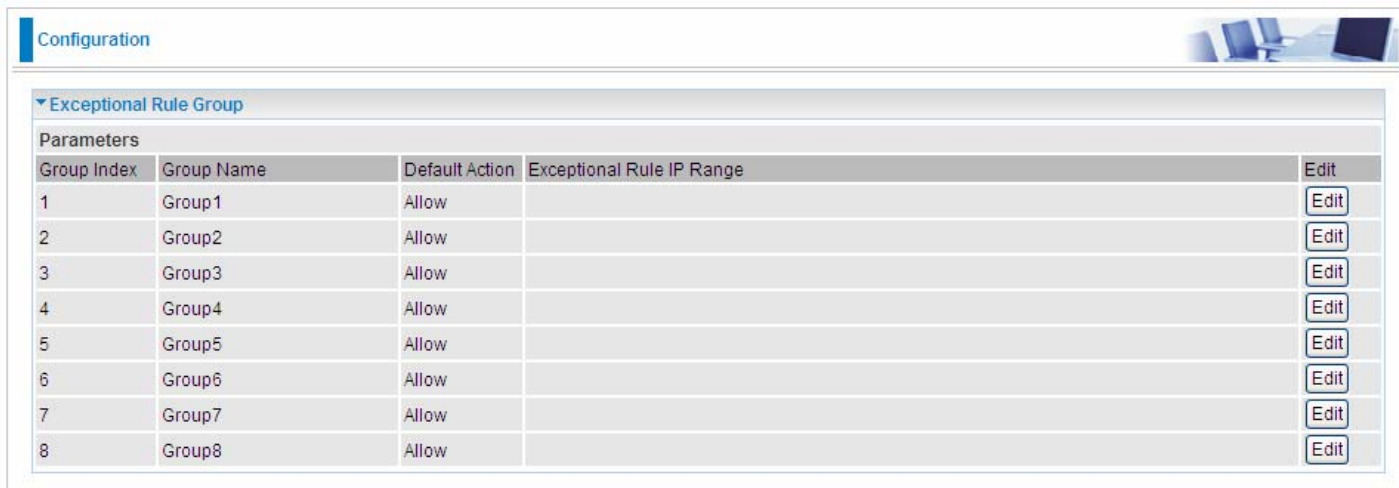
Burst Size(Bytes): Set the forcefully Burst Size.

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

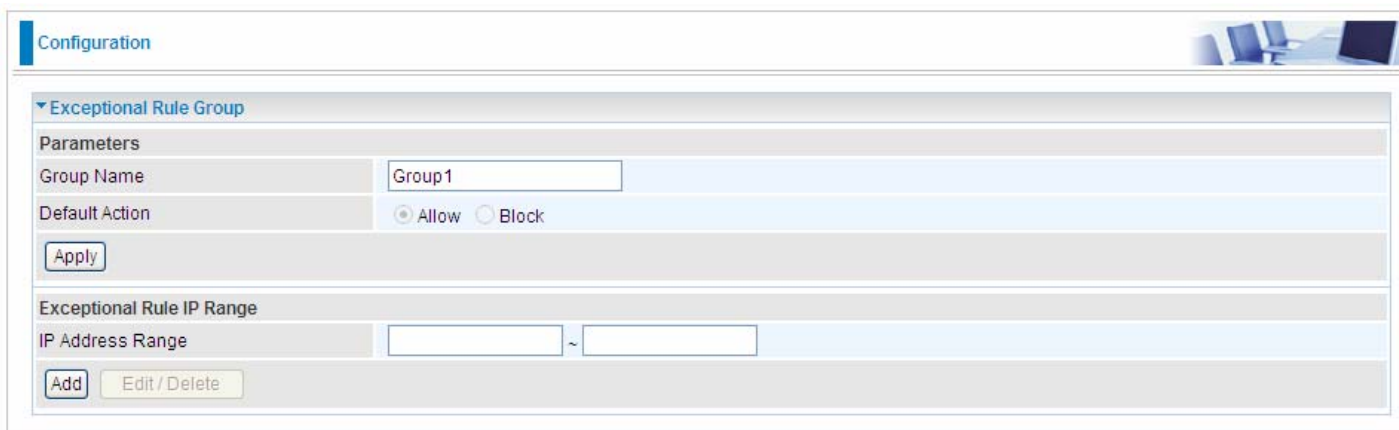
Exceptional Rule is dedicated to giving or blocking Virtual Server/ DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows a web interface for configuring Exceptional Rule Groups. At the top, there is a 'Configuration' header. Below it, a section titled 'Exceptional Rule Group' contains 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 final 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 edit form for an Exceptional Rule Group. It includes a 'Configuration' header and a section titled 'Exceptional Rule Group'. Under 'Parameters', there is a 'Group Name' field with 'Group1' entered, and a 'Default Action' section with radio buttons for 'Allow' (selected) and 'Block'. Below this is an 'Apply' button. Under 'Exceptional Rule IP Range', there is an 'IP Address Range' field with two input boxes separated by a tilde (~), and 'Add' and 'Edit / Delete' buttons below it.

Default Action: Please first set the range to make “**Default Action**” setting available. Set “Allow” to ban the listed IP or IPs to access the Virtual Server and DMZ Host

Check “Block” to grant access to the listed IP or IPs to 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 to 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
<input type="radio"/>	Block	172.16.1.102 ~ 172.16.1.106	<input type="checkbox"/>
<input type="radio"/>	Block	172.16.1.108 ~ 172.16.1.108	<input type="checkbox"/>

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.

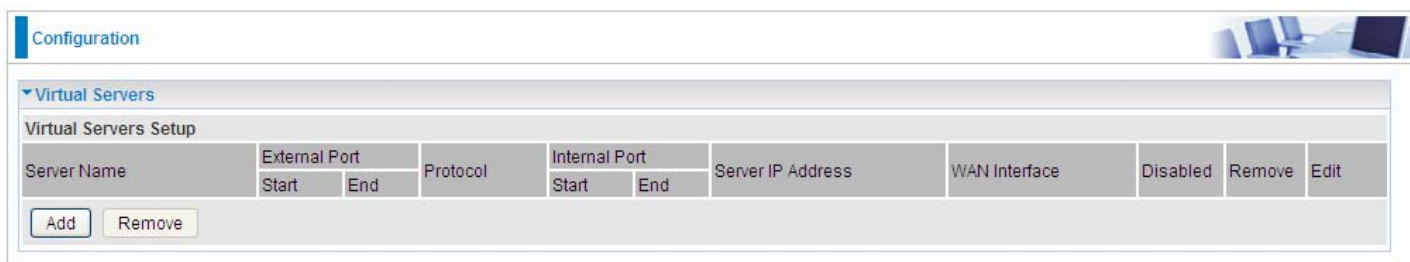
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing 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					

Add Remove

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

Exceptional Rule Group: None

External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

Interface: select from the drop-down menu the interface you want the virtual server(s) to apply.

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

access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

● Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Virtual 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
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

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	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit

Add Remove

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	✓	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	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	✓	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		<input checked="" type="checkbox"/>	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

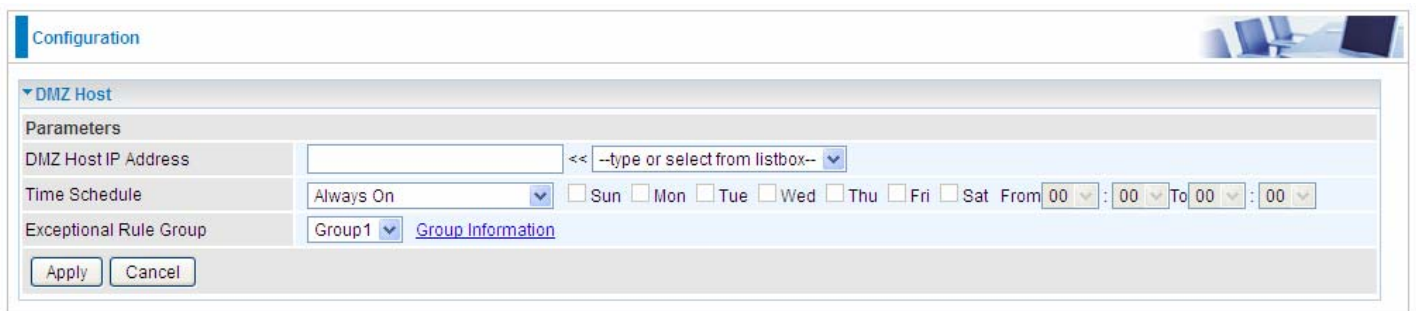
Parameters

DMZ Host IP Address: [] << --type or select from listbox--

Time Schedule: Always On [v] Sun Mon Tue Wed Thu Fri Sat From 00:00 To 00:00

Exceptional Rule Group: None [v]

Apply Cancel



Configuration

DMZ Host

Parameters

DMZ Host IP Address: [] << --type or select from listbox--

Time Schedule: Always On [v] Sun Mon Tue Wed Thu Fri Sat From 00:00 To 00:00

Exceptional Rule Group: Group1 [v] [Group Information](#)

Apply Cancel

Group Index	1
Group Name	Group1
Action	Block
IP Address Range	172.16.1.102~172.16.1.106 172.16.1.108~172.16.1.108

(Group Information)

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 DMZ Host 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.



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.



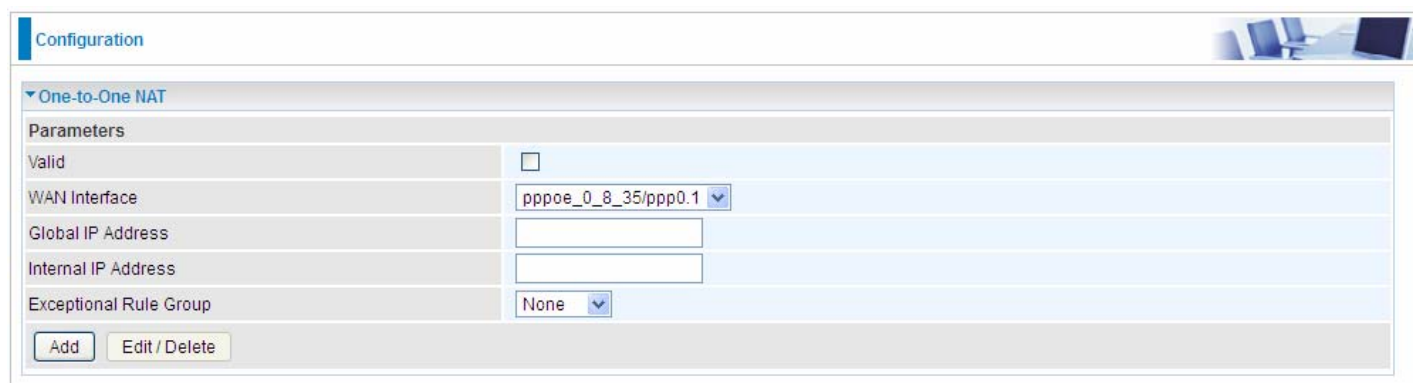
Attention

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 configuration window titled "Configuration" with a sub-section for "One-to-One NAT". Under "Parameters", there are several fields: "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 configuration area, there are two buttons: "Add" and "Edit / Delete".

Valid: Check whether to validate 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.

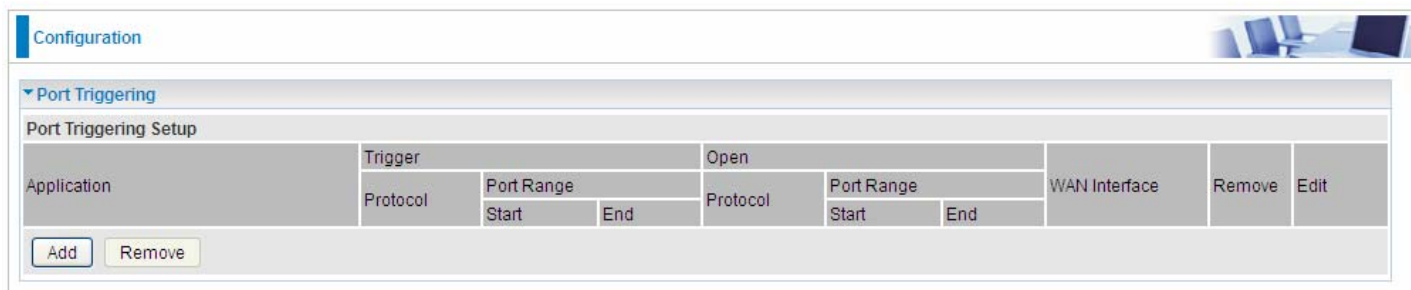
Exceptional Rule Group: Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 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

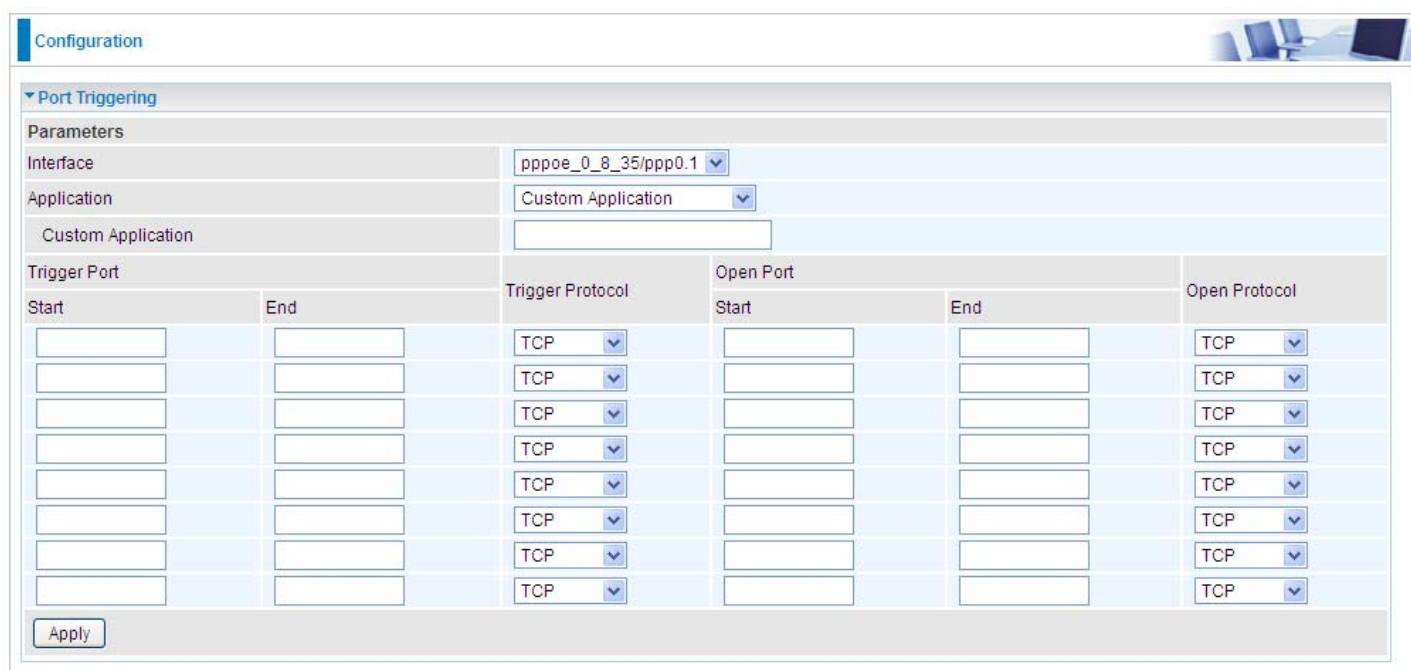
Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.



The screenshot shows the 'Port Triggering Setup' configuration page. It features a table with columns for 'Application', 'Trigger' (Protocol, Port Range), 'Open' (Protocol, Port Range), 'WAN Interface', 'Remove', and 'Edit'. The 'Port Range' column is further divided into 'Start' and 'End' sub-columns. Below the table are 'Add' and 'Remove' buttons.

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range	Port Range			
		Start End		Start End				

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



The screenshot shows the 'Port Triggering Parameters' configuration page. It includes fields for 'Interface' (set to 'pppoe_0_8_35/ppp0.1'), 'Application' (set to 'Custom Application'), and a 'Custom Application' text input. Below these is a table for 'Trigger Port' and 'Open Port' configurations. The table has columns for 'Start', 'End', 'Trigger Protocol', 'Start', 'End', and 'Open Protocol'. Each row contains input fields for 'Start' and 'End' ports and a dropdown menu for 'Protocol' (all set to 'TCP'). An 'Apply' button is located at the bottom left.

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application: Preinstalled applications or Custom Application user can customize the utility yourself.

Custom Application: It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

Trigger Port

① **Start:** Enter a port number as the triggering port starting number.

① **End:** Enter a port number as the triggering port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

① **Start:** Enter a port number as the open port starting number.

② **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: [Empty]

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
4099	4099	TCP	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 **Virtual Servers Setup** table.

Configuration

Port Triggering

Port Triggering Setup


Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Start	End			
Aim Talk	TCP	4099 - 4099	TCP	5191	5191	ppp0.1	<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>