

User's Manual

CS-5800

Gigabit Content Security Router



Copyright

Copyright© 2012 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

CE mark Warning

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

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 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

WEEE Caution



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Customer Service

For information on customer service and support for the Gigabit Content Security Router, please refer to the following Website URL:

<http://www.planet.com.tw>

Before contacting customer service, please take a moment to gather the following information:

- ◆ Gigabit Content Security Router serial number and MAC address
- ◆ Any error messages that displayed when the problem occurred
- ◆ Any software running when the problem occurred
- ◆ Steps you took to resolve the problem on your own

Revision

User's Manual for PLANET Gigabit Content Security Router

Model: CS-5800

Rev: 1.0 (July, 2012)

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 FEATURES.....	1
1.2 PACKAGE CONTENTS	2
1.3 PHYSICAL SPECIFICATION	2
1.4 SPECIFICATION	4
CHAPTER 2: INSTALLATION PROCEDURE	6
2.1 SYSTEMATIC SETTING PROCESS	6
2.2 SETTING FLOW CHART.....	7
CHAPTER 3: HARDWARE INSTALLATION.....	9
3.1 INSTALLING THE DEVICE ON A STANDARD 19" RACK	9
3.2 SECURITY ROUTER NETWORK CONNECTION.....	10
CHAPTER 4: LOGIN SECURITY ROUTER	12
CHAPTER 5: SYSTEM STATUS	14
5.1 HOME PAGE.....	14
5.1.1 WAN Status	14
5.1.2 Physical Port Status	16
5.1.3 System Information	17
5.1.4 Security Status	17
5.1.5 Log Setting Status	18
5.2 CHANGE AND SET LOGIN PASSWORD AND TIME.....	18
5.2.1 Password Setting.....	18
5.2.2 Network Time	19
CHAPTER 6: NETWORK.....	21
6.1 NETWORK CONNECTION	21
6.1.1 Host Name and Domain Name.....	21
6.1.2 IP Mode.....	21
6.1.3 LAN Setting	21
6.1.3.1 IPv4 Only.....	22
6.1.3.2 Dual-Stack IP (IPv4 and IPv6).....	23
6.1.4 WAN & DMZ Settings.....	25
6.1.4.1 IPv4 Only.....	25
6.1.4.2 Dual-Stack IP (IPv4 and IPv6).....	36
6.2 MULTI- WAN SETTING	40

6.2.1 Load Balance Mode	40
6.2.2 Network Detection Service.....	47
6.2.3 Protocol Binding.....	49
CHAPTER 7: PORT MANAGEMENT	59
7.1 SETUP.....	59
7.2 PORT STATUS	61
7.3 IP/ DHCP	62
7.3.1 IPv4.....	62
7.3.2 IPv6.....	64
7.4 DHCP STATUS	66
7.5 IP & MAC BINDING (IPv4 ONLY).....	68
7.6 IP GROUPING	71
7.7 PORT GROUP MANAGEMENT	74
CHAPTER 8: QOS (QUALITY OF SERVICE)	75
8.1 BANDWIDTH MANAGEMENT	75
8.1.1 The Maximum Bandwidth provided by ISP.....	76
8.1.2 QoS.....	78
8.1.3 Smart QoS	81
8.1.4 Exception IP address	83
8.2 SESSION CONTROL	84
CHAPTER 9 : FIREWALL.....	86
9.1 GENERAL POLICY	86
9.2 ACCESS RULE.....	89
9.2.1 Default Rule.....	89
9.2.2 Add New Access Rule.....	90
9.3 URL FILTER	92
CHAPTER 10: ADVANCED FUNCTION	96
10.1 DMZ HOST/ PORT RANGE FORWARDING.....	96
10.1.1 DMZ Host	96
10.1.2 Port Range Forwarding	98
10.2 UPNP	100
10.3 ROUTING	101
10.3.1 Dynamic Routing	101
10.3.2 Static Routing	102
10.4 ONE TO ONE NAT	104
10.5 DDNS- DYNAMIC DOMAIN NAME SERVICE	107
10.6 MAC CLONE	109

10.7 INBOUND LOAD BALANCE.....	110
CHAPTER 11: SYSTEM TOOL.....	117
11.1 DIAGNOSTIC.....	117
11.2 FIRMWARE UPGRADE	118
11.3 CONFIGURATION BACKUP.....	119
11.4 SNMP	121
11.5 SYSTEM RECOVER	122
11.6 HIGH AVAILABILITY	122
CHAPTER 12. LOG.....	127
12.1 SYSTEM LOG	127
12.2 SYSTEM STATISTIC	131
12.3 TRAFFIC STATISTIC.....	132
12.4 IP/ PORT STATISTIC.....	135

Chapter 1: Introduction

As Internet becomes essential for your business, the only way to prevent your Internet connection from failure is to have more than one connection. PLANET's Gigabit Content Security Router, CS-5800, reduces the risks of potential shutdown if one of the Internet connections fails. Moreover, it allows you to perform load-balancing by distributing the traffic through three or four WAN connections.

In addition to a Multi-Homing device, PLANET's Gigabit Content Security Router provides a complete security solution in a box. The policy-based firewall, content filtering function makes it a perfect product for your network security. No more complex connection and settings for integrating different security products on the network is required.

This product is built-in bandwidth management function which also supported to offers network administrators an easy yet powerful means to allocate network resources based on business priorities, and to shape and control bandwidth usage.

1.1 Features

- ◆ **Multi-WAN Auto Backup:** The CS-5800 can monitor each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- ◆ **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including “**Auto Load Balance**”, “**Unbinding WAN Balance**” and “**Strategy Routing**”. User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- ◆ **Inbound Load Balancing:** The CS-5800 provides the Inbound Load Balancing for enterprise's internal server. The Inbound Load Balancing can reduce the server loading and system crash risks, in order to improve the server working efficiency.
- ◆ **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including Ping of Death, SYN Flooding, Land attack, IP Spoofing, etc. The access rule function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- ◆ **Content Filtering:** The security gateway can block network connection based on URLs, Scripts (The Java Applet, cookies and Active X), Restrict Application (MSN, Yahoo Messenger, QQ, PPSTREAM and PPTV) and Download/Upload blocking.
- ◆ **Multiple DHCP Server:** The multi DHCP server support 4 sets of Class C IP address, each server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- ◆ **QoS Bandwidth Management:** Featured Smart QoS with dynamic bandwidth management to automatically control P2P and video downloading and other bandwidth hogging to avoid bandwidth insufficient. Prioritizing different person/group or applications in bandwidth using for a better reasonable management.
- ◆ **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows users to alias a dynamic

IP address to a static hostname.

- ◆ **Multiple NAT:** Multiple NAT allows local port to set multi-subnet and connect to the Internet through different WAN IP addresses.
- ◆ **Port Range Forwarding:** The Port Forwarding and DMZ function can let you setup your servers in the Intranet and still provide services to the Internet users.
- ◆ **Easy Management:** Embedded Mirror Port to connect with monitoring devices to monitor online behavior. It also supporting remote management by web browser with user name and password to realize router management from remote places.
- ◆ **Log Feature:** The log and traffic statistic function can helping administrators to record the change/abnormal of the whole network status and take actions according to the log information.

1.2 Package Contents

The following items should be included:

- CS-5800 x 1
- Power Cord x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Cat5 Cable x 1
- Screw Packer x1
- Rack-mount ear x 2

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

1.3 Physical Specification

Front Panel



LED definition

LED	Color	Status	Description
PWR	Green	Steady	Power On
	Off	Off	Power Off
DIAG	Amber	Steady on	System is crashed.
		Blinking	System is on self-test after power on the device.
		Off	System is ready.
WAN/ DMZ: Link/Act	Green	Steady on	Port has been connected & Get IP
		Blinking	Transmit data.
		Off	Not get the IP address, even the port has been connected.
LAN: Link/Act	Green	Steady on	LAN port has been connected.
		Blinking	Transmit data.
LAN/WAN/DMZ: Speed	Green	Steady On	Works on 1000M
	Amber	Steady On	Works on 100M.
	Off	Off	Works on 10M.

Button definition

Button	Description
Reset	Push 5 seconds for "Warm Start", and push 10 seconds for Factory Default.
Power	Rocker switch ,Internal 12V/1.65A

1.4 Specification

Product		Gigabit Content Security Router
Model		CS-5800
Hardware		
Ethernet	LAN	8x 10/100/1000 Mbps RJ-45
	WAN	4~5 x 10/100/1000 Mbps RJ-45, configurable with WAN 5 (WAN 5 / DMZ)
	DMZ	1 x 10/100/1000 Mbps RJ-45
Button	Reset	1 x Reset button for reset to factory default setting
	Power	1 x Power on/off Switch
Software		
Multi-WAN Function		<ul style="list-style-type: none"> ● Inbound / Outbound Load Balance: by session and by IP ● Protocol Binding ● Network Service Detection
Routing		<ul style="list-style-type: none"> ● Dynamic Route RIP v1/v2 ● Static Route ● Strategy Routing
System Performance		<ul style="list-style-type: none"> ● Concurrent session :50000 ● Firewall performance :1Gbps ● Corporation Size: SMB(clients 200~250) ● 3DES performance:270Mbps
Bandwidth Management		<ul style="list-style-type: none"> ● Guaranteed Bandwidth ● Max Bandwidth ● Session Limit ● Port-based QoS
Firewall Security		<ul style="list-style-type: none"> ● NAT ● One-to-One NAT ● Multiple-to-One NAT ● Stateful Packet Inspection(SPI) Firewall ● Denial of Service (DoS) prevention ● IP & Port filtering ● Block Website by Keyword, Content Filter ● Firewall detection: Ping of Death, SYN Flooding, Land attack, IP Spoofing ● Email Alert for Hacker Attack ● IP&MAC Binding ● Support DMZ to protect your network: DMZ Host ● Prevent ARP Attack on LAN
Networking		<ul style="list-style-type: none"> ● Configurable DMZ ● DHCP Server (support class C), client, dynamic IP, static IP,IP Grouping support ● Multiple DHCP Server (support 4 sets of Class C) ● PPPoE / Static IP/ DHCP Client ● Multiple Subnet ● Protocol: TCP /IP, ARP, ICMP, FTP/TFTP, IPv4 ● NAT with port forwarding(Virtual Server) ● DNS Relay ● DDNS: Support DynDNS,3322 ● Password protected configuration or management sessions for web access ● Port Management – Speed/Duplex/Auto Negotiation/VLAN ● Transparent Bridge ● Support IPv4/IPv6
Network Management		<ul style="list-style-type: none"> ● Comprehensive web based management and policy setting ● SNMP v1/v2c ● Monitoring, Logging, and Alarms of system activities

	<ul style="list-style-type: none">● Firmware upgrade through Web browser
VPN Pass through	<ul style="list-style-type: none">● IPSec, PPTP ,L2TP Pass through

Chapter 2: Installation Procedure

In this chapter we are going to introduce hardware installation. Through the understanding of multi-WAN setting process, users can easily setup and manage the network, making security router functioning and having best performance.

2.1 Systematic Setting Process

Users can set up and enable the network by utilizing bandwidth efficiently. The network can achieve the ideal efficiency, block attacks, and prevent security risks at the same time. Through the process settings, users can install and operate Security router easily. This simplifies the management and maintenance, making the user network settings be done at one time. The main process is as below:

Step 1. Hardware installation

Step 2. Login

Step 3. Verify device specification and set up password and time

Step 4. Set WAN connection

Step 5. Set LAN connection: physical port and IP address settings

Step 6. Set QoS bandwidth management: avoid bandwidth occupation

Step 7. Set Firewall: prevent attack and improper access to network resources

Step 8. Other settings: UPnP, DDNS, MAC Clone

Step 9. Management and maintenance settings: Syslog, SNMP, and configuration backup

Step 10. Logout

2.2 Setting Flow Chart

Below is the description for each setting process, and the correspondent contents and purposes.

#	Setting	Content	Purpose
1	Hardware installation	User's demand.	Install Security router hardware based on user physical requirements.
2	Login	Login the device with Web Browser.	Login Security router web-based UI.
3	Verify device specification	Verify Firmware version and working status.	Verify Security router specification, Firmware version and working status.
	Set password and time	Set time and re-new password.	Modify the login password considering safe issue. Synchronize the Security router time with WAN.
4	Set WAN connection	Verify WAN connection setting, bandwidth allocation, and protocol binding.	Connect to WAN. Configure bandwidth to optimize data transmission.
5	Set LAN connection: physical port and IP address settings	Set mirror port and VLAN. Allocate and manage LAN IP.	Provide mirror port, port management and VLAN setting functions. Support Static/DHCP IP allocation to meet different needs. IP group will simplify the management work.
6	Set QoS bandwidth management: avoid bandwidth occupation	Restrict bandwidth and session of WAN ports, LAN IP and application.	To assure transmission of important information, manage and allocate the bandwidth further to achieve best efficiency.
7	Set Firewall: prevent attack and improper access to network resources	Block attack, Set Access rule and restrict Web access.	Administrators can block BT to avoid bandwidth occupation, and enable access rules to restrict employee accessing internet improperly or using MSN, QQ and Skype during working time. They can also protect network from Worm or ARP attacking.
8	Advanced Settings:DMZ/Forwarding, UPnP, DDNS, MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone
9	Management and maintenance settings: Syslog, SNMP, and configuration backup	Monitor Security router working status and configuration backup.	Administrators can look up system log and monitor system status and inbound/outbound flow in real time.
10	Logout	Close configuration	Logout Security router web-based UI.

		window.	
--	--	---------	--

We will follow the process flow to complete the network setting in the following chapters.

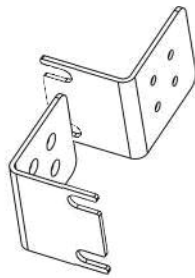
Chapter 3: Hardware Installation

In this chapter we are going to introduce hardware interface as well as physical installation.

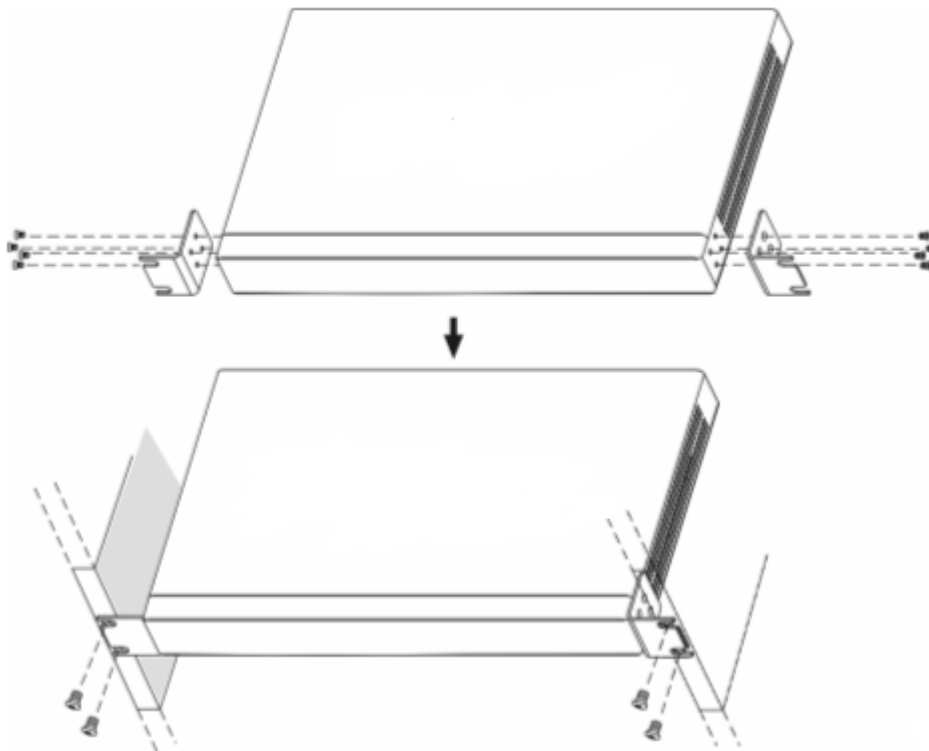
3.1 Installing the Device on a Standard 19" Rack


We suggest to either place the device on a desk or install it in a rack with attached brackets. Do not place other heavy objects together with the device on a rack. Overloading may cause the rack to fail, thus causing damage or danger.

Each device comes with a set of rack installation accessories, including 2 L brackets and 8 screws. Users can rack-mount the device onto the chassis.



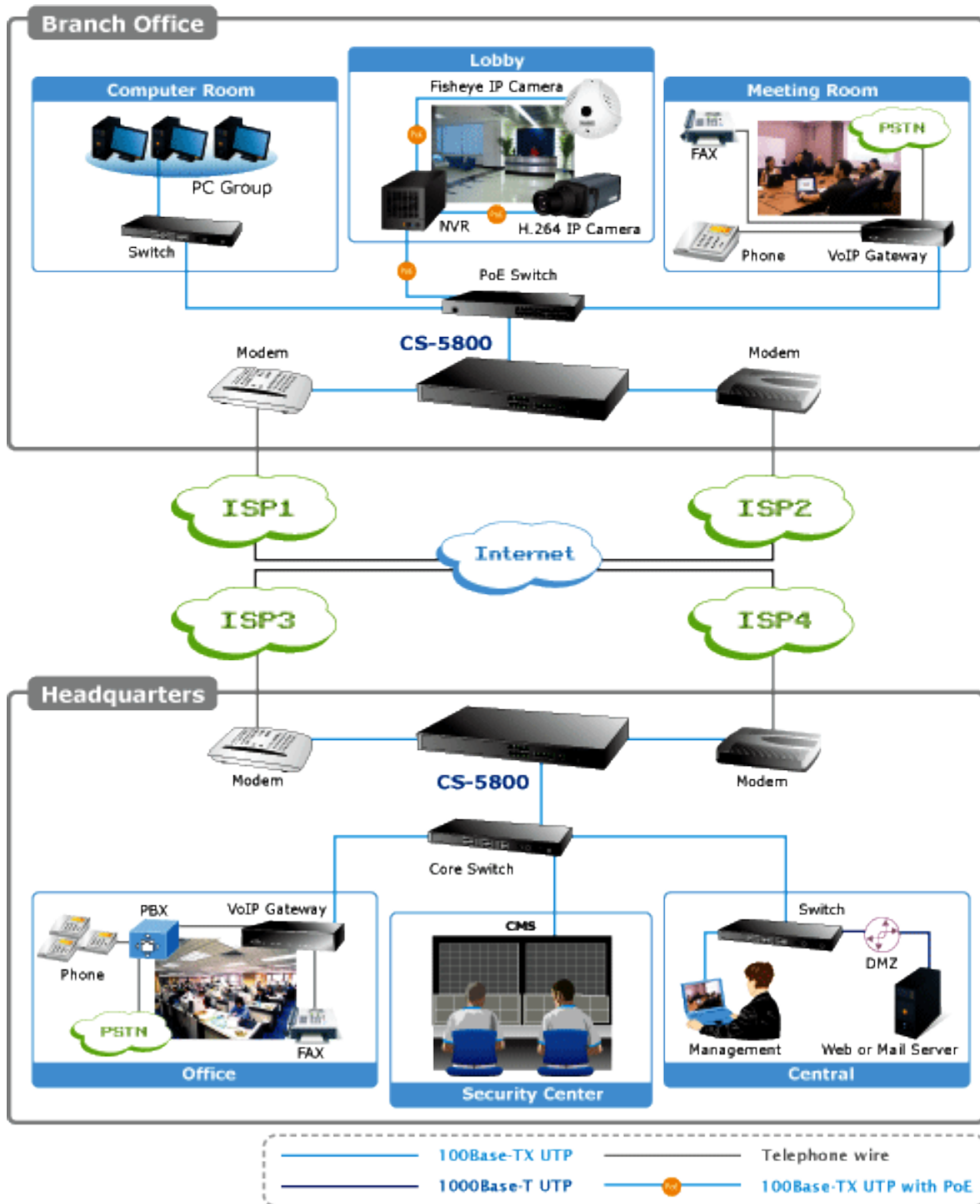
Refer to the figure below for the device installation onto a 19" rack:



 Attention	In order for the device to run smoothly, wherever users install it, be sure not to obstruct the vent on each side of the device. Keep at least 10cm space in front of both the vents for air convection.
---	--

3.2 Security router Network Connection

The device has 4 WAN ports and a hardware DMZ port; therefore, users can connect the device to the Internet, and configure a connection to a Public IP server at the same time.



WAN connection : A WAN port can be connected with xDSL Modem, Fiber Modem, Switching Hub, or through an external router to connect to the Internet.

LAN Connection: The LAN port can be connected to a Switching Hub or directly to a PC. Users can use servers for monitoring or filtering through the port after “Physical Port Management” configuration is done.

DMZ : The DMZ port can be connected to servers that have legal IP addresses, such as Web servers, mail servers, etc.

Chapter 4: Login Security router

This chapter is mainly introducing Web-based UI after connecting Security router.

First, check up Security router IP address by connecting to DOS through the LAN PC under Security router. Go to Start → Run, enter cmd to commend DOS, and enter ipconfig for getting Default Gateway address, as the graphic below, 192.168.1.1. Make sure Default Gateway is also the default IP address of Content Security Router.


```
C:\Documents and Settings\PM01>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : smb.com
    IP Address. . . . .                : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    IP Address. . . . .                : fe80::222:19ff:fe06:b981%9
    Default Gateway . . . . .          : 192.168.1.1


C:\Documents and Settings\PM01>
```

 Attention	When not getting IP address and default gateway by using “ipconfig”, or the received IP address is 0.0.0.0 and 169.X.X.X, we recommend that users should check if there is any problem with the circuits or the computer network card is connected nicely.
---	--

Then, open webpage browser, IE for example, and key in 192.168.1.1 in the website column. The login window will appear as below:



Security router default username and password are both “**admin**”. Users can change the login password in the setting later.

 Attention	For security, we strongly suggest that users must change password after login. Please keep the password safe, or you cannot login to Security router. Press Reset button for more than 10 sec, all the setting will return to default.
---	--

After login, Security router web-based UI will be shown.

Chapter 5: System Status

This chapter introduces the device specification and status after login as well as change password and system time settings for security.

5.1 Home Page

In the Home page, all Security router parameters and status are listed for users' reference.

5.1.1 WAN Status

WAN Status

Interface	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
WAN IP Address	192.168.4.195	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0	---
DNS	192.168.5.121 192.168.5.120	0.0.0.0	0.0.0.0	0.0.0.0	---
Downstream Bandwidth Usage	0	0	0	0	0
Upstream Bandwidth Usage	0	0	0	0	0
DDNS Setup	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	
Quality of Service	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connect	Release Renew	Release Renew	Release Renew	Release Renew	Release Renew

Item	Description
WAN IP Address	Indicates the current IP configuration for WAN port.
Default Gateway	Indicates current WAN gateway IP address from ISP.
DNS	Indicates the current DNS IP configuration.
Downstream Bandwidth Usage(%)	Indicates the current downstream bandwidth usage (%) for each WAN.
Upstream Bandwidth Usage(%)	Indicates the current upstream bandwidth usage (%) for each WAN.
DDNS Setup	Indicates if Dynamic Domain Name is activated. The default configuration is

	"Off".
Quality of Service	Indicates how many QoS rules are set.
Manual Connect	When "Obtain an IP automatically" is selected, two buttons (Release and Renew) will appear. If a WAN connection, such as PPPoE or PPTP, is selected, "Disconnect" and "Connect" will appear.
DMZ IP Address	Indicates the current DMZ IP address.

5.1.2 Physical Port Status

Physical Port Status

Port ID	1	2	3	4	5	6	7	8
Interface	LAN							
Status	Enabled	Connect	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Port ID	Internet	Internet	Internet	Internet	Internet/DMZ
Interface	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
Status	Enabled	Enabled	Enabled	Enabled	Enabled

The status of all system ports, including each connected and enabled port, will be shown on this Home page (see above table). Click the respective status button and a separate window will appear to show detailed data (including setting status summary and statistics) of the selected port.

WAN 1 Information

Summary

Type	10Base-T / 100Base-TX / 1000Base-T
Interface	WAN
Link Status	Down
Physical Port Status	Port Enabled
Priority	Normal
Speed	10 Mbps
Half/Full Duplex	Half
Auto Negotiation	Enabled

Statistics




Received Packets Count	0
Received Packets Byte Count	0
Transmitted Packets Count	0
Transmitted Packets Byte Count	0
Error Packets Count	0

The current port setting status information will be shown in the Port Information Table. Examples: type (10Base-T/100Base-TX/1000Base-T), interface (WAN/ LAN/ DMZ), link status (Up/ Down), physical port status (Port Enabled/ Port Disabled), priority (high or normal), speed status (10Mbps or 100Mbps), duplex status (Half/ Full), auto negotiation (Enabled or Disabled). The table also shows statistics of Receive/ Transmit Packets, Receive/Transmit Packets Byte Count as well as Error Packets Count.

5.1.3 System Information

System Information

LAN IP Address/Subnet Mask	192.168.1.1/255.255.255.0	Serial Number	PLTzBCG3100124232
IPv6 Address/Prefix Length	fc00::1/7	Firmware Version	v1.0.1.01 (May 23 2012 19:26:13)
Working Mode	Gateway	Current Time	Tue Jun 26 2012 16:17:43
System Active Time	1 Days4 Hours56 Minutes42 seconds		

Item	Description		
LAN IP Address/ Subnet Mask	Identifies the current device IP address and subnet mask. The default is 192.168.1.1 and 255.255.255.0		
IPv6 Address/Prefix Length	Identifies the current device IPv6 address and prefix length. The default is fc00::1/7		
Working Mode	Indicates the current working mode. Can be Gateway or Router mode. The default is "Gateway" mode		
System Active time	Indicates how long the device has been running.		
Serial Number:	This number is the device serial number.		
Firmware Version	Information about the device present software version.		
Current Time	Indicates the device present time. <table border="1" data-bbox="502 1169 1428 1312"> <tbody> <tr> <td style="text-align: center;"> Note</td> <td>To have the correct time, users must synchronize the device with the remote NTP server first.</td> </tr> </tbody> </table>	 Note	To have the correct time, users must synchronize the device with the remote NTP server first.
 Note	To have the correct time, users must synchronize the device with the remote NTP server first.		

5.1.4 Security Status

Security Status

Firewall	Status
SPI (Stateful Packet Inspection)	On
DoS (Denial of Service)	On
Block WAN Request	On
Prevent ARP Virus Attack	On
Remote Management	Off
Access Rule	0 rules set

Item	Description
SPI (Stateful Packet	Indicates whether SPI (Stateful Packet Inspection) is on or off. The default

Inspection)	configuration is "On".
DoS (Denial of Service)	Indicates if DoS attack prevention is activated. The default configuration is "On".
Block WAN Request	Indicates that denying the connection from Internet is activated. The default configuration is "On".
Prevent ARP Virus Attack	Indicates that preventing Arp virus attack is activated. The default configuration is "Off".
Remote Management	Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is "Off".
Access Rule	Indicates the number of access rule applied in Security router.

5.1.5 Log Setting Status

Log



Item	Description
Sent Log To	Indicates if Syslog Server is Enabled or Disabled.

5.2 Change and Set Login Password and Time

5.2.1 Password Setting

When you login Security router setting window every time, you must enter the password. The default value for Security router username and password are both "admin". For security reasons, we strongly recommend that you must change your password after first login. Please keep the password safe, or you might not login to Security router. You can press Reset button for more than 10 sec, Security router will return back to default.

Password Setup

User Name	admin
Password	<input type="text"/>
New User Name	admin
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Item	Description
User Name	The default is "admin".
Password	Input the original password. (The default is "admin".)
New User Name	Input the new user name. e.x. Planet
New Password	Input the new password.
Confirm New Password	Input the new password again for verification.
Apply	Click "Apply" to save the configuration.
Cancel	Click "Cancel" to leave without making any change. This action will be effective before "Apply" to save the configuration.

If users have already changed username and password, they should login with current username and password and input "admin" as new username and password if they have to return back to default.

5.2.2 Network Time

Security router can adjust time setting. Users can know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources. You can either select the embedded NTP Server synchronization function or set up a time reference.

Set system time using a NTP server : Security router has embedded NTP server, which will update the time spontaneously.

Network Time

- Set system time using a NTP server.
 Set system time manually.

Time Zone	Beijing (GMT+08:00) ▼
Daylight Saving	<input type="checkbox"/> Enabled from 06 (Month) 25 (Day) to 12 (Month) 25 (Day)
NTP Server	time.nist.gov

Item	Description
Time Zone	Select your location from the pull-down time zone list to show correct local time.
Daylight Saving	If there is Daylight Saving Time in your area, input the date range. The device will adjust the time for the Daylight Saving period automatically.
NTP Server	If you have your own preferred time server, input the server IP address.
Apply	After the changes are completed, click " Apply " to save the configuration.
Cancel	Click " Cancel " to leave without making any change. This action will be effective before "Apply" to save the configuration.

Select System Time Manually: Input the correct time, date, and year in the boxes.

- Set system time using a NTP server.
 Set system time manually.

<input type="text" value="17"/>	Hours	<input type="text" value="0"/>	Minutes	<input type="text" value="12"/>	seconds
<input type="text" value="3"/>	Month	<input type="text" value="3"/>	Day	<input type="text" value="2011"/>	Year

After the changes are completed, click "**Apply**" to save the configuration. Click "**Cancel**" to leave without making any change. This action will be effective before "Apply" to save the configuration.

Chapter 6: Network

This Network page contains the basic settings. For most users, completing this general setting is enough for connecting with the Internet. However, some users need advanced information from their ISP. Please refer to the following descriptions for specific configurations.

6.1 Network Connection

6.1.1 Host Name and Domain Name

Host Name :	Gigabit Content Security Router (Required by some ISPs)
Domain Name :	planet.com (Required by some ISPs)

Device name and domain name can be input in the two boxes. Though this configuration is not necessary in most environments, some ISPs in some countries may require it.

6.1.2 IP Mode

Choose the type of addressing to use on your network:

IP Mode		
Mode	WAN	LAN
<input checked="" type="radio"/> IPv4 Only	IPv4	IPv4
<input type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4 Only: Use only IPv4 addressing.

Dual-Stack IP: Use IPv4 and IPv6 addressing. So that you can configure both IPv4 and IPv6 addresses for LAN, WAN, and DMZ settings on this page.

6.1.3 LAN Setting

6.1.3.1 IPv4 Only

IPv4	IPv6						
LAN Setting							
<table border="1"> <tr> <td colspan="2">MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)</td> </tr> <tr> <td>Device IP Address : 192 . 168 . 1 . 1</td> <td>Subnet Mask : 255 . 255 . 255 . 0</td> </tr> <tr> <td colspan="2" style="text-align: center;">Multiple Subnet Setting:Enabled</td> </tr> </table>		MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)		Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0	Multiple Subnet Setting:Enabled	
MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)							
Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0						
Multiple Subnet Setting:Enabled							
<input type="button" value="Unified IP Management"/>							

This is configuration information for CS-5800 current LAN IP address. The default configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. It can be changed according to the actual network structure.

Multiple-Subnet Setting : (IPv4 Only)

Click "Unified IP Management" to enter the configuration page, as shown in the following figure. Input the respective IP addresses and subnet masks.

LAN Setting							
<table border="1"> <tr> <td colspan="2">MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)</td> </tr> <tr> <td>Device IP Address : 192 . 168 . 1 . 1</td> <td>Subnet Mask : 255 . 255 . 255 . 0</td> </tr> <tr> <td colspan="2" style="text-align: center;">Multiple Subnet Setting:Enabled</td> </tr> </table>		MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)		Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0	Multiple Subnet Setting:Enabled	
MAC Address 00 - 30 - 4F - 00 - A4 - F7 (Default00-30-4f-00-a4-f7)							
Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0						
Multiple Subnet Setting:Enabled							
<input type="button" value="Unified IP Management"/>							

This is configuration information for the device current LAN IP address. The default configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. It can be changed according to the actual network structure.

LAN Setting

Device IP Address . . . Subnet Mask . . .

Multiple Subnet Setting Multiple Subnet

LAN IP Address . . .

Subnet Mask . . .

Dynamic IP

Enable DHCP Server

	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
IP Range Starts	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="100"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="100"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="3"/> . <input type="text" value="100"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="4"/> . <input type="text" value="100"/>
IP Range Ends	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="149"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="2"/> . <input type="text" value="149"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="3"/> . <input type="text" value="149"/>	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="4"/> . <input type="text" value="149"/>

This function enables users to input IP segments that differ from the router network segment to the multi-net segment configuration; the Internet will then be directly accessible. In other words, if there are already different IP segment groups in the Intranet, the Internet is still accessible without making any changes to internal PCs. Users can make changes according to their actual network structure.

61.3.2 Dual-Stack IP (IPv4 and IPv6)

Users have to enable **Dual-Stack IP** in the IP mode section in advance to configure IPv6. Then click the **IPv6** tab, and then enter the IPv6 Address and the Prefix Length. The default IP address is **fc00::1**, and the default prefix length is **7**. It can be changed according to the actual network structure.

IP Mode

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

LAN Setting

IPv6 Address : fc00::1

Prefix Length : 7

Click “Unified IP Management” to enter the configuration page, as shown in the following figure. Input the respective IP addresses and subnet masks.

LAN Setting

IPv6 Address Prefix Length

Dynamic IP

 Enable DHCP Server

	Subnet1
DHCP Server	<input checked="" type="checkbox"/> Enable
IP Range Starts	<input type="text" value="fc00::100"/>
IP Range Ends	<input type="text" value="fc00::17f"/>



Note

To configure global IPv6 prefixes for your LAN devices, go to the WAN Setting, click the **IPv6** tab, and click **Edit** for the WAN interface. Then enter the LAN IPv6 Address.

After the changes are completed, click “**Apply**” to save the configuration. Click “**Cancel**” to leave without making any change.

6.1.4 WAN & DMZ Settings

6.1.4.1 IPv4 Only

WAN Setting

WAN Setting

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	Edit
WAN 2	Obtain an IP automatically	Edit
WAN 3	Obtain an IP automatically	Edit
WAN 4	Obtain an IP automatically	Edit
WAN 5	Obtain an IP automatically	Edit

Item	Description
Interface	An indication of which port is connected.
Connection Type	Obtain an IP automatically, Static IP connection, PPPoE (Point-to-Point Protocol over Ethernet), PPTP (Point-to-Point Tunneling Protocol) or Transparent Bridge.
Config	A modification in an advanced configuration: Click Edit to enter the advanced configuration page.

Obtain an Automatic IP automatically

This mode is often used in the connection mode to obtain an automatic DHCP IP. This is the device system default connection mode. It is a connection mode in which DHCP clients obtain an IP address automatically. If having a different connection mode, please refer to the following introduction for selection of appropriate configurations. Users can also set up their own DNS IP address. Check the options and input the user-defined DNS IP addresses.

Interface:

WAN Connection Type:

Use the Following DNS Server Addresses

DNS Server(Required): . . .

DNS Server(Optional): . . .

Shared-Circuit WAN environment: Yes NO (Filter broadcast packets from WAN)

MTU: Auto Manual bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from : to : (24-Hour Format)

Line-Dropped Scheduling: minutes ahead line-dropped to start new session transferring

Backup Interface:

Item	Description
Use the following DNS Server Addresses:	Select a user-defined DNS server IP address.
DNS Server:	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable groups are two IP groups.
Enable Line-Dropped Scheduling:	<p>The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example:</p> <p>The optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet.</p> <p>Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.</p>
Line-Dropped Period	Input the time rule for disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU:	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

Static IP

If an ISP issues a static IP (such as one IP or eight IP addresses, etc.), please select this connection mode and follow the steps below to input the IP numbers issued by an ISP into the relevant boxes.

Interface: **WAN 1**

WAN Connection Type : Static IP

WAN IP Address : . . .

Subnet Mask : . . .

Default Gateway : . . .

DNS Server(Required) : . . .

DNS Server(Optional) : . . .

Shared-Circuit WAN environment : Yes NO (Filter broadcast packets from WAN)

MTU : Auto Manual bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from : to : (24-Hour Format)

Line-Dropped Scheduling : minutes ahead line-dropped to start new session transferring

Backup Interface : disable

Item	Description
WAN IP address	Input the available static IP address issued by ISP.
Subnet Mask	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway	Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.
DNS Server	Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.

Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

PPPoE

This option is for an ADSL virtual dial-up connection (suitable for ADSL PPPoE). Input the user connection name and password issued by ISP. Then use the PPP Over-Ethernet software built into the device to connect with the Internet. If the PC has been installed with the PPPoE dialing software provided by ISP, remove it. This software will no longer be used for network connection.

Interface: WAN 1

WAN Connection Type : PPPoE

UserName :

Password :

Connect on Demand: Max Idle Time Min.

Keep Alive: Redial Period Sec.

Shared-Circuit WAN environment : Yes NO (Filter broadcast packets from WAN)

MTU : Auto Manual bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from : to : (24-Hour Format)

Line-Dropped Scheduling : minutes ahead line-dropped to start new session transferring

Backup Interface :

Item	Description
User Name	Input the user name issued by ISP.
Password	Input the password issued by ISP.
Connect on Demand	This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break-off resulting from no packet transmissions is five minutes).
Keep Alive	This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is disconnected. It also enables a user to set up a time for redialing. The default is 30 seconds.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click **“Apply”** to save the configuration, or click **“Cancel”** to leave without making any change.

PPTP

This option is for the PPTP time counting system. Input the user's connection name and password issued by ISP, and use the built-in PPTP software to connect with the Internet.

Interface: WAN 1

WAN Connection Type : PPTP

WAN IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255 . 255 . 255 . 0

Default Gateway : 0 . 0 . 0 . 0

UserName :

Password :

Connect on Demand: Max Idle Time 5 Min.

Keep Alive: Redial Period 30 Sec.

Shared-Circuit WAN environment : Yes NO (Filter broadcast packets from WAN)

MTU : Auto Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling : 5 minutes ahead line-dropped to start new session transferring

Backup Interface : disable

Item	Description
WAN IP Address	This option is to configure a static IP address. The IP address to be configured could be one issued by ISP. (The IP address is usually provided by the ISP when the PC is installed. Contact ISP for relevant information).
Subnet Mask	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway Address	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
User Name	Input the user name issued by ISP.

Password	Input the password issued by ISP.
Connect on Demand	This function enables the auto-dialing function to be used for a PPTP dial connection. When the client port attempts to connect with the Internet, the device will automatically connect with the default ISP auto dial connection; when the network has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break off when no packets have been transmitted is five minutes).
Keep Alive	This function enables the PPTP dial connection to redial automatically when the connection has been disconnected. Users can set up the redialing time. The default is 30 seconds.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

Transparent Bridge

If all Intranet IP addresses are applied as Internet IP addresses, and users don't want to substitute private network IP addresses for all Intranet IP addresses (ex. 192.168.1.X), this function will enable users to integrate existing networks without changing the original structure. Select the Transparent Bridge mode for the WAN connection mode. In this way, users will be able to connect normally with the Internet while keeping the original Internet IP addresses in Intranet IP configuration.

If there are two WANs configured, users still can select Transparent Bridge mode for WAN connection mode, and load balancing will be achieved as usual.

Interface: WAN 1

WAN Connection Type: Transparent Bridge ▼

WAN IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS Server(Required): 0 . 0 . 0 . 0

DNS Server(Optional): 0 . 0 . 0 . 0

Internal LAN IP Range 1: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 2: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 3: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 4: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 5: 0 . 0 . 0 . 0 to 0

Shared-Circuit WAN environment: Yes NO (Filter broadcast packets from WAN)

MTU: Auto Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling: 5 minutes ahead line-dropped to start new session transferring

Backup Interface: disable ▼

Back
Apply
Cancel

Item	Description
WAN IP Address	Input one of the static IP addresses issued by ISP.
Subnet Mask	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway Address	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.

DNS Server	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
Internal LAN IP Range	Input the available IP range issued by ISP. If ISP issued two discontinuous IP address ranges, users can input them into Internal LAN IP Range 1 and Internal LAN IP Range 2 respectively.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
Line-Dropped Period:	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling:	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

Router Plus NAT Mode:

When you apply a public IP address as your default gateway, you can setup this public IP address into a LAN PC, and this PC can use this public IP address to reach the Internet. Others PCs can use NAT mode to reach the Internet.

If this WAN network is enabled the Router plus NAT mode, you can still use load balancing function in this WAN network.

Interface: WAN 1

WAN Connection Type: Router Plus NAT Mode ▼

WAN IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS Server(Required): 0 . 0 . 0 . 0

DNS Server(Optional): 0 . 0 . 0 . 0

LAN Default Gateway 1: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 0 . 0 . 0 . 0 to 0

LAN Default Gateway 2: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 0 . 0 . 0 . 0 to 0

LAN Default Gateway 3: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 0 . 0 . 0 . 0 to 0

Shared-Circuit WAN environment: Yes NO (Filter broadcast packets from WAN)

MTU: Auto Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling: 5 minutes ahead line-dropped to start new session transferring

Backup Interface: disable ▼

Back Apply Cancel

Item	Description
WAN IP address	Enter the public IP address.
Subnet mask	Enter the public IP address subnet mask.

WAN default gateway	Enter the WAN default gateway, which provided by your ISP.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
Intranet routing default gateway	Enter one of IP addresses that provide by the ISP as your default gateway.
Intranet IP addresses range	Enter your IP addresses range, which IP addresses are provided by ISP. If you have multiple IP ranges, you need setup group1 and group 2. You can also setup the default gateway and IP range in the group 2.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
Line-Dropped Period	Input the time rule for disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment:	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

Click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

6.1.4.2 Dual-Stack IP (IPv4 and IPv6)

Users have to enable **Dual-Stack IP** in the IP mode section in advance to configure the WAN with IPv6 addressing.

Obtain an Automatic IP automatically:

This mode is often used in the connection mode to obtain an automatic DHCP IP. This is the device system default connection mode. It is a connection mode in which DHCP clients obtain an IP address automatically. If having a different connection mode, please refer to the following introduction for selection of appropriate configurations. Users can also set up their own DNS IP address. Check the options and input the user-defined DNS IP addresses.

Interface: WAN 1

WAN Connection Type : Obtain an IP automatically ▼

Use the Following DNS Server Addresses

DNS Server(Required) : ::

DNS Server(Optional) : ::

MTU : Auto Manual bytes

Item	Description
Use the Following DNS Server Addresses	Select an user-defined DNS server IP address.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
MTU	<p>“Auto” and “Manual” can be chosen. The default value is 1500. Different value could be set in different network environment.</p> <p>(e.g. ADSL PPPoE MTU: 1492)</p> <p>The default is “Auto”.</p>
Use the Following DNS Server Addresses	Select an user-defined DNS server IP address.

Static IP:

If an ISP issues a static IP (such as one IP or eight IP addresses, etc.), please select this connection mode and follow the steps below to input the IP numbers issued by an ISP into the relevant boxes.

Interface: WAN 1

WAN Connection Type: Static IP

WAN IP Address: ::

Prefix Length: 64

Default Gateway: ::

DNS Server(Required): ::

DNS Server(Optional): ::

MTU: Auto Manual 1500 bytes

Item	Description
WAN IP Address	Input the available static IP address issued by ISP.
Prefix Length	The prefix length specified by your ISP.
Default Gateway	Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
MTU	<p>“Auto” and “Manual” can be chosen. The default value is 1500. Different value could be set in different network environment.</p> <p>(e.g. ADSL PPPoE MTU: 1492)</p> <p>The default is “Auto”.</p>

Click **“Apply”** to save the configuration, or click **“Cancel”** to leave without making any changes.

DMZ Setting

For some network environments, an independent Configurable DMZ port may be required to set up externally connected servers such as WEB and Mail servers. Therefore, the device supports a set of independent Configurable DMZ ports for users to set up connections for servers with real IP addresses. The DMZ ports act as bridges between the Internet and LANs.

DMZ Setting

Interface	IP Address	Config.
DMZ	0.0.0.0	Edit

Item	Description
IP address	Indicates the current default static IP address.
Config.	Indicates an advanced configuration modification: Click Edit to enter the advanced configuration page.

The DMZ configuration can be classified by Subnet and Range:

Subnet

The DMZ and WAN located in different Subnets .For example: If the ISP issued 16 real IP addresses: 220.243.230.1-16 with Mask 255.255.255.240, users have to separate the 16 IP addresses into two groups: 220.243.230.1-8 with Mask 255.255.255.248, and 220.243.230.9-16 with Mask 255.255.255.248 and then set the device and the gateway in the same group with the other group in the DMZ.

Interface

Subnet
 Range (DMZ & WAN within same subnet)

Specify DMZ IP Address

Subnet Mask

Item	Description
Specify DMZ IP Address	Enter the DMZ Port IP Address
Subnet Mask	Enter the DMZ Port Subnet Mask

Range

DMZ and WAN are within same Subnet

Interface

Subnet

Range (DMZ & WAN within same subnet)

Interface

IP Range for DMZ port to

Item	Description
Interface	Select a WAN Port witch is the same subnet with DMZ
IP Range for DMZ port	Input the IP range located at the DMZ port.

After the changes are completed, click “**Apply**” to save the configuration, or click “**Cancel**” to leave without making any changes.

6.2 Multi- WAN Setting

6.2.1 Load Balance Mode

Mode

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session <input type="radio"/> By IP	Advanced Function
Unbinding WAN Balance	Un-binding WAN Balance Mode:	<input type="radio"/> By Session <input type="radio"/> By IP	Advanced Function
Strategy Routing	Mode:	<input type="radio"/> By Session <input type="radio"/> By IP	Advanced Function
<div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin: 0;">Set WAN Grouping</p> <p>Strategy Routing Disabled ▼ Import IP Range</p> <p>Self-defined Strategy 1 Disabled ▼</p> <p>Self-defined Strategy 2 Disabled ▼</p> </div>			

Auto Load Balance Mode

When Auto Load Balance mode is selected, the device will use sessions or IP and the WAN bandwidth automatically allocate connections to achieve load balancing for external connections. The network bandwidth is set by what users input for it. For example, if the upload bandwidth of both WANs is 512Kbit/sec, the automatic load ratio will be 1:1; if one of the upload bandwidths is 1024Kbit/sec while the other is 512Kbit/sec, the automatic load ratio will be 2:1. Therefore, to ensure that the device can balance the actual network load, please input real upload and download bandwidths.

Item	Description
Session Balance	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
IP Session Balance	If "By IP" is selected, the WAN bandwidth will automatically allocate connections based on IP amount to achieve network load balance.

Note

For either session balancing or IP connection balancing, collocation with Protocol Binding will provide a more flexible application for bandwidth. Users can assign a specific Intranet IP to go through a specific service provider for connection, or assign an IP for a specific destination to go through the WAN users assign to connect with the Internet.

For example, if users want to assign IP 192.168.1.100 to go through WAN 1 when connecting with the Internet, or assign all Intranet IP to go through WAN 2 when connecting with servers with port 80, or assign all Intranet IP to go through WAN 1 when connecting with IP 211.1.1.1, users can do that by configuring "Protocol Binding".

Attention

When the Auto Load Balance mode is collocated with Protocol Binding, only IP addresses or servers that are configured in the connection rule will follow the rule for external connections; those which are not configured in the rule will still follow the device Auto Load Balance system.

Please refer to the explanations in 6.2.3 Configuring Protocol Binding for setting up Protocol Binding and for examples of collocating router modes with Protocol Binding.

Unbinding WAN Balance Mode

This mode enables users to assign specific intranet IP addresses, destination application service ports or destination IP addresses to go through an assigned WAN for external connection. After being assigned, the specific WAN will only support those assigned Intranet IP addresses, specific destination application service ports, or specific destination IP addresses. Intranet IP, specific destination application service ports and specific destination IP that is not configured under the rules will go through other WANs for external connection. For unassigned WANs, users can select Load Balance mode and select session or IP for load balancing.

Item	Description
Session Balance:	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
IP Balance:	If "By IP" is selected, the WAN bandwidth will automatically allocate connections based on the number of IP addresses to achieve network load balance.



Note

Only when a device assignment is collocated with Protocol Binding can the balancing function be brought into full play. For example, an assignment requiring all Intranet IP addresses to go through WAN 1 when connecting with service port 80, or go through WAN 1 when connecting with IP 211.1.1.1, must be set up in the Protocol Binding Configuration.



Attention

When assigning mode is selected, as in the above example, the IP(s) or service provider(s) configured in the connection rule will follow the rule for external connections, but those which are not configured in the rule will still follow the device Load Balance system to go through other WAN ports to connect with the Internet.

Please refer to the explanations in **6.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding

Strategy Routing Mode

If strategy Routing is selected, the device will automatically allocate external connections based on routing policy (Division of traffic between Telecom and Netcom is to be used in China) embedded in the device. All you have to do is to select the WAN (or WAN group) which is connected with Netcom; the device will then automatically dispatch the traffic for Netcom through that WAN to connect with the Internet and dispatch traffic for Telecom to go through the WAN connected with Telecom to the Internet accordingly. In this way, the traffic

for Netcom and Telecom can be divided.

Set WAN Grouping

If more than one WAN is connected with Netcom, to apply a similar division of traffic policy to these WANs, a combination for the WANs must be made. Click “**Set WAN Grouping**”; an interactive window as shown in the figure below will be displayed.

The screenshot shows a configuration window titled "Set WAN Grouping". On the left side, there is a "Name" field with a text input box. Below it is the "Interface" section, which contains four checkboxes labeled "WAN1", "WAN2", "WAN3", and "WAN4". At the bottom of this section are two buttons: "Add to list" and "Delete selected". To the right of these elements is a large empty rectangular box. At the very bottom of the window are three buttons: "Apply", "Cancel", and "Exit".

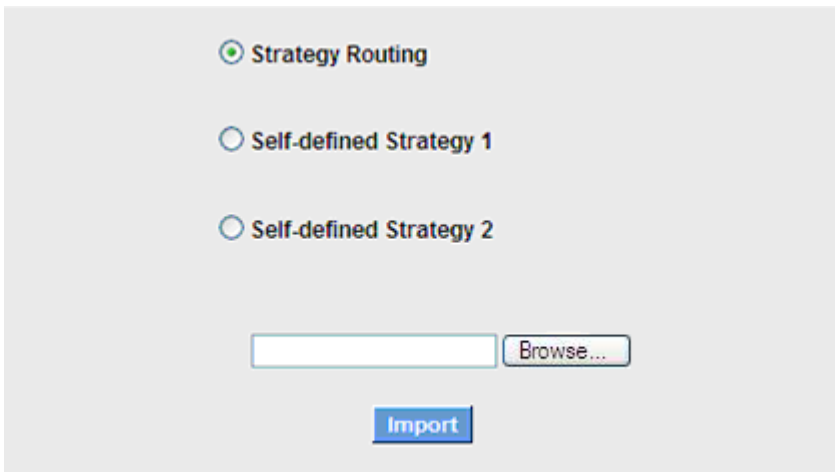
Item	Description
Name	To define a name for the WAN grouping in the box, such as “Education” etc. The name is for recognizing different WAN groups.
Interface	Check the boxes for the WANs to be added into this combination.
Add To List	To add a WAN group to the grouping list.
Delete selected Item	To remove selected WANs from the WAN grouping.
Apply	Click “Apply” to save the modification.
Close	Click “Cancel” to cancel the modification. This only works before “Apply” is clicked.

After the configuration is completed, in the China Netcom Policy window users can select WANs in combination to connect with Netcom.

Import Strategy

A division of traffic policy can be defined by users too. In the "Import Strategy" window, select the WAN or WAN group (ex. WAN 1) to be assigned and click the "Import IP Range" button; the dialogue box for document importation will be displayed accordingly.

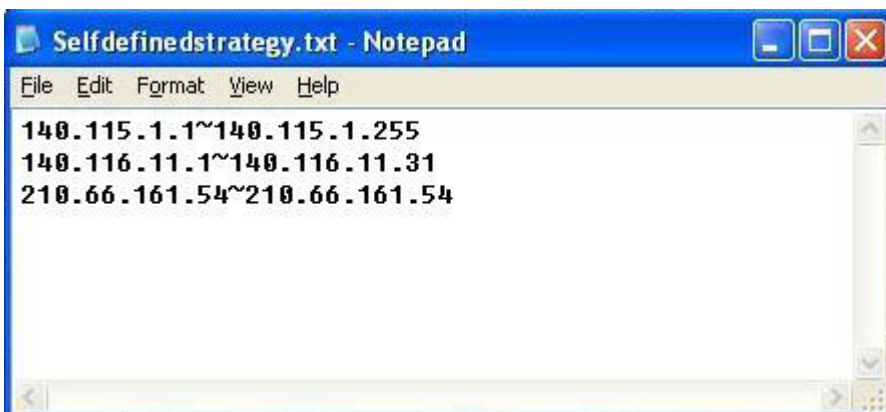
A policy document is an editable text document. It may contain a destination IP users designated. After the path for document importation has been selected, click "Import", and then at the bottom of the configuration window click "Apply". The device will then dispatch the traffic to the assigned destination IP through the WAN (ex. WAN 1) or WAN grouping users designated to the Internet.



To build a policy document users can use a text-based editor, such as Notepad, which is included with Windows system. Follow the text format in the figure below to key in the destination IP addresses users want to assign.

For example, if the destination IP address range users want to designate is 140.115.1.1 ~ 140.115.1.255, key in 140.115.1.1 ~ 140.115.1.255 in Notepad. The next destination IP address range should be keyed in the next line. Attention! Even if only one destination IP address is to be assigned, it should follow the same format.

For example, if the destination IP address is 210.66.161.54, it should be keyed in as 210.66.161.54~210.66.161.54. After the document has been saved (the extension file name is .txt), users can import the IP range of self-defined strategy.



**Note**

China Netcom strategy and self-defined strategy can coexist. However, if a destination IP is assigned by both China Netcom strategy and self-defined strategy, China Netcom strategy will take priority. In other words, traffic to that destination IP will be transmitted through the WAN (or WAN group) under China Netcom strategy.

Session Balance Advanced Function

In general, session balance is to equally and randomly distribute the session connections of each intranet IP. For some special connections, for example, web banking encrypted connection (Https or TCP443), is required to connect from the same WAN IP. If one intranet IP visits web banking website and the connection is distributed into different WAN IP addresses, there will be disconnection or failure. Session balance advanced function targets at solving this issue.

Session balance advanced function can set the same intranet IP keeps having sessions from the same WAN IP for some specific service protocols. Other service protocols can still adopt the original balance mechanism to distribute the sessions equally and randomly. With the original session balance efficiency, advanced function can ensure the connection running without error for some special service protocols.

Mode

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session	Advanced Function	<input type="radio"/> By IP
Unbinding WAN Balance	Un-binding WAN Balance Mode:	<input type="radio"/> By Session	Advanced Function	<input type="radio"/> By IP
Strategy Routing	Mode:	<input type="radio"/> By Session	Advanced Function	<input type="radio"/> By IP
Set WAN Grouping				
Strategy Routing		Disabled	Import IP Range	
Self-defined Strategy 1		Disabled		
Self-defined Strategy 2		Disabled		

Click "Advanced Function" to enter the setting window:

Destination Auto Binding
 User Define Dest. IP or Port Auto Binding

No Aging Time

Protocol : ▾


Port Range : to


TCP[1863~1863]
 TCP[5050~5050]
 UDP[8000~8005]

Item	Description
Destination Auto Binding	Indicates that the session will be connected with the same WAN IP when the destination IP is in the same Class B range.

For example, there are WAN1-1 200.10.10.1 and WAN2- 200.10.10.2, and two intranet IP addresses. When 192.168.1.100 visits Internet 61.222.81.100 for the first time, the connection is through WAN1- 200.10.10.1. If the next destination is to 61.222.81.101 (in the same Class B range), the connection will also be through WAN1- 200.10.10.1. If the destination is to other IP not in the same Class B range as 61.222.81.100, the session will be distributed in the original session balance mechanism.

When the other intranet IP 192.168.1.101 visits 61.222.81.101 for the first time, the connection is through WAN2- 200.10.10.2. If the next destination is to 61.222.81.100 (in the same Class B range), the connection will also be through WAN2 200.10.10.2. If the destination is to other IP not in the same Class B range as 61.222.81.100), the session will be distributed in the original session balance mechanism.

 Note	<p>Not all intranet IP will visit the same Class B range with the same WAN IP. It depends on which WAN the first connection goes to. If the destination IP is in the same Class B range, the connection will go through with the same WAN IP based on the first time learning.</p>
--	--

Item	Description
<p>User Define Dis. Or Port Auto Binding</p>	<p>Indicates that the intranet IP will connect through the same WAN IP when the service ports are self- defined. You can self- define the service ports and destination IP. (If the destination IP is set as 0.0.0.0 to 0, this represents that the destination is to any IP range.)</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center; vertical-align: middle;">  Note </p> <p>You can only choose either Destination Auto Binding or User Define Dis. Or Port Auto Binding.</p> </div>

Take default rules for example:

Destination Auto Binding
 User Define Dest. IP or Port Auto Binding

Service : All Traffic [TCP&UDP/1~65535] ▼

Service Management

Dest. IP ▼ . . .

Enable :

Add to list

HTTPS [TCP/443~443]->0.0.0.0~0.0.0.0

Delete selected Entry

Apply
Cancel
Exit

When any intranet IP connects with TCP443 port or any destination (0.0.0.0 to 0 represents any destination), it will go through the same WAN IP. As for which WAN will be selected, this follows the first- chosen WAN IP distributed by the original session balance mechanism.

For example, there are two intranet IP- 192.168.100.1 and 192.168.100.2. When these intranet IPs first connects with TCP443 port, 192.168.100.1 will go through WAN1, and 192.168,100.2 will go through WAN2. Afterwards, 192.168.100.1 will go through WAN1 when there are TCP443 port connections. 192.168.100.2 will go through WAN2 when there are TCP443 port connections. This rule is by default. You can delete or add rules to meet your connection requirement.

6.2.2 Network Detection Service

This is a detection system for network external services. If this option is selected, information such “**Retry**” or “**Retry Timeout**” will be displayed. If two WANs are used for external connection, be sure to activate the NSD system, so as to avoid any unwanted break caused by the device misjudgment of the overload traffic for the WAN.

▶ Network Service Detection

Interface	WAN 1
<input checked="" type="checkbox"/> Enable	
Retry count	5
Retry timeout	30 seconds
When Fail	Remove the Connection
<input checked="" type="checkbox"/> When In <input type="checkbox"/> OR <input checked="" type="checkbox"/> Out bandwidth is over 1 %, regarded as normal.	
<input checked="" type="checkbox"/> Default Gateway	
<input type="checkbox"/> ISP Host	
<input type="checkbox"/> Remote Host	
<input type="checkbox"/> DNS Lookup Host	

Item	Description
Interface	Select the WAN Port that enables Network Service Detection.
Retry	This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured “Retry Times”, it will be judged as “External Connection Disconnected”.
Retry Timeout	Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.
When Fail	(1) Generate the Error Condition in the System Log: If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections.

	<p>This option is suitable under the condition that one of the WAN connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination.</p> <p>For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 is not to support these destinations, users should select this option. When the WAN1 connection is disconnected, packets for 10.0.0.1~10.254.254.254 cannot be transmitted through WAN 2, and there is no need to remove the connection when WAN 1 is disconnected.</p> <p>(2) Keep System Log and Remove the Connection: If an ISP connection failure is detected, no error message will be recorded in the System Log. The packet transmitted through this WAN will be shifted to the other WAN automatically, and be shifted back again when the connection for the original WAN is repaired and reconnected.</p> <p>This option is suitable when one of the WAN connections fails and the traffic going through this WAN to the destination IP should go through the other WAN to reach the destination. In this way, when any of the WAN connections is broken, other WANs can serve as a backup; traffic can be shifted to a WAN that is still connected.</p>
Default Gateway	<p>The local default communication gateway location, such as the IP address of an ADSL router, will be input automatically by the device. Therefore, users just need to check the option if this function is needed. Attention! Some gateways of an ADSL network will not affect packet detection. If users have an optical fiber box, or the IP issued by ISP is a public IP and the gateway is located at the port of the net café rather than at the IP provider's port, do not activate this option.</p>
ISP Host	<p>This is the detected location for the ISP port, such as the DNS IP address of ISP. When configuring an IP address for this function, make sure this IP is capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port)</p>
Remote Host	<p>This is the detected location for the remote Network Segment. This Remote Host IP should better be capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port).</p>
DNS Lookup	<p>This is the detect location for DNS. (Only a web address such as</p>
Host	<p>www.hinet.net is acceptable here. Do not input an IP address.) In addition, do not input the same web address in this box for two different WANs.</p>

**Note**

In the load balance mode for Assigned Routing, the first WAN port (WAN1) will be saved for the traffic of the IP addresses or the application service ports that are not assigned to other WANs (WAN2, WAN3, and WAN4). Therefore, in this mode, we recommend assigning one of the connections to the first WAN. When other WANs (WAN2, WAN3, or WAN4) are broken and connection error remove (Remove the Connection) has been selected for the connection detection system, traffic will be shifted to the first WAN (WAN1). In addition, if the first WAN (WAN1) is broken, the traffic will be shifted to other WANs in turn. For example, the traffic will be shifted to WAN2 first; if WAN2 is broken too, the traffic will be shifted to WAN3, and so on.

6.2.3 Protocol Binding

WAN Setting

The Security router allows maximum four WAN interface, the bandwidth and real connection of every WAN will impact the load balance mechanism; therefore you need to set the Bandwidth and the Network service detection by each WAN Port correctly. In “**Interface Configuration**”, click “**Edit**” to enter the WAN port configuration.

WAN Setting

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	Edit
WAN 2	Obtain an IP automatically	Edit
WAN 3	Obtain an IP automatically	Edit
WAN 4	Obtain an IP automatically	Edit
WAN 5	Obtain an IP automatically	Edit

Bandwidth Management

When Auto Load Balance mode is selected, the WAN bandwidth will automatically allocate connections through sessions or IP to achieve load balancing for external connections. The network bandwidth is set by what users input for it. For example, if the upload bandwidth of both WANs is 512Kbit/sec, the automatic load ratio will be 1:1; if one of the upload bandwidths is 1024Kbit/sec, while the other is 512Kbit/sec, the automatic load ratio will be 2:1. Therefore, to ensure that the device can balance the actual network load, please input real upload and download bandwidths.

The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	10000	10000
WAN 2	10000	10000
WAN 3	10000	10000
WAN 4	10000	10000
WAN 5	10000	10000

Protocol Binding

Users can define specific IP addresses or specific application service ports to go through a user-assigned WAN for external connections. For any other unassigned IP addresses and services, WAN load balancing will still be carried out.

**Note**

In the load balance mode of Assigned Routing, the first WAN (WAN1) cannot be assigned. It is to be saved for the IP addresses and the application Service Ports that are not assigned to other WANs (WAN2, WAN3, and WAN4) for external connections. In other words, the first WAN (WAN1) cannot be configured with the Protocol Binding rule. This is to avoid a condition where all WANs are assigned to specific Intranet IP or Service Ports and destination IP, no more WAN ports will be available for other IP addresses and Service Ports.

Protocol Binding

Show Priority

Service : All Traffic [TCP&UDP/1~65535] ▼

Service Management

Source IP ▼ 192 . 168 . 1 . to

Dest. IP ▼ . . . to

Interface : WAN 1 ▼

Enabled :


Move Up
Add to list
Move Down

Delete selected item

Show Table Apply Cancel

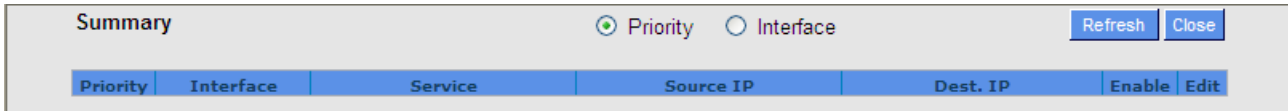
Item	Description
Service	<p>This is to select the Binding Service Port to be activated. The default (such as ALL-TCP&UDP 0~65535, WWW 80~80, FTP 21 to 21, etc.) can be selected from the pull-down option list. The default Service is All 0~65535.</p> <p>Option List for Service Management: Click the button to enter the Service Port configuration page to add or remove default Service Ports on the option list.</p>
Source IP	<p>Users can assign packets of specific Intranet virtual IP to go through a specific WAN port for external connection. In the boxes here, input the Intranet virtual IP address range; for example, if 192.168.1.100~150 is input, the binding range will be 100~150. If only specific Service Ports need to be designated, while specific IP designation is not necessary, input "0" in the IP boxes.</p>
Destination IP	<p>In the boxes, input an external static IP address. For example, if connections to destination IP address 210.11.1.1 are to be restricted to WAN1, the external static IP address 210.1.1.1 ~ 210.1.1.1 should be input. If a range of destinations is to be assigned, input the range such as 210.11.1.1 ~ 210.11.255.254. This means the Class B Network Segment of 210.11.x.x will</p>

	be restricted to a specific WAN. If only specific Service Ports need to be designated, while a specific IP destination assignment is not required, input "0" into the IP boxes.
Interface	Select the WAN for which users want to set up the binding rule.
Enable	To activate the rule.
Add To List	To add this rule to the list.
Delete selected application	To remove the rules selected from the Service List.
Moving Up & Down	The priority for rule execution depends on the rule order in the list. A rule located at the top will be executed prior to those located below it. Users can arrange the order according to their priorities.

 Note	The rules configured in Protocol Binding will be executed by the device according to their priorities too. The higher up on the list, the higher the priority of execution.
--	---

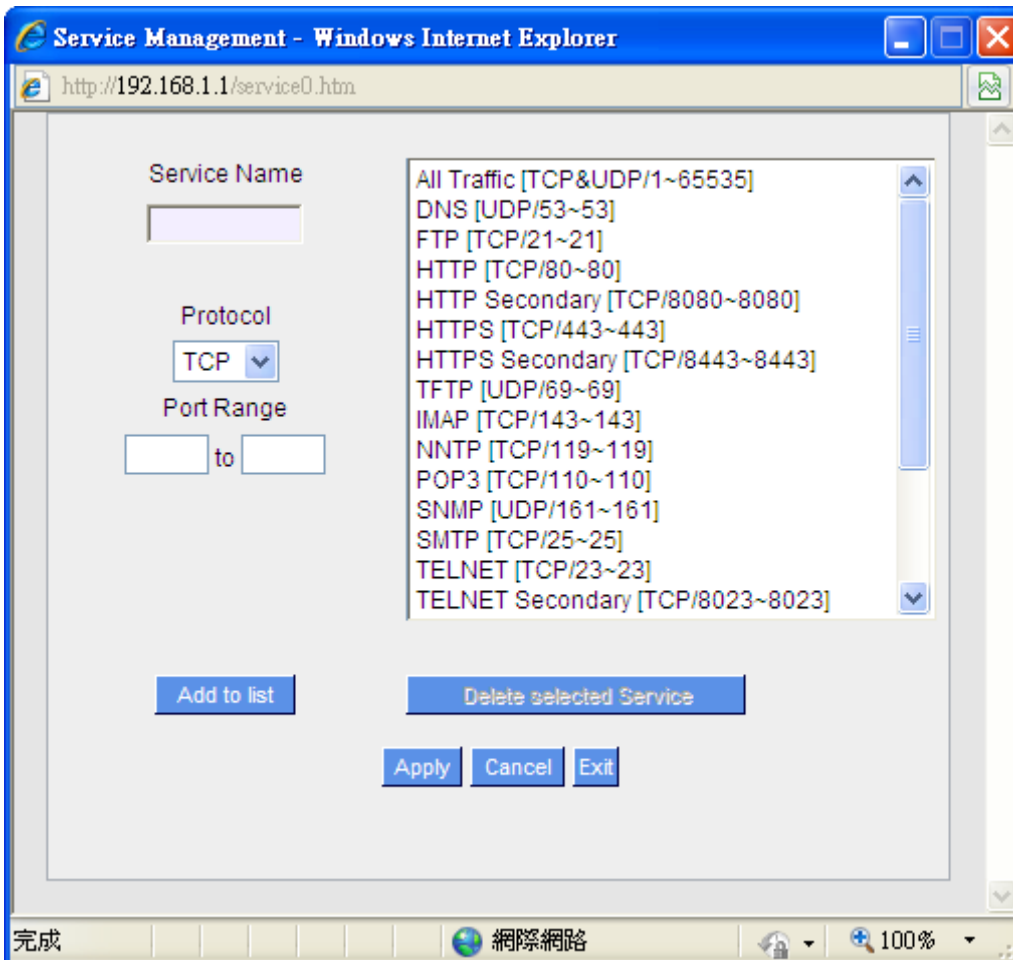
Show Table

Click the “Show Table” button. A dialogue box as shown in the following figure will be displayed. Users can choose to sort the list by priorities or by interface. Click “Refresh” and the page will be refreshed; click “Close” and the dialogue box will be closed.



Add or Remove Service Port

If the Service Port users want to activate is not in the list, users can add or remove service ports from “Service Port Management” to arrange the list, as described in the following:



Item	Description
Service Name	In this box, input the name of the Service Port which users want to activate, such as BT, etc.
Protocol	This option list is for selecting a packet format, such as TCP or UDP for the Service Ports users want to activate.
Port range	In the boxes, input the range of Service Ports users want to add.
Add To List	Click the button to add the configuration into the Services List. Users can add

	up to 100 services into the list.
Delete selected service	To remove the selected activated Services.
Apply	Click the “ Apply ” button to save the modification.
Cancel	Click the “ Cancel ” button to cancel the modification. This only works before “ Apply ” is clicked.

Auto Load Balance mode when enabled

The collocation of the Auto Load Balance Mode and the Auto Load Mode will enable more flexible use of bandwidth. Users can assign specific Intranet IP addresses to specific destination application service ports or assign specific destination IP addresses to the WAN users choose for external connections.

Example 1:How do I set up Auto Load Balance Mode to assign the Intranet IP 192.168.1.100 to WAN2 for the Internet?

As in the figure below, select “All Traffic” from the pull-down option list “Service”, and then in the boxes of “Source IP” input the source IP address “192.168.1.100” to “100”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode.

Protocol Binding

[Show Priority](#)

Service : All Traffic [TCP&UDP/1~65535] ▼

[Service Management](#)

Source IP ▼ 192 . 168 . 1 . 100 to 100

Dest. IP ▼ 0 . 0 . 0 . 0 to
0 . 0 . 0 . 0

Interface : WAN 2 ▼

Enabled :

Move Up
Update this Application
Move Down

All Traffic [TCP&UDP/1~65535]->192.168.1.100~100(0.0.0.0~0.0.0.0)WAN 2

Delete selected item
Add

Show Table
Apply
Cancel

Example 2: How do I set up Auto Load Balance Mode to keep Intranet IP 192.168.1.150 ~ 200 from going through WAN2 when the destination port is Port 80?

As in the figure below, select “HTTP [TCP/80~80]” from the pull-down option list “Service”, and then in the boxes for “Source IP” input “192.168.1.150” to “200”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode.

Protocol Binding

The screenshot shows the configuration for a protocol binding rule. At the top right is a "Show Priority" button. The main configuration area includes:

- Service:** HTTP [TCP/80~80]
- Service Management:** A button above the IP fields.
- Source IP:** 192 . 168 . 1 . 150 to 200
- Dest. IP:** 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0
- Interface:** WAN 2
- Enabled:**

Below the configuration fields are three buttons: "Move Up", "Update this Application", and "Move Down". A list box contains one entry: "HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN 2". At the bottom are "Delete selected item" and "Add" buttons.

Example 3: How do I set up Auto Load Balance Mode to keep all Intranet IP addresses from going through WAN2 when the destination port is Port 80 and keep all other services from going through WAN1?

As in the figure below, there are two rules to be configured. The first rule: select “HTTP [TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of Source IP input “192.168.1.0” to “0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets to Port 80 through WAN2. However, with only the above rule, packets that do not go to Port 80 may be transmitted through WAN2; therefore, a second rule is necessary. The second rule: Select “All Ports [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then input “192.168.1.2 ~ 254” in the boxes of “Source IP”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to

include all Internet IP addresses). Select WAN1 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets that are not going to Port 80 to the Internet through WAN1.

Protocol Binding

[Show Priority](#)

Service : HTTP [TCP/80~80] ▼

[Service Management](#)

Source IP ▼ 192 . 168 . 1 . 0 to 0

Dest. IP ▼ 0 . 0 . 0 . 0 to 0

0 . 0 . 0 . 0

Interface : WAN 2 ▼

Enabled :

[Move Up](#)
[Update this Application](#)
[Move Down](#)

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)WAN 2

All Traffic [TCP&UDP/1~65535]->192.168.1.2~254(0.0.0.0~0.0.0.0)WAN 1

[Delete selected item](#)
[Add](#)

[Show Table](#) [Apply](#) [Cancel](#)

Configuring “Assigned Routing Mode” for load Balance

IP Group: This function allows users to assign packets from specific Intranet IP addresses or to specific destination Service Ports and to specific destination IP addresses through an assigned WAN to the Internet. After being assigned, the specific WAN will only support those assigned Intranet IP addresses, destination Service Ports, or destination IP addresses. Those which are not configured will go through other WANs for external connection. Only when this mode is collocated with “Assigned Routing” can it bring the function into full play.

Example 1:How do I set up the Assigned Routing Mode to keep all Intranet IP addresses from going through WAN2 when the destination is Port 80, and keep all other services from going through WAN1?

As in the figure below, select “HTTP[TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses).

Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. After the rule is set up, only packets that go to Port 80 will be transmitted through WAN2, while other traffics will be transmitted through WAN1.

Protocol Binding

Service : HTTP [TCP/80~80]

Service Management

Source IP : 192 . 168 . 1 . 0 to 0

Dest. IP : 0 . 0 . 0 . 0 to 0

Interface : WAN 2

Enabled :

Move Up Update this Application Move Down

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)WAN 2

Delete selected item Add

Show Table Apply Cancel

Example 2: How do I configure Protocol Binding to keep traffic from all Intranet IP addresses from going through WAN2 when the destinations are IP 211.1.1.1 ~ 211.254.254.254 as well as the whole Class A group of 60.1.1.1 ~ 60.254.254.254, while traffic to other destinations goes through WAN1?

As in the following figure, there are two rules to be configured. The first rule: Select “All Port [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). In the boxes for “Destination IP” input “211.1.1.1 ~ 211.254.254.254”. Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The second rule: Select “All Port [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). In the boxes of “Destination IP” input “211.1.1.1 ~ 60,254,254,254”. Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New”, and the rule will be added to the mode. After the rule has been set up, all traffic that is not going to the assigned destinations will only be transmitted through WAN1.

Protocol Binding

Show Priority

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Source IP 192 . 168 . 1 . 0 to 0

Dest. IP 211 . 1 . 1 . 1 to 211 . 254 . 254 . 254

Interface : WAN 2

Enabled :

Move Up
Update this Application
Move Down

All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)WAN 2

All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)WAN 2

Delete selected item
Add

Show Table
Apply
Cancel

Chapter 7: Port Management

This chapter introduces how to configure ports and understand how to configure intranet IP addresses.

7.1 Setup

Through the device, users can easily manage the setup for WAN ports, LAN ports and the DMZ port by choosing the number of ports, speed, priority, and duplex and enable/disable the auto-negotiation feature for connection setting of each port.

Port Setup

Enable Port 1 as Mirror Port

Port ID	Interface	Disable	Priority	Speed Status	Duplex Status	Auto Neg.	Port VLAN
1	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
2	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
3	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
4	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
5	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
6	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
7	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
8	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
9	WAN 1	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
10	WAN 2	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
11	WAN 3	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
12	WAN 4	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
13	WAN 5	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	

Item	Description
Disabled	This feature allows users turn on/off the Ethernet port. If selected, the Ethernet port will be shut down immediately and no connection can be made. The default value is "on".
Priority	This feature allows users to set the high/low priority of the packet delivery for the Ethernet port. If it is set as High, the port has the first priority to deliver the packet. The default value is "Normal".
Speed	This feature allows users to select the network hardware connection speed for the Ethernet port. The options are 10Mbps and 100Mbps.
Duplex Status	This feature allows users to select the network hardware connection speed working mode for the Ethernet. The options are full duplex and half duplex.
Auto Neg.	The Auto-Negotiation mode can enable each port to automatically adjust and gather the connection speed and duplex mode. Therefore, if Enabled Auto-Neg. selected, the ports setup will be done without any manual setting by

	administrators.
VLAN	<p>This feature allows administrators to set the LAN port to be one or more disconnected network sessions. All of them will be able to log on to the Internet through the device.</p> <p>Members in the same network session (within the same VLAN) can see and communicate with each other. Members in different VLAN will not know the existence of other members.</p>
VLAN All	<p>Set VLAN All port to be the public area of VLAN so that it can be connected to other VLAN networks. A server should be constructed for the intranet so that all VLAN group can visit this server. Set one of the network ports as VLAN All. Connect the server to VLAN All so that computers of different VLAN groups can be connected to this server. Moreover, the port where the administrator locates must be set as VLAN All so that it can be connected to the entire network to facilitate network management.</p>

Mirror Port : Users can configure LAN 1 as mirror port by choosing “Enable Port 1 as Mirror Port”. All the traffic from LAN to WAN will be copied to mirror port. Administrator can control or filter the traffic through mirror port. Once this function is enabled, LAN 1 will be shown as Mirror Port in Physical Port Status, Home page.

Physical Port Status

Port ID	1	2	3	4	5	6	7	8
Interface	LAN							
Status	<u>Enabled</u>	<u>Enabled</u>	<u>Enabled</u>	<u>Enabled</u>	<u>Enabled</u>	<u>Connect</u>	<u>Enabled</u>	<u>Enabled</u>

Port ID	Internet	Internet	Internet	Internet	Internet
Interface	WAN 1	WAN 2	WAN 3	WAN 4	WAN 5
Status	<u>Enabled</u>	<u>Enabled</u>	<u>Enabled</u>	<u>Connect</u>	<u>Enabled</u>

7.2 Port Status

Port ID

Summary

Type	10Base-T / 100Base-TX / 1000Base-T
Interface	LAN
Link Status	Up
Physical Port Status	Port Enabled
Priority Setup	Normal
Speed	1000 Mbps
Half/Full Duplex	Full
Auto Negotiation	Enabled
Port VLAN	VLAN1

Statistics

Received Packets Count	3191
Received Bytes Count	443391
Transmitted Packets Count	29018
Transmitted Bytes Count	7079145
Error Packets Count	0

Summary

There are Network Connection Type, Interface, Link Status (Up/Down), Port Activity (Port Enabled), Priority Setting (High or Normal), Speed Status (10Mbps, 100Mbps or 1000Mbps), Duplex Status (half duplex or full duplex), Auto Neg. (Enabled/Disabled), and VLAN.

Statistics

The packet data of this specific port will be displayed. Data include receive/ transmit packet count, receive/ transmit packet Byte count and error packet count. Users may press the refresh button to update all real-time messages.

7.3 IP/ DHCP

With an embedded DHCP server, it supports automatic IP assignment for LAN computers. (This function is similar to the DHCP service in NT servers.) It benefits users by freeing them from the inconvenience of recording and configuring IP addresses for each PC respectively. When a computer is turned on, it will acquire an IP address from the device automatically. This function is to make management easier.

7.3.1 IPv4

IPv4

IPv6

Enabled DHCP Server

DHCP Dynamic IP

Client Lease Time Minutes

Subnet	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server	Enabled	Disabled	Disabled	Disabled
IP Range Starts	192.168.1.100	192.168.2.100	192.168.3.100	192.168.4.100
IP Range Ends	192.168.1.149	192.168.2.149	192.168.3.149	192.168.4.149
MAC Addresses Pool for this IP Range	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>

DNS

DNS(Required) 1:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
DNS(Optional) 2:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

WINS

WINS Server:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
--------------	---

DNS Local Database

Host Name:

IP Address:

DHCP Dynamic IP

Item	Description
Enable DHCP Server	Check the option to activate the DHCP server automatic IP lease function. If the function is activated, all PCs will be able to acquire IP automatically. Otherwise, users should configure static virtual IP for each PC individually.
Client lease Time	This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Users can change it according to their needs. The time unit is minute.
Range Start	This is an initial IP automatically leased by DHCP. It means DHCP will start the lease from this IP. The default initial IP is 192.168.1.100.
Range End	This is the end IP automatically leased by DHCP. The default initial IP is 192.168.1.149.

DNS (Domain Name Service)

This is for checking the DNS from which an IP address has been leased to a PC port. Input the IP address of this server directly.

Item	Description
DNS (Required) 1	Input the IP address of the DNS server.
DNS (Optional) 2	Input the IP address of the DNS server.

WINS:


If there is a WIN server in the network, users can input the IP address of that server directly.

Item	Description
WINS Server	Input the IP address of WINS.
Apply	Click " Apply " to save the network configuration modification.
Cancel	Click " Cancel " to leave without making any changes.

DNS Local Database:

Normally, DNS sever will be directed to ISP DNS server or internal self- defined DNS server. CS-5800 also provides "easy" self-defined DNS services, called "DNS Local Database", which can map website host domain names and the corresponding IP addresses.

Item	Description
Host Domain Name	Enter the website host domain name. i.e. www.google.com
IP Address	Enter the corresponding IP address of the host domain above.
Add to List	Add the items into the list below.

 Note	(1) Users MUST enable DHCP server service to enable DNS local database. (2) Users must set DHCP server DNS IP address as the router LAN IP
--	---

7.3.2 IPv6

Enabled DHCP Server

DHCP Dynamic IP

Client Lease Time Minutes

Subnet :	Subnet1
DHCP Server :	Enabled
IP Range Starts :	fc00::100
IP Range Ends :	fc00::17f

Unified IP Management

DNS

DNS(Required) 1:	<input type="text" value="::"/>
DNS(Optional) 2:	<input type="text" value="::"/>

DHCP Dynamic IP:

Item	Description
Enable DHCP Server	Check the option to activate the DHCP server automatic IP lease function. If the function is activated, all PCs will be able to acquire IP automatically. Otherwise, users should configure static virtual IP for each PC individually.
Client lease Time	This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Users can change it according to their needs. The time unit is minute.
Range Start	This is an initial IP automatically leased by DHCP. It means DHCP will start the lease from this IP. The default initial IP is 192.168.1.100.
Range End	This is the end IP automatically leased by DHCP. The default initial IP is 192.168.1.149.

DNS (Domain Name Service):

This is for checking the DNS from which an IP address has been leased to a PC port. Input the IP address of this server directly.

Item	Description
DNS Server (Required) 1	Input the IP address of the DNS server.
DNS Server (Required) 2	Input the IP address of the DNS server.

7.4 DHCP Status

This is an indication list of the current status and setup record of the DHCP server. The indications are for the administrator's reference when a network modification is needed.

IPv4
IPv6

IPv4

Status

Subnet	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server	192.168.1.1	192.168.2.1	192.168.3.1	192.168.4.1
Dynamic IP Used	1	0	0	0
Static IP Used	0	0	0	0
DHCP Available	49	50	50	50
Total	50	50	50	50

Client Table

Subnet1 ▼

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC97005	192.168.1.100	00:1a:92:70:43:cd	22 Hours, 32 Minutes, 16 Seconds	

Refresh

IPv4

IPv6

Status

	Subnet	Subnet1
DHCP Server :		fc00::1
Dynamic IP Used		0
Static IP Used		--
DHCP Available		128
Total		128

Client Table

Host Name	IP Address	Client Lease Time
-----------	------------	-------------------

Item	Description
DHCP Server	This is the current DHCP IP.
Dynamic IP Used	The amount of dynamic IP leased by DHCP.
Static IP Used	The amount of static IP assigned by DHCP.
IP Available	The amount of IP still available in the DHCP server.
Total IP	The total IP which the DHCP server is configured to lease.
Host Name	The name of the current computer.
IP Address	The IP address acquired by the current computer.
MAC Address	The actual MAC network location of the current computer.
Client Lease Time	The lease time of the IP released by DHCP.
Delete	Remove a record of an IP lease.

7.5 IP & MAC Binding (IPv4 Only)

Administrators can apply IP & MAC Binding function to make sure that users can not add extra PCs for Internet access or change private IP addresses.

IP&MAC binding

[Show new IP user](#)

Static IP : . . .

MAC Address : - - - - -

Name :

Enabled :

[Add to list](#)

[Delete selected item](#)

Block MAC address on the list with wrong IP address

Block MAC address not on the list

[Apply](#) [Cancel](#)

There are two methods for setting up this function:

Block MAC address on the list with wrong IP address:

This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access.

Block MAC address not on the list:

This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access. When this method is applied, please fill out Static IP with 0.0.0.0, as the figure below:

IP&MAC binding

Show new IP user

Static IP : 0 . 0 . 0 . 0
MAC Address : - - - - -
Name :
Enabled :

Add to list

Delete selected item

- Block MAC address on the list with wrong IP address
- Block MAC address not on the list

Apply Cancel

IP & MAC Binding

IP&MAC binding

Show new IP user

Static IP : 0 . 0 . 0 . 0
MAC Address : - - - - -
Name :
Enabled :

Add to list

Delete selected item

- Block MAC address on the list with wrong IP address
- Block MAC address not on the list

Apply Cancel

Item	Description
Static IP:	There are two ways to input static IP: 1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a specific assigned IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty. 2. If users want DHCP to assign a static IP for a PC every single time, users should input the IP address users want to assign to this computer in the boxes. The server or PC which is to be bound will then acquire a static virtual IP whenever it restarts.
MAC Address:	Input the static real MAC (the address on the network card) for the server or PC which is to be bound.
Name:	For distinguishing clients, input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
Enabled:	Activate this configuration.
Add to list:	Add the configuration or modification to the list.
Delete selected item:	Remove the selected binding from the list.
Add:	Add new binding.

Block MAC address on the list with wrong IP address: When this option is activated, MAC addresses which are not included in the list will not be able to connect with the Internet.

Show New IP user:

This function can reduce administrator's effort on checking MAC addresses one by one for the binding. Furthermore, it is easy to make mistakes to fill out MAC addresses on the list manually. By checking this list, administrator can see all MAC addresses which have traffic and are not bound yet. Also, if administrators find that one specific bound MAC address is shown on the list, it means that the user changes the private IP address.

IP & MAC binding List				Submit	Select All	Refresh	Close
IP Address	MAC Address	Name	Enable				
192.168.1.100	00:1f:c6:7b:8a:bd	<input type="text"/>	<input type="checkbox"/>				



Item	Description
Name	Input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
Enabled	Choose the item to be bound.
Apply	Activate the configuration.
Select All	Choose all items on the list for binding.
Refresh	Refresh the list.
Close	Close the list.

7.6 IP Grouping

IP Group function can combine several IP addresses or IP address ranges into several groups. When you manage user internet access privileges by IP address, you can set up every management functions for users who have same internet access privileges in the same IP group in order to decrease the effort of setting rules for each IP address. For example, you can choose to set up QoS or Access Rule by IP grouping. Thus, you will simplify setting rules.

IP Grouping consists of Local IP Group and Remote IP Group. Local IP Group refers to LAN IP groups, and remote IP Group refers to WAN IP groups. Local IP Group list will automatically learn IP addresses having packets that pass through firewall. Moreover, if user changes the IP address, the IP in the list will change accordingly well. For IP information which is in group list, it won't update automatically along with IP list of the left side. Administrators need to modify it manually.

Item	Description
User Edit IP	The IP list will show the list which learns the IP addresses automatically on the left under side. You can also modify IP addresses manually.
Name	Input the name of IP address (or range) showed below.
IP Address	Input IP address (or range). For example, 192.168.1.200 ~ 250.
Add to IP List	After setting name and IP address, push this button to add the information into the IP list below. If this IP (or range) is already in the list, you can not add it again.

Local Group Set	You can choose from the IP list on the left side to set up a local IP group.
IP Group	Choose IP Group that you would like to modify. If you would like to add new groups, please push "Add new group" button.
Group Name	When you add new groups, please note if the group name is in the column.
Delete Group	Choose the group that you would like to delete from the pull- down list, and push the "Delete Group" button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
 button	You can choose several IPs from IP list on the left side, and push this button to have them added into the group the right side.
Delete 	Delete self- defined IP or IP range.
Apply	Click "Apply" to save the network configuration modification
Cancel	Click "Cancel" to leave without making any changes.

Remote IP Group Management:

Basically, Remote IP Group setups are exactly the same as Local IP Group setups. However, remote IP group does not have automatically learning functions. Instead, you need to define addresses, ranges and groups manually. For example, 220.130.188.1 to 200 (range).

The screenshot displays the configuration interface for Remote IP Group Management. It is divided into two main sections: 'User Edit IP' and 'Remote Group Set'.

User Edit IP: This panel contains a 'Name' input field, an 'IP Address' input field with four separate boxes for each octet and a 'to' label, and an 'Add to IP list' button.

Remote Group Set: This panel features a dropdown menu for 'IP Group', an 'Add Group' button, and a 'Delete Group' button.

Below these panels are two empty tables representing IP lists:

- IP List (Left):** A table with columns 'Name', 'IP Address', 'Edit', and 'Delete'. The 'IP Address' column has a downward arrow. The table is currently empty.
- Group Name (Right):** A text input field for 'Group Name'.
- Group List (Right):** A table with columns 'Name', 'IP Address', and 'Delete'. The 'IP Address' column has an upward arrow. The table is currently empty.

A right-pointing arrow (>>>>>) is positioned between the two IP list tables, indicating the flow of data from the left list to the right list.

It is the same setting methods. You should set the IP address or the range of remote IP from the left side first, and choose to add IP address information from the left side into the remote group.

7.7 Port Group Management

Service ports can be grouping as IP grouping. It is convenient to set QoS, firewall access rules, and other functions.

user edit port

Name :

Protocol : TCP

Port Range: to

Port List


Name	Protocol	Port	Delete
All Traffic	BOTH	1~65535	
DNS	UDP	53~53	
FTP	TCP	21~21	
HTTP	TCP	80~80	
HTTP Secondary	TCP	8080~8080	
HTTPS	TCP	443~443	
HTTPS Secondary	TCP	8443~8443	
TFTP	UDP	69~69	
IMAP	TCP	143~143	
NNTP	TCP	119~119	
POP3	TCP	110~110	
SNMP	UDP	161~161	
SMTP	TCP	25~25	

Port Group Set

Group :

Group Name :

Name	Protocol	Port	Delete

Item	Description
User edit port	Input the name, protocol, and port range for the specific service port.
Name	Name the Port in order to identify its property. For example, Virus 135.
Protocol	Choose the port protocol form the pull down list like TCP, UDP or TCP and UDP.
Port Range	Input the port range. For example, 135 to 135.
Add to Port List	After setting name, protocol and port range, push this button to add the information into the Port list below. This port can be from some port groups.
Group Name	When you add new groups, please note if the group name is in the column. For example, Virus.
Delete Group	Choose the group that you would like to delete from the pull- down list, and push the “Delete Group” button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
 button	You can choose several ports from Port list on the left side, and push this button to have them added into the group the right side.
Delete	Delete self- defined port or port range.
Apply	Click “Apply” to save the network configuration modification

Chapter 8: QoS (Quality of Service)

QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IP addresses to save bandwidth or provide priority to specific applications or services, and also to enable other users to share bandwidth, as well as to ensure stable and reliable network transmission. To maximize the bandwidth efficiency, network administrators should take account of the practical requirements of a company, a community, a building, or a café, etc., and modify bandwidth management according to the network environment, application processes or services.

8.1 Bandwidth Management

The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	10000	10000
WAN 2	10000	10000
WAN 3	10000	10000
WAN 4	10000	10000
WAN 5	10000	10000

Quality of Service

Interface : WAN 1 WAN 2 WAN 3 WAN 4 WAN 5

Service : All Traffic [TCP&UDP/1~65535] ▼

Service Management

IP Address ▼ : 0 . 0 . 0 . 0 to 0

Direction : Upstream ▼

Mini. Rate : Kbit/sec Max. Rate : Kbit/sec

Bandwidth sharing : Share total bandwidth with all IP addresses.
 Assign bandwidth for each IP address.

Enabled :

Move Up
Add to list
Move Down

Delete selected item

Enabled Smart QoS

Exception IP address

Interface : WAN 1 WAN 2 WAN 3 WAN 4 WAN 5

Source IP . . . to / Group :

. . .

Direction : Do not control upstream bandwidth
 Do not control downstream bandwidth
 Do not control bi-direction bandwidth

Enabled :

8.1.1 The Maximum Bandwidth provided by ISP

The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 2	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 3	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 4	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 5	<input type="text" value="10000"/>	<input type="text" value="10000"/>

In the boxes for WAN1 and WAN2 bandwidth, input the upstream and downstream bandwidth which users applied for from bandwidth supplier. The bandwidth QoS will make calculations according to the data users input. In other words, it will guarantee a minimum rate of upstream and downstream for each IP and Service Port based on the total actual bandwidth of WAN1 and WAN2. For example, if the upstream bandwidths of both WAN1 and WAN2 are 512Kbit/Sec, the total upstream bandwidth will be: WAN1 + WAN2 = 1024Kbit/Sec. Therefore, if there are 50 IP addresses in the Intranet, the minimum guaranteed upstream bandwidth for each

IP would be $1024\text{Kbit}/50=20\text{Kbit/Sec}$. Thus, 20Kbit/Sec can be input for "Mini. Rate" Downstream bandwidth can be calculated in the same way.

**Attention**

The rules configured in Protocol Binding will be executed by the device according to their priorities too. The higher up on the list, the higher the priority of execution. The unit of calculation in this example is Kbit. Some software indicates the downstream/upstream speed with the unit KB. $1\text{KB} = 8\text{Kbit}$.

8.1.2 QoS


To satisfy the bandwidth requirements of certain users, the device enables users to set up QoS with Rate Control method.


Rate Control

The network administrator can set up bandwidth or usage limitations for each IP or IP range according to the actual bandwidth. The network administrator can also set bandwidth control for certain Service Ports. A guarantee bandwidth control for external connections can also be configured if there is an internal server.

Quality of Service

The screenshot displays the 'Rate Control' configuration page. At the top, there are checkboxes for selecting an interface: WAN 1, WAN 2, WAN 3, WAN 4, and USB. Below this is a dropdown menu for 'Service' set to 'All Traffic [TCP&UDP/1-65535]'. A 'Service Management' button is located below the service dropdown. The 'IP Address' field is set to '0.0.0.0 to 0'. The 'Direction' dropdown is set to 'Upstream'. The 'Mini. Rate' and 'Max. Rate' fields are both empty, with units of 'Kbit/sec'. Under 'Bandwidth sharing', the radio button for 'Assign bandwidth for each IP address.' is selected. The 'Enabled' checkbox is unchecked. At the bottom of the configuration area, there are three buttons: 'Move Up', 'Add to list', and 'Move Down'. Below these buttons is a large empty rectangular box. At the very bottom of the form, there is a 'Delete selected item' button.

Item	Description
Interface	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service Port	Select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select "All (TCP&UDP) 1~65535". If only FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
IP Address	This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 150". The rule will control IP addresses from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input "0" in the boxes of IP address. This means all Intranet IP addresses will be restricted. QoS can also control the range of Class B.
Direction	<p>Upstream: Means the upload bandwidth for Intranet IP.</p> <p>Downstream: Means the download bandwidth for Intranet IP.</p> <p>Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server.</p> <p>Server in LAN, Downstream: If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.</p>
Min. & Max. Rate(Kbit/Sec)	<p>The minimum bandwidth: The rule is to guarantee minimum available bandwidth.</p> <p>The maximum bandwidth: This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule.</p> <div data-bbox="504 1693 1430 1827" style="border: 1px solid black; padding: 5px;">  <p>Attention</p> <p>The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.</p> </div>
Bandwidth Assign Type	<p>Sharing total bandwidth with all IP addresses: If this option is selected, all IP addresses or Service Ports will share the bandwidth range (from minimum to maximum bandwidth).</p> <p>Assign bandwidth for each IP address: If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum.). For</p>

	<p>example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.</p> <div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;"> Attention</p> <p>If “Share-Bandwidth” is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small.</p> <p>For example, if users do not want an FTP to occupy too much bandwidth, users can select the “Share-Bandwidth Mode”, so that no matter how much users use FTPs to download information, the total occupied bandwidth is fixed.</p> </div>
Enable	Activate the rule.
Add to list	Add this rule to the list.
Move up & Move down	QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. Usually the service ports which need to be restricted, such as BT, e-mule, etc., will be moved to the bottom of the list. The rules for certain IP addresses would then be moved upward.
Delete selected items	Remove the rules selected from the Service List.
Show Table	Display all the Rate Control Rules users made for the bandwidth. Click “Edit” to modify.
Apply	Click “Apply” to save the configuration
Cancel	Click “Cancel” to leave without making any change.

Show Table

Summary										
Service	IP Address	Direction	Mini. Rate (Kbit/sec)	Max. Rate (Kbit/sec)	Bandwidth sharing	Enabled	Interface (WAN)	Edit		
<div style="text-align: right;"> <input checked="" type="radio"/> Rule <input type="radio"/> Interface Refresh Close </div>										

8.1.3 Smart QoS

Enabled Smart QoS

When the utility of any wan's bandwidth is over than %, Enable Smart QoS(0: Always Enabled)

Each IP's upstream bandwidth threshold : Kbit/sec

Each IP's downstream bandwidth threshold : Kbit/sec

Each IP's Maximum bandwidth :

Upstream (WAN 1 : Kbit/sec WAN 2 : Kbit/sec WAN 3 : Kbit/sec
WAN 4 : Kbit/sec WAN 5 : Kbit/sec)

Downstream (WAN 1 : Kbit/sec WAN 2 : Kbit/sec WAN 3 : Kbit/sec
WAN 4 : Kbit/sec WAN 5 : Kbit/sec)

Penalty mechanism

Item	Description
Enabled QoS	Choose to apply QoS function.
When the usage of any WAN's bandwidth is over___%, Enable Smart QoS	Input the required rate value into the column. The default is 60%.
Each IP's upstream bandwidth threshold (for all WAN)	Input the max. upstream rate for intranet IPs.
Each IP's downstream bandwidth threshold (for all WAN)	Input the max. downstream rate for intranet IPs.
Each IP's bandwidth is over maximum threshold, its maximum bandwidth will remain	When any IP uses more bandwidth than the above upstream or downstream settings, the IP will be restricted for the following upstream or downstream bandwidth settings.
Penalty Mechanism	After choosing "Enabled Penalty Mechanism", the device will enable the penalty conditions internally. When the IP still uses more upstream or downstream bandwidth than the setting, the device will execute the penalty conditions automatically.
Show Penalty List	The IPs which are under penalty mechanism will be shown on the list.

Advanced

When the usage of certain WAN's bandwidth is under %, then stop to add new punished IP

Enabled Session Control Mechanism

Every second to detect whether internal IP's bandwidth are over than limit

If the punished IP still keep upper bounded limit on, then decrease its bandwidth to %

When the usage of all WANs' bandwidth are lower than % disable Smart QoS,
and after minutes to release punished IP

Item	Description
When the usage of certain WAN's bandwidth is under __%, then stop to add new punished IP	When the usage of certain WAN's bandwidth is under __%, will stop to punish the IP which is over the limit. While the bandwidth is over the certain percentage, penalty mechanism will be activated.
Every __ second to detect whether internal IP's bandwidth are over than limit	Detect usage of internal IP's bandwidth every __ second.
If the punished IP still keep upper bounded limit on, then decrease its bandwidth to __%	If the punished IP still keep over the limit, the limit bandwidth will be decrease to __%.
When the usage of all WANs' bandwidth are lower than __% disable Smart QoS, and after __ minutes to release punished IP	Smart QoS will be disabled when the usage of bandwidth is lower than __%. Punished IP will be released after __ minute.

8.1.4 Exception IP address

If some users are allowed to avoid traffic management control, you can use this function to fulfill the requirement.

Exception IP address

Interface : WAN 1 WAN 2 WAN 3 WAN 4 WAN 5

Source IP . . . to / Group :

Direction : Do not control upstream bandwidth
 Do not control downstream bandwidth
 Do not control bi-direction bandwidth

Enabled :

Item	Description
WAN	Select WAN ports.
Source IP	Enter the exempted IP range, or select the exempted IP group.
Do not control Direction	Select do not control upload, download, or both of them.
Enabled	Enable this policy.
Add to List	Add this policy into the exempted list.
Delete Selected item	Delete selected list.
Apply	Click “Apply” button to saving configuration.
Cancel	Click “Cancel” button to reject modification.

8.2 Session control

Session management controls the acceptable maximum simultaneous sessions of Intranet PCs. This function is very useful for managing connection quantity when P2P software such as BT, Thunder, or emule is used in the Intranet causing large numbers of sessions. Setting up proper limitations on sessions can effectively control the sessions created by P2P software. It will also have a limiting effect on bandwidth usage.

In addition, if any Intranet PC is attacked by a virus like Worm. Blaster and sends a huge number of session requests, session control will restrict that as well.

Session Control and Scheduling

Session Control

<input checked="" type="radio"/> Disabled	
<input type="radio"/> Single IP cannot exceed <input type="text" value="200"/> Session	
<input type="radio"/> Single IP cannot exceed TCP <input type="text" value="100"/> , UDP <input type="text" value="100"/> Session	
<input type="radio"/> When single IP exceed <input type="text" value="200"/> Session	<input type="radio"/> block this IP's new sessions for <input type="text" value="5"/> minutes
<input type="radio"/> block this IP's all sessions for <input type="text" value="5"/> minutes	

Scheduling

Apply this rule <input type="text" value="Always"/> <input type="button" value="v"/>	<input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="23"/> : <input type="text" value="59"/> (24-Hour Format)
<input checked="" type="checkbox"/> Everyday	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat

Item	Description
Disabled	Disable Session Control function.
Single IP cannot exceed __ session	This option enables the restriction of maximum external sessions to each Intranet PC. When the number of external sessions reaches the limit, to allow new sessions to be built, some of the existing sessions must be closed. For example, when BT or P2P is being used to download information and the sessions exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.
When single IP exceed __	<p><input checked="" type="radio"/> block this IP's new sessions for <input type="text" value="5"/> minutes</p> <p>If this function is selected, when the user's port session reach the limit, this user will not be able to make a new session for five minutes. Even if the previous session has been closed, new sessions cannot be made until the setting time ends.</p> <p><input type="radio"/> block this IP's all sessions for <input type="text" value="5"/> minutes</p> <p>If this function is selected, when the user's port connections reach the limit, all the</p>

	lines that this user is connected with will be removed, and the user will not be able to connect with the Internet for five minutes. New connections cannot be made until the delay time ends.
Scheduling	If "Always" is selected, the rule will be executed around the clock. If "From..." is selected, the rule will be executed according to the configured time range. For example, if the time control is from Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.
Apply	Click "Apply" to save the configuration.
Cancel	Click "Cancel" to leave without making any change.

Exempted Service Port or IP Address

Exempted Service Port or IP Address

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Source IP : . . . 0 to 0

Enabled :

Maximum connections limit : Unlimited Not exceed 300

Add to list

Delete selected item

Item	Description
Service Port	Choose the service port.
IP Address	Input the IP address range or IP group.
Enabled	Activate the rule.
Add to list	Add this rule to the list.
Delete selected item	Remove the rules selected from the Service List.
Apply	Click " Apply " to save the configuration.
Cancel	Click " Cancel " to leave without making any change.

Chapter 9 : Firewall

This chapter introduces firewall general policy, access rule, and content filter settings to ensure network security.

9.1 General Policy

The firewall is enabled by default. If the firewall is set as disabled, features such as SPI, DoS, and outbound packet responses will be turned off automatically. Meanwhile, the remote management feature will be activated. The network access rules and content filter will be turned off.

General Policy

Firewall	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
SPI (Stateful Packet Inspection)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
DoS (Denial of Service)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Advanced Function
Block WAN Request	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
Remote Management	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	Port 8080
Multicast Pass Through	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	
Prevent ARP Virus Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Router sends ARP 5 times per-second.

Apply Cancel

Item	Description
Firewall	This feature allows users to turn on/off the firewall.
SPI (Stateful Packet Inspection)	This enables the packet automatic authentication detection technology. The Firewall operates mainly at the network layer. By executing the dynamic authentication for each connection, it will also perform an alarming function for application procedure. Meanwhile, the packet authentication firewall may decline the connections which use non-standard communication protocol.
DoS (Denial of Service)	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and so on.
Block WAN request	If set as Enabled, then it will shut down outbound ICMP and abnormal packet responses in connection. If users try to ping the WAN IP from the external, this will not work because the default value is set as activated in order to decline the outbound responses.
Remote Management	To enter the device web- based UI by connecting to the remote Internet, this feature must be activated. In the field of remote browser IP, a valid external IP address (WAN IP) for the device should be filled in and the modifiable default control port should be adjusted (the default is set to 80, modifiable).
Multicast Pass	There are many audio and visual streaming media on the network. Broadcasting

Through	may allow the client end to receive this type of packet message format. This feature is off by default.
Prevent ARP Virus Attack	This feature is designed to prevent the intranet from being attacked by ARP spoofing, causing the connection failure of the PC. This ARP virus cheat mostly occurs in Internet cafes. When attacked, all the online computers disconnect immediately or some computers fail to go online. Activating this feature may prevent the attack by this type of virus.

Advanced Setting

Advance DoS Settings

Packet Type	WAN Threshold	LAN Threshold
<input checked="" type="checkbox"/> TCP SYN Flood	Threshold counted by all packets <input type="text" value="15000"/> Packets/Sec	Threshold counted by all packets <input type="text" value="50000"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="1000"/> Packets/Sec	Single Destination IP Threshold <input type="text" value="5000"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="50"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input checked="" type="checkbox"/> UDP_Flood	Threshold counted by all packets <input type="text" value="15000"/> Packets/Sec	Threshold counted by all packets <input type="text" value="50000"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="1000"/> Packets/Sec	Single Destination IP Threshold <input type="text" value="5000"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="50"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input checked="" type="checkbox"/> ICMP_Flood	Threshold counted by all packets <input type="text" value="200"/> Packets/Sec	Threshold counted by all packets <input type="text" value="200"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="50"/> Packets/Sec	Single Destination IP Threshold <input type="text" value="200"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="5"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input type="checkbox"/> Exception Source IP		IP Add <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> to /Group <input type="text" value="test"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		IP Add <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> to /Group <input type="text" value="test"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
<input type="checkbox"/> Exception Destination IP		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Firewall/DoS Log
Show Blocked IP
Apply
Cancel

Item	Description
Packet Type	This device provides three types of data packet transmission: TCP-SYN-Flood, UDP-Flood and ICMP-Flood.
WAN Threshold	When all packet values from external attack or from single external IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes OBJ 176). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.
LAN Threshold	When all packet values from internal attack or from single internal IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.
Exempted Source IP	Input the exempted source IP.
Exempted Dest. IP	Input the exempted Destination IP addresses.
Apply	Click " Apply " to save the configuration.
Cancel	Click " Cancel " to leave without making any change.

Firewall / DoS Log

System Log
 Current Time: Fri Mar 4 17:36:25 2011 Firewall/DoS Log

Time ▲	Event-Type	Message
--------	------------	---------

Show the Firewall/Log.

Show Blocked IP

Summary

IP Address	Time(sec)
------------	-----------

Show the blocked IP list and the remained blocked time.

9.2 Access Rule

Users may turn on/off the setting to permit or forbid any packet to access internet. Users may select to set different network access rules: from internal to external or from external to internal. Users may set different packets for IP address and communication port numbers to filter Internet access rules.

Network access rule follows IP address, destination IP address, and IP communications protocol status to manage the network packet traffic and make sure whether their access is allowed by the firewall.

9.2.1 Default Rule

The device has a user-friendly network access regulatory tool. Users may define network access rules. They can select to enable/ disable the network so as to protect all internet access. The following describes the internet access rules:

- All traffic from the LAN to the WAN is allowed - by default.
- All traffic from the WAN to the LAN is denied - by default.
- All traffic from the LAN to the DMZ is allowed - by default.
- All traffic from the DMZ to the LAN is denied - by default.
- All traffic from the WAN to the DMZ is allowed - by default.
- All traffic from the DMZ to the WAN is allowed - by default.

Users may define access rules and do more than the default rules. However, the following four extra service items are always on and are not affected by other user-defined settings.

- * HTTP Service (from LAN to Device) is on by default (for management)
- * DHCP Service (from LAN to Device) is set to on by default (for the automatic IP retrieval)
- * DNS Service (from LAN to Device) is on by default (for DNS service analysis)
- * Ping Service (from LAN to Device) is on by default (for connection and test)

Access Rule

Jump to /Page entries per page [Next Page >>](#)

Priority	Enabled	Action	Service	Source Interface	Source	Destination	Time	Day	Edit	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN3	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN4	Any	Any	Always			

In addition to the default rules, all the network access rules will be displayed as illustrated above. Users may follow or self-define the priority of each network access rule. The device will follow the rule priorities one by one, so please make sure the priority for all the rules can suit the setting rules.

Item	Description
Edit	Define the network access rule item
Delete	Remove the item.
Add New Rule	Create a new network access rule
Return to Default Rule	Restore all settings to the default values and delete all the self-defined settings.

9.2.2 Add New Access Rule

Service

Action :	Allow	
Service :	All Traffic [TCP&UDP/1-65535]	Service Management
Log :	No log	
Source Interface :	LAN	
Source IP :	ANY	
Dest. IP :	ANY	

Scheduling

Apply this rule	Always		:		to		:		(24-Hour Format)						
<input type="checkbox"/>	Everyday	<input type="checkbox"/>	Sun	<input type="checkbox"/>	Mon	<input type="checkbox"/>	Tue	<input type="checkbox"/>	Wed	<input type="checkbox"/>	Thu	<input type="checkbox"/>	Fri	<input type="checkbox"/>	Sat

Item	Description
Action	Allow: Permits the pass of packets compliant with this control rule. Deny: Prevents the pass of packets not compliant with this control rule.
Service Port	From the drop-down menu, select the service that users grant or do not give permission.
Service Port Management	If the service that users wish to manage does not exist in the drop-down menu, press – Service Management to add the new service. From the pop-up window, enter a service name and communications protocol and port, and then click the “Add to list” button to add the new service.
Log	No Log: There will be no log record. Create Log when matched: Event will be recorded in the log.
Interface	Select the source port whether users are permitted or not (for example: LAN, WAN1,

	WAN2 or Any). Select from the drop-down menu.
Source IP	Select the source IP range (for example: Any, Single, Range, or preset IP group name). If Single or Range is selected, please enter a single IP address or an IP address within a session.
Dest. IP	Select the destination IP range (such as Any, Single, Range, or preset IP group name) If Single or Range is selected; please enter a single IP address or an IP address within a session.
Scheduling	Select "Always" to apply the rule on a round-the-clock basis. Select "from", and the operation will run according to the defined time.
Apply this rule	Select "Always" to apply the rule on a round-the-clock basis. If "From" is selected, the activation time is introduced as below
... to ...	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)
Day Control	"Everyday" means this period of time will be under control everyday. If users only certain days of a week should be under control, users may select the desired days directly.
Apply	Click "Apply" to save the configuration.
Cancel	Click "Cancel" to leave without making any change.

9.3 URL Filter

The device supports two webpage restriction modes: one is to block certain forbidden domains, and the other is to give access to certain web pages. Only one of these two modes can be selected.

- Block Forbidden Domains
 Accept Allowed Domains

- Forbidden Domains Enabled
 Enable Website Blocking by Keywords

Scheduling

Apply this rule	Always ▾	00 : 00 to 00 : 00 (24-Hour Format)
<input type="checkbox"/> Everyday	<input type="checkbox"/> Sun	<input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat

Block Forbidden Domain

Fill in the complete website such as www.sex.com to have it blocked.

- Block Forbidden Domains
 Accept Allowed Domains

- Forbidden Domains Enabled

Forbidden Domains

Forbidden Domains

Add

Exception IP address ▾ : 0 . 0 . 0 . 0 to 0

Group test ▾ IP Grouping

Item	Description
Forbidden Domains Enabled	Click to enable the forbidden domains function. Default is Disabled.
Add	Input the website to be controlled. For example, www.playboy.com
Exception IP Address	Input the IP or IP ranges not to be controlled.
Add to list	Click "Add to list" to create a new website to be controlled.
Delete selected domain	Click to select one or more controlled websites and click this option to delete.
Apply	Click " Apply " to save the configuration.
Cancel	Click " Cancel " to leave without making any change.

Website Blocking by Keywords

Enable Website Blocking by Domain Keywords

Website Blocking by Domain Keywords

Keywords

Add

Exception IP address 0 . 0 . 0 . 0 to 0

Group test IP Grouping

Item	Description
Enabled	Click to activate this feature. The default setting is disabled. For example: If users enter the string "sex", any websites containing "sex" will be blocked.
Keywords (Only for English keyword)	Enter keywords.
Add to List	Add this new service item content to the list.
Delete selected item	Delete the service item content from the list

Apply	Click "Apply" to save the modified parameters.
Cancel	Click "Cancel" to cancel all the changes made to the parameters.

Accept Allowed Domains

In some companies or schools, employees and students are only allowed to access some specific websites.

This is the purpose of the function.

- Block Forbidden Domains
 Accept Allowed Domains

Allowed Domains Enabled

Allowed Domains

Item	Description
Enabled	Activate the function. The default setting is "Disabled."
Domain Name	Input the allowed domain name, etc. www.google.com
Add to list	Add the rule to list.
Delete selected item	Users can select one or more rules and click to delete.
Apply	Activate the function. The default setting is "Disabled."

Exception IP address :

You can exempted some IP addresses or IP group from the "Allow Domain".

Exception

Item	Description
Exception IP address/Group	Enter the exempted IP addresses or IP group.
Add to list	Click this button to add exempted IP addresses or IP group.
Delete selected range	Click this button to delete selected exempted IP address or IP group.

Content Filter Scheduling

Select **“Always”** to apply the rule on a round-the-clock basis. Select **“from”**, and the operation will run according to the defined time. For example, if the control time runs from 8 a.m. to 6 p.m., Monday to Friday, users may control the operation according to the following illustrated example.

Scheduling

Item	Description
Always:	Select “Always” to apply the rule on a round-the-clock basis. Select “from” , and the operation will run according to the defined time.
...to...:	Select “Always” to apply the rule on a round-the-clock basis. If “From” is selected, the activation time is introduced as below
Day Control:	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)

Chapter 10: Advanced Function

This chapter will introduce to you the advance router settings In the advance settings, you can:

1. Setup DMZ servers forwarding to WAN, for example, the Web or FTP servers.
2. Setup static routing entries or dynamic routing protocol.
3. Setup one to one NAT function to mapping public IP address and private IP address.
4. Setup dynamic DNS service.
5. Setup MAC address in interfaces.

10.1 DMZ Host/ Port Range Forwarding

DMZ Host

DMZ Private IP Address 192.168.1.0

Port Range Forwarding

Service :	All Traffic [TCP&UDP/1~65535]
	Service Management
IP Address :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Interface :	ANY
Enabled :	<input type="checkbox"/>
	Add to list
	Delete selected application

[Show Table](#)

[Apply](#)

[Cancel](#)

10.1.1 DMZ Host

When the NAT mode is activated, sometimes users may need to use applications that do not support virtual IP addresses such as network games. We recommend that users map the device actual WAN IP addresses

directly to the Intranet virtual IP addresses, as follows:

If the "DMZ Host" function is selected, to cancel this function, users must input "0" in the following "DMZ Private IP". This function will then be closed. After the changes are completed, click "Apply" to save the network configuration modification, or click "Cancel" to leave without making any changes.

10.1.2 Port Range Forwarding

Setting up a Port Forwarding Virtual Host: If the server function (which means the server for an external service such as WWW, FTP, Mail, etc) is contained in the network, we recommend that users use the firewall function to set up the host as a virtual host, and then convert the actual IP addresses (the Internet IP addresses) with Port 80 (the service port of WWW is Port 80) to access the internal server directly. In the configuration page, if a web server address such as 192.168.1.50 and the Port 80 has been set up in the configuration, this web page will be accessible from the Internet by keying in the device actual IP address such as, <http://210.66.155.78>.

At this moment, the device actual IP will be converted into "192.168.1.50" by Port 80 to access the web page.

In the same way, to set up other services, please input the server TCP or UDP port number and the virtual host IP addresses.

Port Range Forwarding

Service : All Traffic [TCP&UDP/1~65535]

IP Address : . . .

Interface : ANY

Enabled :

Item	Description
Service	To select from this option the default list of service ports of the virtual host that users want to activate. Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and 21~21 for FTP. Please refer to the list of default service ports.
IP Address	Input the virtual host IP address.
Interface	Select the WAN port.
Enabled	Activate this function.
Service Management	Add or remove service ports from the list of service ports.
Add to list	Add to the active service content.

Service Port Management

The services in the list mentioned above are frequently used services. If the service users want to activate is not in the list, we recommend that users use "Service Port Management" to add or remove ports, as follows:

Item	Description
Service Name	Input the name of the service port users want to activate on the list, such as E-donkey, etc.
Protocol	To select whether a service port is TCP or UDP.
Port Range	To activate this function, input the range of the service port locations users want to

	activate.
Add to list	Add the service to the service list.
Delete selected item	To remove the selected services.
Apply	Click the “Apply” button to save the modification.
Cancel	Click the “Cancel” button to cancel the modification. This only works before “Apply” is clicked.
Close	Quit this configuration window.

10.2 UPnP

UPnP (Universal Plug and Play) is a protocol set by Microsoft. If the virtual host supports UPnP system (such as Windows XP), users could also activate the PC UPnP function to work with the device.

UPnP Setup

Item	Description
Service Port	Select the UPnP service number default list here; for example, WWW is 80~80, FTP is 21~21. Please refer to the default service number list.
Host Name or IP Address	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.
Enabled	Activate this function.
Service Port Management	Add or remove service ports from the management list.

Add to List	Add to active service content.
Delete Selected Item	Remove selected services.
Show Table	This is a list which displays the current active UPnP functions.
Apply	Click "Apply" to save the network configuration modification.

10.3 Routing

In this chapter we introduce the Dynamic Routing Information Protocol and Static Routing Information Protocol.

Dynamic Routing

Working Mode:	<input checked="" type="radio"/> Gateway <input type="radio"/> Router
RIP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Receive RIP versions :	None <input type="button" value="v"/>
Transmit RIP versions :	None <input type="button" value="v"/>

Static Routing

Dest. IP :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Hop Count :	<input type="text"/>
Interface :	LAN <input type="button" value="v"/>
<input type="button" value="Add to list"/>	
<div style="border: 1px solid black; height: 100px; width: 100%;"></div>	
<input type="button" value="Delete selected item"/>	

10.3.1 Dynamic Routing

The abbreviation of Routing Information Protocol is RIP. There are two kinds of RIP in the IP environment – RIP I and RIP II. Since there is usually only one router in a network, ordinarily just

Static Routing will be used. RIP is used when there is more than one router in a network, and if an administrator doesn't want to assign a path list one by one to all of the routers, RIP can help refresh the paths. RIP is a very simple routing protocol, in which Distance Vector is used. Distance Vector determines transmission distance in accordance with the number of routers, rather than based on actual session speed. Therefore, sometimes it will select a path through the least number of routers, rather than through the fastest routers.

Dynamic Routing

Working Mode:	<input checked="" type="radio"/> Gateway <input type="radio"/> Router
RIP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Receive RIP versions :	None
Transmit RIP versions :	None

Item	Description
Working Mode	Select the working mode of the device: NAT mode or Router mode.
RIP	Click "Enabled" to open the RIP function.
Receive RIP versions	Use Up/Down button to select one of "None", "RIPv1", "RIPv2", "Both RIPv1 and v2" as the "TX" function for transmitting dynamic RIP.
Transmit RIP versions	Use Up/Down button to select one of "None", "RIPv1", "RIPv2-Broadcast", "RIPv2-Multicast" as the "RX" function for receiving dynamic RIP.

10.3.2 Static Routing

When there are more than one router and IP subnets, the routing mode for the device should be configured as static routing. Static routing enables different network nodes to seek necessary paths automatically. It also enables different network nodes to access each other. Click the button "**Show Routing Table**" (as in the figure) to display the current routing list.

Static Routing

Dest. IP : . . .
 Subnet Mask : . . .
 Default Gateway : . . .
 Hop Count :
 Interface : LAN

Item	Description
Dest. IP Subnet Mask	Input the remote network IP locations and subnet that is to be routed. For example, the IP/subnet is 192.168.2.0/255.255.255.0.
Gateway	The default gateway location of the network node which is to be routed.
Hop Count	This is the router layer count for the IP. If there are two routers under the device, users should input "2" for the router layer; the default is "1". (Max. is 15.)
Interface	This is to select "WAN port" or "LAN port" for network connection location.
Add to List	Add the routing rule into the list.
Delete Selected Item	Remove the selected routing rule from the list.
Show Table	Show current routing table.
Apply	Click " Apply " to save the network configuration modification
Cancel	Click " Cancel " to leave without making any changes.

10.4 One to One NAT

As both the device and ATU-R need only one actual IP, if ISP issued more than one actual IP (such as eight ADSL static IP addresses or more), users can map the remaining real IP addresses to the intranet PC virtual IP addresses. These PCs use private IP addresses in the Intranet, but after having One to One NAT mapping, these PCs will have their own public IP addresses.

For example, if there are more than 2 web servers requiring public IP addresses, administrators can map several public IP addresses directly to internal private IP addresses.

Example :Users have five available IP addresses - 210.11.1.1~5, one of which, 210.11.1.1, has been configured as a real IP for WAN, and is used in NAT. Users can respectively configure the other four real IP addresses for Multi-DMZ, as follows:

210.11.1.2 . 192.168.1.3

210.11.1.3 . 192.168.1.4

210.11.1.4 . 192.168.1.5

210.11.1.5 . 192.168.1.6

**Attention**

The device WAN IP address can not be contained in the One-to-One NAT IP configuration.

Enable One-to-One NAT **One to One NAT**

Add Range


Private Range Begin:

Public Range Begin:

Range Length:

Enable Multiple to One NAT

Item	Description
Enabled One to One NAT	To activate or close the One-to-One NAT function. (Check to activate the function).
Private IP Range Begin	Input the Private IP address for the Intranet One-to-One NAT function.
Public IP Range Begin	Input the Public IP address for the Internet One-to-One NAT function.
Range Length	The numbers of final IP addresses of actual Internet IP addresses. (Please do not include IP addresses in use by WANs.)
Add to List	Add this configuration to the One-to-One NAT list.
Delete Selected Item	Remove a selected One-to-One NAT list.
Apply	Click " Apply " to save the network configuration modification.
Cancel	Click "Cancel" to leave without making any changes.

 Attention	<p>One-to-One NAT mode will change the firewall working mode. If this function has been set up, the Internet IP server or PC which is mapped with a LAN port will be exposed on the Internet.</p> <p>To prevent Internet users from actively connecting with the One-on-One NAT server or PC, please set up a proper denial rule for access, as described Firewall.</p>
---	---

Multiple to One NAT

Enable Multiple to One NAT

Multiple to One NAT

Private IP Range: ... to .

Representative Public IP: ...

Interface:

Item	Description
Enable Multiple to One NAT	Click to enable multiple to one NAT function.
Private IP Range	Input intranet IPs for NAT mapping.
Respective Public IP	Input the respective public IP addresses. This should go along with the following interface selection. If the IP address is not within the interface ranges, the setting will not work.
Interface	Select the mapping interface. If the WAN IP above is not within the interface range, the setting will not work.
Add to List	Add this configuration to the One-to-One NAT list.
Delete selected	Remove a selected One-to-One NAT list.

range	
Apply	Click "Apply" to save the network configuration modification.
Cancel	Click "Cancel" to leave without making any changes.

10.5 DDNS- Dynamic Domain Name Service

DDNS supports the dynamic web address transfer for 3322.org、DynDNS.org and DtDNS.com. This is for connections to a website that is built with dynamic IP addresses, and for dynamic IP remote control. For example, the actual IP address of an ADSL PPPoE time-based system or the actual IP of a cable modem will be changed from time to time. To overcome this problem for users who want to build services such as a website, it offers the function of dynamic web address transfer. This service can be applied from www.3322.org, www.dyndns.org, or www.dtdns.com, and these are free.

Also, in order to solve the issue that DDNS server is not stable, the device can update the dynamic IP address with different services at the same time.

DDNS Setup

Interface	Status	Host Name	Config.
WAN 1	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	Edit
WAN 2	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	Edit
WAN 3	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	Edit
WAN 4	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	Edit
USB	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	Edit

Select the WAN port to which the configuration is to be edited, for example, WAN 1. Click the hyperlink to enter and edit the settings.

Interface: WAN 1

 DynDNS.org

User Name:	<input type="text"/>	<input type="button" value="Register"/>
Password:	<input type="password"/>	
Host Name:	<input type="text"/>	<input type="text"/>
Internet IP Address:	0.0.0.0	
Status:	DDNS function is disabled or No Internet connection.	

 3322.org

User Name:	<input type="text"/>	<input type="button" value="Register"/>
Password:	<input type="password"/>	
Host Name:	<input type="text"/>	<input type="text"/>
Internet IP Address:	0.0.0.0	
Status:	DDNS function is disabled or No Internet connection.	

Item	Description
Interface	This is an indication of the WAN port the user has selected.
DDNS	Check either of the boxes before DynDNS.org, 3322.org and DtDNS.com to select one of the four DDNS website address transfer functions.
Username	The name which is set up for DDNS. Input a complete website address such as abc.abcdns.org.cn as a user name for abcDDNS.
Password	The password which is set up for DDNS.
Host Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.
Internet IP Address	Input the actual dynamic IP address issued by the ISP.
Status	An indication of the status of the current IP function refreshed by DDNS.
Apply	After the changes are completed, click " Apply " to save the network configuration modification.
Cancel	Click " Cancel " to leave without making any changes.

10.6 MAC Clone

Some ISP will request for a fixed MAC address (network card physical address) for distributing IP address, which is mostly suitable for cable mode users. Users can input the network card physical address (MAC address: 00-xx-xx-xx-xx-xx) here. The device will adopt this MAC address when requesting IP address from ISP.

MAC Clone

Interface	MAC Address	Config.
WAN 1	00-30-4F-00-A4-F8	Edit
WAN 2	00-30-4F-00-A4-F9	Edit
WAN 3	00-30-4F-00-A4-FA	Edit
WAN 4	00-30-4F-00-A4-FB	Edit
WAN 5	00-30-4F-00-A4-FC	Edit

Select the WAN port to which the configuration is to be edited; click the hyperlink to enter and edit its configuration. Users can input the MAC address manually. Press “Apply” to save the setting, and press “Cancel” to remove the setting. Default MAC address is the WAN MAC address.

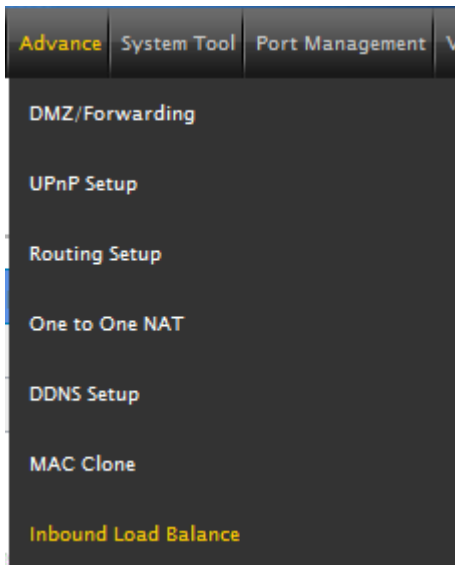
Interface WAN 1

User Defined WAN MAC Address :	<input checked="" type="radio"/> 00 -30 -4F -00 -A4 -F8
	Default 00-30-4F-00-A4-F8
MAC Address from this PC	<input type="radio"/> 00-30-4F-0B-3E-6E

10.7 Inbound Load Balance

SG-4800 not only supports efficient Outbound Load Balance, but Inbound Load Balance. It distributes inbound traffic equally to every WAN port to make best use of bandwidth. It also can prevent traffic from unequally distribution and congested. Users can use only one device to satisfy the demand of Inbound/Outbound Load Balance simultaneously.

Following introduces how to enable and setup Inbound Load Balance step by step.



Inbound Load Balance

Domain Name	Edit
	<input type="button" value="Edit"/>
	<input type="button" value="Edit"/>

1. Click "Edit" to enter setting UI.
2. Enable "Inbound Load Balance."

Inbound Load Balance

Enabled Inbound Load Balance

Domain Name	TTL	Administrator
<input type="text"/>	7200	<input type="text"/> @ <input type="text"/>

DNS Server Settings (NS Record)

Name Server	Interface
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>

Host Record (A Record)

Host Name	WAN IP
<input type="text"/>	<input type="checkbox"/> WAN 1: <u>192.168.4.195</u> <input type="checkbox"/> WAN 2: <u>0.0.0.0</u> <input type="checkbox"/> WAN 3: <u>0.0.0.0</u> <input type="checkbox"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input type="checkbox"/> WAN 1: <u>192.168.4.195</u> <input type="checkbox"/> WAN 2: <u>0.0.0.0</u> <input type="checkbox"/> WAN 3: <u>0.0.0.0</u> <input type="checkbox"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input type="checkbox"/> WAN 1: <u>192.168.4.195</u> <input type="checkbox"/> WAN 2: <u>0.0.0.0</u> <input type="checkbox"/> WAN 3: <u>0.0.0.0</u> <input type="checkbox"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input type="checkbox"/> WAN 1: <u>192.168.4.195</u> <input type="checkbox"/> WAN 2: <u>0.0.0.0</u> <input type="checkbox"/> WAN 3: <u>0.0.0.0</u> <input type="checkbox"/> WAN 4: <u>0.0.0.0</u>

Alias Record (CName Record)

Alias	Target
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Mail Server(MX Record)

[SPF settings](#)

Host Name	Weight	Mail Server
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

3. Configure SG-4800 Domain Name

Inbound Load Balance

Enabled Inbound Load Balance

Domain Name	TTL	Administrator
<input type="text"/>	7200	<input type="text"/> @ <input type="text"/>

Item	Description
Domain Name	Input the Domain Name which is users applied before. The domain name will be shown in following configuration automatically without entering again.
Time To Live	Time To Live (the abbreviation is TTL) is time interval of DNS inquiring (second, 0~65535). Too long interval will affect refresh time. Shorter time will increase system's loading, but the effect of Inbound Load Balance will be more correct. You can adjust according your reality application.
Administrator	Enter administrator's E-mail address, e.g. test@abc.com.tw.

4. DNS Server Settings: Add or Modify NS Record. (NS Record)

NS Record is the record of DNS server to assign which DNS server translates the domain name.

DNS Server Settings (NS Record)

Name Server	Interface
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>
<input type="text"/>	<input checked="" type="radio"/> WAN 1: <u>192.168.4.195</u> <input type="radio"/> WAN 2: <u>0.0.0.0</u> <input type="radio"/> WAN 3: <u>0.0.0.0</u> <input type="radio"/> WAN 4: <u>0.0.0.0</u>

Item	Description
DNS Server	Input registered NS Record, ex. ns1, ns2.
Interface	Assign WAN IP address as corresponding IP of NS Record. The system will show all acquired enabled WAN IP addresses automatically so that users can check directly. But users have to check if the IP addresses are the same as the corresponding settings on DNS service provider. (Ex. ns1.abc.com.tw ⇔ WAN1: 210.10.1.1, ns2.abc.com.tw ⇔ WAN2: 200.1.1.1)

5. Host Record: Add or modify host record. (A Record)

Host Record (A Record)

Host Name	WAN IP
<input type="text"/>	<input type="checkbox"/> WAN 1: 192.168.4.195 <input type="checkbox"/> WAN 2: 0.0.0.0 <input type="checkbox"/> WAN 3: 0.0.0.0 <input type="checkbox"/> WAN 4: 0.0.0.0
<input type="text"/>	<input type="checkbox"/> WAN 1: 192.168.4.195 <input type="checkbox"/> WAN 2: 0.0.0.0 <input type="checkbox"/> WAN 3: 0.0.0.0 <input type="checkbox"/> WAN 4: 0.0.0.0
<input type="text"/>	<input type="checkbox"/> WAN 1: 192.168.4.195 <input type="checkbox"/> WAN 2: 0.0.0.0 <input type="checkbox"/> WAN 3: 0.0.0.0 <input type="checkbox"/> WAN 4: 0.0.0.0
<input type="text"/>	<input type="checkbox"/> WAN 1: 192.168.4.195 <input type="checkbox"/> WAN 2: 0.0.0.0 <input type="checkbox"/> WAN 3: 0.0.0.0 <input type="checkbox"/> WAN 4: 0.0.0.0

Item	Description
Host Name	Input the host name which provides services. E.g. mail server or FTP.
WAN IP	Check corresponding A Record IP (WAN Port IP). If more than one IPs is checked, Inbound traffic will be distributed on this WANs.

6. Alias Record: Add or modify alias record. (CNAME Record)

This kind of record allows you to assign several names to one computer host, which may provide several services on it.

For instance, there is a computer whose name is "host.mydomain.com" (A record). It provides WWW and Mail services concurrently. Administrator can configure as two CNAME: WWW and Mail. They are "www.mydomain.com" and "mail.mydomain.com". They are both orientated to "host.mydomain.com."

You can also assign several domain names to the same IP address. One of the domains will be A record

corresponding server IP, and the others will be alias of A record domain. If you change your server IP, you don't have to modify every domain one by one. Just changing A record domain, and the other domains will be assigned to new IP address automatically.

Alias Record (CName Record)

Alias	Target
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Item	Description
Alias	Input Alias Record corresponding to A Record.
Target	Input the existed A Record domain name.

7. Mail Server: Add or modify mail server record.

MX Record is directed to a mail server. It orientates to a mail server according to the domain name of an E-mail address. For example, someone on internet sends a mail to user@myhomain.com. The mail server will search MX Record of mydomain.com through DNS. If the MX Record exists, sender PC will send mails to the mail server assigned by MX Record.

Mail Server(MX Record)

[SPF settings](#)

Host Name	Weight	Mail Server
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Item	Description
Host Name	Display the host name without domain name of mail host.
Weight	Indicate the order of several mail hosts, the smaller has more priority.
Mail Server	Input the server name which is saved in A Record or external mail server.

Click "**Apply**" button to save the configuration. Besides, users have to configure DNS service port as following description.

8. Enable DNS Query (DNS service port) in Access Rule of Firewall setting.

Add a new access rule in Firewall setting to enable DNS service port of the WAN on which Inbound Load Balance need to be enabled.

Item	Description
Action	Check "Allow".
Service Port	From the drop-down menu, select "DNS [UDP/53~53]."
Log	Check "Enable" if DNS Query data should be recorded.
Interface	Check the WAN port on which Inbound Load Balance is enabled.
Source IP	Select "Any".
Dest. IP	Select WAN port and input correspondingly IP of the domain name. Take the previous example, input 210.10.1.1.
Scheduling	Select "Always".

9. Enable internal IP and service port corresponding to A Record in Port Range Forwarding of Advanced Function.

Port Range Forwarding

Service : All Traffic [TCP&UDP/1~65535]

IP Address : . . .

Interface : ANY

Enabled :

Item	Description
Service Port:	Activate the service port of A Record server, e.g. SMTP [TCP/25~25] for Mail.
Internal IP:	Input the internal IP of A Record, e.g. 192.168.8.100 of Mail server.
Interface:	Select the WAN port of A Record and corresponding IP.
Enable:	Activate the configuration.
Add to List:	Add to the active service content.

Chapter 11: System Tool

System Tool

This chapter introduces the management tool for controlling the device and testing network connection. For security consideration, we strongly suggest to change the password. Password and Time setting is in Chapter 5.2.

11.1 Diagnostic

The device provides a simple online network diagnostic tool to help users troubleshoot network-related problems. This tool includes **DNS Name Lookup** (Domain Name Inquiry Test) and **Ping** (Packet Delivery/Reception Test).

DNS Lookup Ping

Ping host or IP address

DNS Name lookup

On this test screen, please enter the host name of the network users want to test. For example, users may enter www.yahoo.com.tw and press "Go" to start the test. The result will be displayed on this page.

DNS Lookup Ping

Look up domain name

Name: www.yahoo.com.tw
Address: 203.84.219.114

Ping

DNS Lookup Ping

Ping host or IP address


Status Test Succeeded
Packets: 4/4 transmitted,4/4 received,0 % loss
Round Trip Time: Minimum = 3.2 ms
 Maximum = 3.7 ms
 Average = 3.4 ms

This item informs users of the status quo of the outbound session and allows the user to know the existence of computers online.

On this test screen, please enter the host IP that users want to test such as 168.95.1.1 Press "Go" to start the test. The result will be displayed on this screen.

11.2 Firmware Upgrade

Users may directly upgrade the device firmware on the Firmware Upgrade page. Please confirm all information about the software version in advance. Select and browse the software file, click "**Firmware Upgrade Right Now**" to complete the upgrade of the designated file.

 Attention	Please read the warning before firmware upgrade. Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.
---	---

Firmware Upgrade

- Warning**
1. Choosing previous firmware versions will restore all settings to default.
 2. Firmware upgrading may take a few minutes, don't turn off power or press reset.
 3. Don't close the window or disconnect during upgrading process.
 4. Please suspend on-line traffics when upgrading the new firmware.

Firmware Version : v1.0.1 .01 (May 23 2012 19:26:13)

11.3 Configuration Backup

Import Configuration File

Export Configuration File

IP & MAC Binding

QoS

Protocol Binding

Save The Configuration into the Flash Memory

- Every hours Save the Configuration File into Flash Memory.
- When You Reset the Router, The System Will Save The Configurations Into The Flash Memory Automatically.




Import Configuration File

This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to **import** the file.

Export Configuration File

This feature allows users to backup all parameter settings. Click "Export" and select the location to save the "config.exp" file. And you also can separately export the rules (IP&MAC binding, QoS, and Protocol Binding) or import these rules from "Import Configuration File" above.

Save The Configuration into the Flash Memory

Item	Description		
Every_ hours Save the Configuration File into Flash Memory.	Set how many time to save the Configuration File into Flash Memory. The default time is 24 hours. <table border="1" data-bbox="408 389 1428 488"><tr><td data-bbox="408 389 579 488"> Attention</td><td data-bbox="579 389 1428 488">We recommend don't un-tick this item, cause if the rule not save to the flash memory, after reset the router the configuration will be clear.</td></tr></table>	 Attention	We recommend don't un-tick this item, cause if the rule not save to the flash memory, after reset the router the configuration will be clear.
 Attention	We recommend don't un-tick this item, cause if the rule not save to the flash memory, after reset the router the configuration will be clear.		
When You Reset the Router, The System Will Save The Configurations Into The Flash Memory Automatically.	Check this item and before the router reboot, the configuration will be save to the flash memory. You also can click the "Save to Flash" button to save the configuration to the flash memory, the default is checked.		

11.4 SNMP

Simple Network Management Protocol (SNMP) refers to network management communications protocol and it is also an important network management item. Through this SNMP communications protocol, programs with network management (i.e. SNMP Tools-HP Open View) can help communications of real-time management. The device supports standard SNMP v1/v2c and is consistent with SNMP network management software so as to get hold on to the operation of the online devices and the real-time network information.

SNMP Setup

Enabled SNMP

System Name	CS-5800
System Contact	
System Location	
Get Community Name	public
Set Community Name	private
Trap Community Name	public
Send SNMP Trap to	<input type="text"/>

(IPv4)

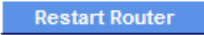
Apply Cancel

Item	Description
Enabled	Activate SNMP feature. The default is activated.
System Name	Set the name of the device such as Planet.
System Contact	Set the name of the person who manages the device (i.e. John).
System Location	Define the location of the device (i.e. Taipei).
Get Community Name	Set the name of the group or community that can view the device SNMP data. The default setting is "Public".
Set Community Name	Set the name of the group or community that can receive the device SNMP data. The default setting is "Private".
Trap Community Name	Set user parameters (password required by the Trap-receiving host computer) to receive Trap message.
Send SNMP Trap to	Set one IP address or Domain Name for the Trap-receiving host computer.
Apply	Press "Apply" to save the settings.
Cancel	Press "Cancel" to keep the settings unchanged.

11.5 System Recover

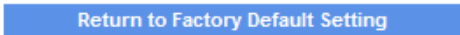
Users can restart the device with System Recover button.

Restart



Restart Router

Factory Default



Return to Factory Default Setting

Restart

As the figure below, if clicking “Restart Router” button, the dialog block will pop out, confirming if users would like to restart the device.

Restart



Restart Router

Message from webpage

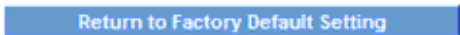


Are you sure you want to restart router?

OK

Cancel

Factory Default



Return to Factory Default Setting

Return to Factory Default Setting

If clicking “Return to Factory Default Setting”, the dialog block will pop out, if the device will return to factory default. It's recommended to save the current configuration before upgrading firmware. After firmware upgraded, import the configuration file after returning to factory default to ensure system stable. (Please refer to 12.3)

11.6 High Availability

High Availability is adopted in the network that requires fault tolerance and backup mechanism. Two similar devices are used to be the backup for each other. One of these devices is employed for major network transmitting, and the other redundant device will take over when the master device fails to assure that network transmitting and services never break down. Therefore, administrators will have more opportunity and time to deal with the master device problems.

Besides general HA, Planet also provides advanced HA function that enables two devices to operate simultaneously. It brings full cost efficiency without making another device idle. It does not have to be the same model. All of Planet devices which support HA can achieve the function.

High Availability

High Availability	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Mode:	<input type="radio"/> Hardware Backup Mode	<input checked="" type="radio"/> Two devices are operating simultaneously
Operation:	<input checked="" type="radio"/> Master Mode (DHCP Enable)	<input type="radio"/> Slave Mode (DHCP Disable)
Master / Slave Mode setting Of two devices must be different		
WAN Backup:	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 (The checked WAN are not working in this device.)	
LAN Gateway Backup:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
MAC Address of the backup device:	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	
Status:	Disable	

Apply Cancel

Item	Description
High Availability	<p>Enable: Activate HA function.</p> <p>Disable: Disable HA function.</p>
Mode	<p>(1) Hardware Backup Mode</p> <p>It is the general backup mode. The master device takes responsibility of network transmitting and the other one is set as idle. When the master device fails transmitting, it will send out the message to the idle device for taking over network transmitting immediately.</p> <p>(2) Two devices are operating simultaneously</p> <p>Two devices operate outbound linking simultaneously, but they are still separated as Master device and Backup device. In normal situation, Master device is major DHCP IP issuer, and Backup device will disable DHCP issuing automatically. When Master device fails transmitting, the Backup device will take over all outbound links and enable DHCP server to provide IP addresses.</p>

Following is the description of the two different modes.

High Availability Enable Disable
Mode: Hardware Backup Mode Two devices are operating simultaneously
Operation: Master Mode Backup Mode
 Master / Slave Mode setting Of two devices must be different
Status: Normal
Status of the backup device: Normal

Item	Description
Operation-Master Mode	Indicates the master device will operate for all outbound links. When the master device fails transmitting, the backup device will take over.
Status	“Status- Normal” indicates the device operates well.
Status of the backup device	Indicates status of backup device. If the status is normal, administrators can login the device remotely to manage. (Remote Management should be enabled). “Status- Abnormal” indicates the backup device can not be detected or does exist, and need to inspect the backup device actual status.

High Availability Enable Disable
Mode: Hardware Backup Mode Two devices are operating simultaneously
Operation: Master Mode Backup Mode
 Master / Slave Mode setting Of two devices must be different
LAN IP of the backup device: . . .
MAC Address of the backup device: : : : : :
Status: Disable

Item	Description
Operation-Backup Mode	Indicates the backup device will take over when the master fails transmitting. WAN and LAN IP setting in backup device should be the same as those of master device. The backup device should not be in charge of network transmitting and DHCP server. ※ If the original LAN IP addresses are issued by Master device, DHCP server

	setting of Backup device should be the same as Master device. The Backup device can keep DHCP functioning and there will be no LAN disconnection.
LAN IP of the backup device	Input LAN IP of Master mode, which is backed up.
MAC Address of the backup device	Input Master device MAC address, which is backed up.
Status	<p>“Status- Normal” indicates the status is idle. Master device operates normally.</p> <p>“Status- Backup” indicates the device takes over all the network transmitting. The status will return to “Normal” when Master device boots normally and send a message to the backup device. Then, the status will return to Normal, which the backup device remains idle.</p>

Two devices are operating simultaneously:

High Availability Enable Disable

Mode: Hardware Backup Mode Two devices are operating simultaneously

Operation: Master Mode (DHCP Enable) Slave Mode (DHCP Disable)

Master / Slave Mode setting Of two devices must be different

WAN Backup: WAN 1 WAN 2 WAN 3 WAN 4
 WAN 5
(The checked WAN are not working in this device.)

LAN Gateway Backup: 192 . 168 . 1 . 5

MAC Address of the backup device: 00 : 30 : 4f : 12 : 34 : 56

Status: Disable

Item	Description
Operation-Master Mode	Besides operating network with another device, Master device is also the DHCP server to issue LAN IP addresses. Although Slave device also supports outbound linking, its DHCP server is disabled.
WAN Backup (The Checked WANs are not working in this device.)	The checked WANs will works in the other device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in the other device, WAN3 and WAN4 should be checked.
LAN Gateway Backup	Input LAN IP of Slave device. The IP should be different from LAN IP of Master device.
MAC Address of the backup device	Input LAN MAC of Slave device. It should be different from LAN MAC of Master device.

Status	“Status-Normal” means both two devices operate normally. “Status-Backup” indicates Slave mode has problems, and the device enables backup to take over WAN
---------------	--

High Availability Enable Disable

Mode: Hardware Backup Mode Two devices are operating simultaneously

Operation: Master Mode (DHCP Enable) Slave Mode (DHCP Disable)
 Master / Slave Mode setting Of two devices must be different

WAN Backup: WAN 1 WAN 2 WAN 3 WAN 4
 WAN 5
 (The checked WAN are not working in this device.)

LAN Gateway Backup: 192 . 168 . 1 . 5

MAC Address of the backup device: 00 : 30 : 4f : 12 : 34 : 56

Status: Disable

Item	Description
Operation-Slave Mode	<p>Although working with master device, Backup device's DHCP server is disabled. LAN users need to transmit traffic through the WAN on Slave device. You should add LAN IP of Slave device into Master device DHCP server default gateway, which is DHCP server IP address.</p> <p>For example, if the DHCP server's IP of Master device is 192.168.1.1, and the subnet mask is 255.255.255.0, Slave device should be in the same subnet, ex. 192.168.1.2.</p>
WAN Backup (The Checked WANs are not working in this device.)	The checked WANs will work in another device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in another, WAN3 and WAN4 should be checked.
LAN Gateway Backup	Input the LAN IP of Master device. It should be different from Slave device's IP. (Must be in the same subnet.)
MAC Address of the backup device	Input the LAN MAC of Master device. It should be different from Slave device's LAN MAC.
Status	“Status-Normal” indicates both devices work normally; “Status-Backup” indicates the Backup device is enabled for backing up Master device to take over WAN connection and DHCP issuing function.

Chapter 12. Log

From the log management and look up, we can see the relevant operation status, which is convenient for us to facilitate the setup and operation.

12.1 System Log

Its system log offers three options: system log, E-mail alert, and log setting.

Syslog Configuration

Enable Syslog

Syslog Server : Name or IP Address

Log Setting

Alert Log		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> Unauthorized Login Attempt	

General Log		
<input type="checkbox"/> Deny Policies	<input type="checkbox"/> Allow Policies	<input checked="" type="checkbox"/> Authorized Login

[View System Log](#)

[Outgoing Log Table](#)

[Incoming Log Table](#)

[Clear Log Now](#)

[Apply](#)

[Cancel](#)

System Log

Syslog Configuration

Enable Syslog

Syslog Server : Name or IP Address

Item	Description
Enabled	If this option is selected, the System Log feature will be enabled.
Syslog Server	The device provides external system log servers with log collection feature. System log is an industrial standard communications protocol. It is designed to dynamically capture related system message from the network. The system log provides the source and the destination IP addresses during the connection, service number, and type. To apply this feature, enter the system log server name or the IP address into the empty "system log server" field.

Log Setting

Log Setting

Alert Log		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> Unauthorized Login Attempt	

General Log		
<input type="checkbox"/> Deny Policies	<input type="checkbox"/> Allow Policies	<input checked="" type="checkbox"/> Authorized Login

[View System Log](#)
[Outgoing Log Table](#)
[Incoming Log Table](#)
[Clear Log Now](#)

Alert Log

The device provides the following warning message. Click to activate these features: Syn Flooding, IP Spoofing, Win Nuke, Ping of Death / Unauthorized Login Attempt.

Item	Description
Syn Flooding	Bulky syn packet transmission in a short time causes the overload of the system storage of record in connection information.
IP Spoofing	Through the packet sniffing, hackers intercept data transmitted on the network. After they access the information, the IP address from the sender is changed so that they can access the resource in the source system.
Win Nuke	Servers are attacked or trapped by the Trojan program.
Ping of Death	The system fails because the sent data exceeds the maximum packet that can be handled by the IP protocol.
Unauthorized Login	If intruders into the device are identified, the message will be sent to the system log.

General Log

The device provides the following warning message. Click to activate the feature. System error message, blocked regulations, regulation of passage permission, system configuration change and registration verification.

Item	Description
Deny Policies	If remote users fail to enter the system because of the access rules; for instance, message will be recorded in the system log.
Allow Policies	If remote users enter the system because of compliance with access rules; for instance, message will be recorded in the system log.
Authorized Login	Successful entry into the system includes login from the remote end or from the LAN into this device. These messages will be recorded in the system log.

The following is the description of the four buttons allowing online inquiry into the log.

View System Log

This option allows users to view system log. The message content can be read online via the device. They include **All Log**, **System Log**, **Access Log**, and **Firewall Log**, which is illustrated as below.

System Log		
Current Time: Tue Jun 26 18:35:04 2012	All Log	Refresh Close
Time ▲	Event-Type	Message
Apr 27 13:48:58 2012	System Log	5WAN_8LAN_QoS_Security_Router : System is up

Outgoing Packet Log

View system packet log which is sent out from the internal PC to the Internet. This log includes LAN IP, destination IP, and service port that is applied. It is illustrated as below.

Time ▲	Event-Type	Message
Feb 6 03:46:03 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->77.239.233.64:20301 on ixp2
Feb 6 03:46:06 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->84.10.118.17:10682 on ixp7
Feb 6 06:27:54 2006	Connection Refused - Policy violation	TCP 192.168.1.1:80->192.168.1.100:1224 on ixp0
Feb 6 08:18:58 2006	Connection Refused - Policy violation	TCP 192.168.1.101:18195->163.253.104.148:1234 on ixp1
Feb 6 08:19:53 2006	Connection Refused - Policy violation	TCP 192.168.1.101:51671->3.139.58.12:1234 on ixp1

Incoming Packet Log

View system packet log of those entering the firewall. The log includes information about the external source IP addresses, destination IP addresses, and service ports. It is illustrated as below.

Incoming Log Table

Current Time: Fri Mar 4 20:14:20 2011

Time ▲	Event-Type	Message
Feb 6 02:34:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->255.255.255.255:68 on ixp2
Feb 6 02:57:54 2006	Connection Refused - Policy violation	UDP 192.168.1.100:137->192.168.1.255:137 on ixp0
Feb 6 03:06:39 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.102:68 on ixp2
Feb 6 03:15:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.100:68 on ixp4
Feb 6 03:45:58 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->75.128.47.253:27220 on ixp0
Feb 6 03:46:00 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->91.153.161.189:27310 on ixp0
Feb 6 03:46:02 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->24.160.250.156:19343 on ixp0

Clear Log Now

This feature clears all the current information on the log.

12.2 System Statistic

The device has the real-time surveillance management feature that provides system current operation information such as port location, device name, current WAN link status, IP address, MAC address, subnet mask, default gateway, DNS, number of received/ sent/ total packets , number of received/ sent/ total Bytes, Received and Sent Bytes/Sec., total number of error packets received, total number of the packets dropped, number of session, number of the new Session/Sec., and upstream as well as downstream broadband usage (%).

System Statistic


[Next Page](#)

Interface :	WAN 1	WAN 2	WAN 3	WAN 4
Device Name :	eth1	eth2	eth3	eth4
Status :	Connect	Enabled	Enabled	Enabled
Device IP Address :	192.168.4.103	0.0.0.0	0.0.0.0	0.0.0.0
MAC Address :	00-30-4F-32-30-31	00-30-4F-32-30-32	00-30-4F-32-30-33	00-30-4F-32-30-34
Subnet Mask :	255.255.254.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway :	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS :	192.168.5.121	0.0.0.0	0.0.0.0	0.0.0.0
Network Service Detection :	Test Succeeded	Test Failed	Test Failed	Test Failed
Received Packets :	3266	0	0	0
Transmitted Packets :	122	0	0	0
Total Packets :	3388	0	0	0
Received Packets Byte :	332884	0	0	0
Transmitted Packets Byte :	19797	0	0	0
Total Packets Byte :	352681	0	0	0
Received Byte/Sec :	293	0	0	0
Transmitted Byte/Sec :	0	0	0	0
Error Packets :	0	0	0	0
Dropped Packets :	0	0	0	0
Sessions :	0	0	0	0
New Sessions/Sec :	0	0	0	0
Upstream Bandwidth Usage :	0	0	0	0
Downstream Bandwidth Usage :	0	0	0	0

12.3 Traffic Statistic

Six messages will be displayed on the **Traffic Statistic** page to provide better traffic management and control.


Traffic Statistic


Traffic Type	Inbound IP Address 
	<ul style="list-style-type: none">Inbound IP AddressOutbound IP AddressInbound ServiceOutbound ServiceInbound SessionOutbound Session

By Inbound IP Address

The figure displays the source IP address, bytes per second, and percentage.

Traffic Statistic


Traffic Type	Inbound IP Address 	
<input checked="" type="checkbox"/> Enabled Traffic Statistic		
Source IP	bytes/sec	%
192.168.1.100	294	100




By outbound IP Address

The figure displays the source IP address, bytes per second, and percentage.

Traffic Statistic

Traffic Type	Outbound IP Address 	
<input checked="" type="checkbox"/> Enabled Traffic Statistic		
Source IP	bytes/sec	%
192.168.1.100	31	100



By Outbound Service

The figure displays the network protocol type, destination IP address, bytes per second, and percentage.

Traffic Statistic

Traffic Type
 Enabled Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	http(80)	32	56
TCP	1144	17	30
TCP	1863	3	6
UDP	137	2	4
TCP	netbios(139)	1	2

By Inbound Service

The figure displays the network protocol type, destination IP address, bytes per second, and percentage.

Traffic Statistic

Traffic Type
 Enabled Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	1863	37	65
TCP	1144	11	20
TCP	http(80)	8	14

By Outbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

Traffic Statistic

Traffic Type

Protocol	Dest. Port	bytes/sec	%
----------	------------	-----------	---

By Inbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address,

destination port, bytes per second and percentage.

Traffic Statistic

Traffic Type		Inbound Session				
<input checked="" type="checkbox"/> Enabled Traffic Statistic						
Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2940	192.168.5.126	1144	9	100

12.4 IP/ Port Statistic

The device allows administrators to inquire a specific IP (or from a specific port) about the addresses that this IP had visited, or the users (source IP) who used this service port. This facilitates the identification of websites that needs authentication but allows a single WAN port rather than Multi-WANs. Administrators may find out the destination IP for protocol binding to solve this login problem. For example, when certain port software is denied, inquiring about the IP address of this specific software server port may apply this feature. Moreover, to find out BT or P2P software, users may select this feature to inquire users from the port.

IP/Port Statistic

Enabled IP/Port Statistic IP Address

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
-----------	----------	-------------	-----------------	----------	------------	----------------------	--------------------

Specific IP Status :

Enter the IP address that users want to inquire, and then the entire destination IP connected to remote devices as well as the number of ports will be displayed.

IP/Port Statistic

Enabled IP/Port Statistic IP Address

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2959	WAN1	74.120.121.3	80	8	32
192.168.1.100	TCP	2940	WAN1	192.168.5.126	1144	11	20
192.168.1.100	TCP	3036	WAN1	192.168.5.27	445	1	1
192.168.1.100	TCP	2958	WAN1	65.54.189.156	1863	0	0
192.168.1.100	TCP	2942	WAN1	192.168.5.121	49156	0	0
192.168.1.100	TCP	3128	WAN1	118.160.195.248	1894	0	0
192.168.1.100	TCP	2947	WAN1	192.168.5.120	49157	0	0

Specific Port Status

Enter the service port number in the field and IP that are currently used by this port will be displayed.

IP/Port Statistic

Enabled IP/Port Statistic Port Port: 0 Search

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2959	WAN1	74.120.121.3	80	8	33
192.168.1.100	TCP	3576	WAN1	203.69.113.18	80	0	0

Refresh