Free Communication, Wonderful Life

Thank you for purchasing EchoLife HG520 Home Gateway of Huawei.

EchoLife HG520 Home Gateway

User Manual

Manual Version: T1-20060310-V1.10

Product Version: V100R001

Trademarks

, HUAWEI, EchoLife are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

Note:

The HG520 is used indoors only. Pay attention to the following when installing and using the HG520.

⚠ Basic requirements

- Read this manual carefully before installing and using the equipment.
- Take waterproof measures during storage, transportation and operation of the equipment.
- Avoid collision during storage, transportation and operation of the equipment.
- Do not dismantle the equipment by yourself. In case of failure, send the equipment to an authorized maintainer.
- Without prior written consent from Huawei, no company or individual is allowed to decompile, disassemble, modify or reverse engineer the equipment and shall be solely responsible for any effect resulted from such action.
- While using the equipment, observe related laws and regulations, and respect the legal rights of others.

⚠ Environmental Requirements

- Place the equipment in a well-ventilated place. Avoid direct irradiation of any strong light (such as sunlight).
- Keep the equipment clean.
- Place the equipment on a flat and stable platform which is beyond the reach of children.

- Do not put heavy objects on the equipment.
- Leave at least 10 cm space around the equipment for heat dissipation.
- Do not put the equipment on any object that is flammable or not transcalent, such as foam and rubber.
- Do not cover the equipment with any object or block the ventilation holes of the equipment.
- Keep the equipment away from any heat source or exposed fire, such as an electronic warmer and a candle.
- Keep the equipment away from appliances with a strong electric field or magnetic field, such as a microwave oven and a refrigerator.
- Keep the equipment away from moisture or containers with liquid, such as a vase and a cup.

⚠ Usage

- Do not allow children to use the equipment alone.
- Do not allow children to touch or play with the small fittings, to avoid danger of deglutition.
- Use the power adapter provided with the equipment only.
- Use the accessories approved by the manufacturer.
- The power supply shall meet the equipment specifications.
- Before plugging or unplugging the cables, turn off the equipment and unplug the power supply.
- While plugging or unplugging the cables, keep your hands dry and do not touch the metallic part of a cable.
- Do not trample on, stretch, or over bend the equipment cables, to avoid equipment failure.

- Do not use broken or worn wires. If a wire is broken or worn, contact your supplier for change.
- In a lightning storm, turn off the equipment and unplug the power supply, to avoid lightning strike.
- Unplug the power supply if the equipment is not used for a long time.
- In case of exceptions, turn off the equipment and unplug the power supply immediately. Then contact your supplier for maintenance. For example, the equipment emits smoke, peculiar smell or exceptional sounds.

⚠ Cleaning

- Before cleaning the equipment, turn off the equipment and unplug the power supply.
- Clean the equipment shell with a piece of soft cloth.
- It is forbidden to spray liquid onto the equipment, to avoid damage to the internal circuit.
- Keep the power socket clean and dry, to avoid electric shock or other dangers.

Note:

If the device is in use for a long time, temperature of the shell will go up. Please don't worry. This is no exception and the device can work normally.

About This Manual

This manual introduces function, features and operations of EchoLife HG520. The main contents are as follows:

To know	Refer to
Features, network application and hardware structure	**Chapter 1 Introduction**
Installation	**Chapter 2 Installation**
Basic configuration	**Chapter 3 Configuration Preparation**
Detail configuration introduction	**Chapter 4 Configuring HG520**
Introduce HG520's WAN connection mode	**Chapter 5 Connection Mode**
Describe frequently encountered problems and solutions	**Chapter 6 Troubleshooting**
Technical specifications	**Chapter 7 Technical Specifications**
Technical terms and abbreviations	**Chapter 6 Acronyms and Abbreviations**

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Table of Contents

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

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.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Chapter 1 Introduction

EchoLife HG520 Home Gateway (thereinafter referred to as HG520) is a kind of home gateway design for family and SOHO users. It provides high-speed ADSL and ADSL2+ interfaces for external broadband WAN access. It also provides WLAN, Ethernet and USB Client interfaces for internal connection with different family service terminals such as PC, STB, IAD and EPHONE.

HG520 has powerful routing and bridging functions. It supports the advanced NAT/Firewall technique, UpnP, flexible network configuration and the QoS strategy. With other network equipment, it provides end-to-end quality assurance. It extends the high-speed and high quality broadband services to service terminals inside families. HG520 also supports data, communications and entertainment services

1.1 Functions

HG520 are designed with the following functions:

- Built-in ADSL modem for high-speed Internet access.
  Support Network Address Translation (NAT) and IP filtering.
  Support network sharing and firewall protection.
- Four Ethernet interfaces for Internet access through LAN.
- Support DHCP protocol.
- Support Web-based configuration and status view.
- Support remote/local upgrade through HTTP and TFTP.
- Support IEEE 802.11g 54Mbit/s and can be used as a wireless access point equipment.

1.2 Network Application

HG520 is located on the user access layer of the network. It enables small and medium enterprises and family users to access an IP network through the ADSL uplink port.

HG520 provides both wired and wireless access. Figure 1-1 shows the network topology of HG520.

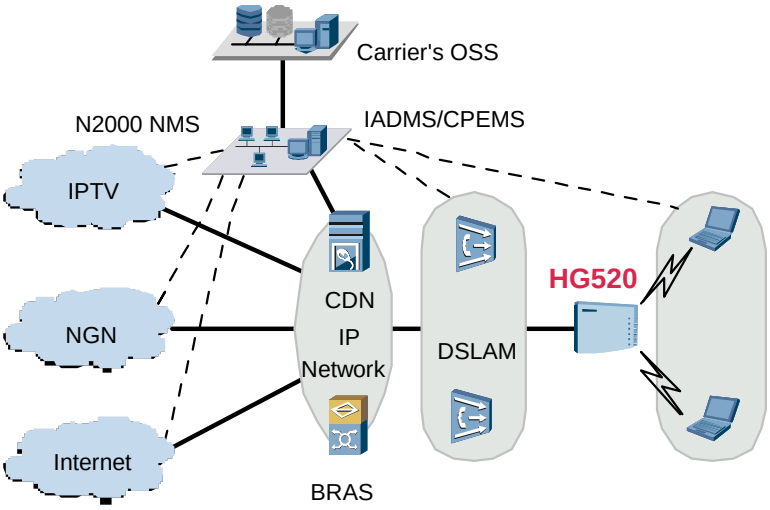


Figure 1-1 Network Topology of HG520

1.3 Appearance

Figure 1-2 shows the appearance of HG520.

1.1.1 Front Panel

Figure 1-3 shows the front panel of HG520.

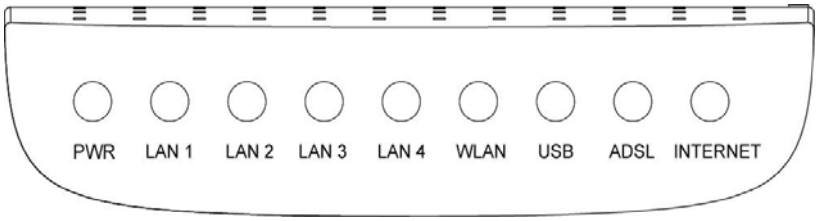


Figure 1-3 Front panel of HG520

Table 1-1 describes the different LED behaviors on the front panel of HG520.

Table 1-1 Description of indicators

Indicator	Color	Status	Function
PWR	Green	On	Power is switched on.
		Off	Power is switched off.
LAN1-4	Green	On	LAN connection is established.
		Off	LAN connection is not established.
		Blinking	LAN data is being transmitted.
WLAN	Green	On	WALN connection is established.
		Off	No WLAN connection is established.
		Blinking	The WLAN data is being transmitted.
USB	Green	On	USB connection is established.
		Off	USB connection is not established.
		Blinking	USB data is being transmitted.
ADSL	Green	On	ADSL link is established.
		Off	ADSL connection is not established.
		Blinking	The ADSL link is in the activation process.
INTERNET	Green	On	Internet connection is established.
		Off	Internet connection is not established.
		Blinking	Data is being transmitted.

1.3.2 Rear Panel

Figure 1-4 shows the rear panel of HG520.

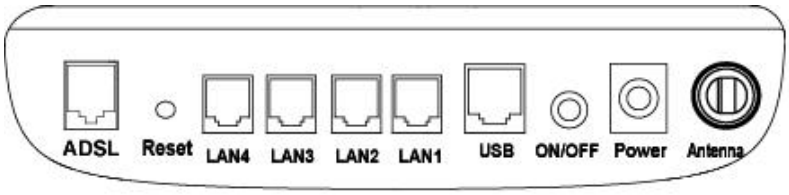


Figure 1-4 Rear panel of HG520

For the description of external interfaces, see Table 1-2.

Table 1-2 Description of external interfaces

Port	Function
ADSL	RJ-11 port for connection with the telephone jack or a splitter via a telephone line.
Reset	Restore the default settings
LAN1-4	RJ-45 port for connection with the Ethernet port of a computer or a LAN hub.
USB	USB port for connection with other device via a USB cable.
ON/OFF	Switch on/off HG520
Power	Connect to the power adapter
Antenna	Antenna for wireless Internet connection

Chapter 2 Installation

2.1 Connecting Cables

Place HG520 in a safe and accessible location where you can easily view the LED indicators on the front panel of the device.

HG520 should be connected to a phone port, a power socket, and a computer or the network before it functions.

⚠ **Caution:**

If you need to install a telephone between HG520 and the wall socket, make sure you install a splitter first to prevent loss in voice quality.

You are now ready to connect HG520. Follow these steps:

I. Disconnect the power – Make sure you turn off the power for the computer and HG520.

II. Connect the ADSL cable

Use a telephone cable to connect the DSL interface of HG520 to either of the following interfaces:

- Wall socket: Plug one end of the twisted-pair cable (standard phone line) into the ADSL port on the rear panel of HG520 and insert the other end into the wall socket.
- External splitter: Or you can insert one end of the twisted-pair ADSL cable into the modem connector on the external splitter.
- Insert the other end into the ADSL connector on the back panel of HG520.
- After installed, you can connect telephone to the phone connector on the external splitter.

III. Connect HG520 to your computer – Use an Ethernet cable provided to connect HG520 and your computer or notebook PC through the 10/100Base-TX Ethernet ports.

IV. Connect the power supply and start up HG520– Use the power adapter supplied and switch the power switch to the ON position. The Power LED indicator lights up and remain lit. Check and make sure the electronic current and voltage meet the requirement of the supplied power adapter. Check and make sure that the LAN: LINK and ADSL: LINK LED indicators light up in green. This indicates a successful connection between the ISP and the user's PC.

🕮 **Note:**

- Please note that the cable supplied is the straight-through cable. Be sure that the cable connected between LAN and HG520 does not exceed 100 meters.
- Use crossover cable to connect HG520 and the uplink port of a switch or hub.

2.2 Power on/off HG520

1) To power on HG520, plug the power adapter into the power jack, and press the power switch to the ON position.
2) Check the LEDs. Refer to 6.1 if any LED does not light up when powering on.
3) To power off, press the power switch to the OFF position, and then unplug the power adapter from the power jack.

2.3 Getting online

PPPoE dial-up users need to obtain an account with username and password provided by the ADSL ISP, and have the PPPoE dial-up application installed on the PC. User is able to start surfing the Internet by entering the username and password after executing the PPPoE dial-up application.

If other connection methods are used to access the Internet, users need to configure the HG520 in compliance with the actual situation before you can use the modem.

Note:

- The factory default IP is 192.168.1.1. Log onto the HG520 (both the default user name and password are “admin”) to check the Internet connection status. Please contact the ISP in case of any need for changing the modem’s configurations.
- Be sure the device has to be stored, transported, and operated in a non-humid and dust-free environment. Be careful not to drop down the device.

Chapter 3 Configuration Preparation

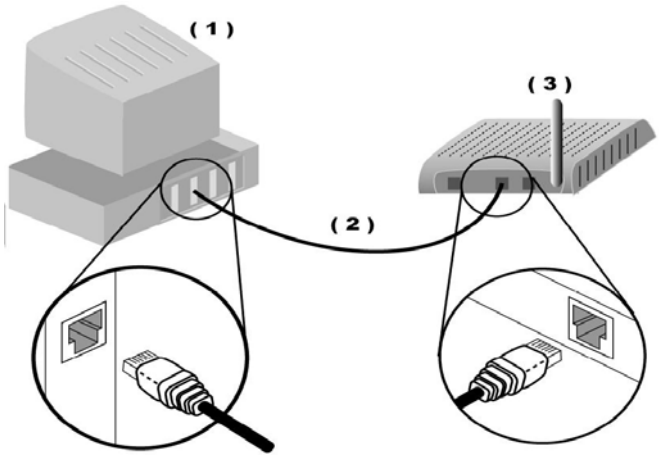
The default value of HG520 meets the need of most of the network environment. Beginners and the users with simple network environment are able to plug and play with no need to configure HG520.

However, if the network location of HG520 is within the network scope, and special requirements or modifications were done to the cooper wire loop quality/quantity, network protocol, network topology structures and other aspects. For instance, if you need to set a special value for the VPI/VCI, it is highly recommended that you configure the related settings for HG520 to adapt to the new network environment.

3.1 Build up a Configuration Environment

Before the configuration, ensure that you have made the following preparations:

4) Connect HG520 and your computer with the straight-through cable as shown in Figure 3-1.
5) Power on HG520 and start up the computer.
6) Configure the computer to obtain IP address automatically. Or you can configure the computer IP address to be in the same network segment as HG520. The default IP address of HG520 is192.168.1.1.



(1) computer (2) straight-through cable (3) HG520

Figure 3-1 Connecting HG520 and Computer

3.2 Configure IP Settings on PC

The factory default IP address for HG520 is 192.168.1.1. The subnet mask is 255.255.255.0. Before configuring HG520, you need to make sure that the IP address on your PC is set to be on the same network as HG520.

1. Enter the IP address (192.168.1.1 by default) of HG520 in the address bar of IE browser. The dialog box of Figure 3-2 will appear.
2. Enter the user name and password. Both of them are **admin** by default as shown in Figure 3-2.

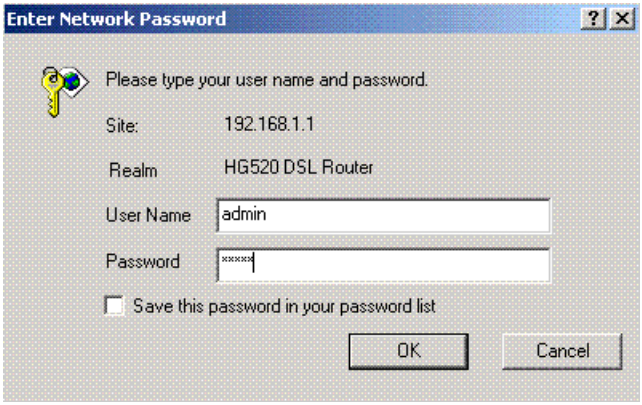
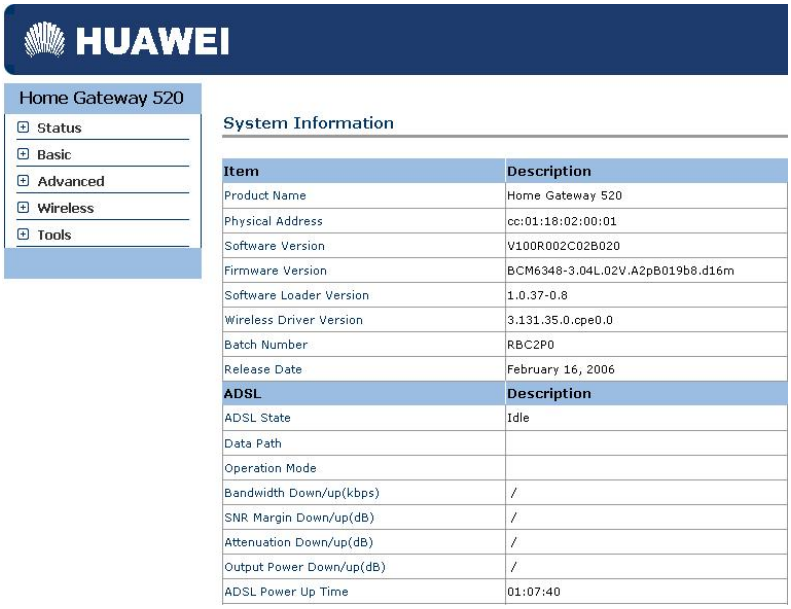


Figure 3-2 Authentication

3. Click **OK**.

After the authentication is completed, the browser will display the home page of HG520 as shown in Figure 3-3.



Item	Description
Product Name	Home Gateway 520
Physical Address	cc:01:18:02:00:01
Software Version	V100R002C02B020
Firmware Version	BCM6348-3.04L.02V.A2pB019b8.d16m
Software Loader Version	1.0.37-0.8
Wireless Driver Version	3.131.35.0.cpe0.0
Batch Number	RBC2P0
Release Date	February 16, 2006
ADSL	**Description**
ADSL State	Idle
Data Path	
Operation Mode	
Bandwidth Down/up(kbps)	/
SNR Margin Down/up(dB)	/
Attenuation Down/up(dB)	/
Output Power Down/up(dB)	/
ADSL Power Up Time	01:07:40

Figure 3-3 HG520 home page

The left side is the navigation tree of the operation interface. Click a hyperlink and the corresponding page will appear on the right. You can configure the services according to the prompts.

Note:

If you have problems during configuration, contact your Internet service provider for help.

Chapter 4 Configuring HG520

This chapter provides step-by-step guideline to configure the HG520.

4.1 Before You Start

After the log-in is completed, the Web configuration interface appears. The left side of the page is navigator items. Go to each page to configure by clicking the hyper link button. The right side of the page shows the actual configuration and system management page.

You may check the detail of traffic statistics, configure PVC parameters and security settings, together with upgrade firmware by clicking the either of the four buttons on the HG520 web page.

Whenever you made a configuration, remember to save the changes and reboot so to activate the changes.

4.2 System Information

HG520 provides you with the ADSL operation status and service information. To monitor the ADSL operation status you can click the **Status** link.

System Information

Item	Description
Product Name	Home Gateway 520
Physical Address	02:10:18:01:00:01
Software Version	V100R002C02B020
Firmware Version	BCM6348-3.04L.02V.A2pB019b8.d16m
Software Loader Version	1.0.37-4.3
Wireless Driver Version	3.131.35.0.cpe0.0
Batch Number	RBC2P0
Release Date	February 16, 2006
ADSL	**Description**
ADSL State	Idle
Data Path	
Operation Mode	
Bandwidth Down/up(kbps)	/
SNR Margin Down/up(dB)	/
Attenuation Down/up(dB)	/
Output Power Down/up(dB)	/
ADSL Power Up Time	01:05:59
ADSL Active Time	00:00:00
PPP Select	ppp_8_35_1

Figure 4-1 System Information

Table 4-1 System Status Description

Item	Description
Product Name	Shows the name and model type of the device
Physical Address	Show the MAC address of the device
Software Release	Show the software release version of the device
Firmware Version	Show the firmware release version of the device

Item	Description
Software Loader Version	Show the software loader version of the device
Wireless Driver Version	Show the wireless driver version of the device
Batch Number	Show the batch number of the released software version
Release Date	Show the release date of the software version
ADSL State	Show the ADSL status. It includes start to handshake, start to train and activated.
Data Path	Show the current data path, including Hi-speed and Interactive modes.
Operation Mode	Indicate standard ADSL connection mode, including Multimode, G.mdt. T1.413, and G.lite etc.
Bandwidth Down/Up (kbps)	Indicate the down/up bandwidth after it is activated.
SNR Margin Down/Up (dB)	Indicate the down/up SNR margin.
Attenuation Down/Up (dB)	Indicate the down/up attenuation.
Output Down/Up (dB)	Indicate the Down/Up output
ADSL Power Up Time	Show how long the ADSL has been powered up.
ADSL Active Time	Show how long the ADSL is activated.
PPP Select	Show the different options of PPP parameters.

4.2.2 Service Information

The second item under the System status is Service Information. You can view the information of IP address on the LAN port, subnet mask, MAC address, speed, duplex mode and status. It also shows

the PVC, VPI/VCI, IP address, subnet mask, gateway, routing mode and status on the WAN port.

Service Information

LAN Interface					
IP Address	Subnet	MAC Address	Speed	Mode	Status
192.168.1.1	255.255.255.0	02:10:18:01:00:01	100M	Full	✔

WAN Interface						
PVC	VPI/VCI	IP Address	Subnet	Gateway	Mode	Status
PVC-0	8/35	0.0.0.0	0.0.0.0	0.0.0.0	PPPoE	✖

Figure 4-2 Service Information

Parameter Definition

Parameter	Definition
IP address	It is the address of a website that the computer recognizes for connection. The default IP address for the LAN port is 192.168.1.1.
Subnet Mask	The subnet mask consists of network address and subnet mask. It is meant for confirming the subnet that certain IP address belongs to.
MAC address	It is the address for subnet of the Ethernet and is used for identifying different network devices.
Speed	Ethernet transmission speed.
Full/half duplex	In terms of network transmission, full duplex refers to receive and transmit packages simultaneously, while half duplex means only receive or transmit.
Status	Show the Ethernet status.
PVC/VPI/VCI	Show the PVC the device is using when transmitting packet to remote router.

Parameter	Definition
Gateway	A gateway is often associated with both a router, which directs the packets of data that arrive at the gateway, and a switch, which furnishes the path in and out of the gateway for a given packet.
Protocol	Show the protocol this device applies for connecting to the Internet.

4.2.3 Traffic Statistics

This page provides the statistics of ATM, LAN and DSL. It also includes the packet transmitted and received from LAN and WAN ports. Click **Renew** to update the statistics.

Traffic Statistics

ATM Statistics			
PVC	PVC-0	CRC error count	0
Tx Pkts count	0	Rx Pkts count	0
Tx Bytes count	0	Rx Bytes count	0
Tx Cells count	0	Rx Cells count	0
Tx Errs count	0	Rx Errs count	0
Tx Drops count	0	Rx Drops count	0
LAN Statistics			
Tx Pkts count	24	Rx Pkts count	25
Tx Bytes count	12915	Rx Bytes count	3260
Tx Errs count	0	Rx Errs count	0
Tx Drops count	0	Rx Drops count	0
USB Statistics			
Tx Pkts count	0	Rx Pkts count	0
Tx Bytes count	0	Rx Bytes count	0
Tx Errs count	0	Rx Errs count	0
Tx Drops count	0	Rx Drops count	0
Wireless Statistics			
Tx Pkts count	0	Rx Pkts count	0
Tx Bytes count	0	Rx Bytes count	0
Tx Errs count	0	Rx Errs count	0
Tx Drops count	0	Rx Drops count	0
DSL Statistics			
Tx CRC count	0	Rx CRC count	0
Tx FEC count	0	Rx FEC count	0
Tx HEC count	0	Rx HEC count	0

Clear Refresh

Figure 4-3 Traffic Statistics

Parameter Definitions

Parameter	Definition
ATM Statistics	Shows the packets amount transmitted and received via this interface. It also tells the bytes of each packet, cell counts, errors, and the number of packet that is dropped.
LAN Statistics	Shows the packets amount transmitted and received via this interface. It also tells the bytes of each packet, cell counts, errors, and the number of packet that is dropped.
USB Statistics	Shows the packets amount transmitted and received via this interface. It also tells the bytes of each packet, cell counts, errors and the number of packet that is dropped.
Wireless Statistics	Shows the packets amount transmitted and received via this interface. It also tells the bytes of each packet, cell counts, errors and the number of packet that is dropped.
DSL Statistics	Shows the packets amount transmitted and received via this interface. It also tells the bytes of each packet, cell counts, errors and the number of packet that is dropped.

4.3 Basic Configurations

4.3.1 ADSL Mode

You will see the ADSL Mode by clicking **ADSL Mode** from the Main menu. You can configure the ADSL mode here, though ADSL mode is generally configured as default parameters with no need of further configuration. However, if your ISP requests you to modify the default ADSL configuration, you may select the proper ADSL mode in this section. Single click **Submit** to complete the configurations.

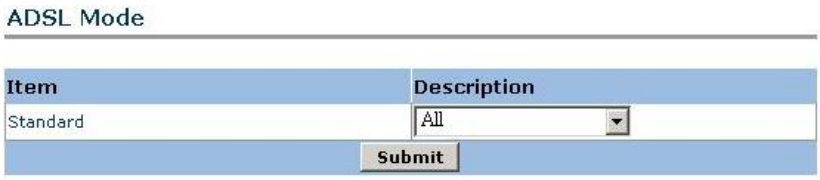


Figure 4-4 HG520 ADSL Mode

The table below explains the different options of ADSL mode shown in the drop-down menu.

Parameter	Definition
All	ADSL device monitors automatically for the most appropriate ADSL modes according to the network situation. They include G.dmt, G.lite, and T1.413.
G.dmt.bisplus	It consists of ADSL2+, ADSL2 and ADSL.
G.dmt.bisplus (AnnexM)	G.dmt.bisplus (AnnexM) consists of G.dmt,bisplus and Annex M.
G.dmt.bisplus (AnnexL)	G.dmt.bisplus (AnnexL) consists of G.dmt,bisplus and Annex L.
G.dmt.bis	G.dmt.bit consists of ADSL2 and Annex L modes.
Multimode	ADSL device monitors automatically for the most appropriate ADSL modes according to the network situation.
G.dmt	G.dmt mode (also called as G.992.1 standard) is created by the International Telecommunication Union, with downstream speed up to 8Mbit/s, and upstream speed up to 896kbit/s.
G.lite	G.Lite mode (also called as G.992.2) is approved by the International Telecommunication Union, with downstream speed up to 1.5Mbit/s.

Parameter	Definition
T1.413	T1.413 is approved by American National Standards Institution, with a speed up to 8Mbit/s.

4.3.2 WAN Setting

You can configure VPI/VC of the PVC on the WAN Settings page and select different connection mode. Click “New” to enter the page for setting up new PVC and selecting the connection mode. You can set up to eight PVC and the “New” button will be hidden to reject any new request when there are already 8 PVC on the WAN Settings.

Single click the pencil icon under the **Actions** to modify an existing PVC. Single click the trashcan icon under the **Actions** to delete an existing PVC. Click **Submit** to activate the settings after you finish the setting up. All the settings will be activated only after you reboot HG520.

WAN Settings

PVC	VPI/VCI	IP Address	Subnet	Mode	Encapsulation	Actions
PVC-0	1/39	0.0.0.0	0.0.0.0	Bridge	LLC	none
PVC-1	8/35	0.0.0.0	0.0.0.0	MER	LLC	
PVC-2	8/36	0.0.0.0	0.0.0.0	MER	LLC	

Note: Click 'New' to create a new entry, and you need to reboot to activate this configuration.

New Reboot

Figure 4-5 WAN Settings

There are 5 different connection modes under the WAN Settings:

I. PPPoA (PPP over ATM) and PPPoE

The configuration pages for these two modes are very similar, with the only difference of choosing PPPoA or PPPoE for connecting to the Internet.

When you are in the configuration page, enter the VPI/VCI parameters and select the connection mode and encapsulation mode to ensure your packet is transmitted in a more efficient rate. Single click “submit” button to complete the settings. Go the **Tool** > **Save & Reboot** to save the changes.

- The configuration page is shown as Figure 4-6 when the connection mode is PPP over ATM (PPPoA).
- The configuration page is shown as Figure 4-7 when the connection mode is PPP over Ethernet (PPPoE).

Generally speaking, the default connection and service modes will satisfy your demand. However, you can configure settings based on Internet Service Provider’s request if there is such need.

You are free to skip the blank items on the configuration and HG520 will use the factory default settings for operation. Take the “**Dial on demand, Inactivity Timeout**” feature as example, if you do not configure this item for the PCV under the PPPoA mode, the default time would be 0. And if you set up the “**Dial on demand, Inactivity Timeout**”, the PVC will interrupt the Internet connection when you are not using the Internet.

ATM PVC Configuration

Item	Description
PVC	PVC- 1
VPI/VCI	/
Mode	PPP over ATM (PPPoA)
Encapsulation	LLC
Service Category	UBR Without PCR
PPP Username	
PPP Password	
PPPoE Service Name	
Authentication Method	AUTO
☐ Dial on demand,Inactivity Timeout (minutes)	[1-4320]
☐ PPP IP extension	
☐ Use Static IP Address	
☐ enable dialling manually	
☑ Enable NAT	
☑ Enable Firewall	
☑ Enable IGMP Multicast	
☐ Enable 802.1q	
VLAN ID[0-4095]	
Submit	Cancel

Figure 4-6 ATM PVC Configuration under PPPoA Mode

ATM PVC Configuration

Item	Description
PVC	PVC- 1
VPI/VCI	/
Mode	PPP over Ethernet (PPPoE)
Encapsulation	LLC
Service Category	UBR Without PCR
PPP Username	
PPP Password	
PPPoE Service Name	
Authentication Method	AUTO
☐ Dial on demand,Inactivity Timeout (minutes)	[1-4320]
☐ PPP IP extension	
☐ Use Static IP Address	
☐ enable dialling manually	
☑ Enable NAT	
☑ Enable Firewall	
☑ Enable IGMP Multicast	
☐ Enable 802.1q	
VLAN ID[0-4095]	
Submit	Cancel

Figure 4-7 ATM PVC Configuration PPPoE Mode

II. MAC Encapsulation Routing (MER) Mode

It is recommended that you configure as being assigned an automatic IP address. If you want to manually configure to MER mode, please ask the WAN IP address, subnet mask, gateway address and DNS server address from your ISP.

You are free to skip the blank items on the configuration and HG520 will use the factory default settings for operation. Generally speaking, the default connection and service modes will satisfy your demand. However, you can configure settings based on Internet Service Provider's request if there is such need.

ATM PVC Configuration

Item	Description
PVC	PVC- 1
VPI/VCI	/
Mode	MAC Encapsulation Routing (MER)
Encapsulation	LLC
Service Category	UBR Without PCR
Obtain an IP address automatically	
Use the following IP address:	
WAN IP Address	
WAN Subnet Mask	
Obtain default gateway automatically	
Use the static IP Address	
Obtain DNS server automatically	
Use the following DNS server :	
Primary DNS server	192.168.2.7
Secondary DNS server	192.168.5.1
Enable NAT	
Enable Firewall	
Enable IGMP Multicast	
Enable 802.1q	
VLAN ID[0-4095]	
Submit	Cancel

Figure 4-8 ATM PVC Configuration – MER Mode

III. IPoA (Internet Protocols over ATM) Mode

It is recommended that you use the default DNS server and gateway, which means you do not need to make configuration. If you want to manually configure to IPoA mode, please ask the WAN IP address, subnet mask, gateway address and DNS server address from your ISP.

ATM PVC Configuration

Item	Description
PVC	PVC- 1
VPI/VCI	/
Mode	IP over ATM (IPoA)
Encapsulation	LLC
Service Category	UBR Without PCR
WAN IP Address	
WAN Subnet Mask	
☐ Use the static gateway	
☑ Use the following DNS server addresses:	
Primary DNS server	192.168.2.7
Secondary DNS server	192.168.5.1
☑ Enable NAT	
☑ Enable Firewall	
☑ Enable IGMP Multicast	
☐ Enable 802.1q	
VLAN ID[0-4095]	
Submit	Cancel

Figure 4-9 ATM PVC Configuration – IPoA Mode

IV. Bridging Mode

Please install PPPoE dial-up software if you use Bridging mode. If you select the static IP address, please ask the IP address of your computer, subnet mask, and DNS server address from your ISP.

ATM PVC Configuration

Item	Description
PVC	PVC- 1
VPI/VCI	/
Mode	Bridging
Encapsulation	LLC
Service Category	UBR Without PCR
Enable 802.1q	
VLAN ID[0-4095]	
Submit	Cancel

Figure 4-10 ATM PVC Configuration -- Bridging Mode

4.3.3 LAN Setting

It refers to the configurations on the LAN port, for which you can set up the IP address and subnet mask. Enter the proper IP address and subnet mask in the space as shown in Figure 4-11. Click **Submit** to activate the configuration. If you want to save the changes, go to **Tool**>**Save and Reboot** to make the changes permanent.

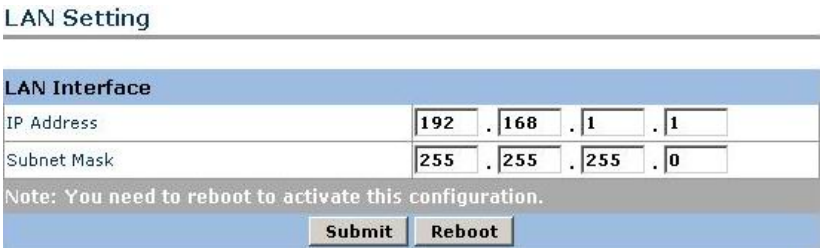


Figure 4-11 LAN Setting

4.3.4 DHCP Setting

DHCP is short for Dynamic Host Configuration Protocol. It is for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administration to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

1) DHCP Server

You can configure the DHCP server on the HG520 device for an efficient dynamic addressing.

On the DHCP Server Settings page, enter the Start IP address, the End IP address, and the lease time. Single click **Submit** button to complete the configuration. Lease time refers to the time frame that you are allowed to use the assigned IP address. You will have to file application for a new IP address once the lease time expires.

Click **Refresh** to renew the DHCP Server settings you just made.

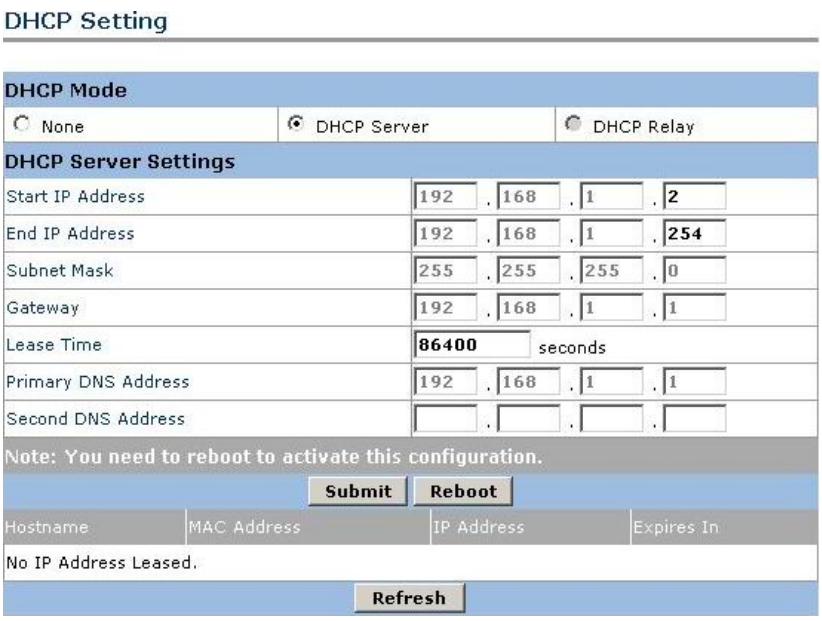


Figure 4-12 DHCP Sever Setting

2) DHCP Relay

DHCP relay is a relay agent for DHCP packets. It is used on a subnet with DHCP clients to "relay" their requests to a subnet that has a DHCP server on it. Because DHCP packets can be broadcast, they will not be routed off of the local subnet. The DHCP relay takes care of this for the client.

Enter the DHCP Server IP address and click “Submit” to activate the settings. This function does not work when the PVC setting of NAT feature is configured in the HG520.

Figure 4-13 DHCP Relay Setting

4.3.5 DNS Settings

DNS (Domain Name System) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.

Enter the DNS server IP address provided by the ISP on the DNS Settings page and single click **Submit** to complete the settings.

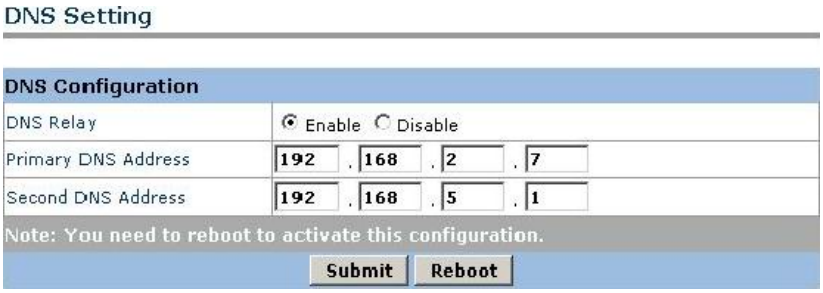


Figure 4-14 DNS Setting

4.3.6 NAT

NAT (Network Address Translation) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

There are three different setting options under the NAT:

- DMZ
- NAPT
- REDIRECT

DMZ (Demilitarized Zone) refers to an isolated area. It is a buffer area between the non-secure system and the secure system and it is for the purpose of solving the issue raised when a firewall is installed and the external networks are blocked to connect to the internal servers. This demilitarized zone lies between the corporate internal networks and external networks, in which certain servers, such as corporate Web servers, FTP servers and corporate bulletin are located. With the configuration of such DMZ feature, the internal networks are more securely protected.

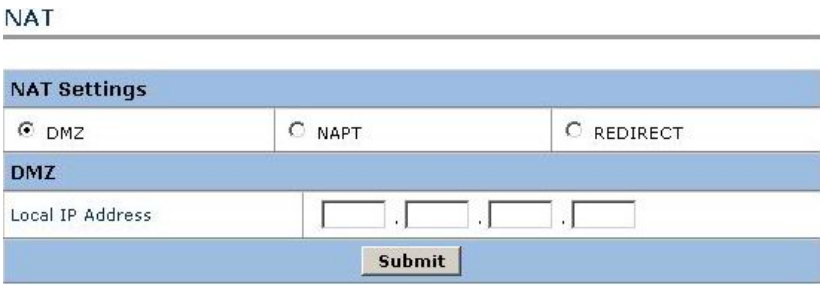


Figure 4-15 NAT — DMZ Setting

NAPT (Network Address and Port Translation) is an extension to basic NAT, in that many network addresses and their TCP/UDP ports are translated to a single network address and its TCP/UDP ports. Please be noted that this feature works only when the PVC with NAT feature is activated.

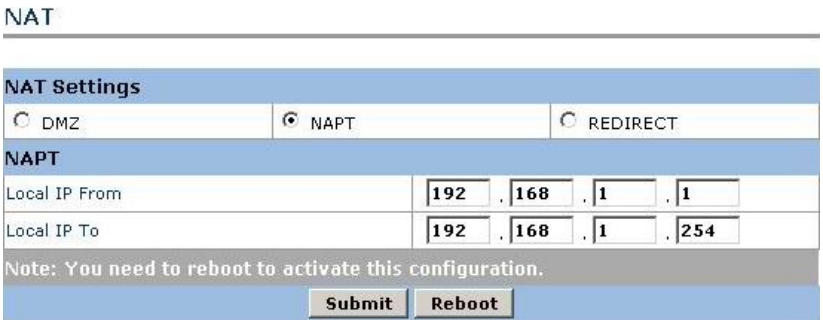


Figure 4-16 NAT- NAPT Settings

REDIRECT refers to redirect the packets. Servers redirect packets to the configured internal IP addresses and ports according to the IP addresses and TCP/UDP port range of which the packets are coming from. This feature only works when the PVC settings of NAT feature are configured.

Single click REDIRECT button as shown in Figure 4-17 and you will be prompted to the REDIRECT setting page as shown in Figure 4-18.

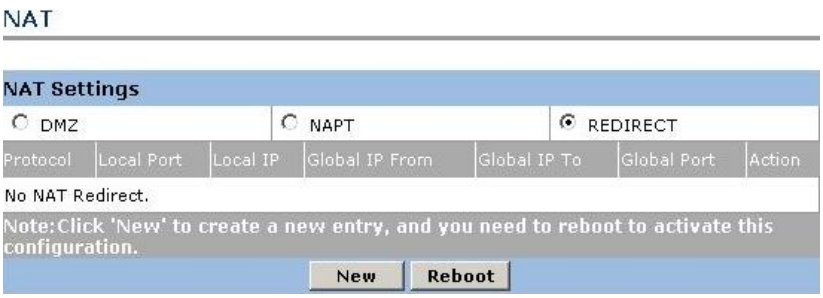


Figure 4-17 Advanced Setup — NAT — Multi NAT

Single click **New** to open a REDIRECT setup page as shown in Figure 4-18.

Here is the task you want to fulfill: the HTTP service is activated on the No.80 port of IP address of 192.168.1.2. User communicates with No.30 port of IP address of 10.132.41.116 via the Internet. When receiving such communication request, HG520 will redirect the request to the No.80 port of IP address of 192.168.1.2 and feedback to No.30 port of IP address of 10.132.41.116 that the request has been made.

And that's how you should configure such request: Set the local port number as 80, local IP as 192.168.1.2, Global Addresses From as 10.132.41.116, Global Addresses To as 10.132.41.126, and the Destination From/To port as 30-40. Single click **Submit** button to save the settings. You have to reboot the device to activate the settings.

NAT

NAT Settings	
Protocol	☑ TCP ☐ UDP
Local Port	80
Local IP	192 . 168 . 1 . 2
Global Address From	10 . 132 . 41 . 116
Global Address To	10 . 132 . 41 . 126
Destination From Port	30
Destination To Port	40
Submit	

Figure 4-18 NAT-REDIRECT Setting

4.3.7 IP Route Settings

IP Route settings include the setting of destination, netmask, next hop, IF name and route type. Single click **New** button on Figure 4-19 to create a new IP route.

Enter the settings and single click **Submit** to complete the settings.

IP Route

Destination	NetMask	Next Hop	IF Name	Route Type	Action
No Ip route.					
Note:Click 'new' to create a new entry.					
New					

Figure 4-19 IP Route Settings

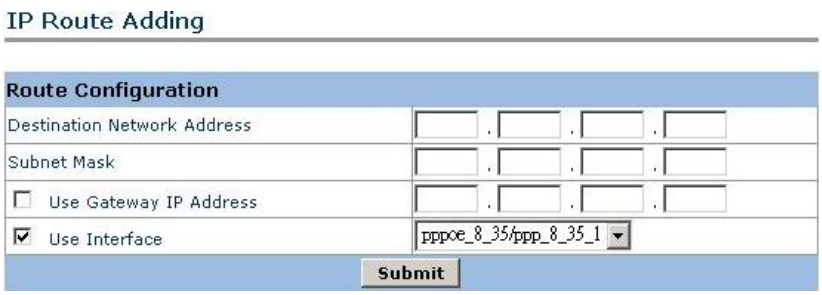


Figure 4-20 IP Route Adding

4.4 Advanced Settings

Advanced Settings allow you to configure SCL, RIP, ACL, SNTP, IP Filter, Multinat, parental control setting and blocked protocol.

4.4.1 SCL (Service Control List) Setting

This feature allows you to assign LAN port or WAN port as the interface when you visit the services (such as FTP, FTTP and ICMP, etc.).

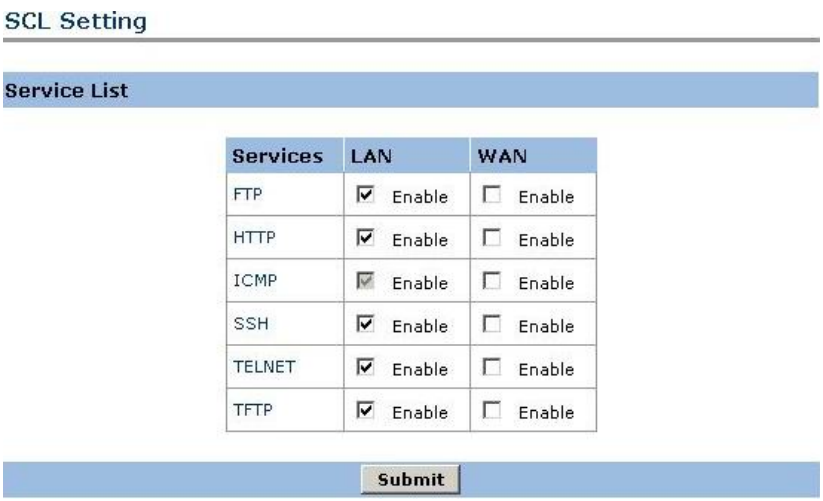


Figure 4-21 SCL Setting

4.4.2 RIP

RIP (Routing Information Protocol) is an Interior gateway protocol that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables.

RIP Setting

RIP Parameters	
RIP Status	Enabled Disabled
Age(seconds)	180
Update Time(seconds)	30

IF Name	Metric	Send Mode	Receive Mode	Enabled
br0	1	RIP2COMPAT	RIP2	
ppp_8_35_1	1	Not	Not	

Submit

Figure 4-22 RIP Setting

4.4.3 QoS Setting

QoS (Quality of Service) refers to that the network guarantees the expected bandwidth, delay, delay fluctuation (延遲抖動), and rate of packet loss are reachable during the Internet communication process.

QoS Setting

Class	MARK				TRAFFIC CLASSIFICATION RULES		
Traffic Class Name	Priority	IP Prec	IP TOS	WAN 802.1P	Lan Port	Description	Remove
dd	Low					Protocol: TCP/UDP VLan ID: 0 IP Prec: 0 TOS: Normal Service DSCP: 0	

Add Remove

Figure 4-23 QoS Setting

Single click **Add** to open a QoS configuration page. Select the parameter based on your actual situation and demand, and enter the IP address, subnet mask and UDP/TCP code. When you are done, single click **Submit** at the bottom of the page to save the changes.

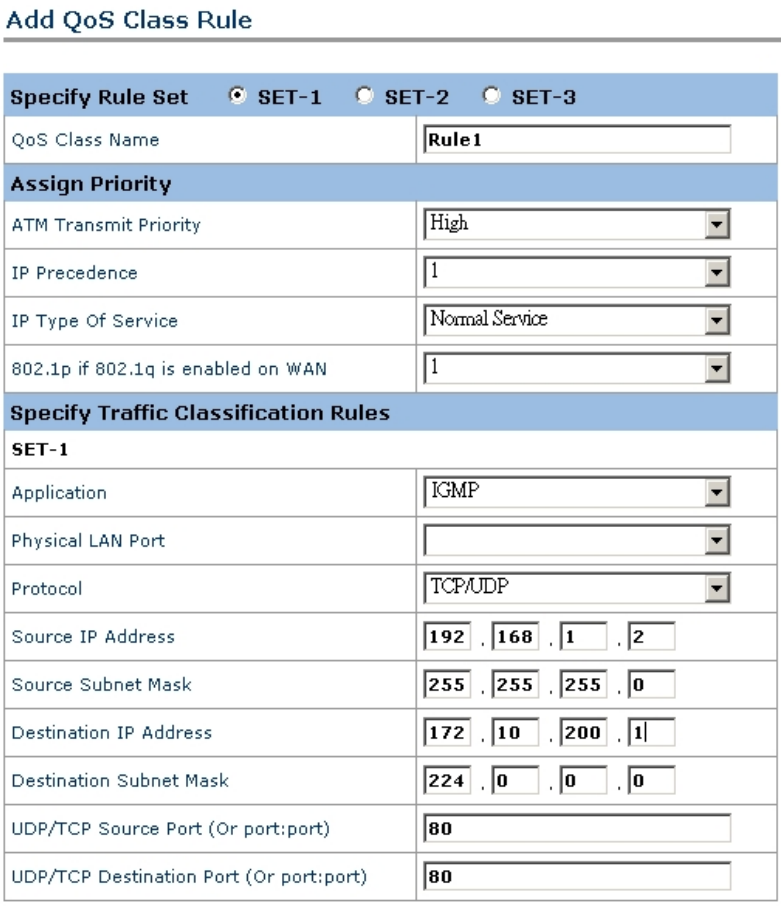


Figure 4-24 Add QoS Class Rule

4.4.4 ACL (Access Control List) Setting

We may configure ACL on HG520 to avoid any unauthorized user to control the device. ACL keeps the records of the unique authentication code, limit of authority, and expiry of such authentication of the authorized user. With this feature configured, HG520 will only allow the access of authorized user and avoid any illegal access.

Enter the IP addresses of the LAN port and select **Enable**, these IP addresses will be allowed to access the services listed on the Service Control List. You can also control the access from the WAN port to HG520 by repeating the same procedure.

ACL Setting

LAN	WAN
Enable Disable	Enable Disable
Add IP Address(max 5)	Add IP Address(max 5)
. . . Add	. . . Add

Interface	IP Address	Oper.Status	Action
LAN	1.1.1.1		

4.4.5 SNTP Setting

NTP (Network Time Protocol) is a time protocol used to synchronize the time display of different computers in the same network. SNTP (Simple Network Time Protocol) is a simplified NTP, which remove the unnecessary internal algorithm in the servers.

Just use the factory default settings of NTP during the selection of the first and second NTP time server.

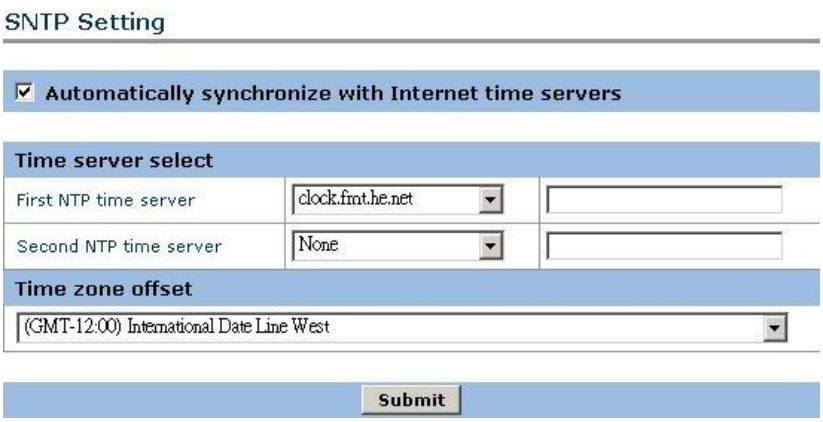
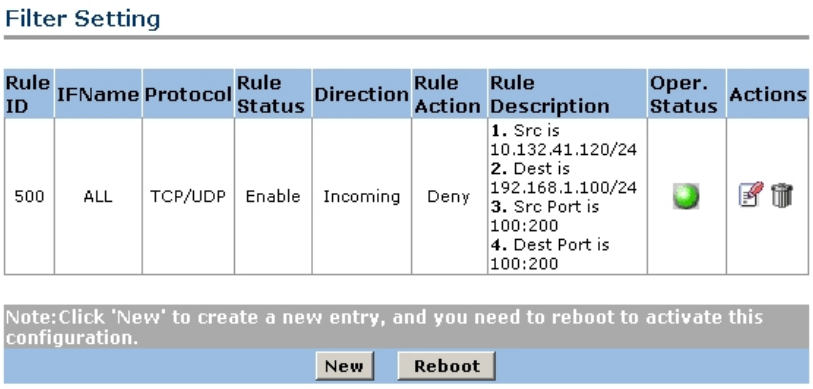


Figure 4-25 SNTP Setting

4.4.6 IP Filter

IP Filter is a software package that can be used to provide network address translation (NAT) or firewall services. It restricts the IP address of a computer or the IP address of a segment to access the Internet via certain ports.

If the IP filter feature is activated, it allows/rejects the packet from a specific port of a specific IP address to be forwarded to a local specific port of a specific IP address. Take Figure 4-27 as example, the packets from port 100 to port 200 of IP address 10.132.41.120 are not allowed to be forwarded to local port 100 to port 200 of IP address 192.168.1.100. You can add you own rules based on actual needs.



Filter Setting

Rule ID	IFName	Protocol	Rule Status	Direction	Rule Action	Rule Description	Oper. Status	Actions
500	ALL	TCP/UDP	Enable	Incoming	Deny	**1.** Src is 10.132.41.120/24 **2.** Dest is 192.168.1.100/24 **3.** Src Port is 100:200 **4.** Dest Port is 100:200		

Note:Click 'New' to create a new entry, and you need to reboot to activate this configuration.

New Reboot

Figure 4-26 IP Filter

Single click **New** button to open the Rule Information setting page. Enter the parameters and single click **Submit** to save the configurations.

Figure 4-27 IP Filter Setting

4.4.7 Multinat Setting

Multi-NAT can be used where you have been allocated multiple public IP addresses by your ISP. Instead of a many-to-one relationship, you can have a one-to-one relationship between a public IP address and an internal/private IP address. This means that you have the protection of NAT (Network Address Translation) but the PC can be

addressed directly from the outside world by its fake public IP address, but still by only opening specific ports to it.

Take Figure 4-28 as example, when internal IP address 192.168.1.56 accesses Internet, Internet will identify this IP address as 192.168.1.166. Internet user can access the service provided on IP address 192.168.1.56 via 192.168.1.166.

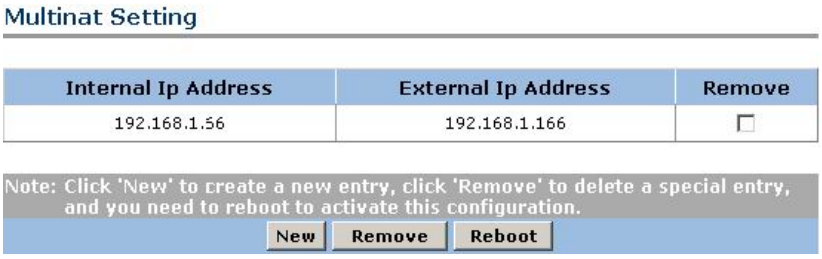


Figure 4-28 Multinat Setting

Single click **New** button to open the configuration page. Enter the internal and external IP addresses.

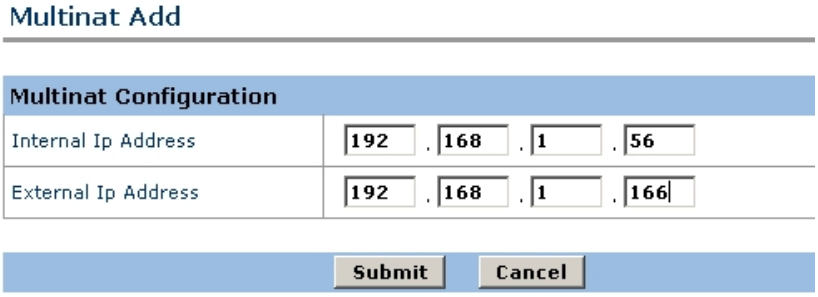


Figure 4-29 Multinat Setting -- Add

4.4.8 Parental Control

This feature restricts the time user can access the Internet. Single click **New** from Parental Control main page and you will be directed to Figure 4-30. Select the MAC address of the computer that you want to control, enter which days of a week and what time of a day you want to control. When done, single **Submit** to activate the settings and the controlled days of the week and blocking time will be shown as in Figure 4-31.

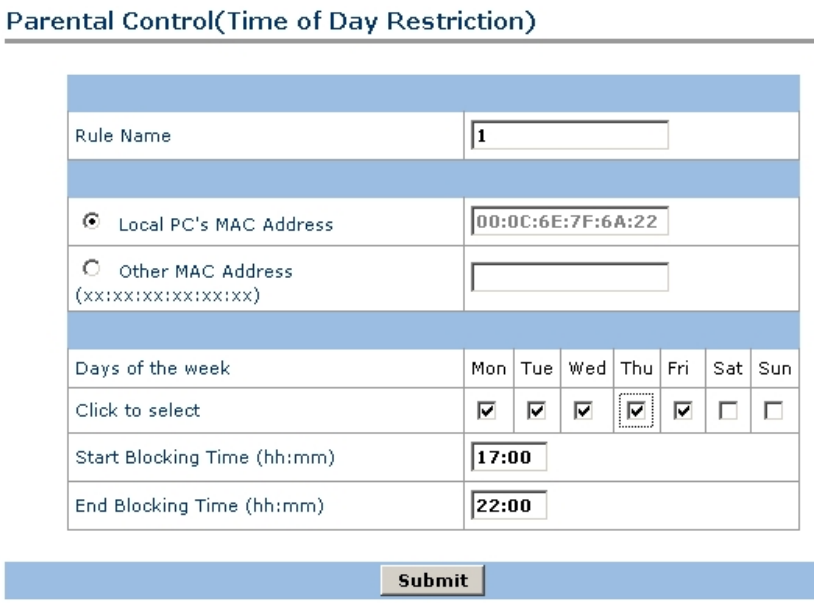


Figure 4-30 Parental Control Setting

Parental Control(Max 16)

Rulename	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
1	00:0c:6e:7f:6a:22	x	x	x	x	x			17:00	22:00	☐

Add Remove

Figure 4-31 Parental Control

4.4.9 Port Mapping

Port mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

Single click **Add** button to activate this feature, create mapping groups of appropriate LAN and WAN interfaces.

Single click **Remove** button to remove a group and add ungrouped interface to the default group.

You can configure up to 16 entries.

Port Mapping (maximum 16 entries)

☐ Enable virtual ports on eth0

Group Name	Interfaces	Remove	Edit
Default	eth0, nas_0_35, nas_7_35, nas_8_35, Wireless, Wireless		
A	USB	☐	Edit

Add Remove

Figure 4-32 Port Mapping

- Click **Add** in Figure 4-32 and you are prompted to Figure 4-33. First enter the group name. Select interfaces from **Available Interfaces** and click "←" to add them into **Grouped Interfaces**. You can create new groups by repeating these steps. Please be noted that each group name should be different.

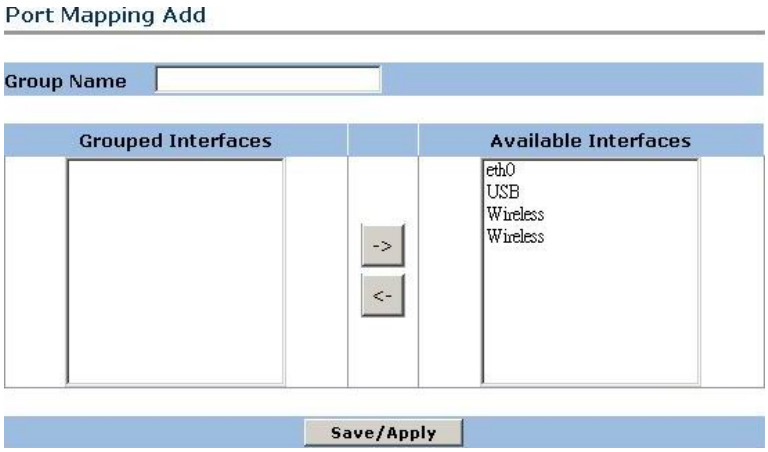


Figure 4-33 Port Mapping — Add

- Click **Save/Apply** to validate the modification.

To remove a group, check the Remove box and click **Remove**.

Note:

The selected interfaces will be removed from the existing group and added to the new group.

4.4.10 Protocol Block

This feature refuses user to access certain websites, or denies the visit from certain IP address for security or other reasons. It blocks the protocols you do not need to use. Apart from the default protocols, there is a **Customer Define** option for you to add more protocols that you want to block.

Select the protocols that you wish to block and click **Submit** to save the change.

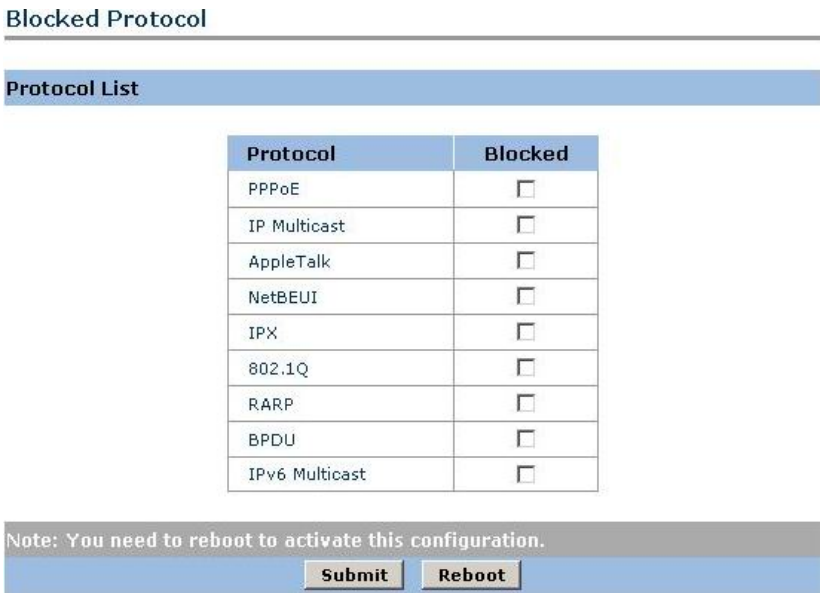


Figure 4-34 Blocked Protocol

From the Customer Define page as shown in Figure 4-35, click **New** to enter the Customer Define Add page and this page will appear as shown in Figure 4-36.

Figure 4-35 Customer Define

In Figure 4-36, enter the protocol and type filed that you want to block and click **Save** to activate the change. The new blocked protocol will then be shown in Customer Define page.

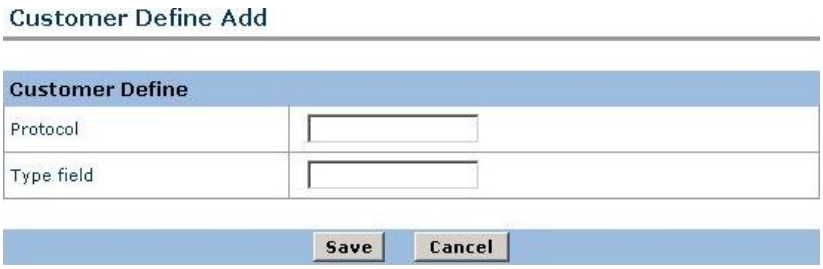


Figure 4-36 Customer Define Add

4.5 Wireless Setup

HG520 is designed with wireless function, which enables access to Internet without the need of deployment of cables if the environment does not allow or there are no cables available.

4.5.1 Configuring Basic Features

This page allows you to configure basic features of the wireless interface.

Figure 4-37 Wireless Setup — Basic

Follow the steps below to configure the basic wireless setting:

- Check **Enable Wireless** to activate the wireless function.
- Check **Hide Access Point** from active scans. If this function is checked, other clients cannot know the existence of your access point. If it is not checked, you open this access point for others to access as long as they pass the authentication.
- Enter the **SSID** name. (SSID = Service Set Identifier)
- Select the **Country** that you are using the wireless.
- Check **Enable Guest SSID** so that when the main SSID does not work you can use the guest SSID to access WAN.
- Click **Save/Apply** to save the configuration.

4.5.2 Configuring Security

HG520 provides multiple wireless security settings, including:

- Shared (WEP)
- 802.1X
- WPA
- WPA-PSK
- WPA2
- WPA2-PSK
- Mixed WPA2/WPA
- Mixed WPA2/WPA –PSK

Open is an option on the drop-down menu, but it provides no security control for the wireless access.

I. Shared (WEP) configuration

During data transmission, Wired Equivalent Privacy (WEP) encrypts data over radio waves to ensure the security. However, it provides limit security protection though it is easy to be configured. See Figure 4-38 for Shared key configuration.

1. Set the following parameters to enable WEP:
   - Select **SSID**
   - **Network Authentication**: Shared
   - **WEP Encryption**: Enabled
   - **Encryption Strength**: 128-bit (recommended for higher security) or 64-bit
2. Configure WEP keys. You can configure from 1 to four network keys.

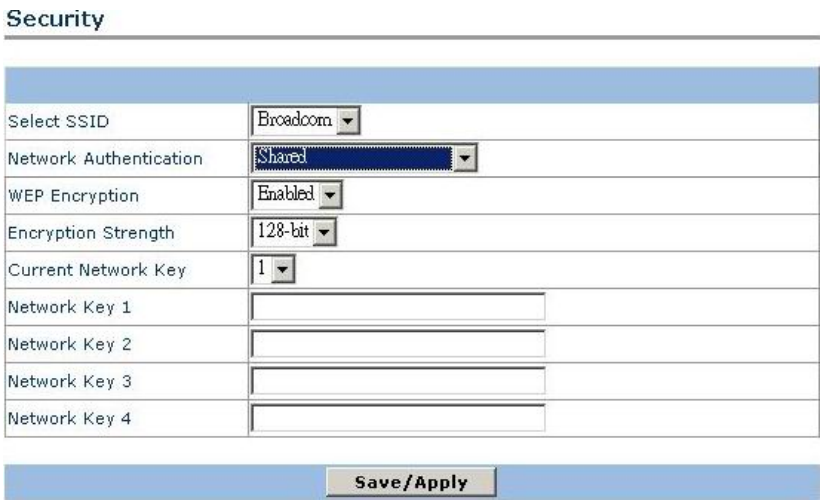


Figure 4-38 Wireless Setup — Security — WEP

- Enter 13 ASCII characters or 26 hexadecimal digits in the Network Key 1to 4 if you choose 128-bit encryption keys.
- Enter 5 ASCII characters or 10 hexadecimal digits in the Network Key 1to 4 if you choose 64-bit encryption keys.

3. Select the key to be used from the four network keys from **Current Network Key**.
4. Click **Save/Apply** to save the configuration.

II. 802.1X configuration

802.1X authentication must be run on the Radius server to improve the security of WEP. Therefore, the Radius server must be running before you enable 802.1X.

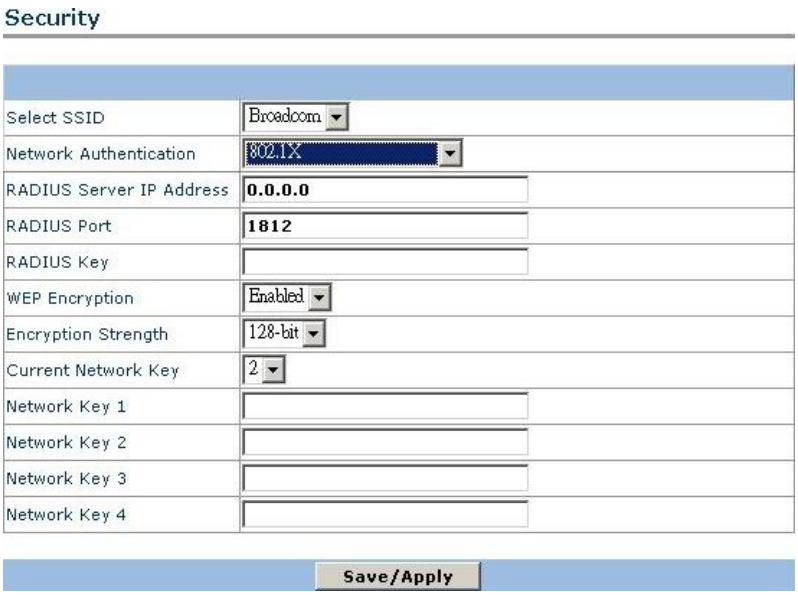


Figure 4-39 Wireless Setup — Security — 802.1X

1. Select **SSID**.
2. Select **802.1X** in **Network Authentication** to enable 802.1X.
3. Enter the IP address, the port number (default: 1812), and the key of your RADIUS server.
4. **Encryption Strength**: 128-bit (recommended for higher security) or 64-bit.
5. Follow the same instruction on 4.5.2 I. Shared (WEP) configuration to configure the four network keys.
6. Click **Save/Apply** to save the configuration.

III. WPA/WPA2 configuration

WPA (Wi-Fi Protected Access) provides powerful wireless security protection. It improves the data encryption through the

temporal key integrity protocol (TKIP) and advanced encryption standard (AES), whose functions can be enabled via the WPA configuration.

And Similar to 802.1X, WPA must work with RADIUS server.

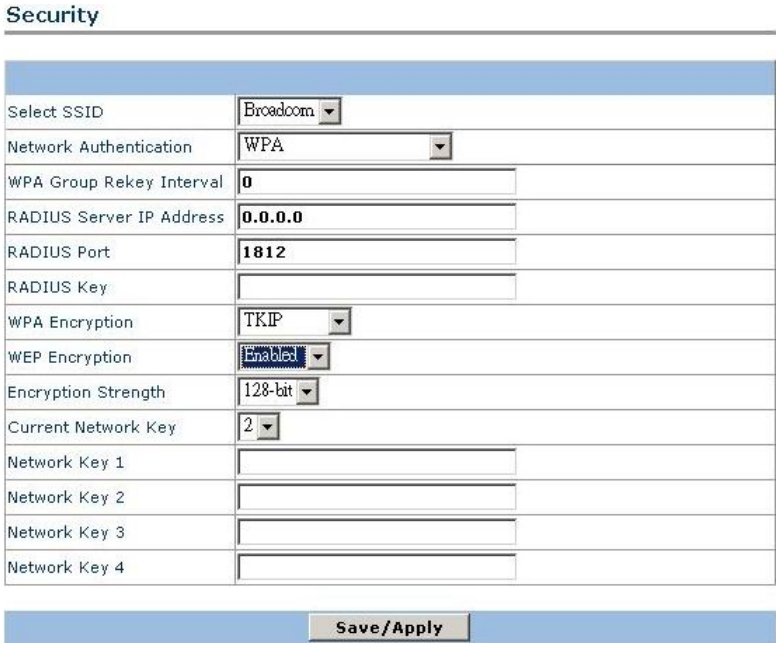


Figure 4-40 Wireless Setup — Security — WPA

1. Enable **WPA**. Follow the steps below to set the parameters:
   - Select **WPA** from **Network Authentication**.
   - **WPA Group Rekey Interval:** The interval is estimated in second. The default value is 0 (no re-keying).
   - **RADIUS Server IP Address/Port/Key**: Make sure it matches the settings of your RADIUS server.

- **WPA Encryption**: Select from TKIP, AES and TKIP+AES.
- **WEP Encryption**: Default: disabled.
- **Encryption Strength**: 128-bit (recommended for higher security) or 64-bit
- Follow the same instruction on 4.5.2 I. Shared (WEP) configuration to configure the four network keys.

2. Click **Save/Apply** to save the configuration.

Ensure that your wireless network adapter matches the security method before you decide which one to use.

The following is the setup page for WPA2.

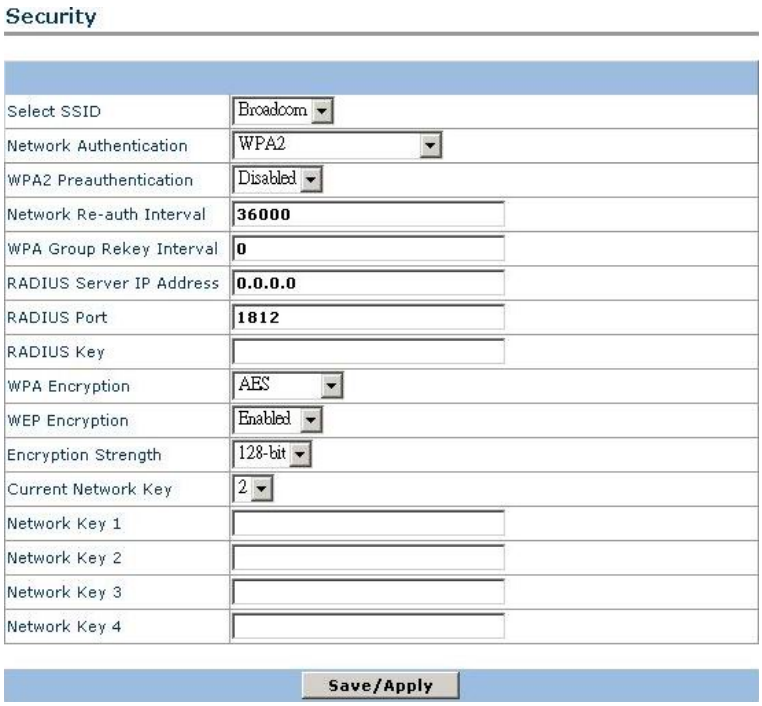


Figure 4-41 Wireless Setup — Security — WPA2

1. Enable **WPA2**. Follow the steps below to set the parameters:
   - **Network Authentication**: WPA2.
   - **WPA2 Preauthenticaton**: Expedite the 802.1X authentication. Up to this point, key caching only reduced the time to connect to the network when the client had previously been associated to the access point. A way was needed to establish a PMK (pairwise master key) security association when a client had not yet been associated to the access point. Preauthentication enables a client to establish a PMK security association to an access point with which the client has yet not been associated.
   - **Network re-auth Interval:** Define how long you want the network to re-authenticate when accessing the Internet (default value is 36000 seconds).
   - **WPA Group Rekey Interval:** The interval is estimated in second. The default value is 0 (no re-keying).
   - **RADIUS Server IP Address/Port/Key**: Make sure it matches the settings of your RADIUS server.
   - **WPA Encryption**: Select from TKIP, AES and TKIP+AES.
   - **WEP Encryption**: Default: disabled.
   - **Encryption Strength**: 128-bit (recommended for higher security) or 64-bit.
   - Follow the same instruction on 4.5.2 I. Shared (WEP) configuration to configure the four network keys.
2. Click **Save/Apply** to save the configuration.

Ensure that your wireless network adapter matches the security method before you decide which one to use.

IV. WPA-PSK/WPA2-PSK configuration

WPA-PSK is used when there is no RADIUS server activated.

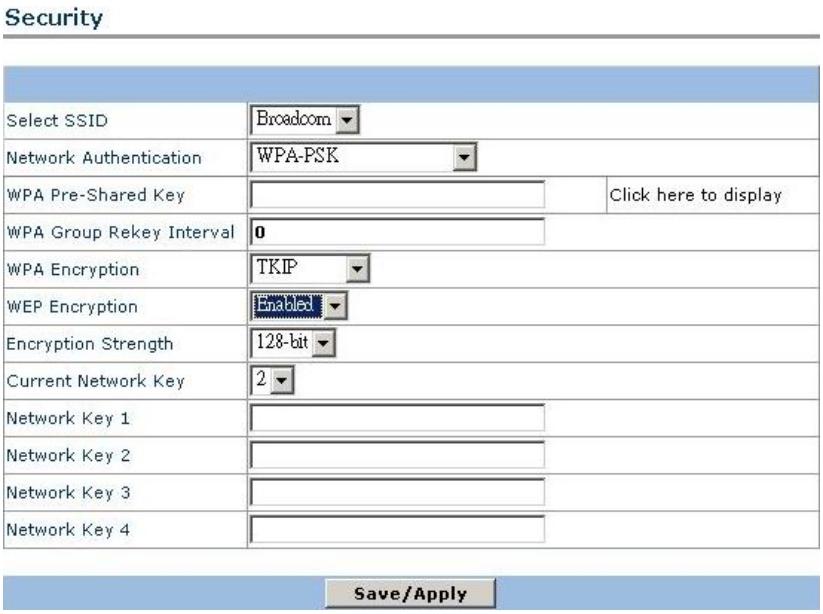


Figure 4-42 Wireless Setup — Security — WPA-PSK

1. Select **WPA-PSK** in Network Authentication to enable it.
2. Enter 8 to 63 ASCII codes or 64 hexadecimal (0–9, A–F) digits in **WPA Pre-Shared Key**. If you forget the key, simply click **Click here to display** and the key will show.
3. **WPA Group Rekey Interval:** The interval is estimated in second. The default value is 0 (no re-keying).
4. **WPA Encryption**: Select from TKIP, AES and TKIP+AES.
5. **WEP Encryption**: Default is disabled.

6. **Encryption Strength**: 128-bit (recommended for higher security) or 64-bit.
7. Follow the same instruction on 4.5.2 I. Shared (WEP) configuration to configure the four network keys.
8. Click **Save/Apply** to save the configuration.

Follow the same step to configure WPA2-PSK.

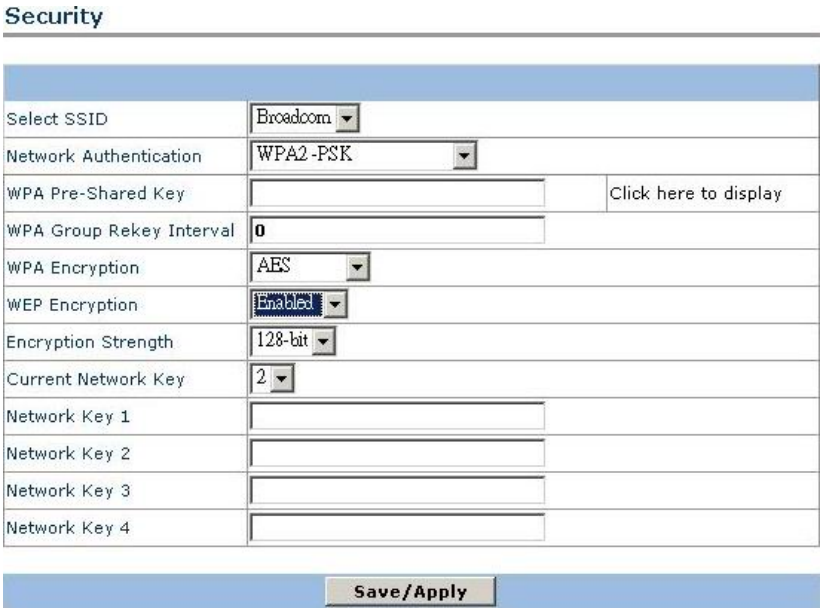


Figure 4-43 Wireless Setup — Security — WPA2-PSK

V. Mixed WPA2/WPA configuration

Mixed WPA2/WPA combines the features of the two functions to provide stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of

assurance that only authorized users can access their wireless networks.

Follow the steps below to configure the mixed WPA2/WPA function.

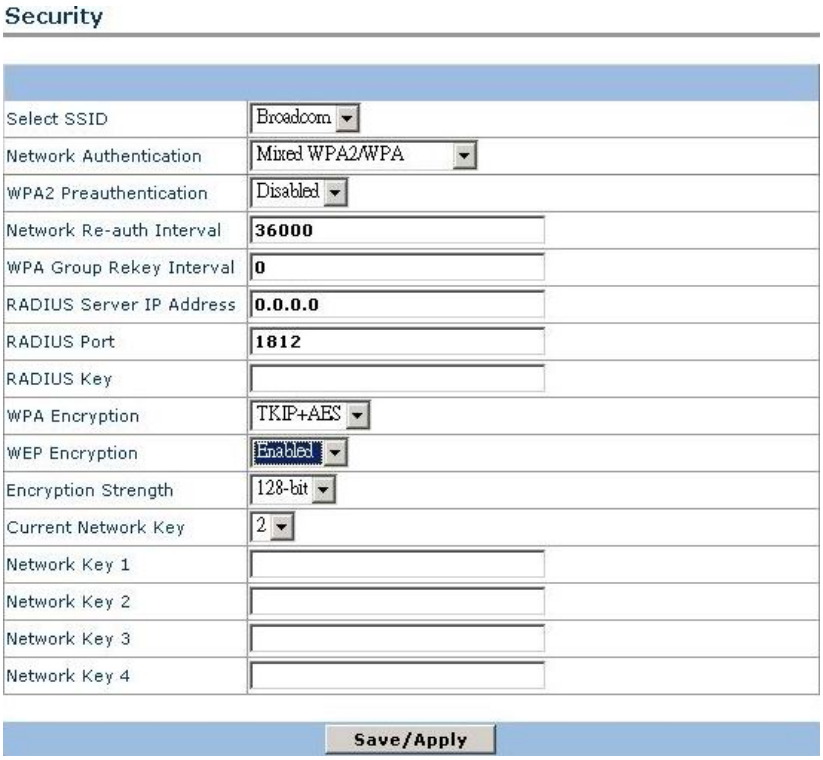


Figure 4-44 Wireless Setup — Security — Mixed WPA2/WPA

1. Select Mixes WPA2/WPA in Network Authentication to enable it.
2. The configuration method of the rest parameters is the same as WPA and WPA2.

3. When you are done, Click **Save/Apply** to save the configuration.

VI. Mixed WPA2/WPA — PSK configuration

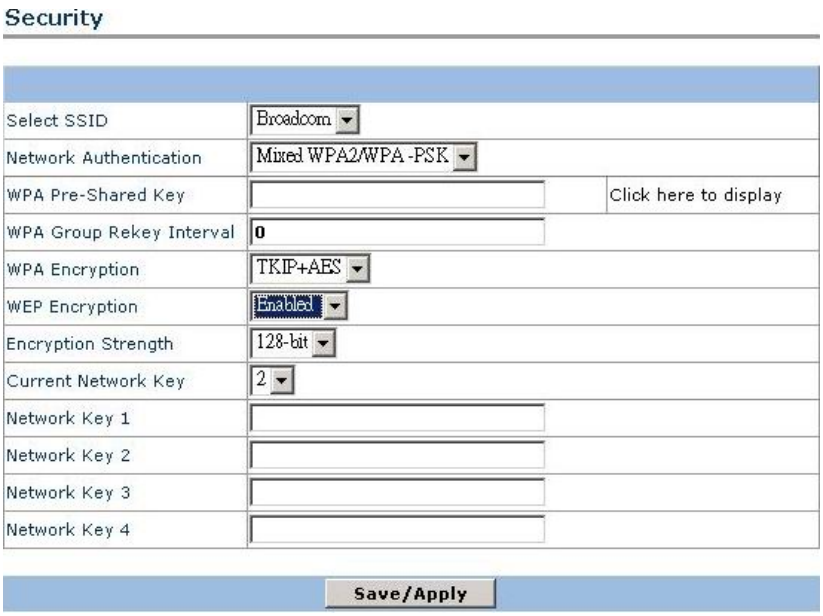


Figure 4-45 Wireless Setup — Security — Mixed WPA2/WPA-PSK

1. Select Mixed WPA2/WPA-PSK in Network Authentication to enable it.
2. The configuration method of the rest parameters is the same as WPA-PSK and WPA2.
3. When you are done, click **Save/Apply** to save the configuration.

4.5.3 Configuring MAC Filter

Wireless MAC filter controls access by the MAC addresses.

Figure 4-46 Wireless Setup — MAC Filter

1. When you select **Allow** in **MAC Restrict Mode**, only MAC addresses in the filter table can access HG520.
2. If you select **Deny** in **MAC Restrict Mode**, all MAC addresses except that in the filter table can access HG520.
3. If you select **Disabled**, then this function will not be activated.
4. Click **Add** to add a filter rule and enter the MAC address that you want to control.

5. Click **Save/Apply** to save the configuration.
6. To delete a configuration rule, select the Remove check box. Then click **Remove**.

4.5.4 Configuring Wireless Bridge

Wireless bridges have ports that connect two or more separate Ethernet LANs. The bridge receives packets on one port and

re-transmits them on another port. A bridge will not start re-transmission until it receives a complete packet. Because of this, station on either side of a bridge can transmit packets simultaneously without causing collisions. This page allows you to configure wireless bridge features of the wireless LAN interface.

Follow the steps below to configure wireless bridge.

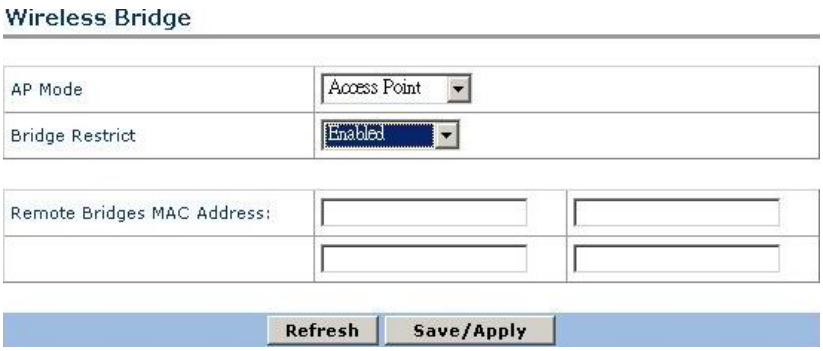


Figure 4-47

1. Select **Access Point** or **Wireless Bridge** from **AP Mode**. Select **Wireless Bridge** will disables access point functionality, while select **Access Point** enables access point functionality.
2. Select **Enabled (Scan)** from Bridge Restrict will enable the wireless bridge restriction and only those bridges selected in Remote Bridges will be granted access. Select **Disabled** in Bridge Restrict which disables wireless bridge restriction and any wireless bridge will be granted access.

3. Enter the Remote Bridge MAC Addresses to tell which access point is connected as a group via your access point or wireless bridge.

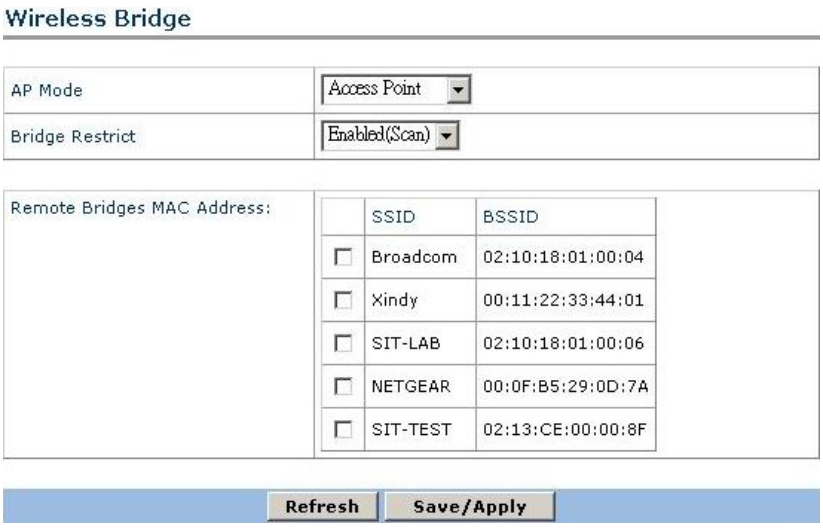


Figure 4-48

4.5.5 Configuring Advanced

Advanced

AP Isolation	Off
Band	2.4GHz - 802.11g
Channel	11 Current Channel: 11
Rate	Auto
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
XPress™ Technology	Disabled
54g™ Mode	54g Auto
54g Protection	Auto
Regulatory Mode	Disabled
Pre-Network Radar Check	60
In-Network Radar Check	60
TPC Mitigation(db)	0(off)
Transmit Power	100%

Save/Apply

Figure 4-49 Wireless Setup — Advanced

In most cases, HG520 works with default settings. If you are not familiar with these parameters, modification is not recommended.

- **AP Isolation**: Prevents one wireless client communicating with another wireless client.

- **Channel**: Select the appropriate channel from the provided list. All devices in your wireless network must use the same channel in order to function correctly. It is 11 by default.
- **Rate**: The range is 1Mbit/s–54Mbit/s. The transmission rate depends on the speed of your wireless network. You can select one rate or the default **Auto**. If you select **Auto**, HG520 will automatically obtain the fastest rate.
- **Multicast Rate**: In layered multicasting, data is transmitted in multiple layers. The source encodes the signal in layers, and a subset of these layers is sent to the receivers, depending on the receiver requirements, and the congestion of the path from the source to the receiver. Layered multicasting is a form of multirate multicasting, since different receivers in the same multicast group can receive traffic at different rates.
- **Basic Rate**: Select the basic rate that wireless clients support.
- **Fragmentation Threshold**: It is 2346 by default. The range is 256–2346 bytes.

  This value specifies the maximum packet size after data fragmentation.

  If there is a high packet error rate, you can lower the fragmentation threshold.

  Setting the fragmentation too low may result in poor network performance.

  Only slight adjustment of this value is recommended.

- **RTS Threshold**: It is 2347 by default. The range is 0–2347 bytes.
  If there is inconsistent data flow, you can make slight adjustment of this value.
  If the network packet is smaller than the RTS threshold, RTS/CTS will not be enabled.
  HG520 sends Request to Send (RTS) to a particular receiving station and negotiates the transmission of data frame.
  After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the transmission. Then the transmission begins.
- **DTIM Interval**: The range is 1–255 milliseconds. It is the interval of Delivery Traffic Indication Message (DTIM). DTIM interval is in countdown mode. It informs clients to listen to broadcast messages.
  When HG520 has stored broadcast information for clients, it sends the next DTIM according to the DTIM Interval. Clients receive the beacon and begin to receive the broadcast message. It is 1 by default.
- **Beacon Interval**: The range is 50–2000 milliseconds.
  The Beacon Interval is the frequency interval of the beacon. A beacon is a packet broadcast by HG520 to synchronize the wireless network. It is 100 by default.
- **XPress™ Technology**: this technology can improve the data transmission rate. By default, it is disabled.
- **54g™ Mode**: There are 3 options:
  Select **54g Auto** for wide compatibility.
  Select **54g Performance** for the fastest performance.

Select **54g LRS** if you are not familiar with 802.11b equipment.

- **54g protection:** In **Auto** mode, HG520 can improve 802.11g performance in 802.11g/802.11b mixed network through RTS/CTS.
  The **off** protection mode can maximize 802.11g throughput in most cases.

- **Pre-Network Radar Check**: **To be defined**
- **In-Network Radar Check**: **To be defined**
- **TPC Mitigation**: Transmit power control is a method of lowering the transmit power used by a WLAN and it reduces WLAN interference with satellite services in the 5GHz band. With the 802.11h amendment to the 802.11a PHY and MAC layer, TPC mitigation becomes a reality in the 5-GHz band. Manufacturers are now poised to implement one standards-based solution to address interference concerns around the world.
- **Transmit Power**: The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm. The larger the percentage of transmit power, the clearer the signal sent.

4.5.6 Quality of Service over the 802.11 Interface

QoS manages time-sensitive multimedia and voice application traffic to ensure that this traffic receives higher priority, greater bandwidth, and less delay than best-effort data traffic.

WLANs are now used to transport high-bandwidth, intensive data applications in conjunction with time-sensitive multimedia applications. This requirement has led to the necessity for wireless QoS.

Configure wireless QoS function in Figure 4-50.

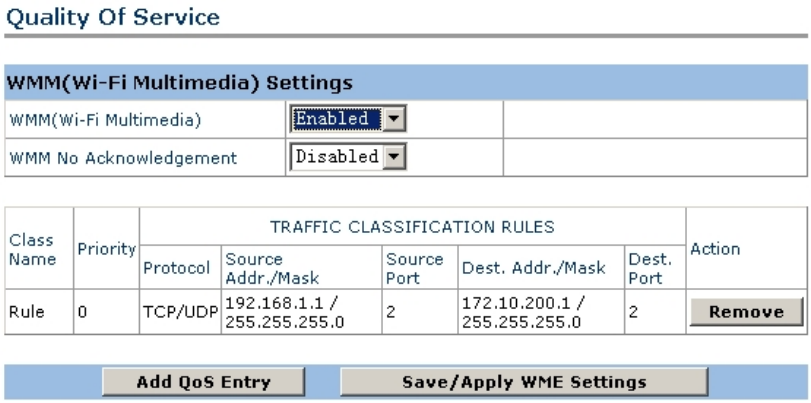


Figure 4-50 Quality of Service

First select **Enabled** for **WMM**, and **Disabled** for **WMM No Acknowledgement** and click **Add QoS Entry** to open a QoS configuration page as shown in Figure 4-51

Follow the step below to configure wireless QoS:

1) Enter the **Traffic Class Name**. Do not use digit (1,2,3 etc.).

2) Select the **Wireless Transmit Priority** from the drop-down menu according to your demand. For example, you can select **Video Priority** which guarantees the transmission speed and quality of image if you are using HG520 for video conferencing.
3) Select **Protocol**.
4) Enter Source and Destination IP Address and Subnet Mask, UDP/TCP Source and Destination Port.
5) When you are done, single click **Save/Apply** to save the change.

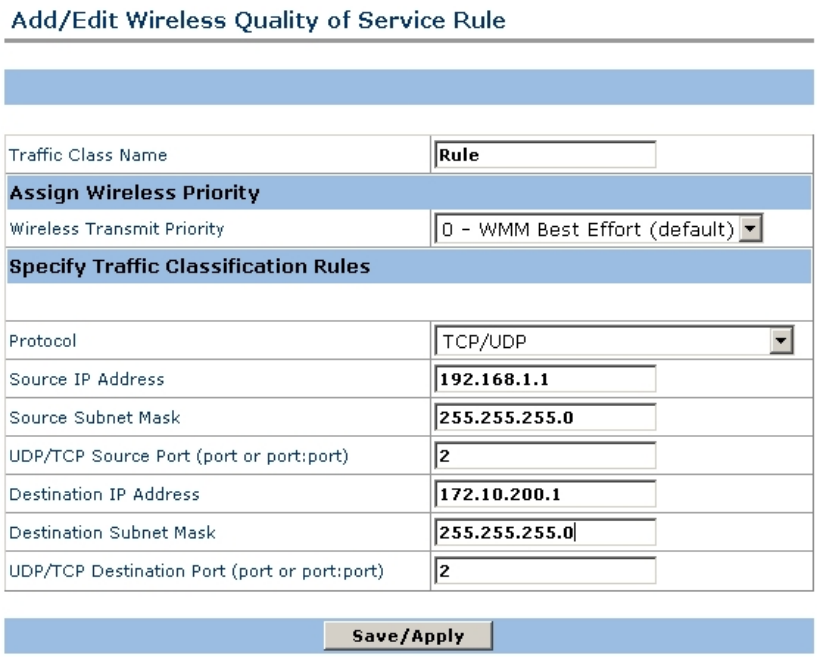


Figure 4-51 Quality of Service -- Add

4.5.7 Viewing Station Info

This page shows authenticated wireless stations and their status.

Station Info

BSSID	Associated	Authorized
00:0E:35:B9:E5:A5		

Refresh

Figure 4-52 Wireless Setup — Station Info

4.6 Tools

HG520 supports tools that enable you to customize and upgrade firmware for your gateway. There are seven main functions: User Management, Diagnostics, Backup Setting, System Management, Firmware Upgrade, Log, and Save & Reboot.

4.6.1 User Management

Single click **Tools** from the navigation tree and the sub-items under it appear.

You can change the user ID and privilege form the User Management page.

User Management

User ID	Privilege	Actions
admin	Administrator	
user	User	
Click 'New' to create a new User ID.		
	New	

Figure 4-53 User Management

Single click **New** button to open the page for adding a new user. Enter the new user name and password and single click **Add** to add the new user.

User Management

User ID	Privilege	Actions
admin	Administrator	
user	User	
Click 'New' to create a new User ID.		
User ID		
Privilege	Administrator User	
Password		
Confirm Password		
	Add Cancel	

Figure 4-54 Add a new user

4.7 System Diagnostics

This feature displays the connection status of HG520's Ethernet and ADSL ports. Figure 4-55 shows that the ADSL connection is FAIL,

which means the ADSL port does not successfully connect to external network.

You may check another system diagnostics by clicking **Next Connection**. Single click **Test with OAM F4** and you can check the connection status of ATM OAM F4 segment ping.

System Diagnostics

Item	Status
Test service name	br_1_39
Modem Connction Test	
Test your Ethernet Connection	PASS
Test ADSL line for sync	FAIL
Test your USB Connection	DOWN
Test your Wireless Connection	PASS
ATM Connction Test	
Test ATM OAM F5 segment ping	FAIL
Test ATM OAM F5 end-to-end ping	FAIL

Next Connection

Test With OAM F5 | Test With OAM F4

Figure 4-55 System Diagnostics

4.7.2 Backup Settings

If you select **Backup Settings**, a pop-up window appears and asks where you want the information to be backed up. Browse the route to tell where to save it and single **OK** button.

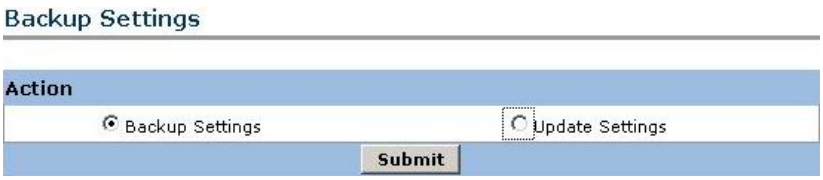


Figure 4-56 Backup Settings

Select **Update Settings** and you will see the following figure. Browse and select the setting file you backed up last time and the settings of HG520 will restore to the settings you made previously.

Figure 4-57 Backup Update Settings

4.7.3 System Log

Select **View System Log** to check the system log page. Select **Save System Log** to save the log to the hardware.

Figure 4-58 System Log Main Page

System Log

Date/Time	Facility	Severity	Message
Jan 1 01:08:56	syslog	emerg	BCM96345 started: BusyBox v1.00 (2006.02.08-07:13+0000).
Jan 1 01:08:56	user	crit	kernel: eth0 Link UP.
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: Unable to send OAM cell over VPI/VCI 8/3 (error 9).
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: Unable to send OAM cell over VPI/VCI 8/4 (error 9).
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: Unable to send OAM cell over VPI/VCI 8/3 (error 9).
Jan 1 01:08:56	user	crit	kernel: OAM loopback response not received on VPI/VCI 8/36.
Jan 1 01:08:56	user	crit	kernel: Unable to send OAM cell over VPI/VCI 8/4 (error 9).

Refresh Close

Figure 4-59 View System Log

If you single click **Configure System Log**, you may configure log level and the display level. When you are done with the settings, single **Submit** to save the changes.

Configure System Log

Item	Description
Log Status	○ Disable ◉ Enable
Log Level	Debugging
Display Level	Error
Mode	Local

Submit

Figure 4-60 Configure System Log

4.7.4 Alarm Setting

Set up the Alarm Setting in the four categories of the following figure to monitor the relevant connection status of HG520. In normal condition, we do not recommend the use of this feature in order to guarantee a better connection rate.

Alarm Setting

Item	Description	Limit
Loss of Signal(Times)		[0-65535]
Loss of Frame(Times)		[0-65535]
Loss of Link(Times)		[0-65535]
Errored Second(Times)		[0-65535]

Submit View

Figure 4-61 Alarm Setting

4.7.5 Firmware Upgrade

HG520 provides you with firmware upgrade management utility to upgrade your firmware. Single click **Browse** button to upload the firmware version you wish to update and single click **Upgrade** to update the firmware.

Firmware Upgrade

Item	Description
Version	V100R002B021
Firmware Date	February 16, 2006
Specify a firmware file to upgrade	
瀏覽...	
Upgrade	

Figure 4-62 Firmware Upgrade

4.7.6 Save & Reboot

Save & Reboot provides three functions: Save, Reboot, and Factory Setting Reboot.

- Select **Save** and single click **Submit** to save the settings.
- Select **Reboot** and single click **Submit** to reboot HG520.
- If you want to restore to the default factory settings, select **Factory Setting Reboot** and single click **Submit**

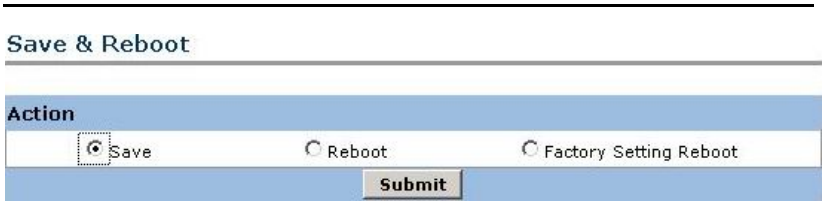


Figure 4-63 Save & Reboot

Chapter 5 Connection Mode

5.1 HG520 Connection Mode

HG520 supports 5 connection modes:

- PPPoA Mode: PPPoA dialup mode
- PPPoE (PPP over Ethernet) Mode: PPPoE dialup mode
- MER Mode: MAC Encapsulation Routing Mode
- IPoA Mode: IPoA Routing Mode
- Bridging Mode: Commonly used bridging mode

5.2 Configuration Modes

5.2.1 PPPoA Dialup Mode

HG520 Configuration Parameter	
Parameter	Description
WAN Connection Mode	Select “PPP over ATM (PPPoA)”.
ATM PVC Configuration	Provided by the service provider.
DHCP Configuration	Recommended: Activate DHCP server.
User PC Configuration	
IP Address and Subnet Mask	Recommend: Automatically obtain IP address.
DNS Configuration	Recommend: Automatically obtain DNS server IP address.

5.2.2 PPPoE Dialup Mode

Parameter	Description
HG520 Configuration Parameter	
WAN Connection Mode	Select “PPP over Ethernet (PPPoE)”.
ATM PVC Configuration	Provided by the service provider.
DHCP Configuration	Recommended: Activate DHCP server.
User PC Configuration	
IP Address and Subnet Mask	Recommend: Automatically obtain IP address.
DNS Configuration	Recommend: Automatically obtain DNS server IP address.

5.2.3 MER Mode

Parameter	Description
HG520 Configuration Parameter	
WAN Connection Mode	Select “MAC Encapsulation (MER)”.
ATM PVC Configuration	Provided by the service provider.
IP Address	Configure as obtain IP address automatically or provided by ISP according to actual situation.
DHCP Configuration	Recommended: Activate DHCP server.
User PC Configuration	
IP Address and Subnet Mask	Recommend: Automatically obtain IP address.

DNS Configuration	Recommend: Automatically obtain DNS server IP address.

5.2.4 IPoA Mode

Parameter	Description
HG520 Configuration Parameter	
WAN Connection Mode	Select “IP over ATM (IPoA)”.
ATM PVC Configuration	Provided by the service provider.
IP Address	Configure as IP provided by ISP.
DHCP Configuration	Recommended: Activate DHCP server.
User PC Configuration	
IP Address and Subnet Mask	Recommend: Automatically obtain IP address.
DNS Configuration	Recommend: Automatically obtain DNS server IP address.

5.2.5 Bridge Mode

Parameter	Description
HG520 Configuration Parameter	
WAN Connection Mode	Select “Bridging”.
ATM PVC Configuration	Provided by the service provider.

User PC Configuration	
IP Address and Subnet Mask	Recommend: Automatically obtain IP address.
DNS Configuration	Recommend: Automatically obtain DNS server IP address.
Please install dialup software if you select Bridging mode as WAN connection mode. If your computer uses static IP address, please ask the IP address, subnet mask, and DNS server address from your ISP.	

Chapter 6 Troubleshooting

6.1 Quick Troubleshooting

Failures	Instructions
Power light is out	1. Ensure power adapter is well connected; 2. Ensure the right power adapter is used.
ADSL light is out	1. Ensure the ADSL line is well connected; 2. Ensure the telephone line before entering the house is valid, try to test with a telephone; 3. Check that there is no junction box before connecting HG520, which has such components like capacitors or diodes that could hinder back high frequency signals; 4. Ensure the HG520 and telephones are connected in the right way.
LAN light is out	1. Ensure you use the right cables from the Modem to your PC; 2. Ensure the connection is secured; 3. Check if the NIC LED lights up; 4. Ensure your Network Adapter works normally by examining whether the item of “Networking Adapters” is labeled with “？” or “！”. If it is, you may delete it and then click “Refresh” to reinstall. Otherwise, you may try the NIC in another slot. As a last resort, you have to replace the NIC.
WLAN light is out	1.Make sure you enabled the wireless function on the HG520 Web UI and enter the correct authentication password;

Failures	Instructions
USB light is out	1. Ensure the USB cable is firmly connected to the USB port; 2. Make sure the driver is installed successfully. 3. Make sure there are traffics between PC and USB port.
Unable to access the Internet	Take the most commonly used connection mode (Using bridged mode on the server side. Client uses the PPPoE dial-up application to connect to the Internet) as an example: 1. Ensure any of the problems above is not the reason; 2. Ensure that the PPPoE dial-up application is well installed and configured; 3. Ensure that you have entered the correct User ID and password; 4. After dial-up successfully, if you are still not able to connect to the Internet, check if the Proxy server on your browser is set up correctly. The Proxy server must be disabled; 5. Try to connect to different web sites to make sure that it is not the problem of the web site server.

Chapter 7 Technical Specifications

I. ADSL/ADSL2+ Standards

- Built-in ADSL/ADSL2+ broadband network function requires no external ADSL modem
- Compatible with Annex A ANSI T1.413 Issue 2, ITU-T G.992.1 (G.DMT), G.992.2 (G.Lite), G.992.3 (ADSL2) and G.992.5 (ADSL2+)
- Support dual latency (fast and interleave) auto-connection
- Support ITU-T G.994.1 (G.hs) handshake protocol

II. WLAN

- Support multiple WLANs
- 802.11g
- 802.11a
- WPA security
- 64/128 digits WEP encryption and TKIP encryption
- Access control based on MAC address

III. Routing Features

- Support RIP1 (RFC 1058), RIP2 (RFC1389) and static routing
- Support NAT, NAPT and extended ALG
- Support DHCP Server/Client
- Support DNS Relay
- Support IGMP Proxy, IGMP Snooping
- Support Port Mapping

IV. Bridging protocols

- Support the auto-sensing transparent bridging (IEEE802.1d transparency) from Ethernet to ADSL
- Support up to 256 MAC addresses for learning

V. Security

- Powerful wireless network security
- Dynamic packet-detection firewall
- Access Control List
- IP/Domian/URL/MAC filtering
- Supports PAP and CHAP with PPP (RFC 1334)
- Support SPI (Stateful Packet Inspection)
- Prevent port scanning and illegal packet attack
- Prevent DOS, SYN Flooding, ICMP Redirection, LAND nd Smurf attack
- Support DMZ

VI. WAN protocols

- Multiple protocol over AAL5: LLC and VC-Mux (RFC 1483/2684)
- PPPoA (RFC 2364)
- PPPoE (RFC 2516)
- IPoA
- Bridged Static IP (RFC2684)
- RFC 2684 Routed
- RFC2684 Bridged
- Router+Bridged
- RFC Bridged DHCP Client

VII. ATM

- Support ATM Forum UNI 3.1/4.0
- Support up to 8 ATM PVCs (Permanent Virtual Circuit) to work simultaneously
- Support each PVC to provide different packet-separation level QoS
- Support ATM-based QoS and CBR, UBR, RtVBR and nrtVBR services
- Support OAM F4/F5 loop (I.610)

VIII. Network management

- Support web-based configuration and status monitoring
- Support remote/local firmware upgrade through HTTP and TFTP
- Support system log view
- Prevent mis-upgrade
- Support backup and restoration of configuration parameters
- Support software upgrade through Ethernet ports
- Provide solutions for various broadband applications, including: ADSL broadband access, family-scoped interior networking and broadband sharing, realization of value added services, such as videophone, IPTV, VOD, and music downloading through the cooperation of service terminals

IX. Data Transmission Rate

- G.dmt full rate: Downstream up to 8 Mbit/s, Upstream up to 896 Kbit/s
- G.lite: Downstream up to 1.5 Mbit/s, Upstream up to 512 Kbit/s

- T1.413：Downstream up to 8 Mbit/s, Upstream up to 896 Kbit/s
- G.992.5 (ADSL2+): Downstream up to 24 Mbit/s Upstream up to 1.2Mbit/s.

X. Radio Parameters

- Media Access Control: CSMA/CA with ACK
- Modulation mode: 802.11b: DSSS CCK
  802.11g: OFDM
- Frequency range (varies in different countries):
  USA – FCC: 2412 MHz – 2462 MHz
  Canada – IC: 2412 MHz – 2462 MHz
  Europe – ETSI: 2412 MHz – 2472 MHz
  Japan – STD-T66/STD-33m: 2412 MHz – 2484 MHz
- Operation Channels:
  11 channels (US, Canada)
  12 channels (European Telecommunications Standards Institute)
  14 channels (Japan)
- Input Power (max): 15 dBm (11g), 18 dBm (11b)
- Sensibility (typical): –87 dBm/11 Mbit/s; –74 dBm/54 Mbit/s
- Rate:
  802.11b:

1 Mbit/s	2 Mbit/s	5.5 Mbit/s	11 Mbit/s

802.11g:

6 Mbit/s	9 Mbit/s	12 Mbit/s	18 Mbit/s
24 Mbit/s	36 Mbit/s	48 Mbit/s	54 Mbit/s

XI. Operation Environment

- Temperature range: 0℃ – 40℃ (32°F – 96°F)
- Humidity range: 20% – 90%, frozen free

XII. Physical ports

- One ADSL/ADSL2+ port (RJ-11)
- Four 10/100BaseT auto-sensing Ethernet ports (RJ-45)
- One USB 1.1 port
- Screw-on Antenna, for 802.11b/g wireless connection

XIII. Power Specifications

- The input voltage is supplied according to the actual standards of different countries. The socket supports the standards of different delivery areas.
- Input voltage: 12V 1.2A

XIV. Dimension

- L x W x H: 215mm x 172mm x 41mm

Chapter 8 Acronyms and Abbreviations

A

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode

B

BSSID	Basic Service Set Identifier

D

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSLAM	Digital Subscriber Line Access Multiplex

H

HTML	Hypertext Markup Language

I

IP	Internet Protocols
IPoA	Internet Protocols Over ATM
ISP	Internet Service Provider

L

LAN	Local Area Network
M	
MAC	Media Access Control
N	
NIC	Network Interface Card
P	
PSK	Pre-shared key
PPP	Point to Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PVC	Permanent Virtual Connection
R	
RIP	Routing Information Protocol
S	
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
T	
TCP	Transfer Control Protocol
TKIP	Temporal Key Integrity Protocol

V

VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier

W

WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access