HG-A800 Home Gateway

Installation and User Manual

Version 1 – July 2012

Document Control

Date	Doc Version	Change
July 17, 2012	1	1st release of document

Notices

Emergency Calls

This terminal operates using mobile signals, which cannot guarantee connection in all conditions. Therefore, you should never rely solely on the terminal equipment for essential communications such as medical or emergency services.

Temperature

Operating temperature: 0～+50℃
Storage temperature: -40～+85℃

Catalog

1. Overview

The HG-A800 V1.5 is an All-In-One wireless VoIP router. It includes the following main functions:

- ADSL2/2+ modem for broadband connection;
- Four 10M/100M auto-sensing Ethernet ports for wire connection;
- Build-in 802.11n enhanced WLAN complies with IEEE 802.11n draft v2.0 and backward to 802.11b/g specifications. It supports 2x2 MIMO and up to 300Mbps of rate bandwidth. The throughput of WLAN to LAN is more than 100Mbps;
- Supports 1 USB 2.0 host port for Printer and USB storage or 3G dongle application;
- One FXS port for VoIP call;
- Supports TR-069 remote management;

2. Specification

2.1 Features and Technical Specifications

DSL Standards

- ANSI T1.413 issue 2compliant
- ITU-T G.992.1 (G.DMT) compliant
- ITU-T G.992 (G.lite) compliant
- ITU-T G.992.3/4 (ADSL2) compliant
- ITU-T G.992.5 (ADSL2+) along with Annex A and M

Configurations

- Payload Encapsulation
- RFC 2516, PPPoE (PPP over Ethernet)
- RFC 2364, PPPoA (PPP over AAL5)
- RFC 2684, Bridge
- RFC 2684 Routed
- Support 8 PVCs
- Support Port Mapping

IP

- NAT/NAPT
- Firewall, support SPI (Stateful Packet Inspection)
- DHCP Server
- Port forwarding (Support DMZ)
- IP filtering, bridge filtering, web filtering
- Static routing

- Dynamic routing;
- SNTP;
- VPN, support IPSec/PPTP/L2TP;
- Multicast: IGMP Proxy/Snooping;
- ALG;

Ethernet

- IEEE 802.3;
- 4 port Ethernet: 10/100M Ethernet Auto MDI-X;

Wi-Fi

- IEEE 802.11 b/g/n compliance;
- Security: WEP 64/124/256 bits, WPA/WPA2;
- WMM QoS;
- WDS wireless AP;
- RF power: 20dBm;
- Transmission Power:
  - 802.11b: 17+/-1.5dBm;
  - 802.11g: 14+/-1.5dBm;
  - 802.11n: HT20 14+/-1.5dBm; HT40 12+/-1.5dBm;
- Reception Sensibility:
  - 802.11b: -82dBm, ±2dB;
  - 802.11g: -68dBm, ±2dB;
  - 802.11n: HT20 -64dBm, ±2dB; HT40 -60dBm, ±2dB;
- Spurious emission/harmonics: -50dBc;
- Antenna:
  - 2T2R MIMO mode (2 transmitter, 2 receiver);
  - One external antenna with 2dBi gain; One internal antenna with 4dBi gain;
  - Operating Temp: -10~+60℃;
- RF on/off;
- ACS(Automatic channel selection);
- MAC address white-black filter;

Operation and Management (OAM)

- Support Web based management;
- UPnP;
- Telnet/SSH;
- Software upgrade through HTTP/TFTP/FTP;
- TR069 (CPE management through WAN interface);
- SNMP agent and tools;

QoS

- IP QoS: base on source IP address, source and destination port, protocol and DSCP;
- ATM QoS: support CBR, UBR, nrt-VBR, rt-VBR;

- QoS features including support for extended Impulse Noise Protection (INP) for better IPTV quality;

VoIP

- Support SIP or MGCP protocols;
- Support one analog phone;
- Flexible dial plan customization;
- Support multiple CODECs, including G.711, G.729 and so on;
- Supports DTMF tone detection and generation;
- Support Echo Cancellation, Silence suppression, Comfort Noise Generation and Voice Activity Detection(VAD);
- SIP Call Forwarding;
- T.38 Fax Relay;

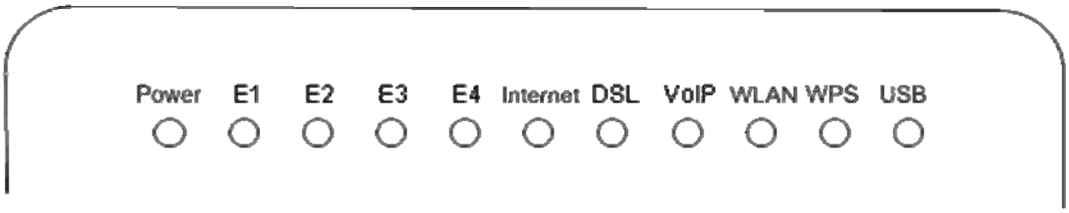
Temperature

- Operating temperature: 0~+50℃
- Storage temperature: -40~+85℃

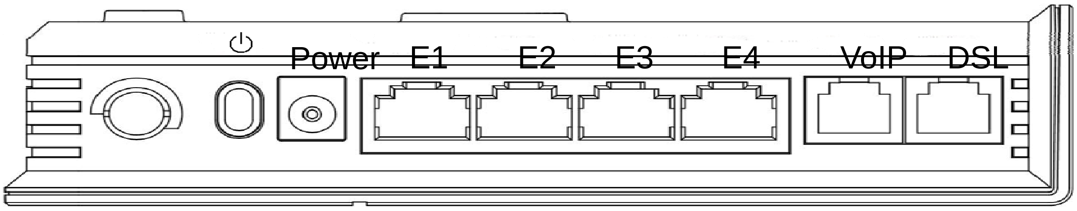
2.2 Interface Introduction

2.2.1 Indicators & Interface

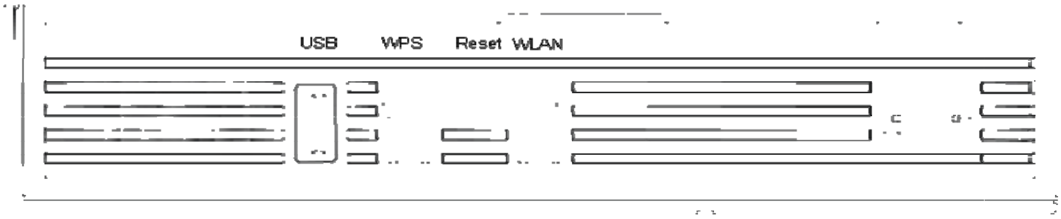
Indicators:



Interface 1:



Interface 2:

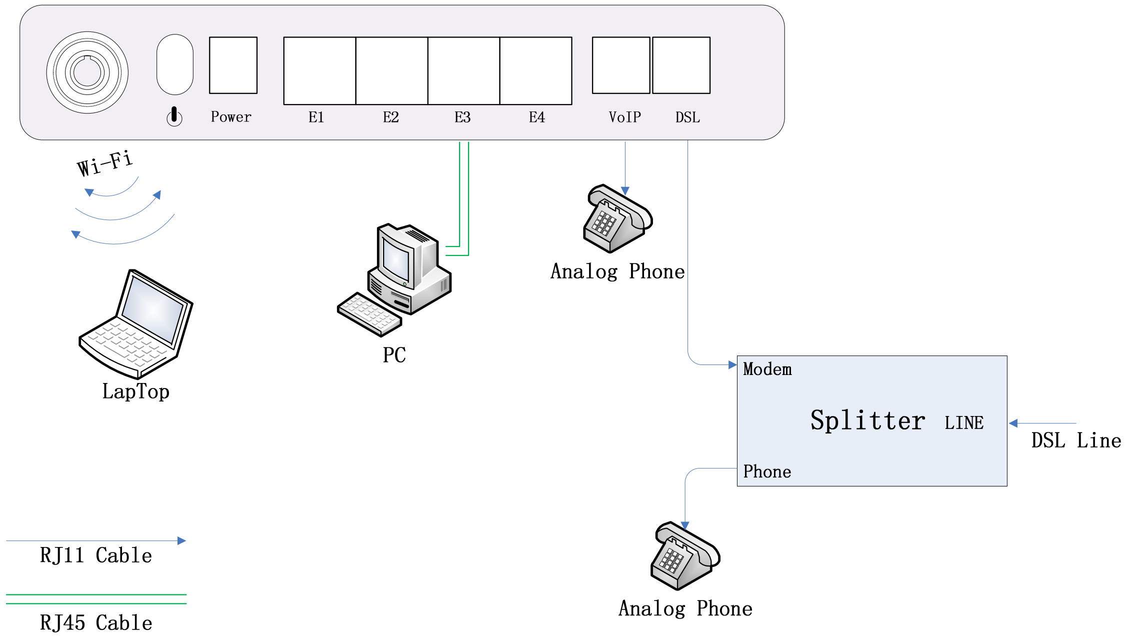


Item	Label	Description
Indicators	Power	On: Modem power up
		Off: Modem Power off
	E1-E4	On: Ethernet is connected
		Blinking green: Ethernet Traffic flows
		Off: Ethernet is disconnected
	Internet	Blinking green: PPP/DHCP negotiation
		Solid green: PPP/DHCP up
		Quick blinking green: Tx/Rx traffic on line
	DSL	On: Modem synchronized to the DSLAM
		Quick blinking green: Modem training, but not synchronized
		Slow blinking green: Modem Idle
	VoIP	On: The analog phone connected to VoIP off-hook
		Off: The analog phone connected to VoIP on-hook
	WLAN	On: WLAN connection is available
		Blinking green: Negotiation or traffic on line
		Off: WLAN connection is not available
	WPS	ON:WLAN connection is setup
		Blinking green: connecting WLAN
		Off: WLAN connection is fail
	USB	On: recognize the USB device
		Blinking green: USB data traffic
		Off: un-plug or un-recognized USB device
Interface 1	⏻	Power switch
	Power	For 12V DC power adapter
	E1-E4	LAN interface for connecting to computers
	VoIP	Connecting to analog telephones
	DSL	Connecting to ADSL enabled telephone line
Interface 2	USB	USB 2.0 host for Printer and USB storage or 3G dongle application
	WPS	WPS switch
	Reset	Restore to factory default settings
	WLAN	WLAN switch
	◯	WLAN antenna

2.2.2 Package Contents

Item	Quantity
Power Adapter	1
Phone Line	2
RJ-45 Cable	1
Modem	1
Splitter	1

2.2.3 Connection Topological Diagram



2.3 Hardware Connection

1. Use a telephone cord to connect the LINE port of the splitter with the phone socket on the wall (only if using ADSL).
2. Use another telephone cord to connect the ADSL port of the splitter with the DSL port of the HG-A800 (only is using ADSL).
3. Connect Ethernet port of the HG-A800 with 10/100BASE-T port of the computer using the network cable that comes with the unit.
4. Plug in the power cord, and turn on the power.

3. Configuration Guide

3.1 Default Configuration

The HG-A800 is pre-configured with the common VCI/VPI settings. The default dial-up mode is bridge encapsulation. For bridge mode, there is no need to configure any more parameters. However, the third party dial-up software is needed for connection with the Internet.

3.2 Customer Configuration

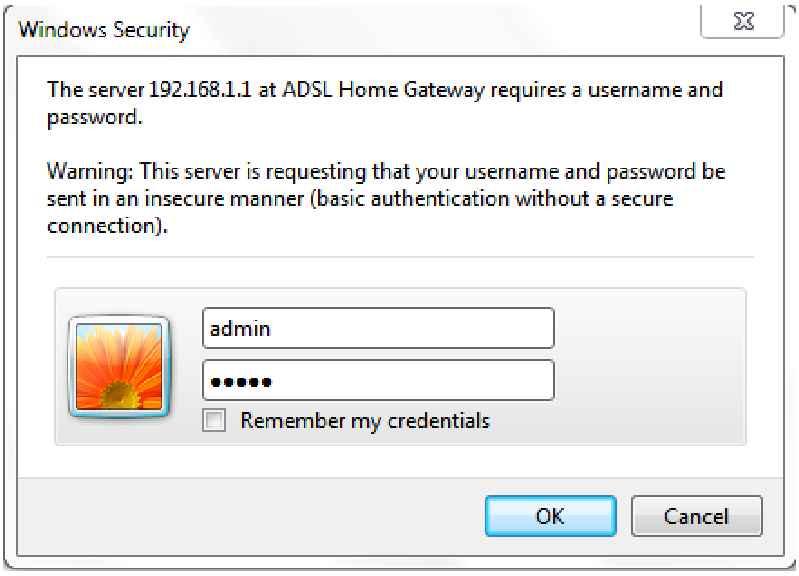
The default IP address for HG-A800 is: 192.168.1.1; The Subnet Mask is：255.255.255.0. Users can configure the HG-A800 through a web browser. The HG-A800 can be used as a gateway and DNS server; users need to set the computer's TCP/IP protocol as follow:

1. Set the computer IP address to the same subnet as the HG-A800 i.e. set the IP address of the PC to one in the range of 192.168.1.2 - 192.168.1.254 excluding 192.168.1.1.
2. Set the computer's gateway address to the IP address of the HG-A800.
3. Set the computer's Primary DNS server to the IP address of the HG-A800 or to that of an effective DNS server.

3.2.1 Log In and HG-A800 status

3.2.1.1. Log in

Power on to start the device, then make sure your computer can PING the HG-A800 (the factory default IP is 192.168.1.1), then run the web browser. Enter **http://192.168.1.1** in the address bar, press ENTER, and the authentication interface will pop up as below:



Windows Security

The server 192.168.1.1 at ADSL Home Gateway requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

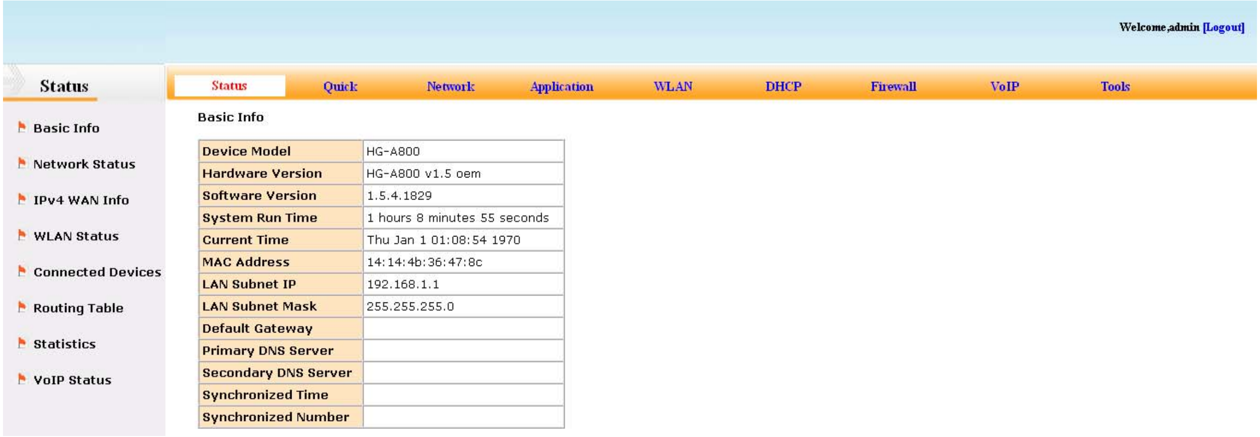
●●●●●

□ Remember my credentials

The default user name and password is **admin** for web log-on. Press **ENTER** or click on ‘**OK**’ to enter the configuration interface.

Warning: Please be sure the IP of the computer network card is in the same IP range as the HG-A800 LAN port before trying to log on (ex: 192.168.1.2 and 192.168.1.1 are in the same IP range). If the login is not displayed please check in Internet Explorer--Tools---Internet Options---Connection---LAN Setup---Proxy server, disable the function ‘Proxy for LAN’ and then retry.

If log on successfully, the main page will be displayed as follows:

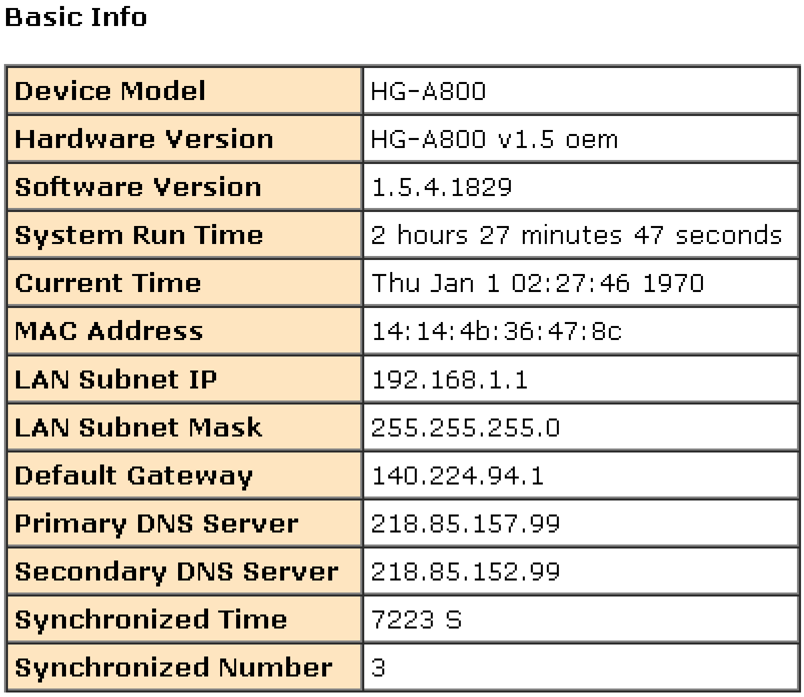


Basic Info

Device Model	HG-A800
Hardware Version	HG-A800 v1.5 oem
Software Version	1.5.4.1829
System Run Time	1 hours 8 minutes 55 seconds
Current Time	Thu Jan 1 01:08:54 1970
MAC Address	14:14:4b:36:47:8c
LAN Subnet IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
Synchronized Time	
Synchronized Number	

3.2.1.2. HG-A800 status

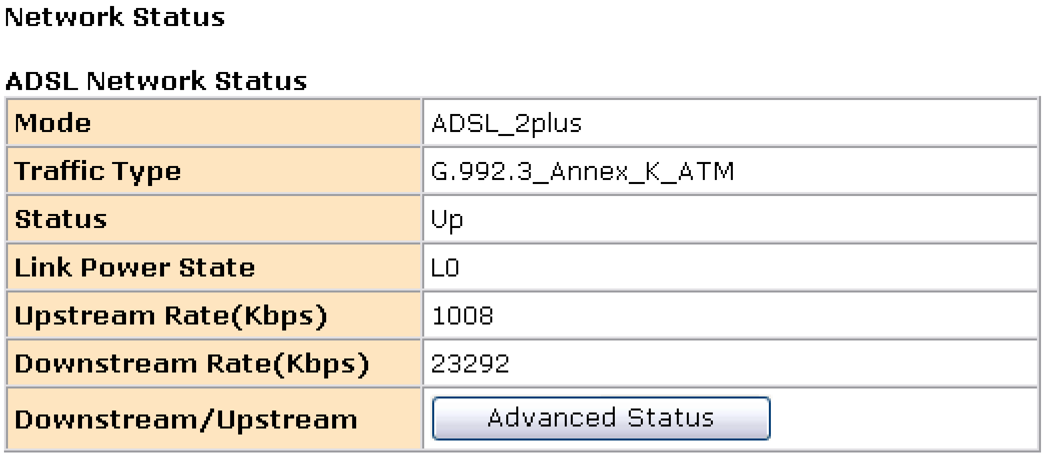
【Status】→【Basic Info】to show device information:



Basic Info

Device Model	HG-A800
Hardware Version	HG-A800 v1.5 oem
Software Version	1.5.4.1829
System Run Time	2 hours 27 minutes 47 seconds
Current Time	Thu Jan 1 02:27:46 1970
MAC Address	14:14:4b:36:47:8c
LAN Subnet IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
Default Gateway	140.224.94.1
Primary DNS Server	218.85.157.99
Secondary DNS Server	218.85.152.99
Synchronized Time	7223 S
Synchronized Number	3

【Status】→【Network Status】to show DSL information:

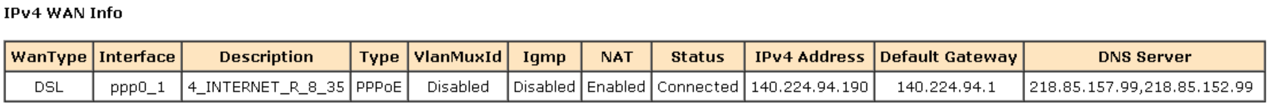


Network Status

ADSL Network Status

Mode	ADSL_2plus
Traffic Type	G.992.3_Annex_K_ATM
Status	Up
Link Power State	L0
Upstream Rate(Kbps)	1008
Downstream Rate(Kbps)	23292
Downstream/Upstream	Advanced Status

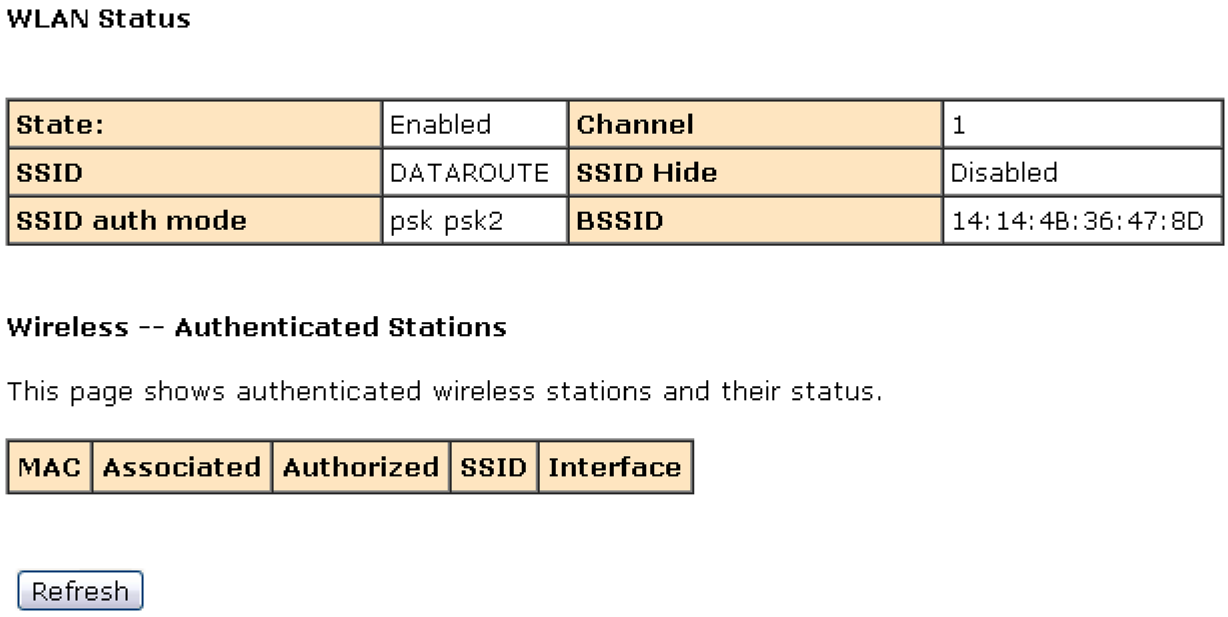
【Status】→【IPv4 WAN Info】to show information of WAN connection:



IPv4 WAN Info

WanType	Interface	Description	Type	VlanMuxId	Igmp	NAT	Status	IPv4 Address	Default Gateway	DNS Server
DSL	ppp0_1	4_INTERNET_R_8_35	PPPoE	Disabled	Disabled	Enabled	Connected	140.224.94.190	140.224.94.1	218.85.157.99,218.85.152.99

【Status】→【WLAN Status】



WLAN Status

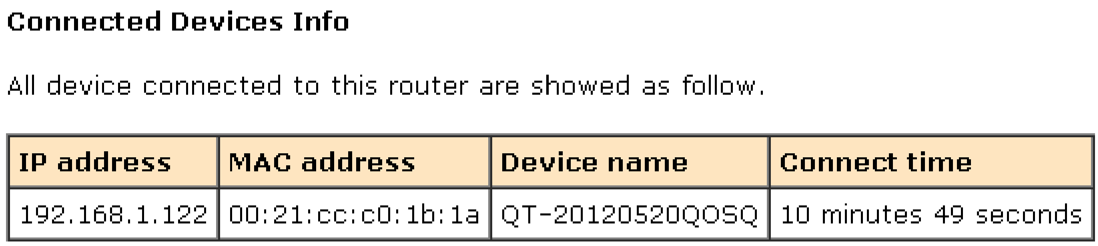
State:	Enabled	**Channel**	1
SSID	DATAROUTE	**SSID Hide**	Disabled
SSID auth mode	psk psk2	**BSSID**	14:14:4B:36:47:8D

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

【Status】→【Connected Devices Info】

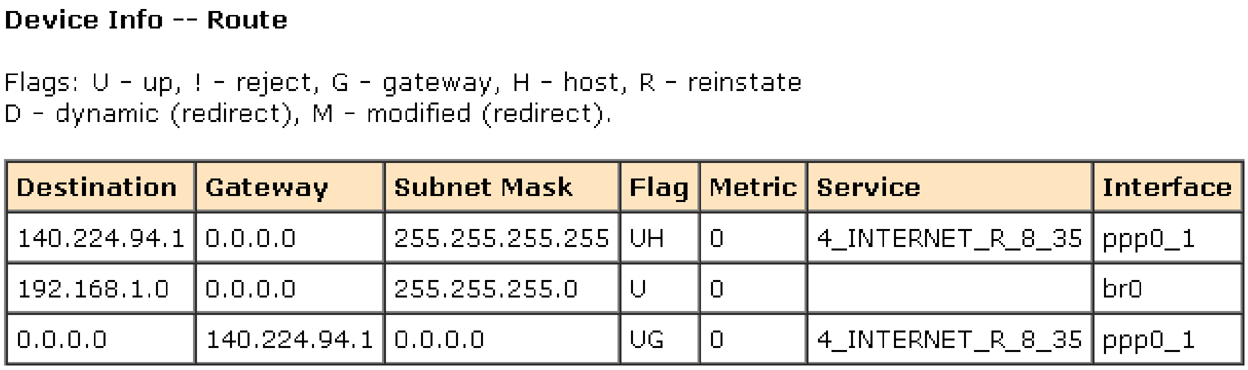


Connected Devices Info

All device connected to this router are showed as follow.

IP address	MAC address	Device name	Connect time
192.168.1.122	00:21:cc:c0:1b:1a	QT-20120520QOSQ	10 minutes 49 seconds

【Status】→【Routing Table】

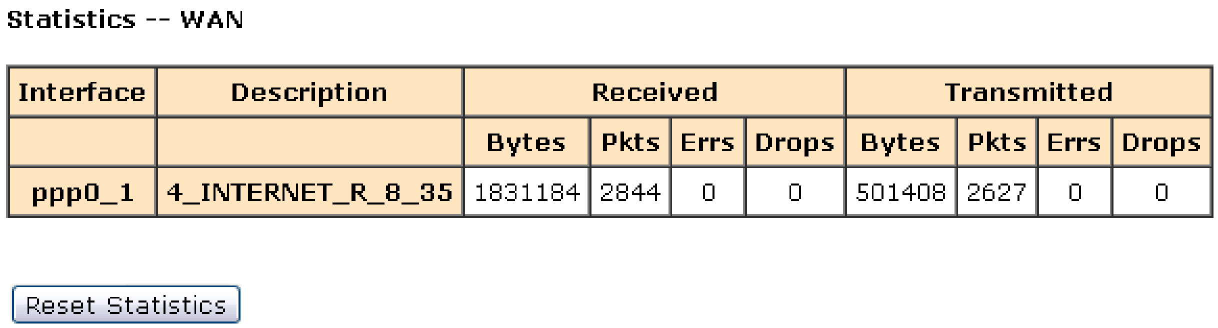


Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
140.224.94.1	0.0.0.0	255.255.255.255	UH	0	4_INTERNET_R_8_35	ppp0_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	140.224.94.1	0.0.0.0	UG	0	4_INTERNET_R_8_35	ppp0_1

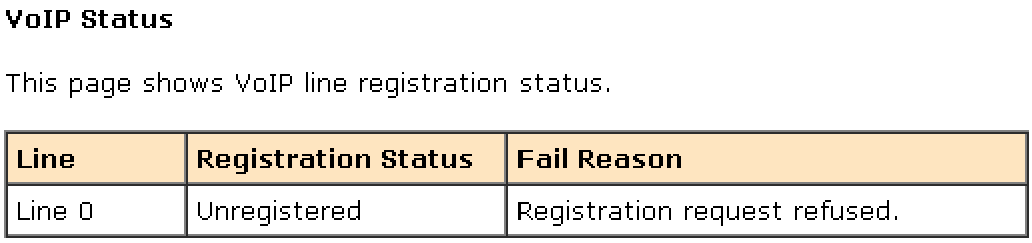
【Status】→【Statistics】



Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0_1	4_INTERNET_R_8_35	1831184	2844	0	0	501408	2627	0	0

【Status】→【VoIP Status】



VoIP Status

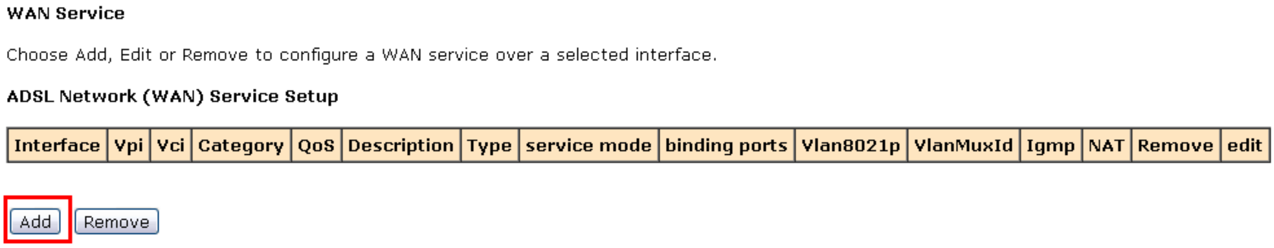
This page shows VoIP line registration status.

Line	Registration Status	Fail Reason
Line 0	Unregistered	Registration request refused.

3.2.2 Network

3.2.2.1. WAN service

Please go to 【Network】→【WAN Service】page.



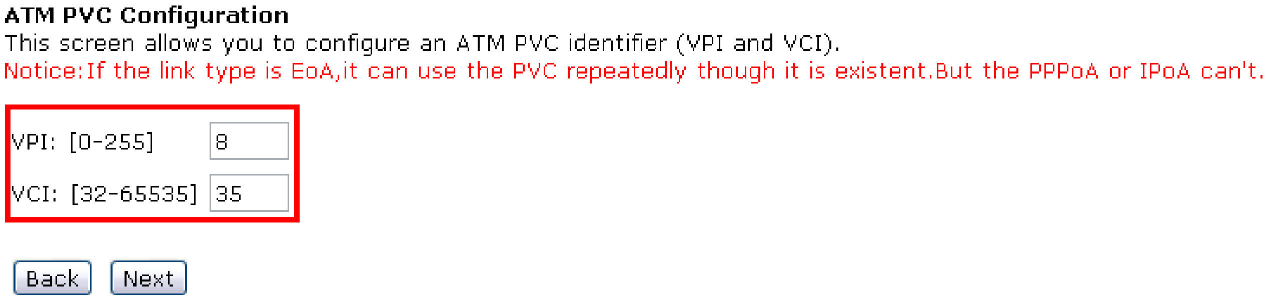
WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.

ADSL Network (WAN) Service Setup

Interface	Vpi	Vci	Category	QoS	Description	Type	service mode	binding ports	Vlan8021p	VlanMuxId	Igmp	NAT	Remove	edit

1) Click **Add** button to configure an ATM PVC identifier;



ATM PVC Configuration

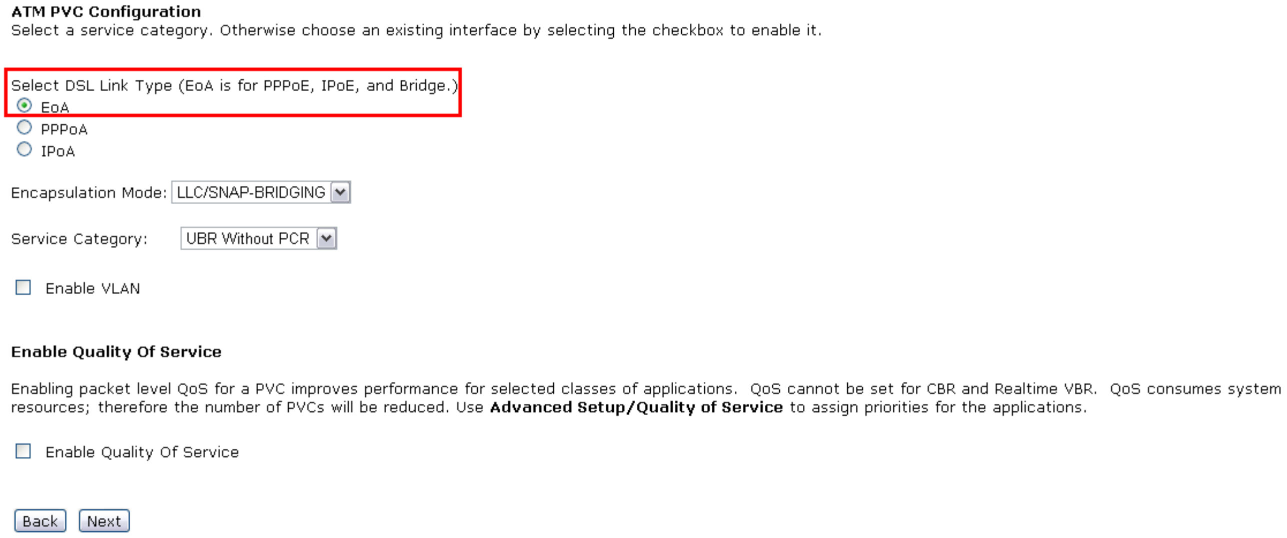
This screen allows you to configure an ATM PVC identifier (VPI and VCI).

Notice:If the link type is EoA,it can use the PVC repeatedly though it is existent.But the PPPoA or IPoA can't.

VPI: [0-255] 8

VCI: [32-65535] 35

2) Click **Next** to select a service category; (here please choose EoA for PPPoE connection)



ATM PVC Configuration
Select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
● EoA
○ PPPoA
○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

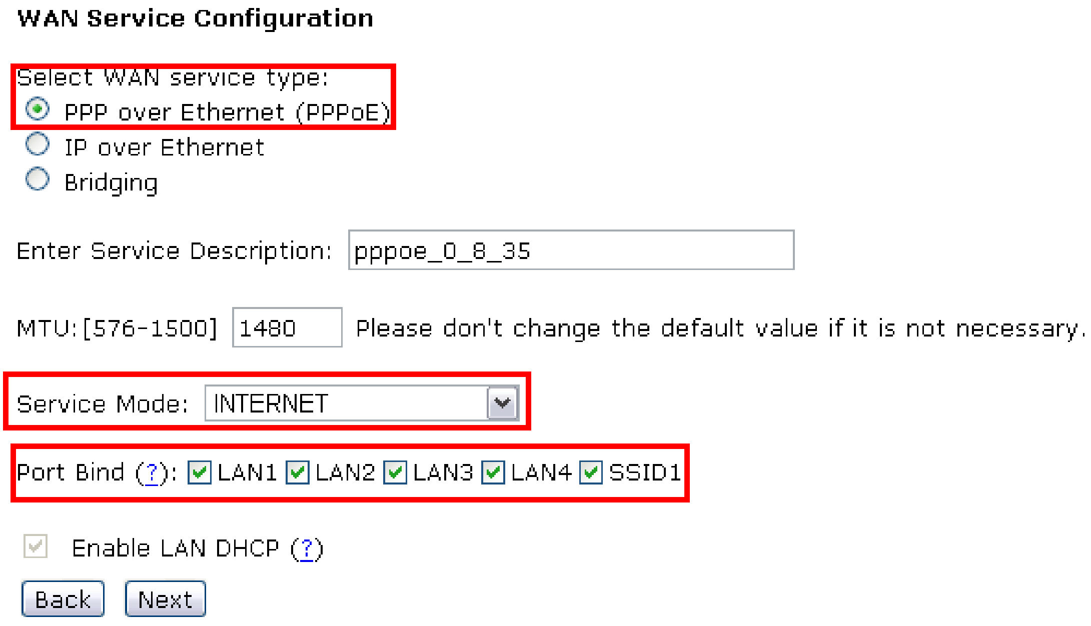
□ Enable VLAN

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

□ Enable Quality Of Service

3) Click Next to select WAN service type; (here please choose PPP over Ethernet)



WAN Service Configuration

Select WAN service type:
● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_8_35

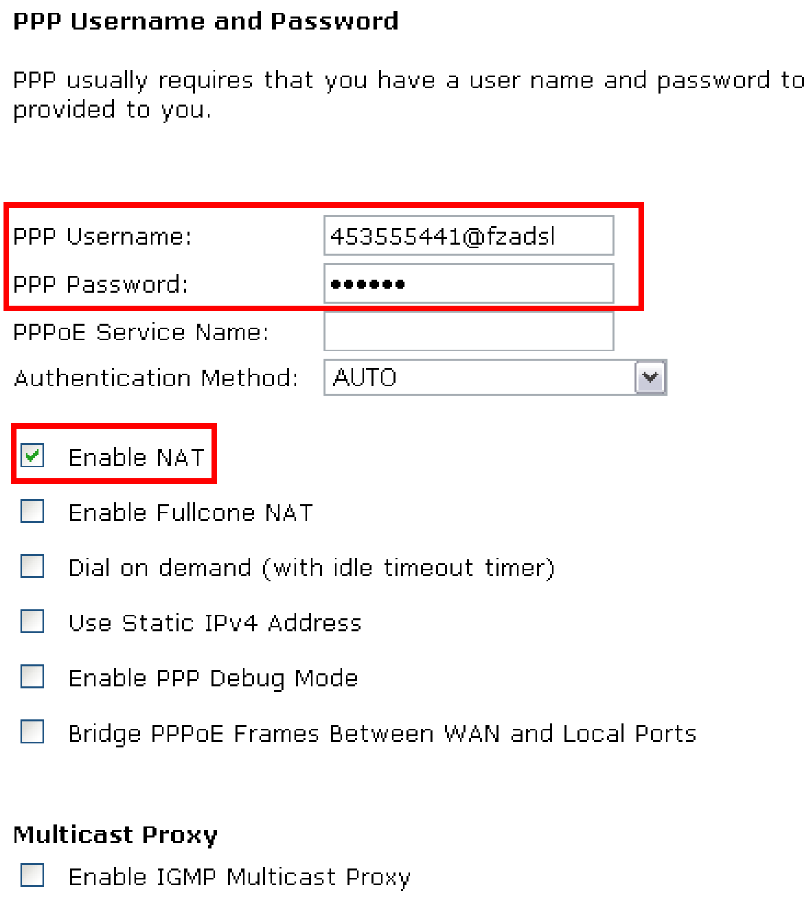
MTU:[576-1500] 1480 Please don't change the default value if it is not necessary.

Service Mode: INTERNET

Port Bind (?): ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ SSID1

☑ Enable LAN DHCP (?)

4) Click **Next** to input the username and password authorized by your ISP; (here please make **Enable NAT** checked)



PPP Username and Password

PPP usually requires that you have a user name and password to provided to you.

PPP Username:	453555441@fzadsl
PPP Password:	••••••
PPPoE Service Name:	
Authentication Method:	AUTO

☑ Enable NAT

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

□ Use Static IPv4 Address

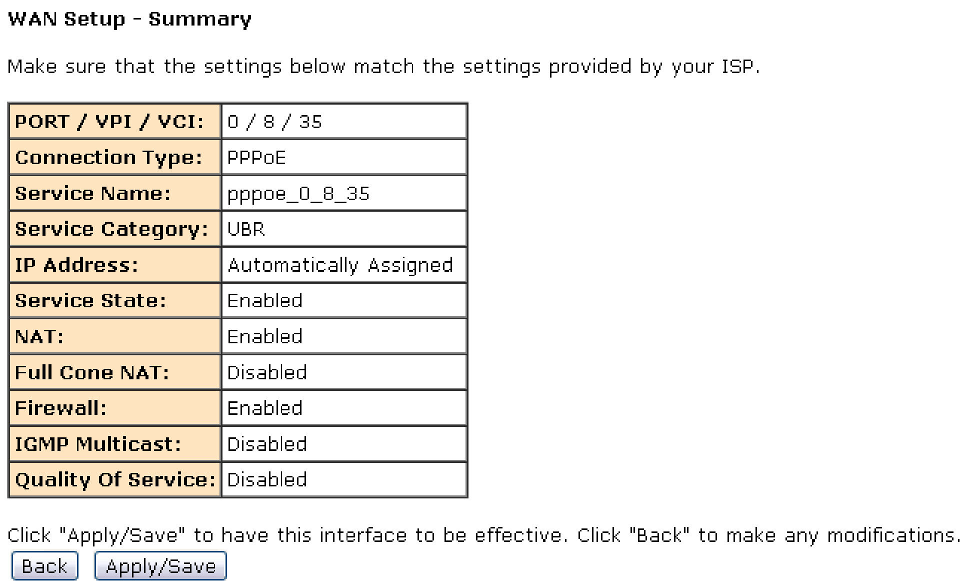
□ Enable PPP Debug Mode

□ Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

□ Enable IGMP Multicast Proxy

5) Click **Next** to check the Summary of this connection;



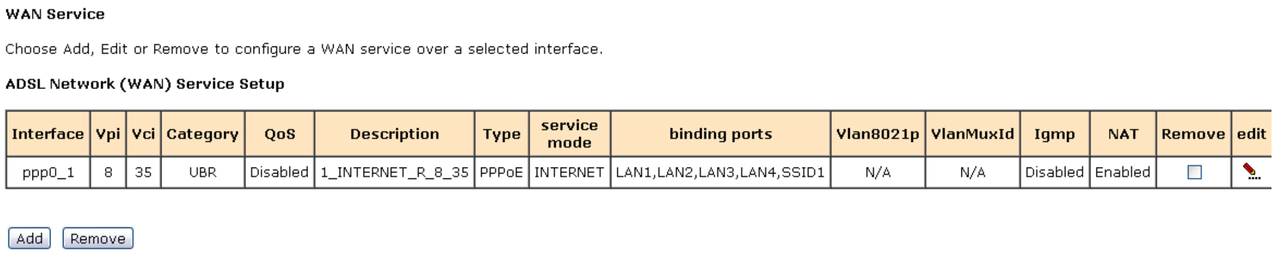
WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_8_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

6) Click **Apply/Save** to enable the connection.



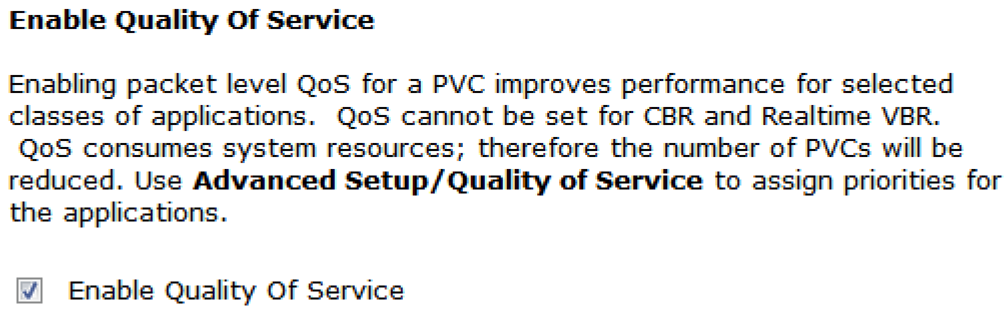
WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.

ADSL Network (WAN) Service Setup

Interface	Vpi	Vci	Category	QoS	Description	Type	service mode	binding ports	Vlan8021p	VlanMuxId	Igmp	NAT	Remove	edit
ppp0_1	8	35	UBR	Disabled	1_INTERNET_R_8_35	PPPoE	INTERNET	LAN1,LAN2,LAN3,LAN4,SSID1	N/A	N/A	Disabled	Enabled	□	✎

Note : if you need the Quality of service, pls enable QoS in WAN service config, then go to 【Network】→【Qos configuration】for the QoS setting.

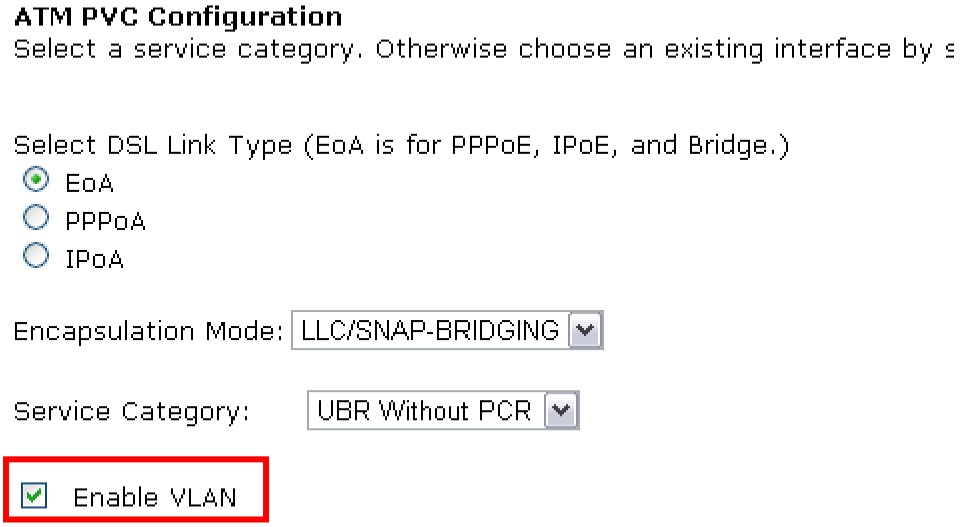


Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

☑ Enable Quality Of Service

Note : if you need the VLAN channel, please “Enable VLAN” and set VLAN id in WAN service config:



ATM PVC Configuration

Select a service category. Otherwise choose an existing interface by s

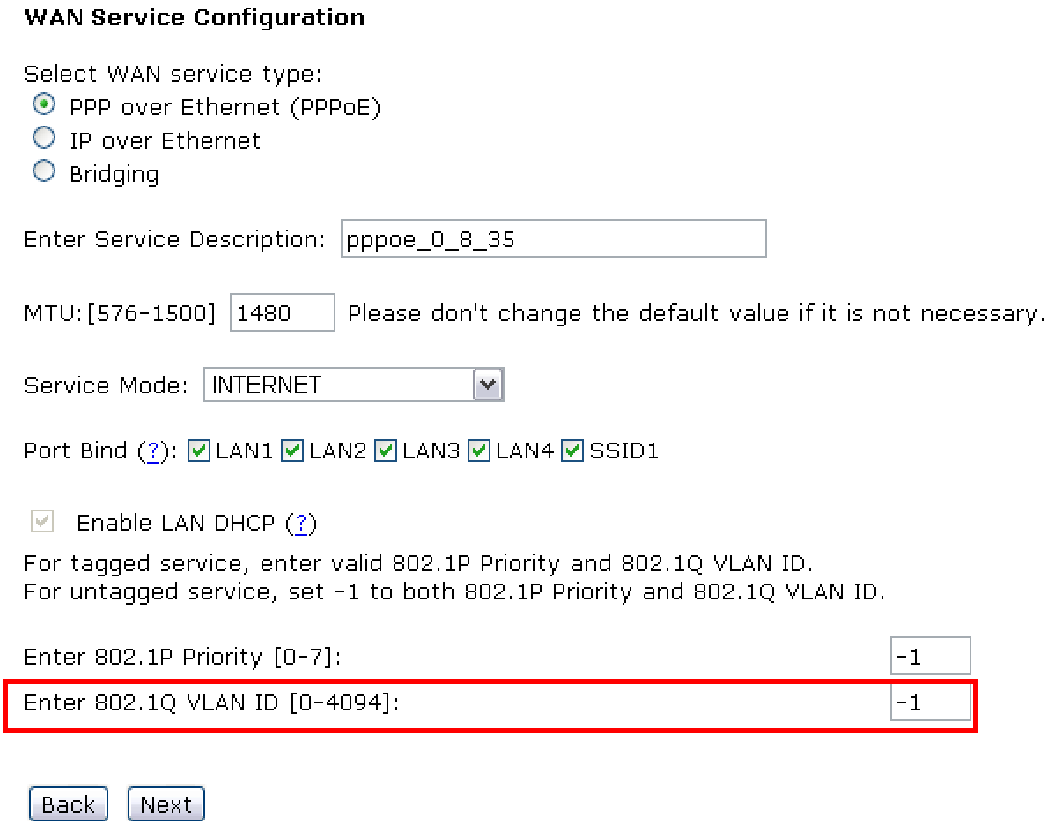
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

● EoA
○ PPPoA
○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

☑ Enable VLAN



WAN Service Configuration

Select WAN service type:
● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_8_35

MTU:[576-1500] 1480 Please don't change the default value if it is not necessary.

Service Mode: INTERNET

Port Bind (?): ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ SSID1

☑ Enable LAN DHCP (?)

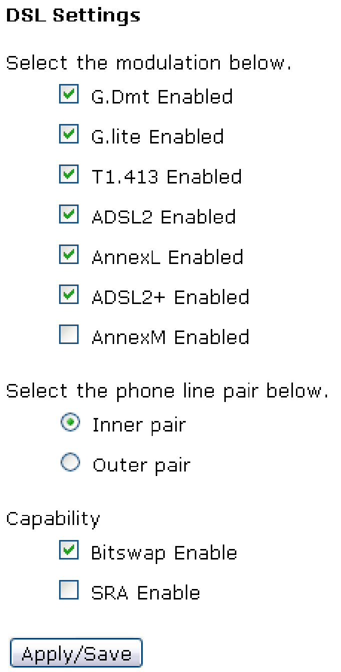
For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

3.2.2.2. DSL Settings

【Network】→【DSL Settings】



DSL Settings

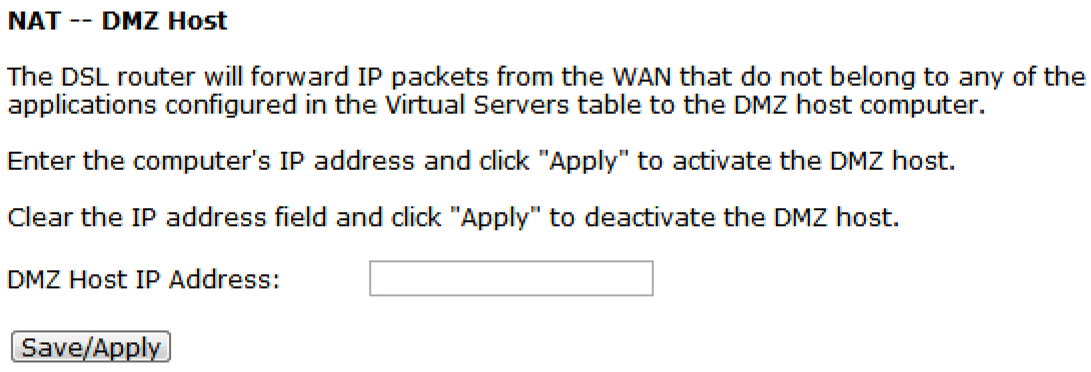
Select the modulation below.
☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

Select the phone line pair below.
● Inner pair
○ Outer pair

Capability
☑ Bitswap Enable
□ SRA Enable

3.2.2.3. DMZ host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

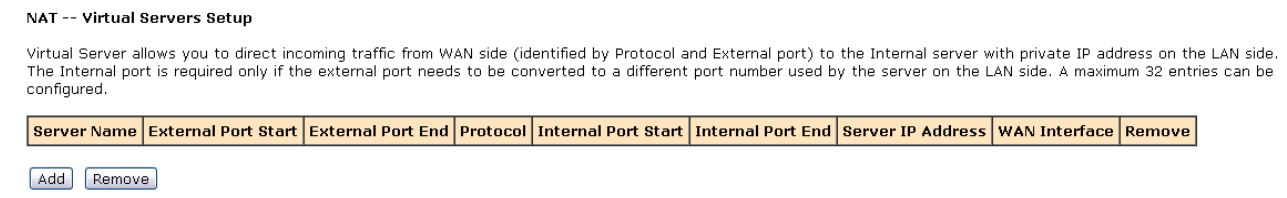
Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

3.2.2.4. Virtual Server

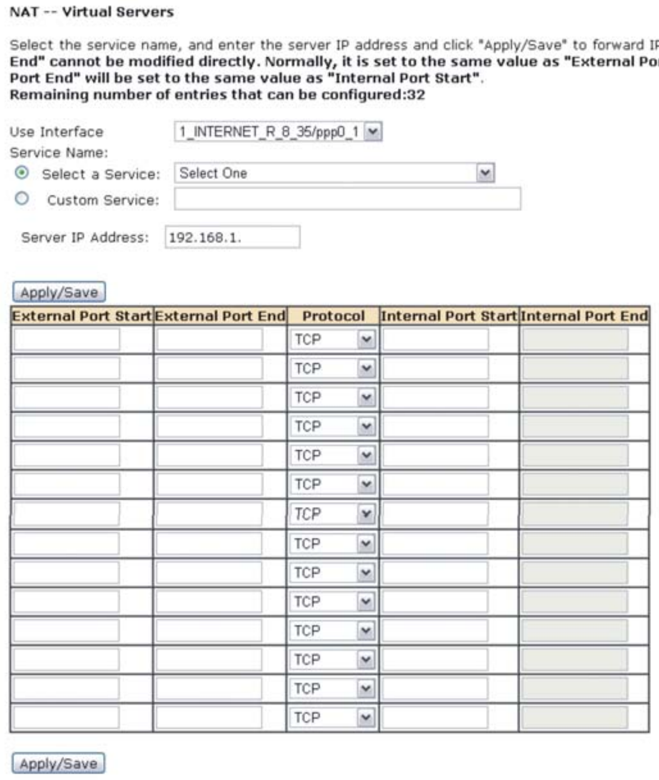
Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
【Network】→【 Virtual Servers Setup】→ click **ADD**



NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**
Remaining number of entries that can be configured:32

Use Interface 1_INTERNET_R_8_35/ppp0_1
Service Name:
● Select a Service: Select One
○ Custom Service:

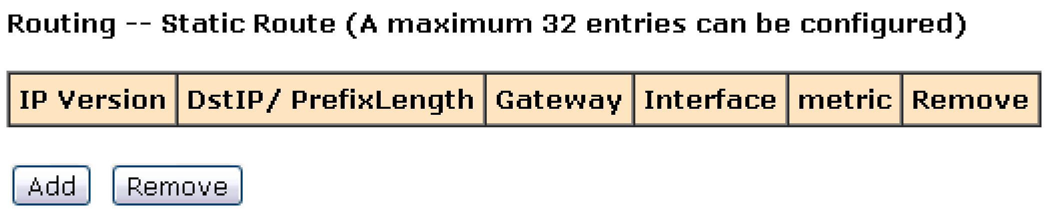
Server IP Address: 192.168.1.

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

3.2.2.5. Static Route

The user can edit the static route table for connecting different network.

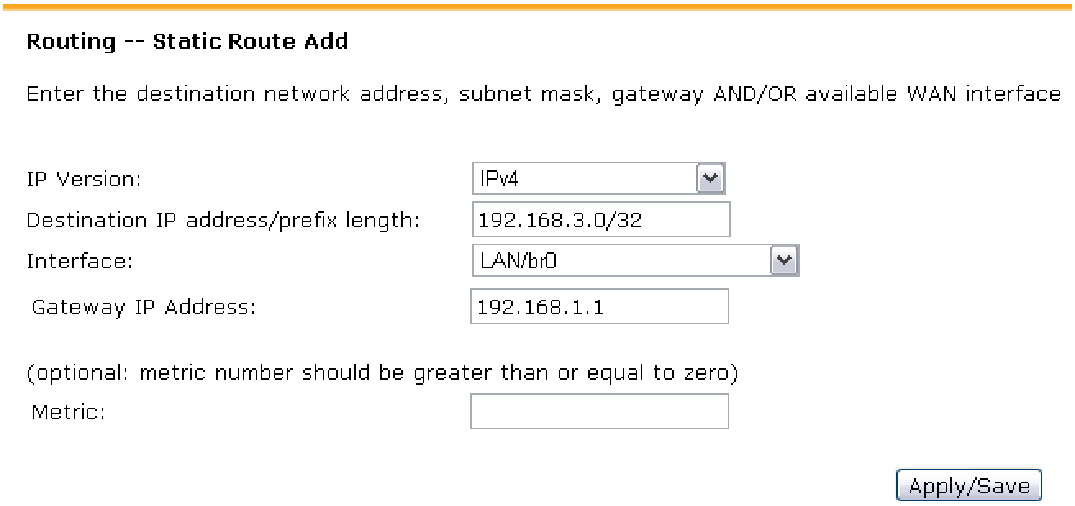
1) 【Network】→【 Static Route】



Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

2) Click **ADD** to edit the IP version, Destination IP, Gateway IP, etc.



Routing -- Static Route Add

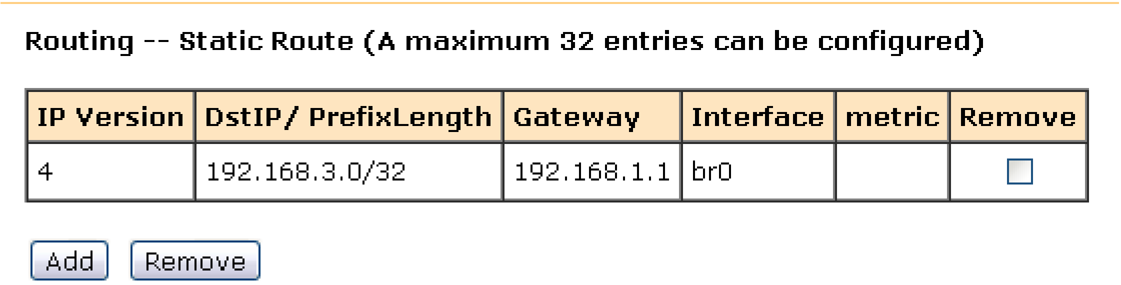
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface

IP Version:	IPv4
Destination IP address/prefix length:	192.168.3.0/32
Interface:	LAN/br0
Gateway IP Address:	192.168.1.1

(optional: metric number should be greater than or equal to zero)

Metric:	

3) Click **Apply**



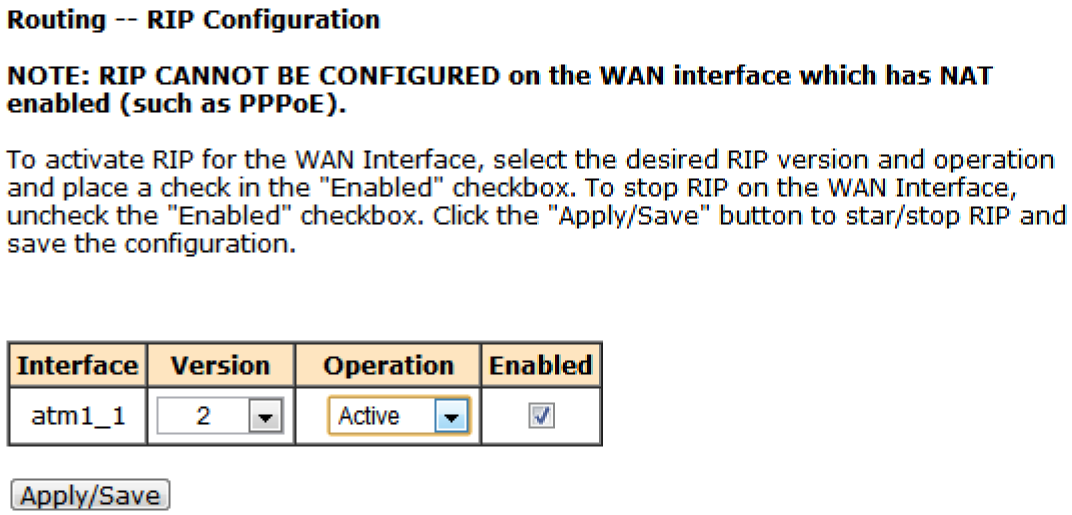
Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
4	192.168.3.0/32	192.168.1.1	br0		□

3.2.2.6. RIP configuration

RIP will send routing updates information of network layout. When the device receive updated information, it will update routing table with new path.

【Network】→【 RIP Configuration】



Routing -- RIP Configuration

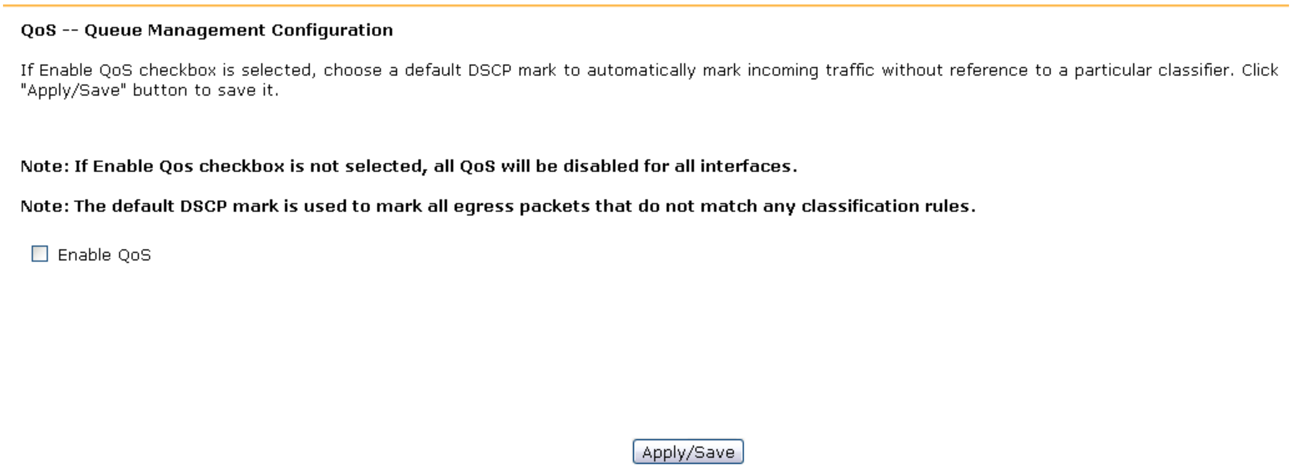
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the "Enabled" checkbox. To stop RIP on the WAN Interface, uncheck the "Enabled" checkbox. Click the "Apply/Save" button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm1_1	2	Active	☑

3.2.2.7. QoS configuration

【Network】→【QoS Configuration】



QoS -- Queue Management Configuration

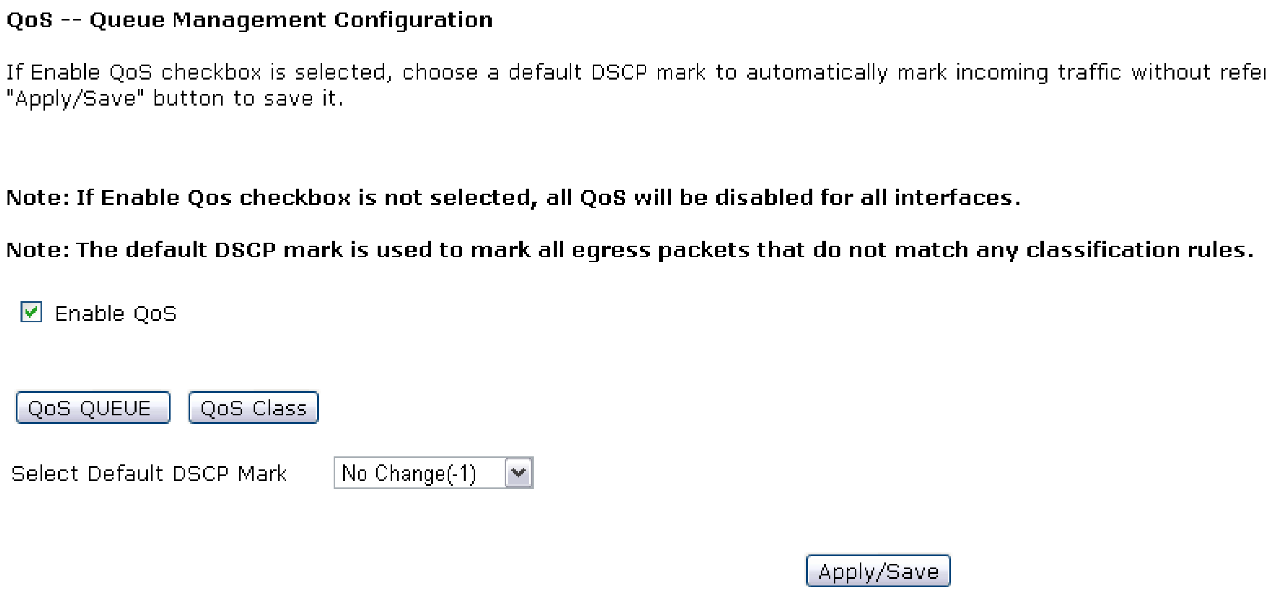
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click "Apply/Save" button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☐ Enable QoS

If **Enable QoS** checkbox is selected, a default DSCP mark should be chosen to automatically mark incoming traffic without reference to a particular classifier. Click **Apply / Save** button to save.



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without refe
"Apply/Save" button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

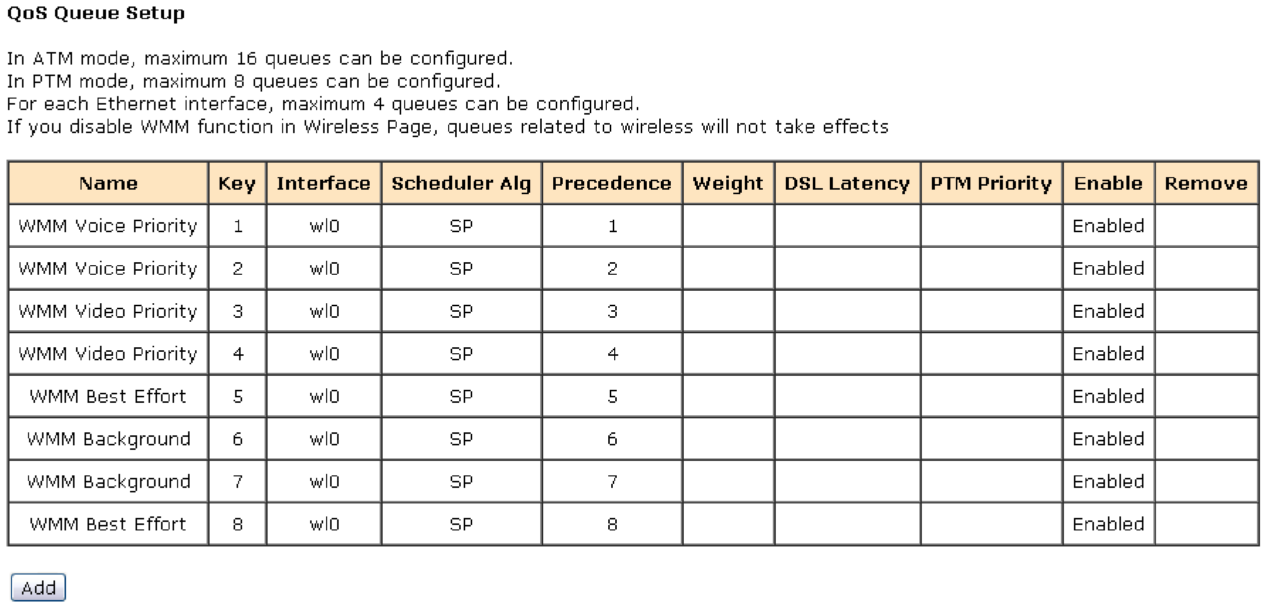
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interface; The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Please click **QoS QUEUE** button to enter the QoS Queue setup page,

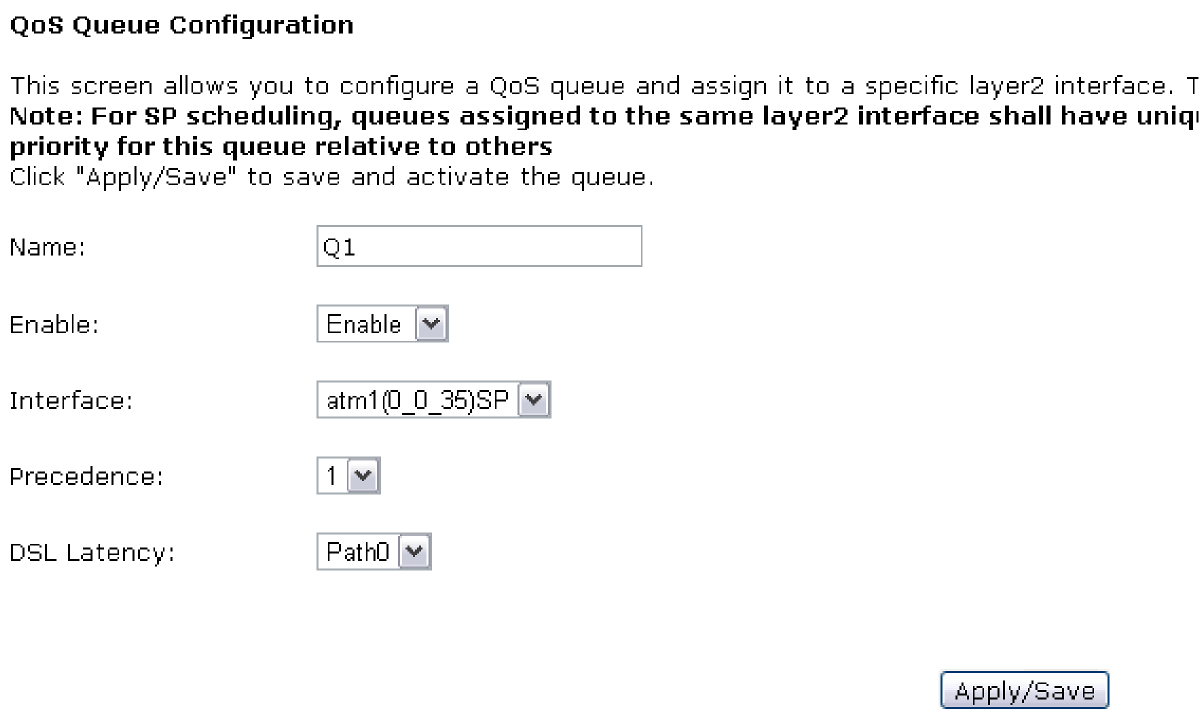


QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	

click **Add** button. This screen allows you to configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface, for example: add Queue Q1 in wan connection(PVC=0/35):

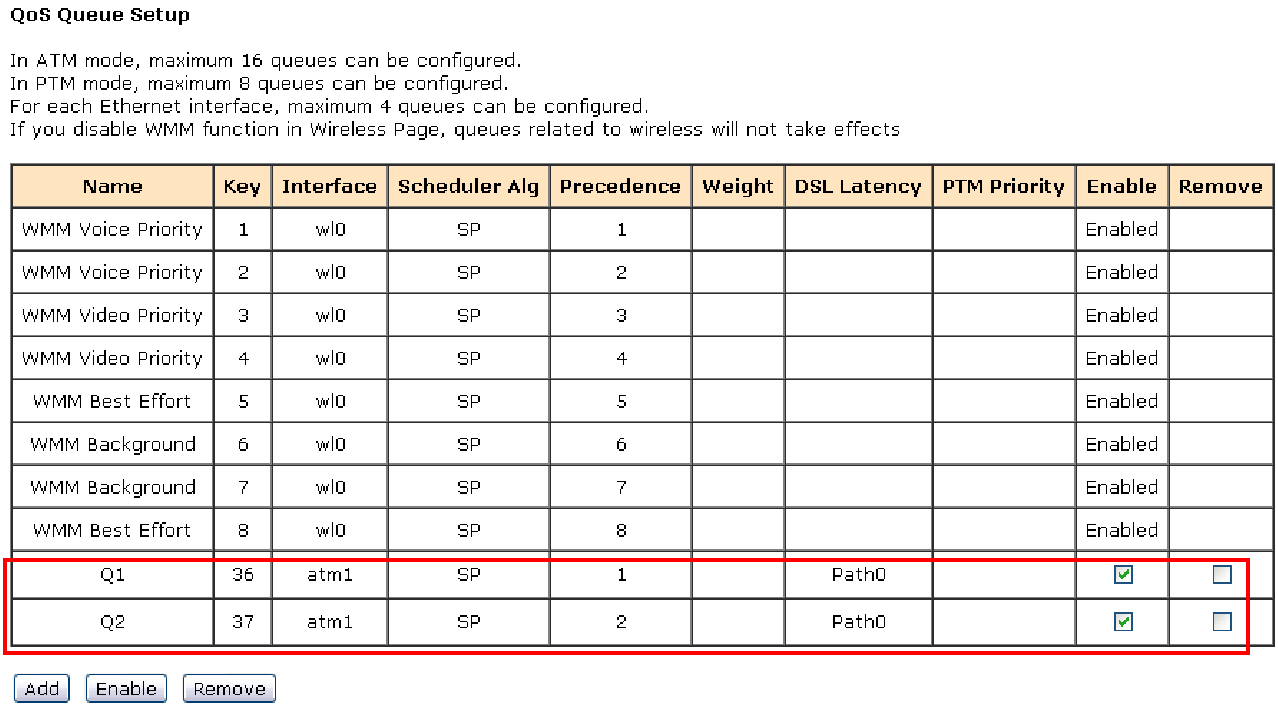


QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. T
Note: For SP scheduling, queues assigned to the same layer2 interface shall have uniq
priority for this queue relative to others
Click "Apply/Save" to save and activate the queue.

Name:	Q1
Enable:	Enable
Interface:	atm1(0_0_35)SP
Precedence:	1
DSL Latency:	Path0

Click **Apply / Save** to save and activate the queue.

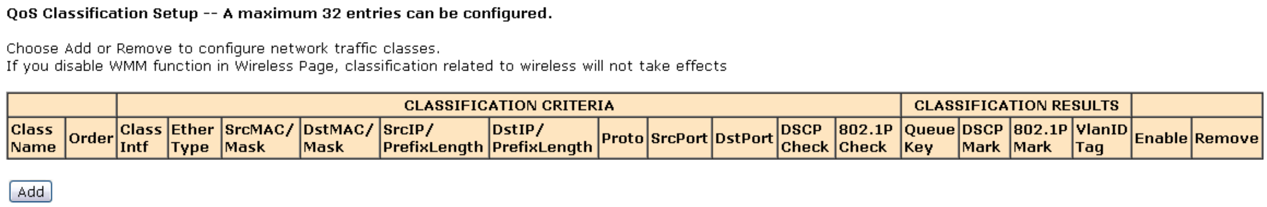


QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Q1	36	atm1	SP	1		Path0		☑	□
Q2	37	atm1	SP	2		Path0		☑	□

Please click **QoS Class** button to enter QoS Classification Setup page,



QoS Classification Setup -- A maximum 32 entries can be configured.

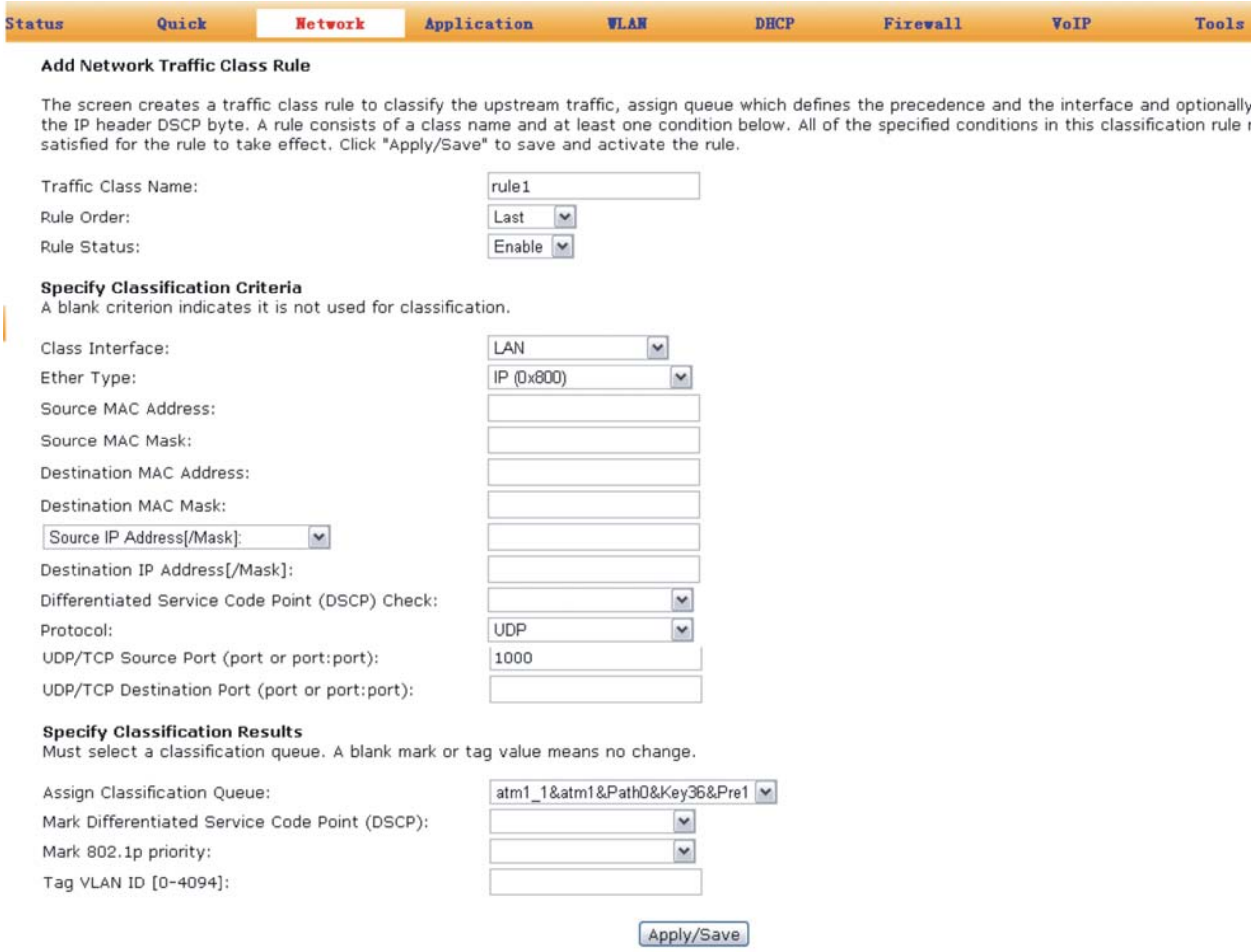
Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove

click **Add** button to configure network traffic classes. This screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the rule.

For example: add rule1 to bandage the data from UDP port 1000 to queue Q1:

1. “Traffic Class Name” : rule1
2. “Rule Status” :Enable the class
3. “Ether Type” : IP (0x800)
4. “Protocol” : protocol UDP and Source Port:1000
5. “Assign Classification Queue” to chose Queue Q1: atm1_1&atm1&Path0&key36&pre1



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule r satisfied for the rule to take effect. Click "Apply/Save" to save and activate the rule.

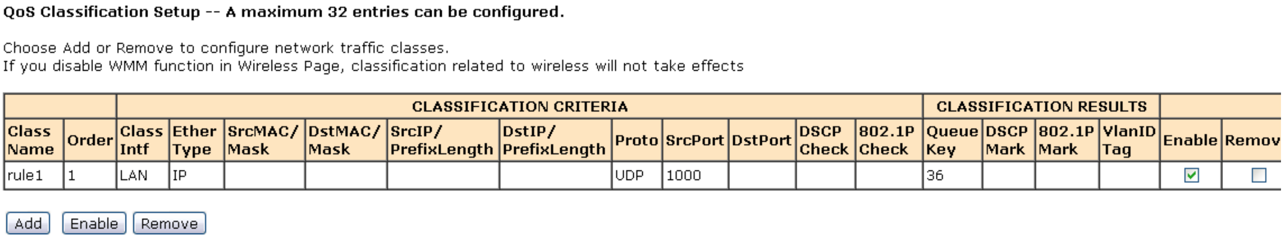
Traffic Class Name:	rule1
Rule Order:	Last
Rule Status:	Enable

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:	LAN
Ether Type:	IP (0x800)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address[/Mask]:	
Destination IP Address[/Mask]:	
Differentiated Service Code Point (DSCP) Check:	
Protocol:	UDP
UDP/TCP Source Port (port or port:port):	1000
UDP/TCP Destination Port (port or port:port):	

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	atm1_1&atm1&Path0&Key36&Pre1
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID [0-4094]:	



QoS Classification Setup -- A maximum 32 entries can be configured.

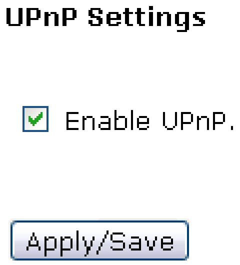
Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remov
rule1	1	LAN	IP					UDP	1000				36				☑	□

3.2.3 Application

3.2.3.1. UPnP Settings

Through the UPnP (Universal Plug and Play) of HG-A800, the external PCs are able to access the resource of the internal PCs connected with the LAN port of HG-A800.
【Application】→【UPnP Settings】

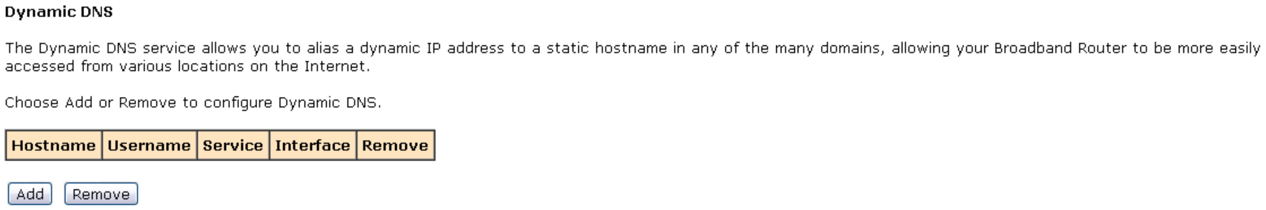


UPnP Settings

☑ Enable UPnP.

3.2.3.2. Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.
【Application】→【Dynamic DNS】



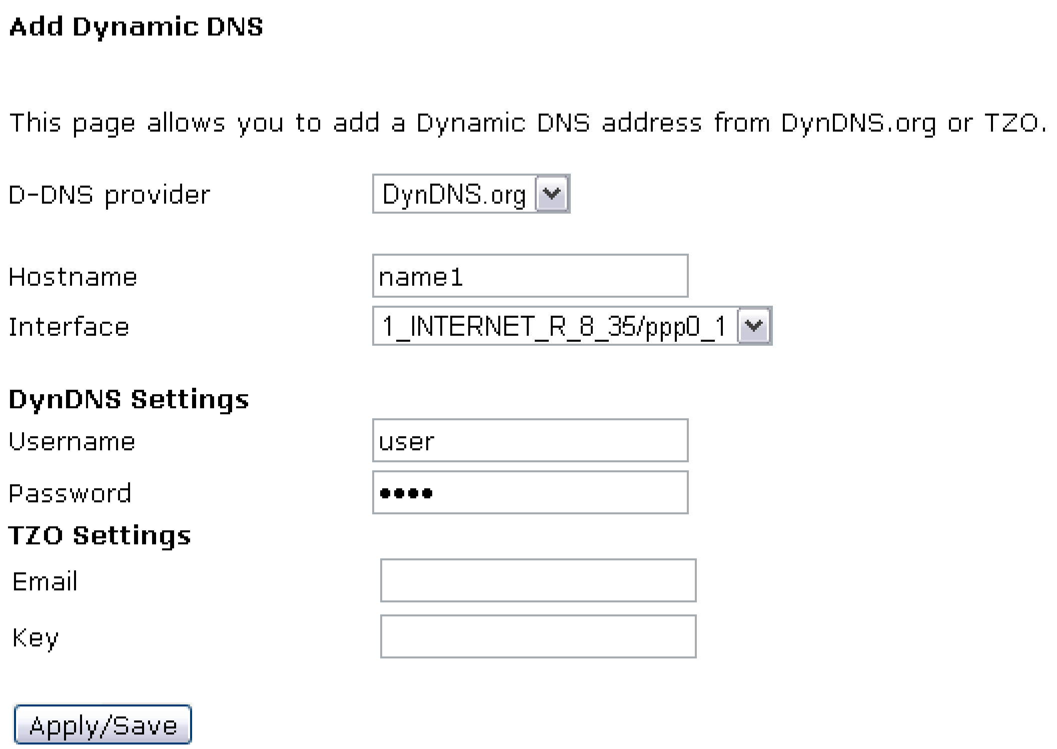
Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

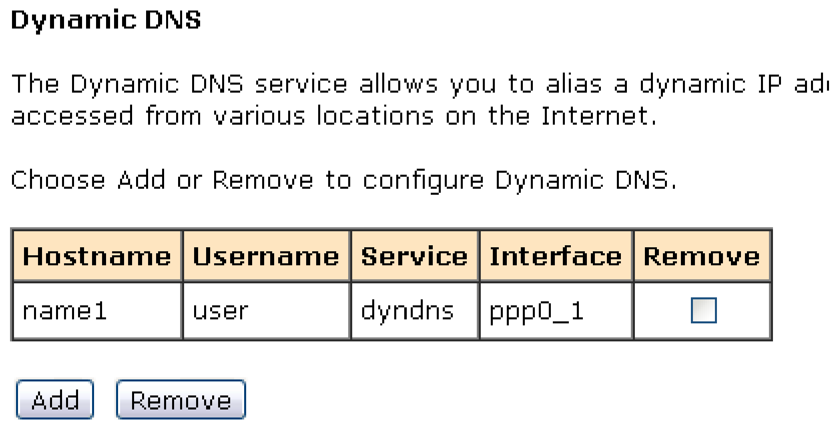
Click **ADD** to add Dynamic DNS, for example:



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	DynDNS.org ▾
Hostname	name1
Interface	1_INTERNET_R_8_35/ppp0_1 ▾
DynDNS Settings	
Username	user
Password	••••
TZO Settings	
Email	
Key	



Dynamic DNS

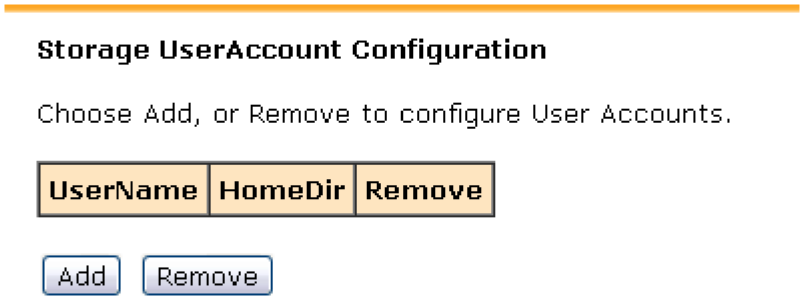
The Dynamic DNS service allows you to alias a dynamic IP ad
accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
name1	user	dyndns	ppp0_1	□

3.2.3.3. Samba Users

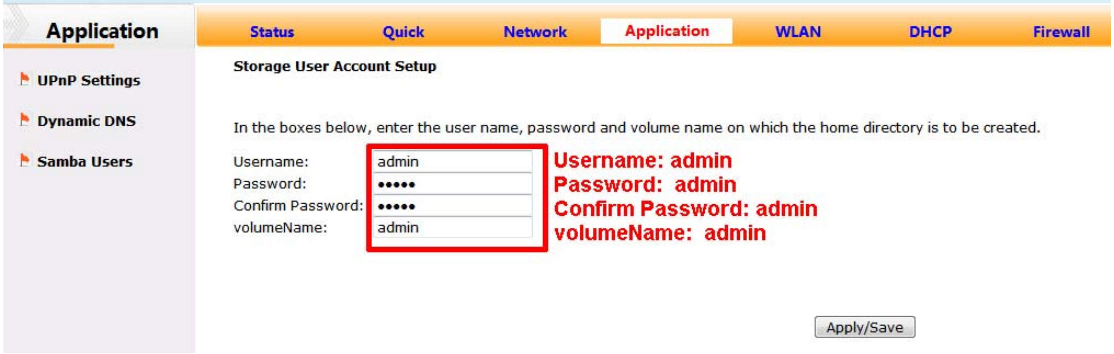
【Application】→【Samba Users】to add the Samba storage account



Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	HomeDir	Remove

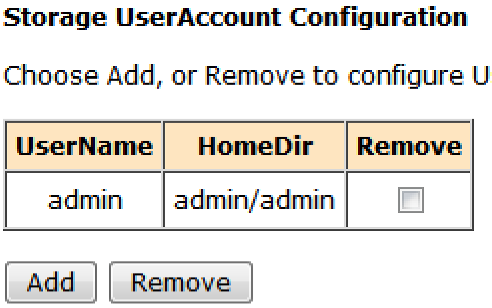


Storage User Account Setup

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username:	admin
Password:	•••••
Confirm Password:	•••••
volumeName:	admin

Username: admin
Password: admin
Confirm Password: admin
volumeName: admin



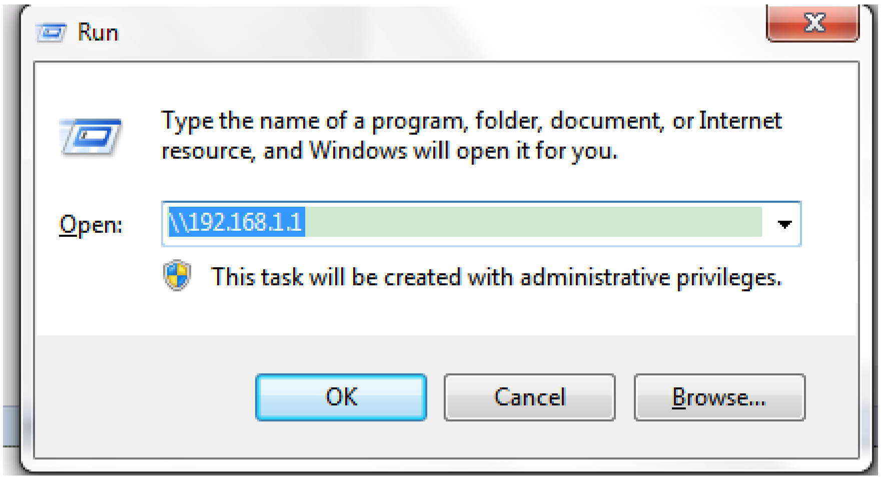
Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	HomeDir	Remove
admin	admin/admin	□

Then you can Visit the USB storage.

For example with Win7 OS, please Run: \\192.168.1.1

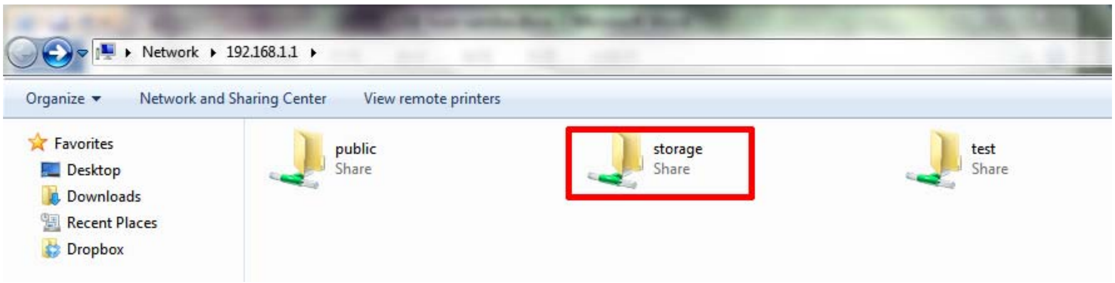


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

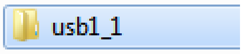
Open: \\192.168.1.1

This task will be created with administrative privileges.

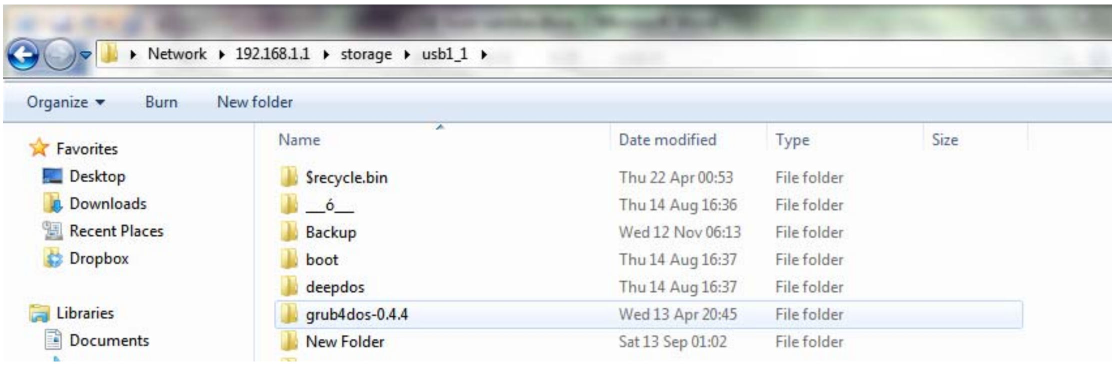
Double click storage:



Double click:



The usb disk will be shown:



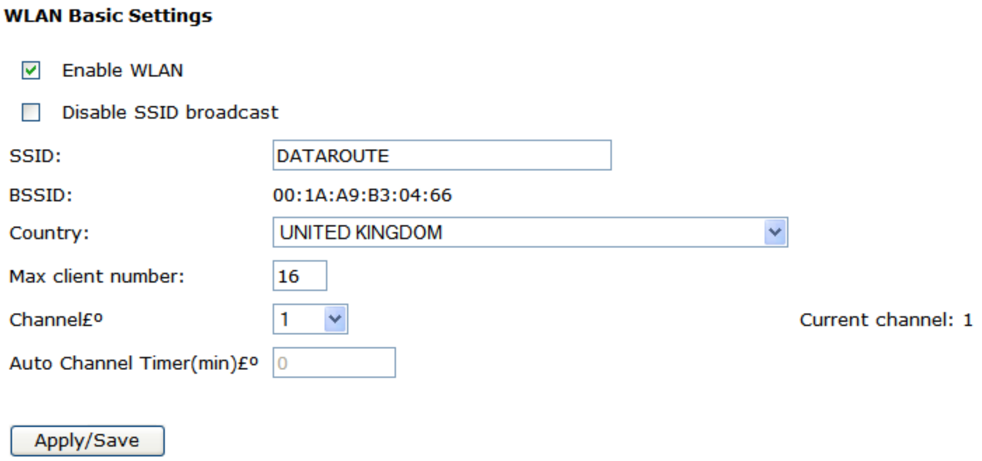
Name	Date modified	Type	Size
$recycle.bin	Thu 22 Apr 00:53	File folder	
__ó__	Thu 14 Aug 16:36	File folder	
Backup	Wed 12 Nov 06:13	File folder	
boot	Thu 14 Aug 16:37	File folder	
deepdos	Thu 14 Aug 16:37	File folder	
grub4dos-0.4.4	Wed 13 Apr 20:45	File folder	
New Folder	Sat 13 Sep 01:02	File folder	

3.2.4 WLAN Configuration

3.2.4.1. WLAN basic setting

Click **WLAN** to configure the wireless feature of the modem.

1) Go to path: 【WLAN】-> 【WLAN Basic】page to enable/disable WLAN feature. Then click **Apply/Save** button;



WLAN Basic Settings

☑ Enable WLAN

□ Disable SSID broadcast

SSID: DATAROUTE

BSSID: 00:1A:A9:B3:04:66

Country: UNITED KINGDOM

Max client number: 16

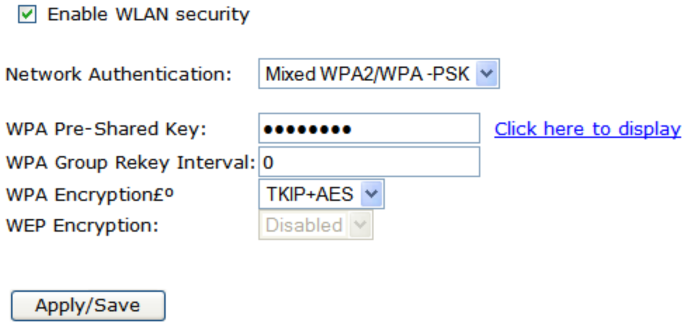
Channel£º 1 Current channel: 1

Auto Channel Timer(min)£º 0

3.2.4.2. WLAN security

Go to path:【WLAN】->【WLAN Security】page to set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click **Apply/Save** when done.

The default Wireless Key is **data1234** – it is strongly recommended that this be changed.



☑ Enable WLAN security

Network Authentication: Mixed WPA2/WPA -PSK

WPA Pre-Shared Key: •••••••• Click here to display

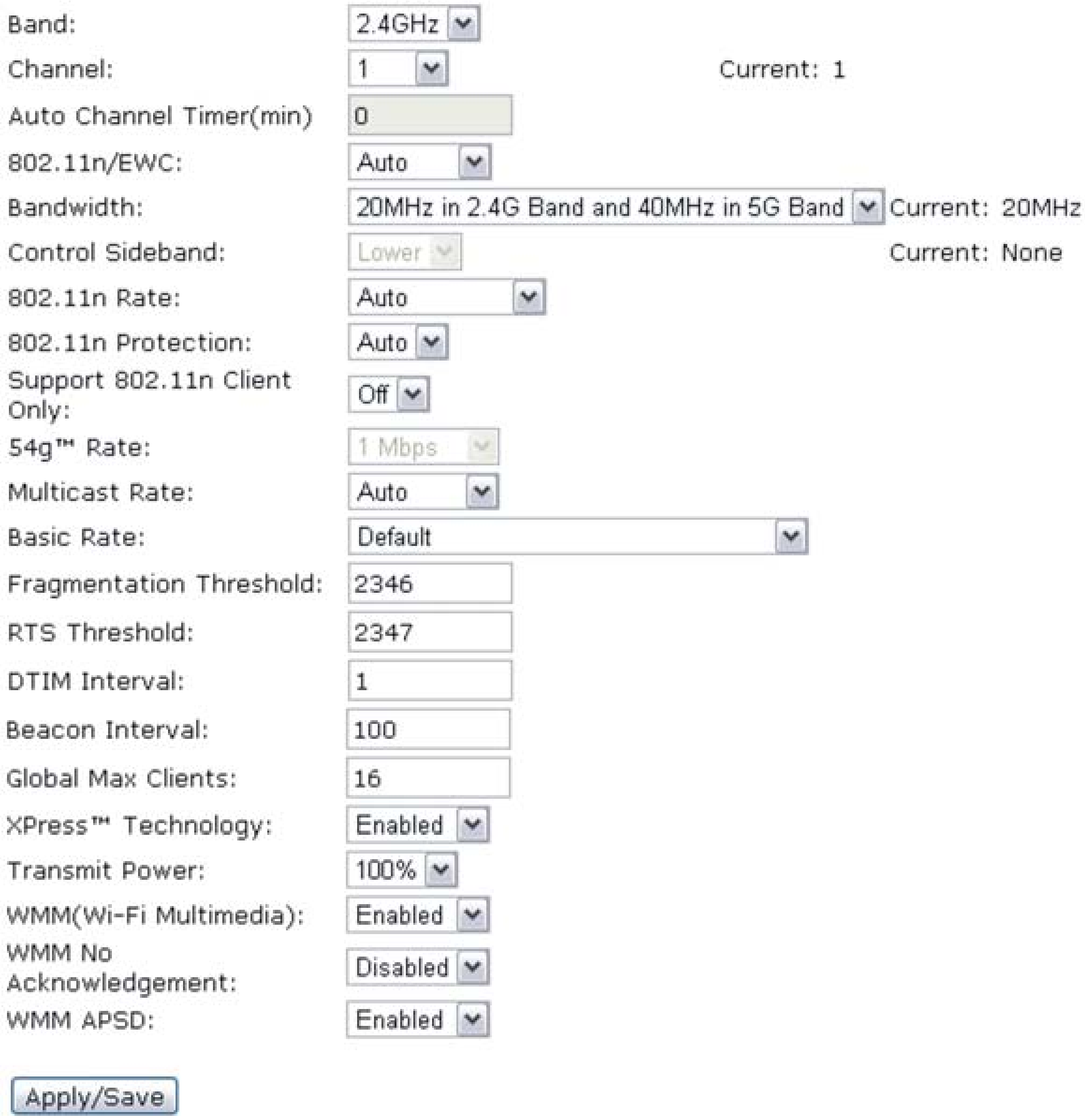
WPA Group Rekey Interval: 0

WPA Encryption£º TKIP+AES

WEP Encryption: Disabled

3.2.4.3. WLAN advance settings

【WLAN】→【Advance Settings】



Band: 2.4GHz

Channel: 1 Current: 1

Auto Channel Timer(min) 0

802.11n/EWC: Auto

Bandwidth: 20MHz in 2.4G Band and 40MHz in 5G Band Current: 20MHz

Control Sideband: Lower Current: None

802.11n Rate: Auto

802.11n Protection: Auto

Support 802.11n Client Only: Off

54g™ Rate: 1 Mbps

Multicast Rate: Auto

Basic Rate: Default

Fragmentation Threshold: 2346

RTS Threshold: 2347

DTIM Interval: 1

Beacon Interval: 100

Global Max Clients: 16

XPress™ Technology: Enabled

Transmit Power: 100%

WMM(Wi-Fi Multimedia): Enabled

WMM No Acknowledgement: Disabled

WMM APSD: Enabled

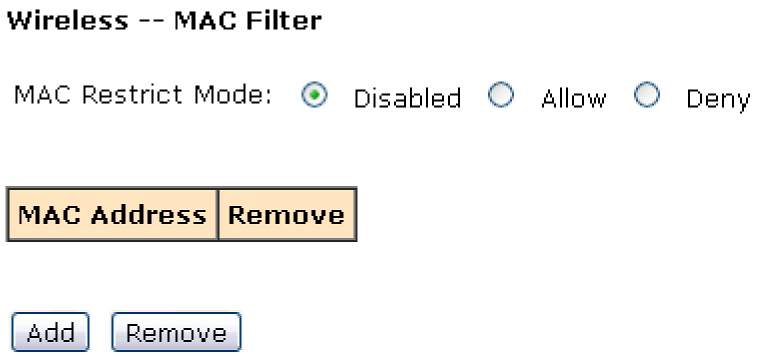
Note:

Item	Description
Band	Set the band of AP，default value: 2.4GHz
Channel	Set the channel of AP, the maximum is 11
Auto Channel Timer(min)	Set the timer for auto-setting the channel
54g™ Rate	Set the 54g™ Rate
Multicast Rate	Specify a transmission speed for AP. As for the "Auto", the AP will automatically according to the environment select a best transmission speed.
Basic Rate	Set the basic rate
Fragmentation Threshold	Default value: 2346。
RTS Threshold	Default value: 2347。
DTIM Interval	specified the DTIM Interval
Beacon Interval	Default value: 100ms
Global Max Clients	The number of clients can access to AP

XPress™ Technology	Enable or disable XPress™
54g™ Mode	54g Auto：Have the greatest compatibility 54g Performance：best performance with 54g device 54g LRS：solve the problem with 802.11b device 802.11b Only：only for 802.11b device
54g™ Protection	When 54g™ protection is enabled, g-mode of 11g will be auto enabled in 11g data transmission.
Preamble Type	Set Preamble Type
Transmit Power	Transmit Power with 20%,40%,60%,80%,100%.
WMM(Wi-Fi Multimedia)	Set Wi-Fi Multimedia
WMM No	Set WMM No
WMM APSD	Set WMM APSD

3.2.4.4. WLAN MAC filters

【WLAN】→【WLAN MAC Filters】



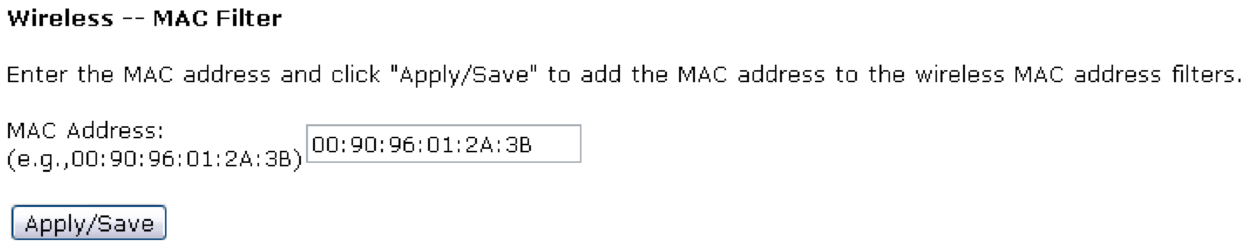
Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

- Allow：The computer with the matching MAC address in the list of MAC address can access to Internet.
- Deny：The computer with the matching MAC address in the list of MAC address can not access to Internet.

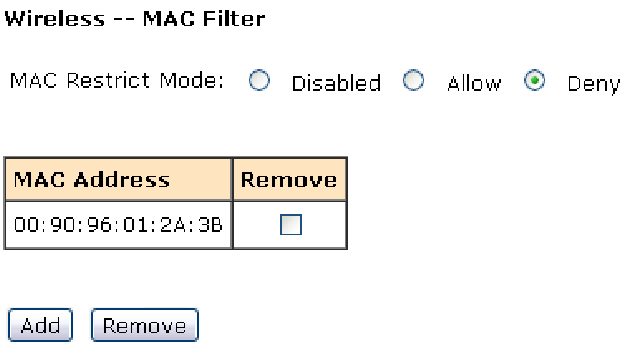
For example: The computer with MAC 00:90:96:01:2A:3B can not surf the internet through HG-A800.



Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:
(e.g.,00:90:96:01:2A:3B) 00:90:96:01:2A:3B



Wireless -- MAC Filter

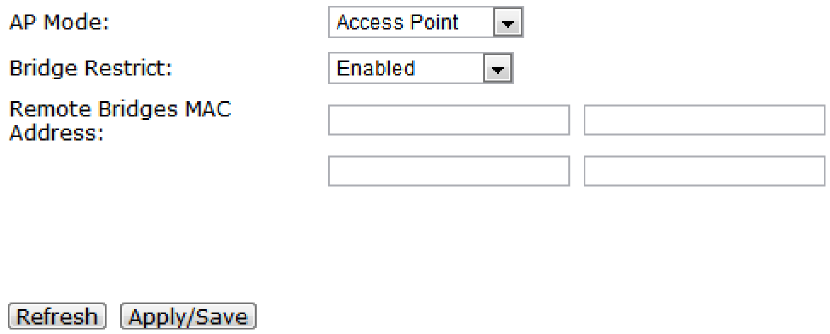
MAC Restrict Mode: ○ Disabled ○ Allow ● Deny

MAC Address	Remove
00:90:96:01:2A:3B	☐

3.2.4.5. WLAN Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. 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.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

【WLAN】→【WLAN Bridge】



AP Mode: Access Point

Bridge Restrict: Enabled

Remote Bridges MAC Address:

Note:

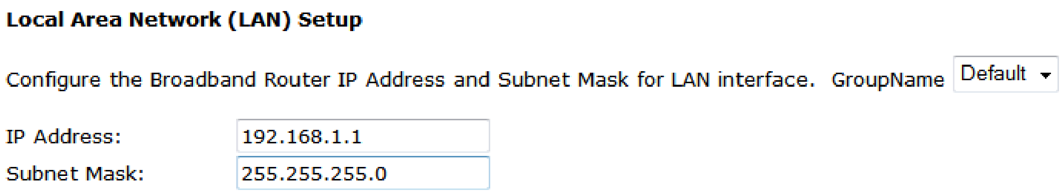
Item		description
AP Mode	Wireless Bridge	Only support wireless bridge, not for AP
	Access Point	Support all AP and wireless bridge
Bridge Restrict	Enabled	No limited to access
	Disabled	Only for specified Remote Bridges MAC Address
Remote Bridges MAC Address		

3.2.5 LAN Configuration

3.2.5.1. Configuration of the HG-A800's IP address

As a network device, ADSL Modem has its own IP address and MAC address. The factory sets the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. The user can

configure these addresses through the **Service Settings** on **DHCP** like this:
For example, change IP address to “192.168.1.10”. Click **LAN**, input **IP address**: 192.168.1.10, then “subnet mask”: 255.255.255.0, Press “Save” when configuration is finished.



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

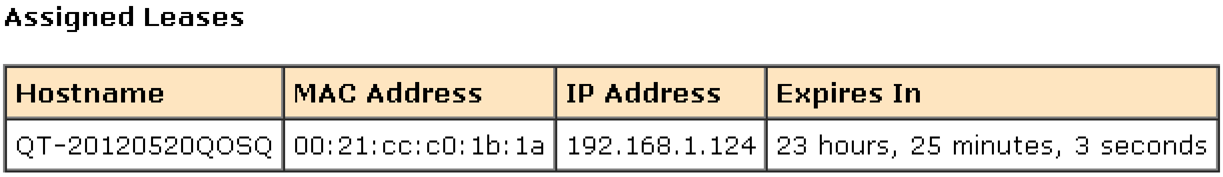
3.2.5.2. DHCP Configuration

【DHCP】→【LAN Setup】

1. Click **DHCP**;
2. Click **Service Settings**;
3. Define the “Start IP address” and the “End IP address” of DHCP server (for example, from 192.168.1.11 to 192.168.1.254);
4. Input the value of lease (Measured by the second, 0 indicates permanently valid);
5. Enable DHCP server, computer will set the IP Address of the PC with one of the addresses 192.168.1.2 ~192.168.1.254 (Excluding 192.168.1.1);

Note: When you use the DHCP Server, please make sure you don’t have multiple DHCP Servers in one LAN.

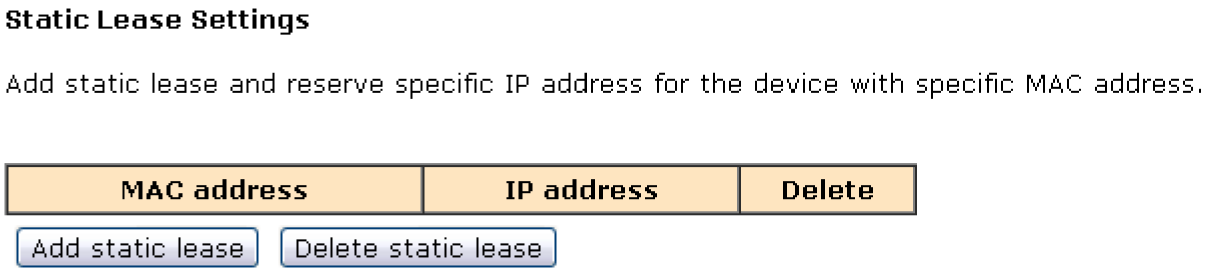
【DHCP】→【Assigned Leases】to show the assigned IP



Assigned Leases

Hostname	MAC Address	IP Address	Expires In
QT-20120520QOSQ	00:21:cc:c0:1b:1a	192.168.1.124	23 hours, 25 minutes, 3 seconds

【DHCP】→【Static Lease】to assign a special IP address to specified MAC.



Static Lease Settings

Add static lease and reserve specific IP address for the device with specific MAC address.

MAC address	IP address	Delete

3.2.6 Firewall

3.2.6.1. Firewall Settings

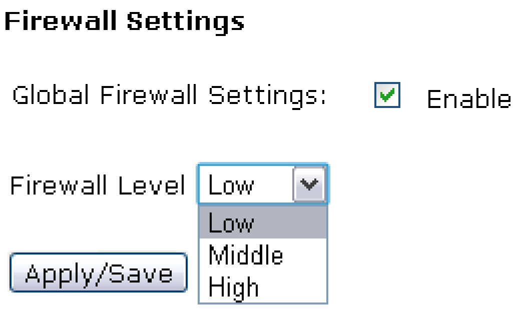
1) Please go to path:【Firewall】→【Firewall Settings】, open the Firewall settings page;

2) Check "Enable", and then click "Apply/Save" to activate Global firewall;

Note: three Firewall levels are supported in the device, they are:

- Low: enable basic firewall features - prevent port scanning; allow PING from WAN side; allow ICMP redirect messages from WAN side.
- Middle: in addition to Low level, prevent ICMP redirect messages.
- High: in addition to Middle level, prevent SYN Flood attack; against PING from WAN side.

3) Select the level of security you need in the "Firewall Level" list, and then click "Apply/Save" to save the setting.



Firewall Settings

Global Firewall Settings: ☑ Enable

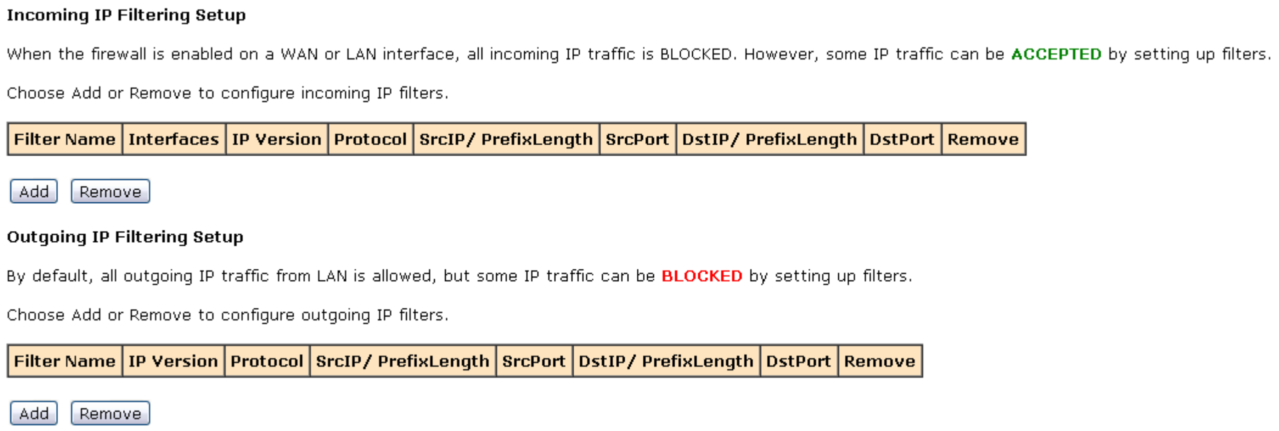
Firewall Level Low

4) After configuring, it will display the new firewall status on the page.

3.2.6.2. IP Filters

The IP filters can refuse or allow the communication between LAN computer and the Internet, can refuse or allow specific IP address's specific port or all ports, can refuse or allow specific protocol type.

【Firewall】→【IP Filter】, enter the page of Incoming IP Filtering Setup。



Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

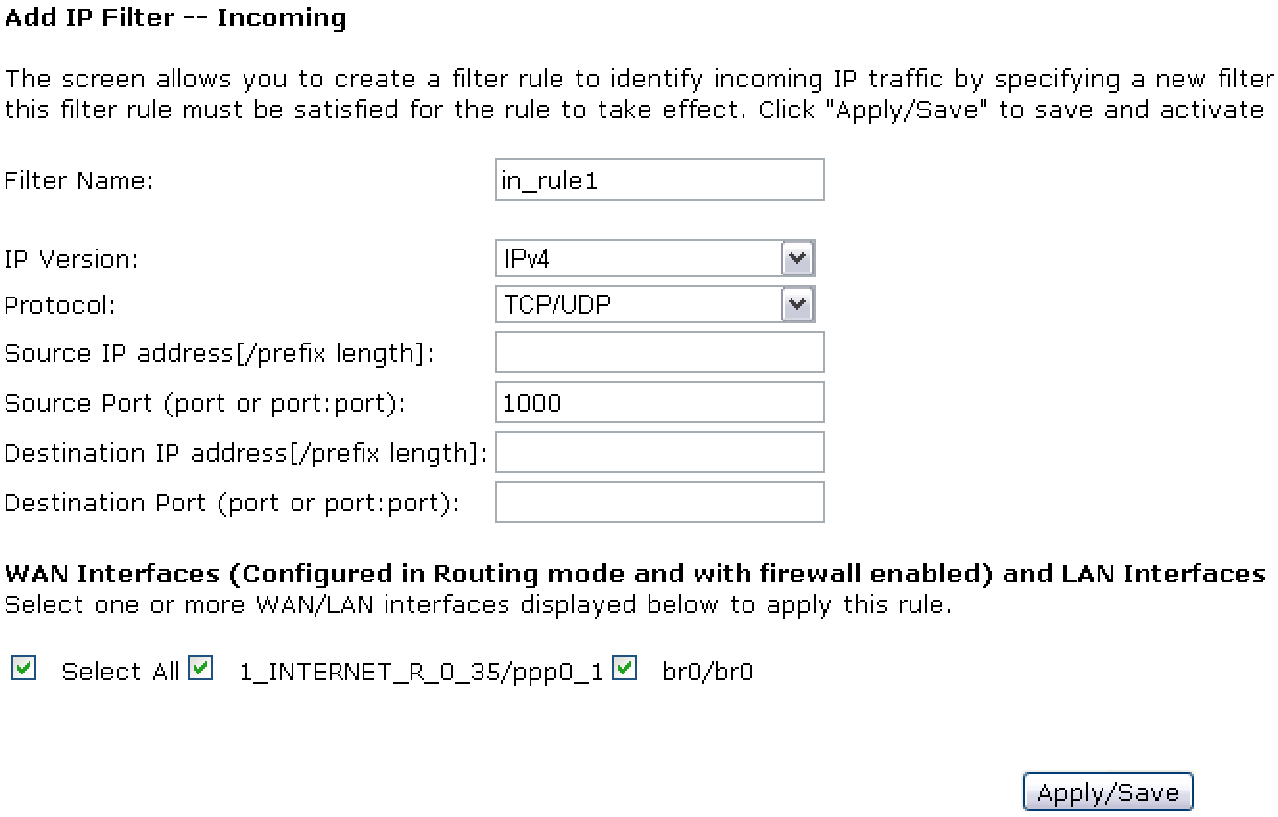
Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

- **Inbound filter**

1) Click Add button to configure incoming IP filters. The following interface allows user to create a filter rule to identify incoming IP traffic by specifying a new filter name, protocol, source port and WAN connection information.

Create a rule like this：only allows the internet data inbound whose protocol is TCP/UDP and source port is 1000. the filter name is in_rule1：

1. “Filter Name”：in_rule1。
2. “Protocol”: choose “TCP/UDP”;
3. “Source Port (port or port:port)”：1000;
4. select “Select All” to take this rule effect to all the internet connections in the HG-A800.



Add IP Filter -- Incoming

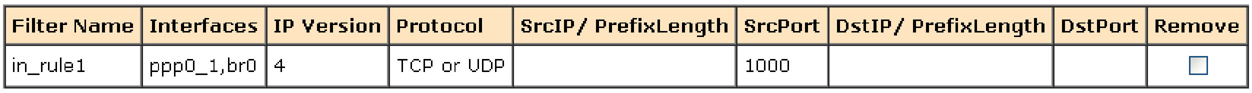
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter
this filter rule must be satisfied for the rule to take effect. Click "Apply/Save" to save and activate

Filter Name:	in_rule1
IP Version:	IPv4
Protocol:	TCP/UDP
Source IP address[/prefix length]:	
Source Port (port or port:port):	1000
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All ☑ 1_INTERNET_R_0_35/ppp0_1 ☑ br0/br0

2) After entering the required settings click the **Apply/Save** button.
3) If success, you will see the new added rule in the below figure:

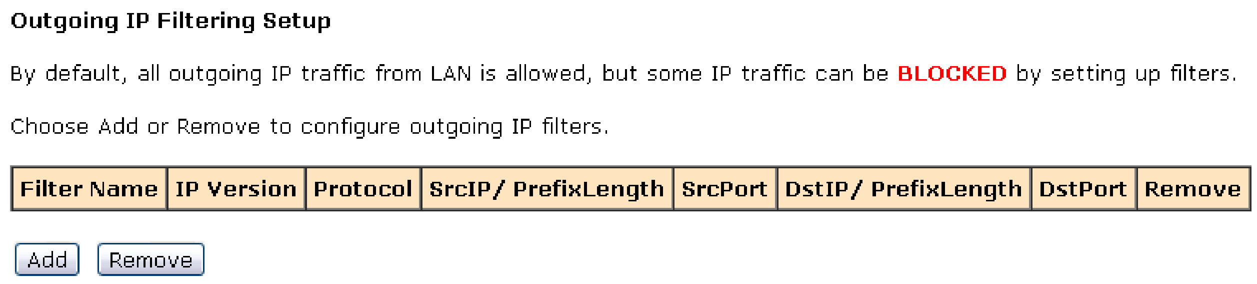


Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
in_rule1	ppp0_1,br0	4	TCP or UDP		1000			□

4) If needs to delete the IP inbound filter rule, choose the radio buttons on the right,and then click the “Remove”.

- Outbound filter

1) Click **Add** button to configure outgoing IP filters. The following interface allows user to create a filter rule to identify incoming IP traffic by specifying a new filter name, protocol, source port and WAN connection information.



Outgoing IP Filtering Setup

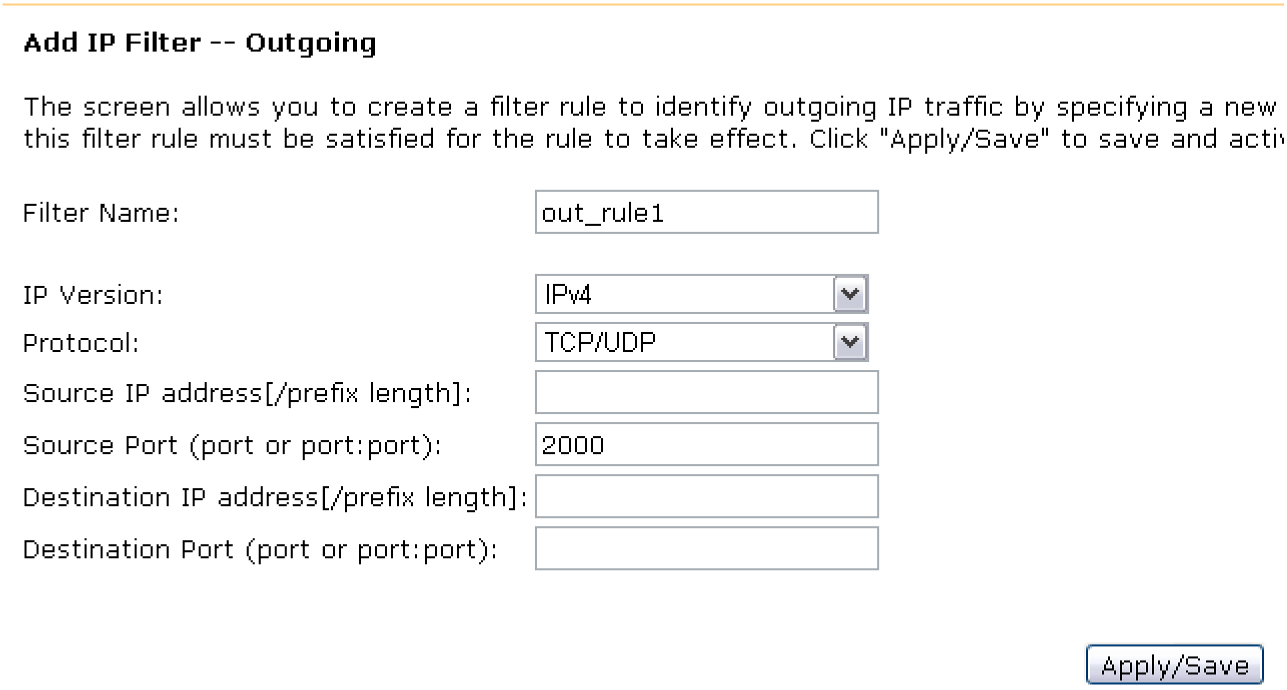
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

Create a rule like this：Do not allow the LAN data outbound whose protocol is TCP/UDP and source port is 2000, the filter name is out_rule1, specific settings:

1. "Filter Name"：out_rule1；
2. "Protocol": choose "TCP/UDP";
3. "Source Port (port or port:port)"：2000。

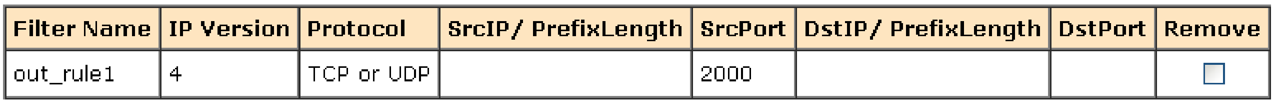


Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new this filter rule must be satisfied for the rule to take effect. Click "Apply/Save" to save and acti

Filter Name:	out_rule1
IP Version:	IPv4
Protocol:	TCP/UDP
Source IP address[/prefix length]:	
Source Port (port or port:port):	2000
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

2) After entering the required settings click the **Apply/Save** button;
3) If success, you will see the new added rule in the below figure：



Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
out_rule1	4	TCP or UDP		2000			□

4) If needs to delete the IP outbound filter rule, choose the radio buttons on the right, and then click the "Remove"

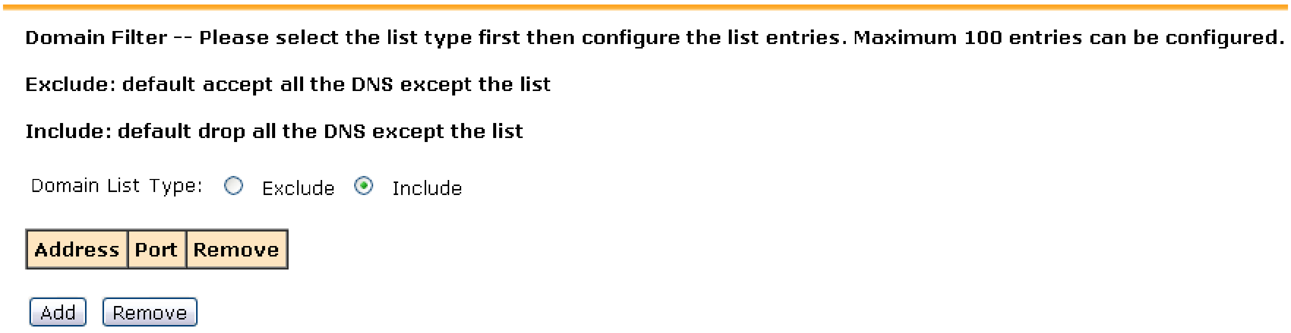
3.2.6.3. Domain Filters

The Domain filter can prevent all the LAN computers from accessing the specific WAN domain name; this feature will refuse all the requests to the specific domain name.

Please go to path:【Firewall】→【Domain Filter】page. Please select the list type first then configure the list entries.

List type:

- Exclude: accept all the DNS except the list;
- Include: drop all the DNS except the list;



Domain Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

Exclude: default accept all the DNS except the list

Include: default drop all the DNS except the list

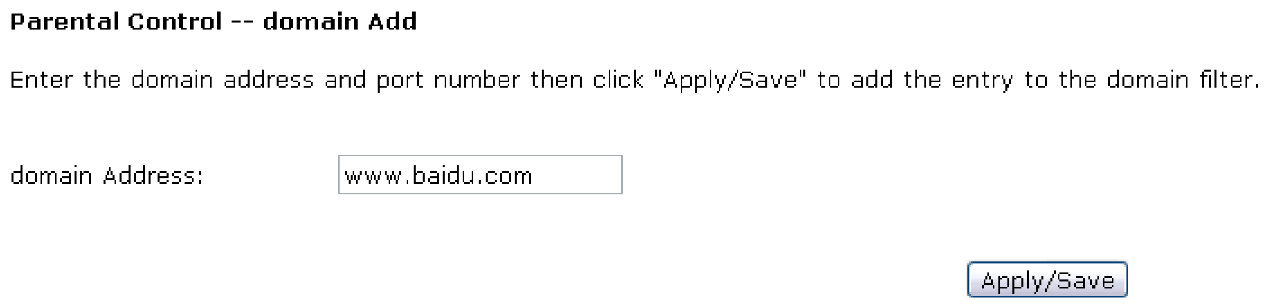
Domain List Type: ○ Exclude ● Include

Address	Port	Remove

For Example:

If you want to forbid the user to browse www.baidu.com, you can have the following settings:

1) Choose the Domain List Type: “Exclude”;
2) Click“add”button, enter the domain filter rule adding page, input the domain address: www.baidu.com。

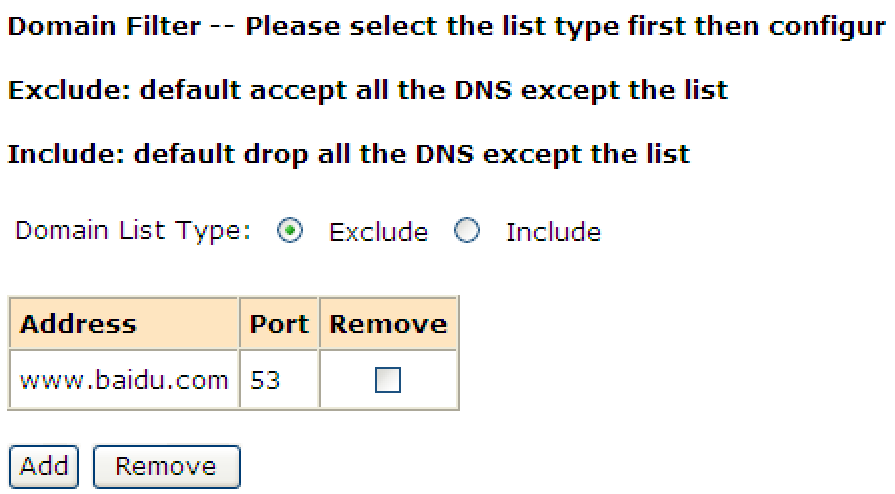


Parental Control -- domain Add

Enter the domain address and port number then click "Apply/Save" to add the entry to the domain filter.

domain Address: www.baidu.com

3) After entering the required settings click the **Apply/Save** button, you will see the defined filter rule in the following figure.



Domain Filter -- Please select the list type first then configur

Exclude: default accept all the DNS except the list

Include: default drop all the DNS except the list

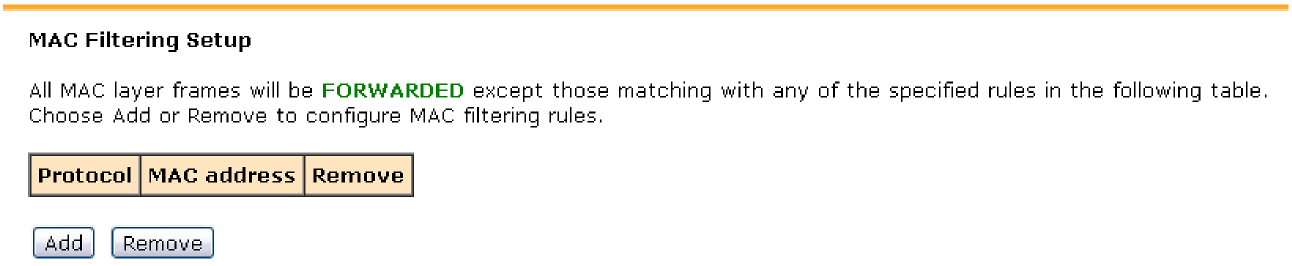
Domain List Type: ● Exclude ○ Include

Address	Port	Remove
www.baidu.com	53	□

Note: ALL the above settings will take effect after rebooting.

3.2.6.4. MAC Filters

Please go to path: 【Firewall】→【MAC Filter】to setup MAC filtering. All MAC layer frames will be forwarded except those matching with any of the specified rules in the settings.



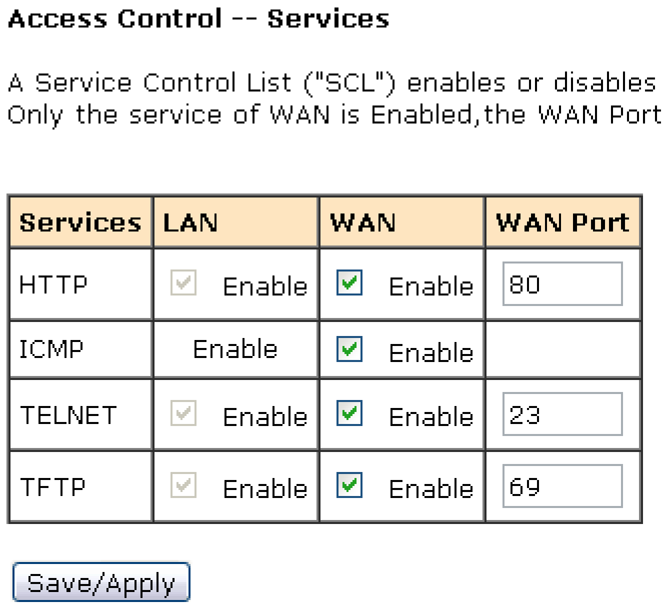
MAC Filtering Setup

All MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table.
Choose Add or Remove to configure MAC filtering rules.

Protocol	MAC address	Remove

3.2.6.5. Access Control(Remote Access)

Go to path:【Firewall】→【Access Control】, enter the access control page, you can enable or disable all kinds of services.



Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.
Only the service of WAN is Enabled,the WAN Port can be configed effectively.

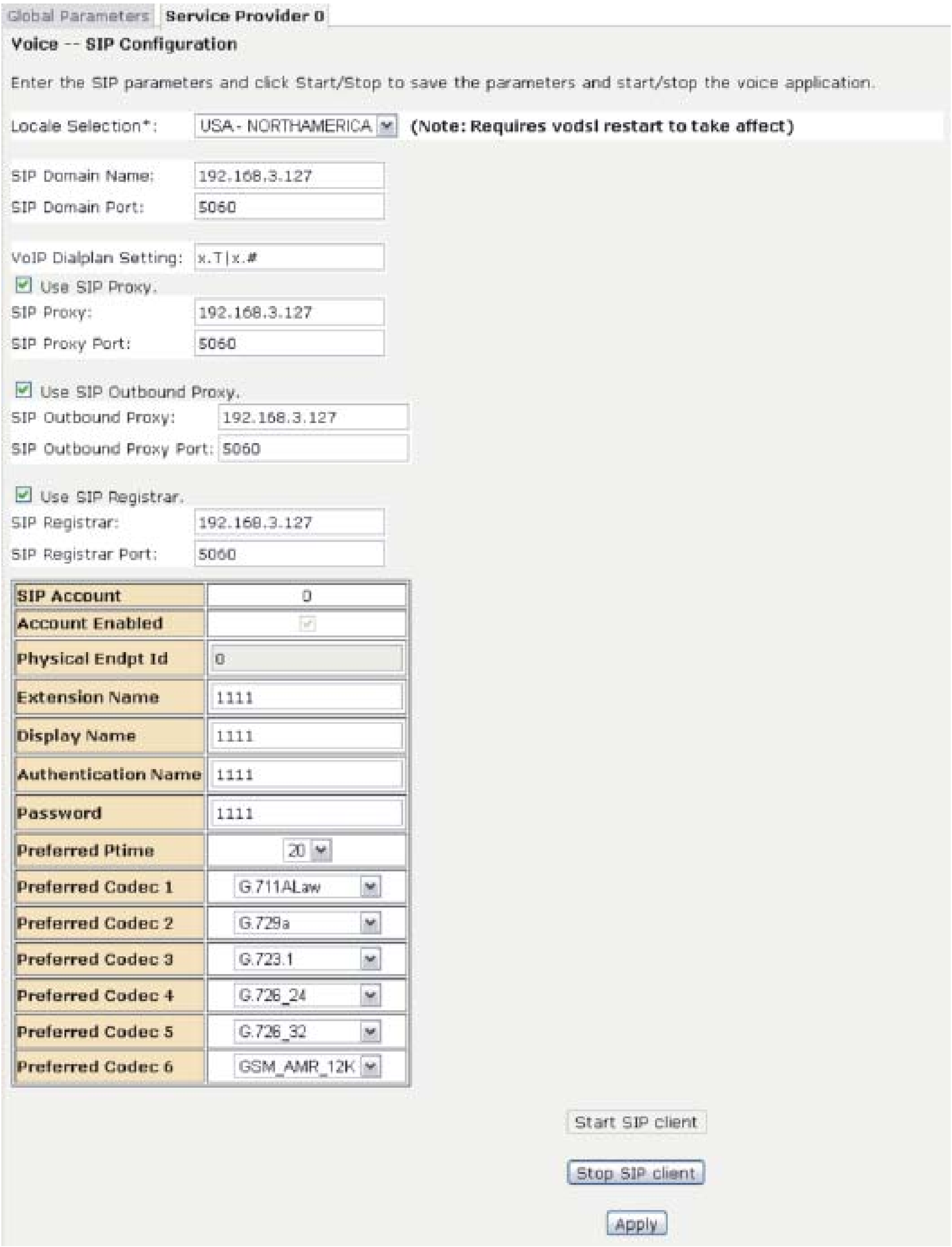
Services	LAN	WAN	WAN Port
HTTP	☑ Enable	☑ Enable	80
ICMP	Enable	☑ Enable	
TELNET	☑ Enable	☑ Enable	23
TFTP	☑ Enable	☑ Enable	69

3.2.7 Voice (VoIP)

3.2.7.1. VoIP Basic Settings

Note: Before using VOIP function, you should setup a WAN connection supporting VoIP function.

1) Go to path:【VOIP】→【Basic Settings】, enter the basic voip configuration page.
2) Input the relevant VoIP information in this page;
3) And then click "Start SIP Client";



Voice -- SIP Configuration

Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.

Locale Selection*: USA - NORTHAMERICA **(Note: Requires vodsl restart to take affect)**

SIP Domain Name: 192.168.3.127

SIP Domain Port: 5060

VoIP Dialplan Setting: x.T|x.#

☑ Use SIP Proxy.

SIP Proxy: 192.168.3.127

SIP Proxy Port: 5060

☑ Use SIP Outbound Proxy.

SIP Outbound Proxy: 192.168.3.127

SIP Outbound Proxy Port: 5060

☑ Use SIP Registrar.

SIP Registrar: 192.168.3.127

SIP Registrar Port: 5060

SIP Account	0
Account Enabled	☑
Physical Endpt Id	0
Extension Name	1111
Display Name	1111
Authentication Name	1111
Password	1111
Preferred Ptime	20
Preferred Codec 1	G.711ALaw
Preferred Codec 2	G.729a
Preferred Codec 3	G.723.1
Preferred Codec 4	G.726_24
Preferred Codec 5	G.726_32
Preferred Codec 6	GSM_AMR_12K

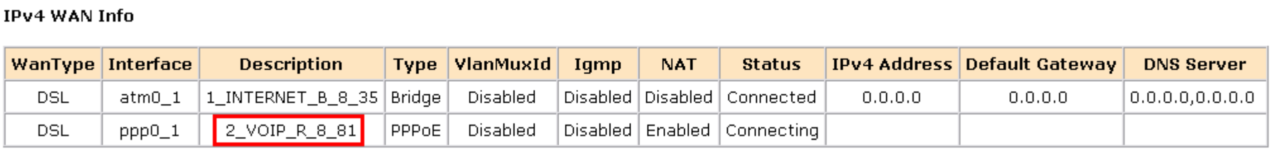
For Example

If a VoIP user wants to register to the VoIP voice sip server. Related information below

- VoIP SIP server：IP:192.168.3.127, port:5060
- VoIP user account：name/password:1111
- HG-A800 can register to the Voip SIP server through PPPoE;

Steps：

1) Setup a new PPPoE WAN connection, and the service mode is VOIP_INTERNET;
2) After establishing the connection, go to the path:【Status】→【Statistics】, to view the status of this WAN connection：

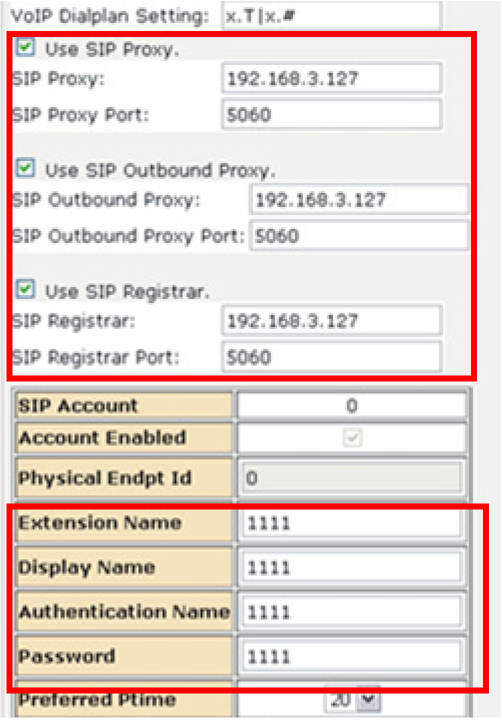


IPv4 WAN Info

WanType	Interface	Description	Type	VlanMuxId	Igmp	NAT	Status	IPv4 Address	Default Gateway	DNS Server
DSL	atm0_1	1_INTERNET_B_8_35	Bridge	Disabled	Disabled	Disabled	Connected	0.0.0.0	0.0.0.0	0.0.0.0,0.0.0.0
DSL	ppp0_1	2_VOIP_R_8_81	PPPoE	Disabled	Disabled	Enabled	Connecting			

3) Go to the path:【VoIP】→【Basic Setting】→【Service Provider 0】,:

1. Click “Use SIP Proxy”, “Use SIP Outbound Proxy” and “Use SIP Registrar”, input VoIP SIP server：192.168.3.127, port：5060.
2. input VoIP user account：name/password:1111.



VoIP Dialplan Setting: x.T|x.#

☑ Use SIP Proxy.

SIP Proxy: 192.168.3.127

SIP Proxy Port: 5060

☑ Use SIP Outbound Proxy.

SIP Outbound Proxy: 192.168.3.127

SIP Outbound Proxy Port: 5060

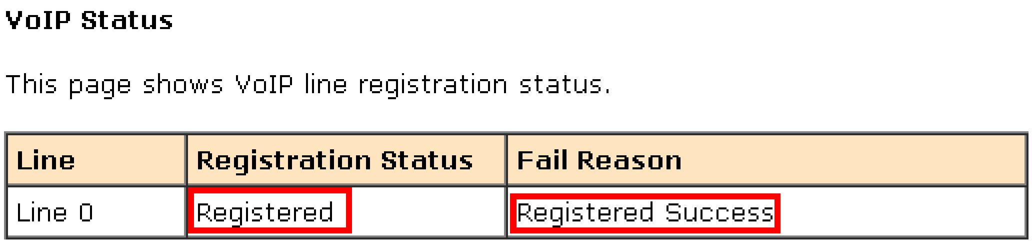
☑ Use SIP Registrar.

SIP Registrar: 192.168.3.127

SIP Registrar Port: 5060

SIP Account	0
Account Enabled	☑
Physical Endpt Id	0
Extension Name	1111
Display Name	1111
Authentication Name	1111
Password	1111
Preferred Ptime	20

4) After entering the required settings , click “Start SIP Client ”to activate the setting. GO to the Path: 【Status】→【VoIP Status】 to show the voip line registration status:



VoIP Status

This page shows VoIP line registration status.

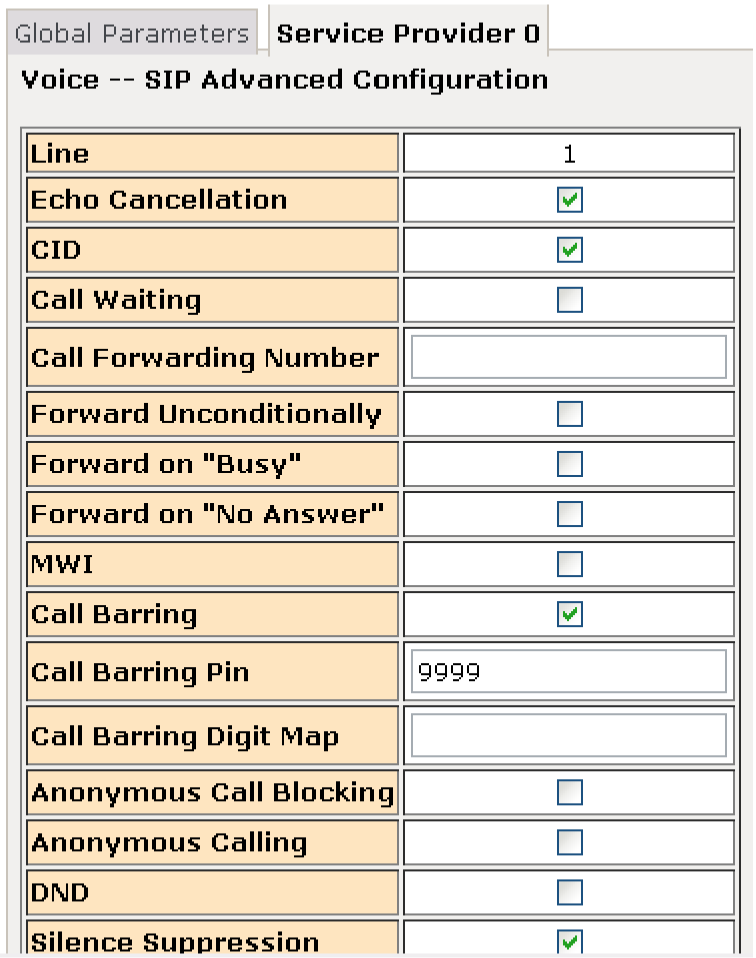
Line	Registration Status	Fail Reason
Line 0	Registered	Registered Success

3.2.7.2. VoIP Advanced Settings

1) Go to the path:【VOIP】→【Advanced Settings】, you can configure the voip advanced settings in this page, such as: Call Forwarding, Voice coding priority and T.38 support, etc.

2) Configure the settings according to the relevant voip information。

3) After entering the required settings , click“Start SIP Client”to activate the setting.



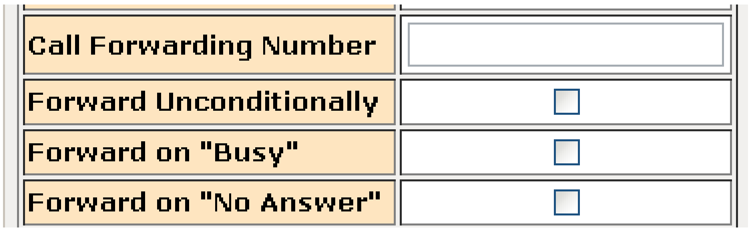
Global Parameters | Service Provider 0

Voice -- SIP Advanced Configuration

Line	1
Echo Cancellation	☑
CID	☑
Call Waiting	□
Call Forwarding Number	
Forward Unconditionally	□
Forward on "Busy"	□
Forward on "No Answer"	□
MWI	□
Call Barring	☑
Call Barring Pin	9999
Call Barring Digit Map	
Anonymous Call Blocking	□
Anonymous Calling	□
DND	□
Silence Suppression	☑

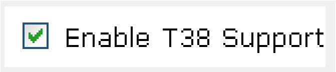
For Example

1) **Call Forwarding Number**: set a number to use call-forwarding. Select the conditions to use call forwarding by ticking the required boxes.



Call Forwarding Number	
Forward Unconditionally	□
Forward on "Busy"	□
Forward on "No Answer"	□

2) Enable T38 Support: enable the T.38 function



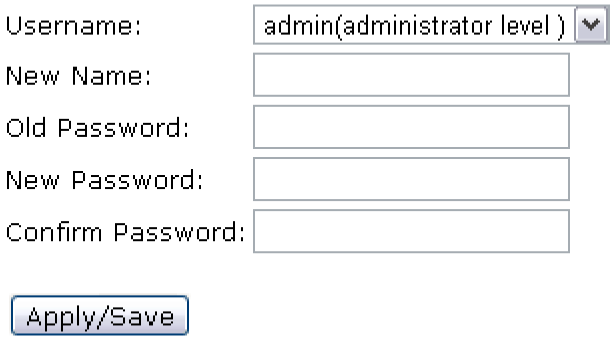
☑ Enable T38 Support

4) After entering the required settings , click "Start SIP Client" to activate the setting.

3.2.8 Tools

3.2.8.1. Account Settings (Users)

When you configure the CPE through an Internet browser, the system requires user name and password to validate access permission. The factory sets the default username of "admin" and the password of "admin". Go to path 【Tools】→【Account Settings】, you can choose the username and change the password.



Username: admin(administrator level)

New Name:

Old Password:

New Password:

Confirm Password:

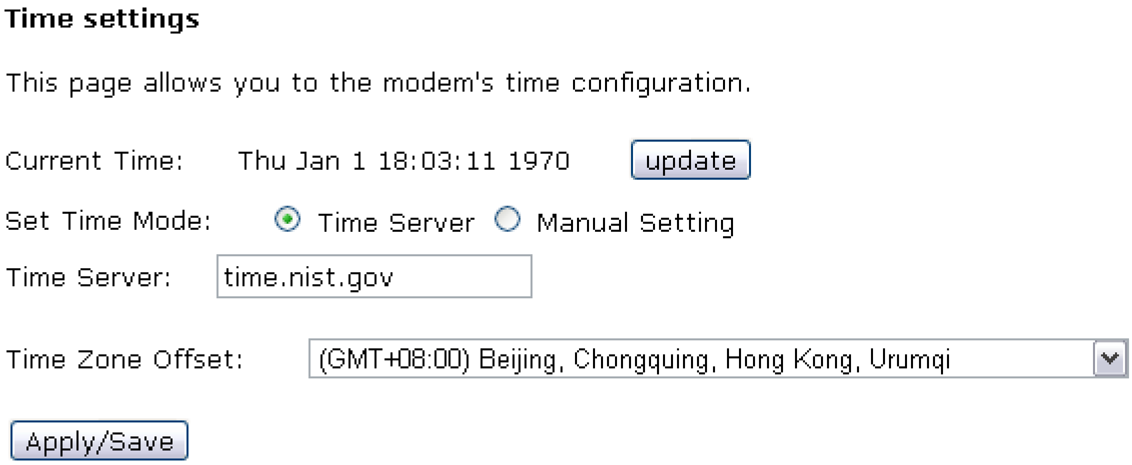
Attention: please remember the password after change, otherwise you will need to reset the device and will lose all configuration settings.

3.2.8.2. Time Settings

【Tools】→【Time Settings】

From this page the current time can be set manually or the CPE can be set to obtain the correct time from an internet time server.

Note: it is recommended that an internet time server is used when available – if the time is set manually it will be lost in the event of a power cut or if the unit is restarted.



Time settings

This page allows you to the modem's time configuration.

Current Time: Thu Jan 1 18:03:11 1970

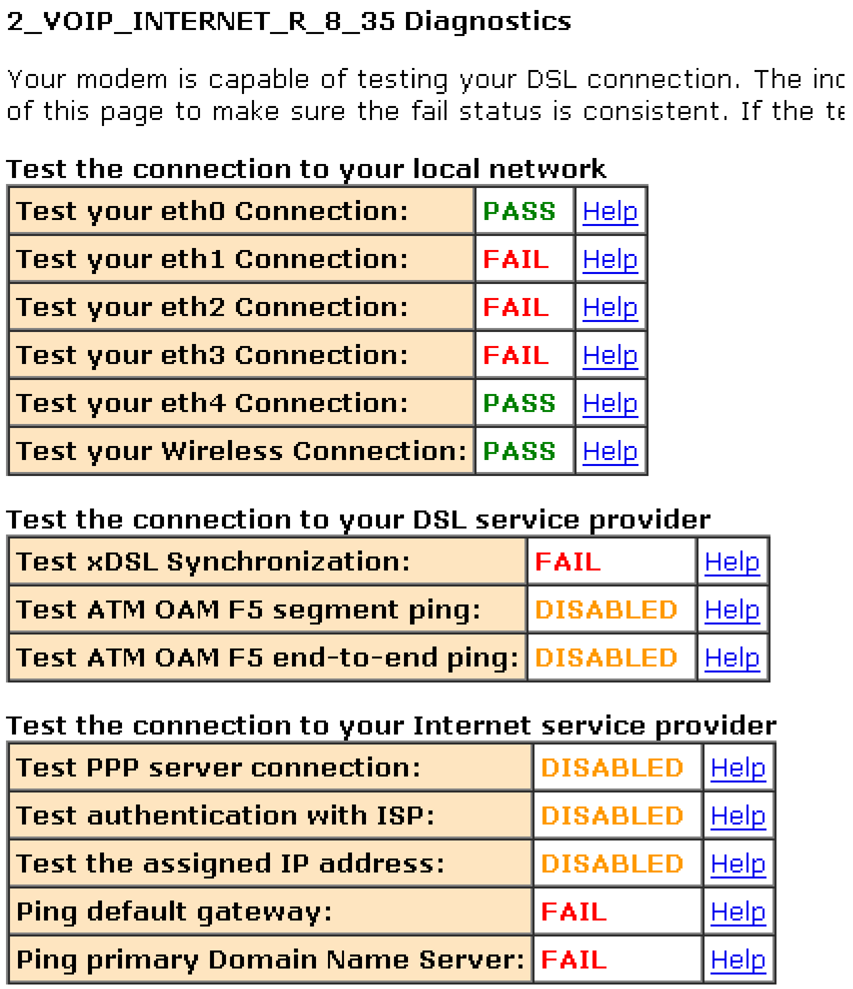
Set Time Mode: ● Time Server ○ Manual Setting

Time Server: time.nist.gov

Time Zone Offset: (GMT+08:00) Beijing, Chongquing, Hong Kong, Urumqi

3.2.8.3. Diagnostics

【Tools】→【Diagnostics】



2_VOIP_INTERNET_R_8_35 Diagnostics

Your modem is capable of testing your DSL connection. The inc
of this page to make sure the fail status is consistent. If the te

Test the connection to your local network

Test your eth0 Connection:	PASS	Help
Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	FAIL	Help
Test your eth4 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

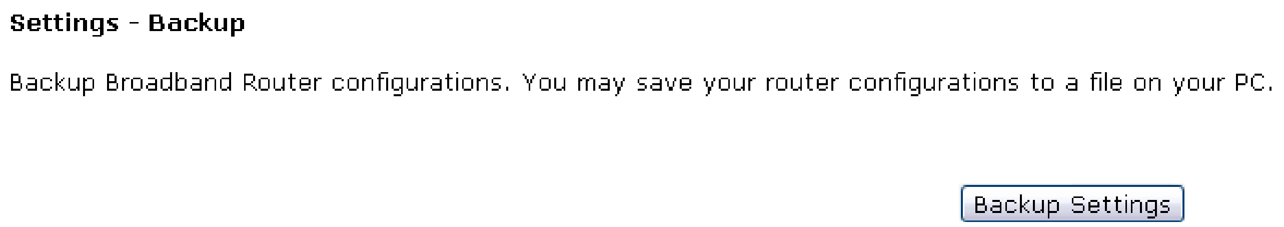
Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

3.2.8.4. Backup Settings

To backup the current configuration to a file:

Please go to path: 【Tools】→【Backup Settings】page. Click Backup Settings button, then a File download window will pop-up. Click **Save** button to download/save current configuration of the device to the PC.

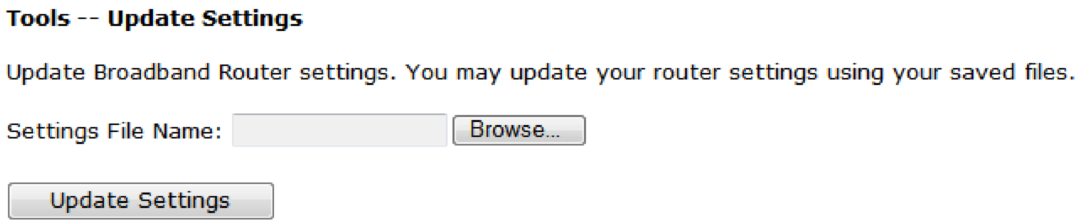


Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

3.2.8.5. Update (Restore) Settings

Please go to path: 【Tools】→【Update Settings】 page. Click **Browse** button to choose a configuration file, then click **Update Settings** to restore configuration.



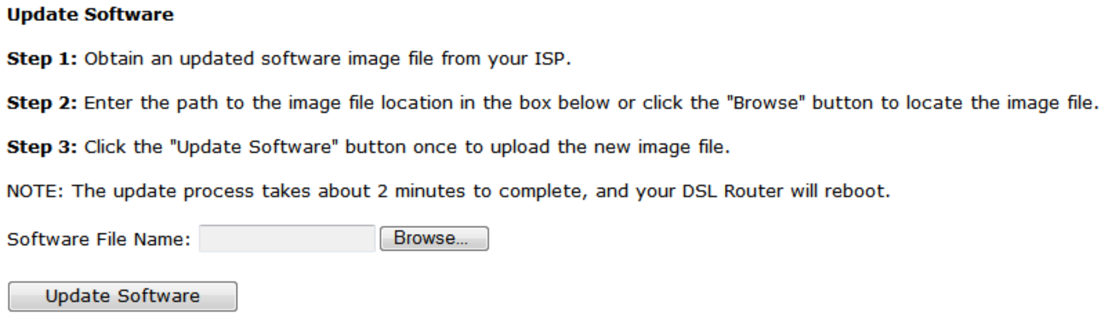
Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

3.2.8.6. Update Software

Please go to path: 【Tools】→【Update Software】 page. Click **Browse** to choose the right software. Then click **Update Software** to update.



Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

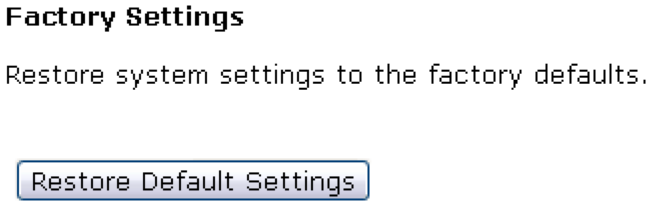
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

3.2.8.7. Factory Settings

To restore the CPE to the factory default configuration either press the **Reset** button on the side of the unit or go to path【Tools】→【Factory Settings】 and click the **Restore Default Settings** button.

Note: all user entered configuration options will be lost.

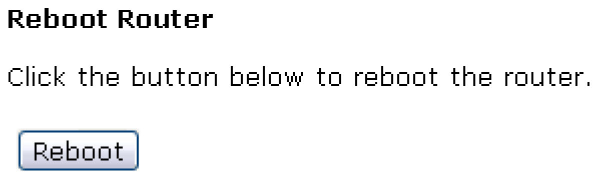


Factory Settings

Restore system settings to the factory defaults.

3.2.8.8. Reboot Router

To perform a soft restart of the CPE go to path【Tools】→【Reboot Router】 and click the **Reboot** button. A restart takes approximately 2 minutes.



Reboot Router

Click the button below to reboot the router.

Reboot

3.2.8.9. System Log

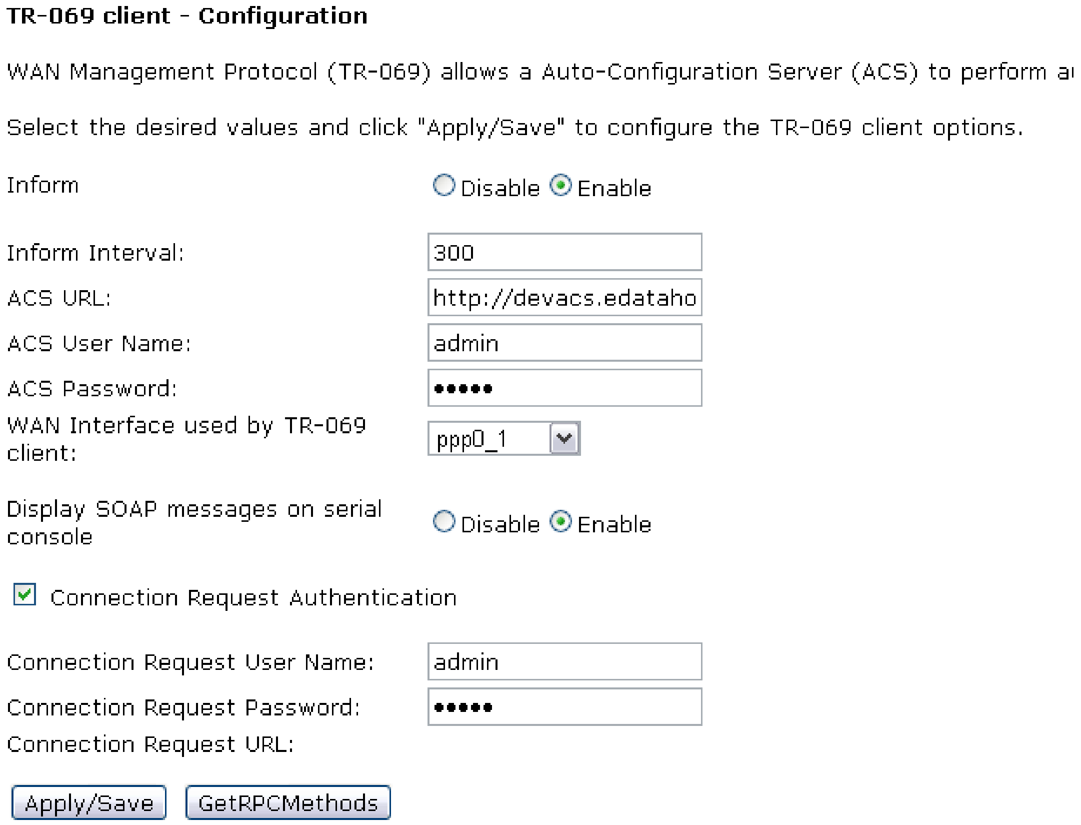
HG-A800 provides system log recording, you can inquire HG-A800 system event to understand what has happened. You can set up special log recording rules, record the system events, it is easy to know the device's operation and safety information.

3.2.8.10. TR-069 Client

The CPE can be provisioned remotely via the use of a TR-069 remote management server.

Please go to path: **【Tools】→【TR-069 Client】** page to setup an auto-configuration server to perform auto-configuration, provision, collection and diagnostics to this device. Select the desired values and click **Apply / Save** to configure the TR-069 client options.

Note: all the parameters in the screenshot should be matched with the TR-069 Server.



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform a

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	○ Disable ● Enable
Inform Interval:	300
ACS URL:	http://devacs.edataho
ACS User Name:	admin
ACS Password:	●●●●●
WAN Interface used by TR-069 client:	ppp0_1
Display SOAP messages on serial console	○ Disable ● Enable

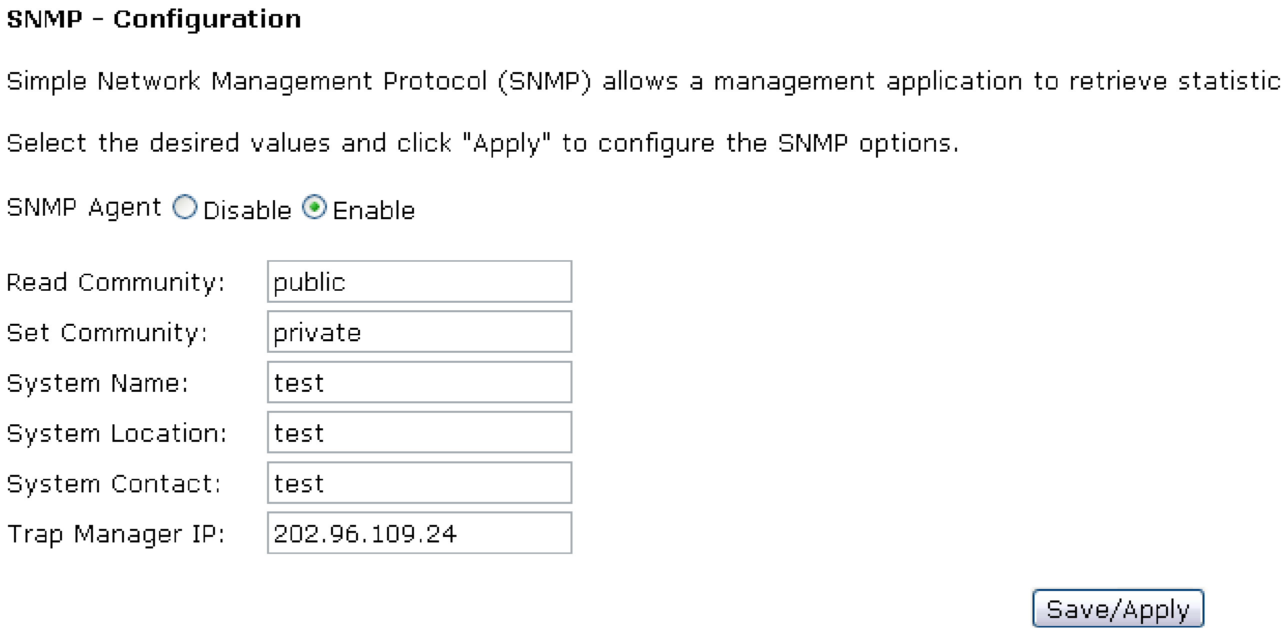
☑ Connection Request Authentication

Connection Request User Name:	admin
Connection Request Password:	●●●●●
Connection Request URL:	

Apply/Save GetRPCMethods

3.2.8.11. SNMP

Please go to path:【Tools】→【SNMP】 page to have the SNMP configuration, so that the SNMP server can have HG-A800 configuration management through the SNMP protocol.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistic

Select the desired values and click "Apply" to configure the SNMP options.

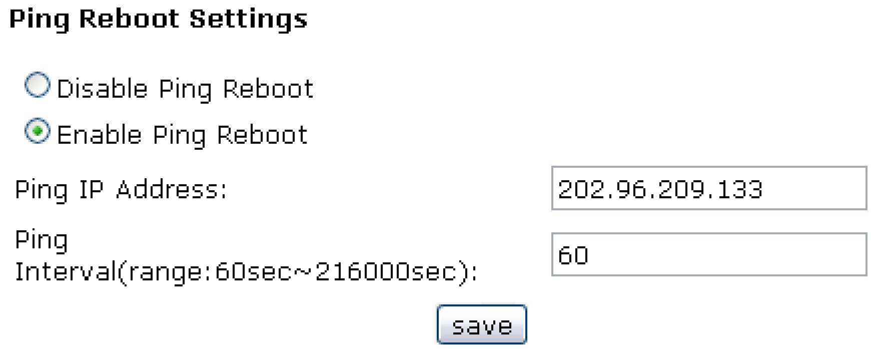
SNMP Agent ○ Disable ● Enable

Read Community:	public
Set Community:	private
System Name:	test
System Location:	test
System Contact:	test
Trap Manager IP:	202.96.109.24

3.2.8.12. PING Reboot

The “Ping Reboot” feature can be used to monitor the status of the internet connection and to automatically restart the CPE when the internet connection is unavailable.

【Tools】→【Ping Reboot 】



Ping Reboot Settings

○ Disable Ping Reboot
● Enable Ping Reboot

Ping IP Address:	202.96.209.133
Ping Interval(range:60sec~216000sec):	60

4. Troubleshooting

4.1 Unable to Access Internet

4.1.1 Check the Line and the Device

1. Check the power supply indicator is on - if not, make sure the connection of power supply is correct; Make sure the output of power supply is correct; Make sure the switch of the power supply is turned on；
2. Check the LAN indicator for the PC is on - if not, check the cable connection between the PC and the HG-A800; Make sure that the correct cable is used;
3. Check the DSL LED to see if it is flashing. If no fast flashing is observed within 3 minutes, please check whether phone line has been correctly placed; whether ADSL filter is correctly used. If multiple extensions have been installed, make sure that the filter is installed prior to the junction box of the phone line. If the above items are confirmed and still no fast flashing of DSL LED is observed, call the ISP to query whether ADSL service has been provided on your line;
4. Check the DSL LED to see whether it is unable to change status from fast flashing to always on, or whether it changes status to fast flashing after some time of being always on. If these phenomena occur constantly, please contact your ISP with a request to check lines and signal quality;

If there is no problem in the above items, the line and the device shall be working. Problems may come from your computer configuration or device configuration.

4.1.2 Check Your Configuration

We explain here the configuration of PPPOE using Windows XP operation system as an example. For other operation systems the process is similar.

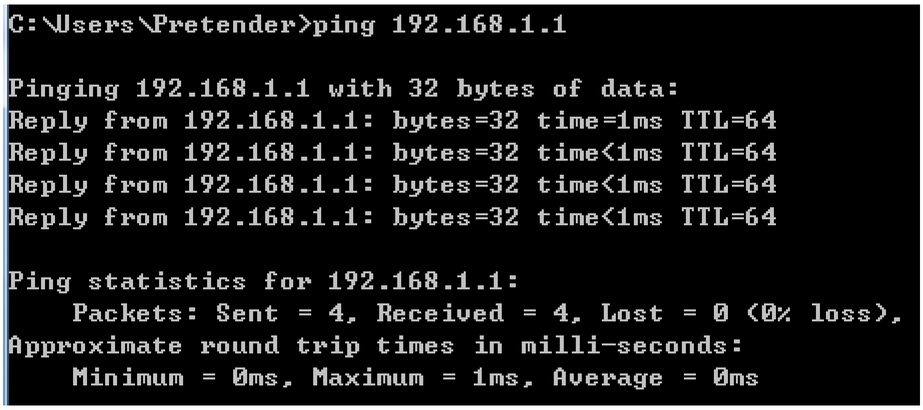
1. Enter the device manager to check if Ethernet adapter is correctly installed. If any problem exists, please re-install it;
2. Check the configuration of Ethernet adapter in PC. Try to manually set IP address that is in band 192.168.1.X without conflict.
3. Try to run command “ping 192.168.1.1” in a command prompt (Start, Programs, Accessories, Command Prompt). If the response returns “time out”, please check Ethernet connection and IP settings;
4. If the HG-A800 is reachable, try to ping a known internet IP, e.g. a DNS server: “ping 208.67.222.222”.

- If ping is reachable, there are no problems in the HG-A800. Please go to step 5;
- If ping is not reachable, see step 6 and check if the configuration is correct.

5. Please try to ping a internet URL, e.g. “ping www.google.com”.

- If ping is reachable, there are problems in the network settings. Please check the settings of the PC terminal, e.g. whether the security level is too high, or whether anti-virus or firewall is installed;
- If ping is not reachable, check the DNS setting of Ethernet adapter.

Note 1：The precondition is that LAN settings in the HG-A800 have not been modified.
Note 2：To start a Command Prompt in Windows click on the Start menu, Programs, Accessories, Command Prompt
Note 3：The returned values of ping command in the following format show the standard of “reachable”



```
C:\Users\Pretender>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. If ping of the modem is reachable but ping of the internet fixed IP is unreachable, attention should be concentrated upon device settings. Please enter the web interface following the instructions in this manual.

（1） Check first the number of connections. If more than one connection exists, for troubleshooting, delete unused connections and leave the one connection you are using.

（2） Check the connection to see whether correct “type” is selected. It’s normal to choose login type of PPPoE. When you use PPPoE to login, the following information should be provided: VPI and VCI, which can be queried from your ISP, user name and password.

（3） Then make sure that “using NAT” and “default gateway” have been selected with a tick. Check whether “connect on demand” has been selected with a tick. If it is selected, the connection is activated only when traffic to the internet arrives. If not selected, check “keep connection”, which should be set to 0 if you demand to keep connection

Make sure that the above parameters are saved after configuration.

FCC WARNING

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.