



ALL-VPN10

VPN/Firewall WLAN-N WAN Router



User's Manual

Content

I.	Introduction.....	5
II.	Multi- WAN VPN Router Installation	7
2.1	Systematic Setting Process.....	7
2.2	Setting Flow Chart.....	7
III.	Hardware Installation.....	10
3.1	LED Signal.....	10
3.2	VPN Router Network Connection	12
IV.	Login.....	13
V.	V. Device Spec Verification, Status Display and Login Password and Time Setting	15
5.1	Home Page.....	15
5.1.1	WAN Status.....	15
5.1.2	Physical Port Status.....	16
5.1.3	System Information	17
5.1.4	Firewall Status	17
5.2	Change and Set Login Password and Time	19
5.2.1	Password Setting	19
5.2.2	Time.....	20
VI.	Network	22
6.1	Network Connection	22
6.1.1	Host Name and Domain Name	22
6.1.2	LAN Setting.....	23
6.1.3	WAN Settings.....	24
6.2	Multi- WAN Setting	34
6.2.1	Load Balance Mode	35
6.2.2	Network Service Detection.....	39
6.2.3	Protocol Binding	41
VII.	Intranet Configuration.....	51
7.1	Port Management.....	51
7.2	IP/ DHCP	52
7.3	DHCP Status	54
7.4	IP & MAC Binding.....	56
VIII.	Wireless Network	60
8.1	Basic Configuration	61
8.2	Security Setting	63
8.3	Station List	71
IX.	QoS (Quality of Service).....	72
9.1	Bandwidth Management	73
9.1.1	The Maximum Bandwidth provided by ISP	74

- 9.1.2 QoS 74
- 9.2 Session control 80
- 9.3 Smart QoS 83
- X. Firewall.....85**
- 10.1 General Policy 85
- 10.2 Access Rule..... 87
 - 10.2.1 Add New Access Rule..... 88
- 10.3 Content Filter 91
- XI. L7 Management95**
- 11.1 L7 Filter (1) Rule list: 95
- 11.2 L7 VIP Priority Channel 99
- 11.3 L7 QoS 104
- 11.4 Application Define 110
- 11.5 Applicatios Status..... 111
- XII. VPN (Virtual Private Network)..... 113**
- 10.1. VPN 113
 - 10.1.1. Add a New VPN Tunnel 114
 - 10.1.2. PPTP Server 134
 - 10.1.3. VPN Pass Through 136
- 10.2. QVM VPN Function Setup 137
- XIII. Advanced Function..... 139**
- 11.1 DMZ Host/ Port Range Forwarding 139
 - 11.1.1 DMZ Host 139
 - 11.1.2 Port Range Forwarding 139
- 11.2 UPnP 142
- 11.3 Routing..... 143
- 11.4 One to One NAT 145
- 10.5 DDNS- Dynamic Domain Name Service 147
- 11.6 MAC Clone 149
- 11.7 USB Storage 150**
- XIV. System Tool..... 155**
- 12.1 Diagnostic 155
- 12.2 Firmware Upgrade 157
- 12.3 Configuration Backup..... 158
- 12.4 SNMP 159
- 12.5 System Recover 161
- XV. Log 163**
- 13.1 System Log 163
- 13.2 System Statistic 166



13.3 Traffic Statistic..... 168

13.4 IP/ Port Statistic..... 168

XVI. Log out 170

Appendix I: Technical Support Information.....171

Appendix II Federal Communication Commission Interference Statement..... 172

I. Introduction

IPSec VPN QoS Router (referred as VPN Router hereby) is a business level security router that efficiently integrates new generation multiple WAN-port devices. It meets the needs of medium enterprises, internet cafés, campus, dorm and communities, etc.

VPN Router has 1~2 10/100 Base-T/TX Ethernets (RJ45) WAN ports. These WAN ports can support auto load balance mode, exclusive mode (remaining WAN balance), and strategy routing mode for high-efficiency network. They offer super flexibility for network set-up. Moreover, these WAN ports also support DHCP, fixed IP, PPPoE, transparent bridge, VPN connection, port binding, static routing, dynamic routing, NAT, one to one NAT, PAT, MAC Clone, as well as DDNS.

To fulfill the requirement for a highly secure and integrated firewall, VPN Router has a 64-bit hardware acceleration, high-speed, high-efficiency processor embedded. With high processing speed, plusing high standard SDRAM and Flash, VPN Router brings users super networking efficiency. Its processing speed and capacity are almost equal to those of expensive enterprise-level VPN Routers. This is why the device is so popular with modern enterprises.

In addition to internet connectability, for the broadband market, VPN Router has the function of VPN virtual network connection. It is equipped with a virtual private network hardware acceleration mode which is widely used in modern enterprises, and offers full VPN functionality.

is a supporter of the IPSec Protocol. IPSec VPN provides DES, 3DES, AES128, AES192, AES256 encryption, MD5, SH1 certification, IKE Pre-Share Key, or manual password interchange. VPN Router also supports aggressive mode. When a connection is lost, VPN Router will automatically re-connect. In addition, the device features NetBIOS transparency.

VPN Router offers the function of a standard PPTP server, which is equipped with connection setting status. Each WAN port can be set up with multiple DDNS at the same time. It is also capable of establishing VPN connections with dynamic IP addresses.

VPN Router also has unique QVM VPN- SmartLink IPSec VPN. Just input VPN server IP, user name, and password, and IPSec VPN will be automatically set up. Through VPN Router exclusive QVM function, it offers easy VPN allocation for users; users can do it even without a network administrator. VPN Router enables enterprises to benefit from VPN without being troubled with technical and network management problems. The central control function enables the host to log in remote client computers at any time. Security and secrecy are guaranteed to meet the IPSec standard, so as to ensure the continuity of VPN service.

The advanced built-in firewall function enables VPN Router to resist most attacks from the Internet. It utilizes active detection technology SPI (Stateful Packet Inspection). The SPI firewall functions mainly within the network by dynamically inspecting each link. The SPI firewall also has a warning function for the application process; therefore, it can refuse links to non-standard communication protocols. VPN Router supports network address translation (NAT) function and routing modes. It makes the network environment more flexible and easier to manage.

Through web- based UI, VPN Router enables enterprises to have their own network access rules . To control web access, users can build and edit filter lists. It also enables users to ban or monitor websites according to their needs. By the filter setting and complete OS management, school and business internet management will be clearly improved. VPN Router offers various on-line SysLog records. It supports on-line management setup tools; it makes setting up networks easy to understand. It also reinforces the management of network access rules, VPN, and all other network services.

VPN Router fully protects the safety of communication between all offices and branches of an organization.



It helps to free enterprises from increasing hacker intrusion. With an exclusive independent operation platform, users are able to set up and use a firewall without professional network knowledge. VPN Router setting up and management can be carried out through web browsers, such as IE, Netscape, etc.

II. Multi- WAN VPN Router Installation

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 VPN 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 efficientness, block attacks, and prevent security risks at the same time. Through the process settings, users can install and operate VPN Router easily. This simplifies the management and maintenance, making the user network settings be done at one time. The main process is as below:

1. Hardware installation
2. Login
3. Verify device specification and set up password and time
4. Set WAN connection
5. Set LAN connection: physical port and IP address settings
6. Set QoS bandwidth management: avoid bandwidth occupation
7. Set Firewall: prevent attack and improper access to network resources
8. Other settings: UPnP, DDNS, MAC Clone
9. Management and maintenance settings: Syslog, SNMP, and configuration backup
10. VPN (Virtual Private Network)
11. Logout

2.2 Setting Flow Chart

Below is the description for each setting process, and the correspondent contents and purposes. For detailed functions, please refer to Appendix I: Setting Interface and Chapter Index.

#	Setting	Content	Purpose
1	Hardware installation	Configure the network to meet user's demand.	Install the device hardware based on user physical requirements.
2	Login	Login the device with Web Browser.	Login the device web- based UI.
3	Verify device specification	Verify Firmware version and working status.	Verify the device specification, Firmware version and working status.
	Set password and time	Set time and re- new password.	Modify the login password considering safe issue. Synchronize 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 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.
6	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 P2P during working time. They can also protect network from Worm or ARP attacking.
7	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
8	Management and maintenance settings: Syslog, SNMP, and configuration backup	Monitor VPN Router working status and configuration backup.	Administrators can look up system log and monitor system status and inbound/outbound flow in real time.

9	VPN Virtual Private Network	Configure VPN tunnels	Configure different types of VPN to meet different application environment.
10	Logout	Close configuration window.	Logout VPN Router web- based UI.

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

III. Hardware Installation

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

3.1 LED Signal

LED Signal Description

LED	Color	Description
Power	Green	Green LED on: Power ON
DIAG	Amber	Amber LED on: System self-test is running. Amber LED blinking: System not ready Amber LED off: System self-test is completed successfully.
Link/Act	Green	Green LED on: Port has been connected & Get IP. Green LED blinking: Packets are transmitting through Ethernet port.
100M- Speed	Amber	Amber LED on: Ethernet is running at 100Mbps. Amber LED off: Ethernet is running at 10Mbps.
WLAN	Green	Green LED on: Wireless function is enabled. Green LED blinking: Packets are transmitting.
WPS	Green	Green LED on: WPS function is working.

Reset

Action	Description
Press Reset Button For 5 Secs	Warm Start DIAG indicator: Amber LED flashing slowly.
Press Reset Button Over 10 Secs	Factory Default DIAG indicator: Amber LED flashing quickly.

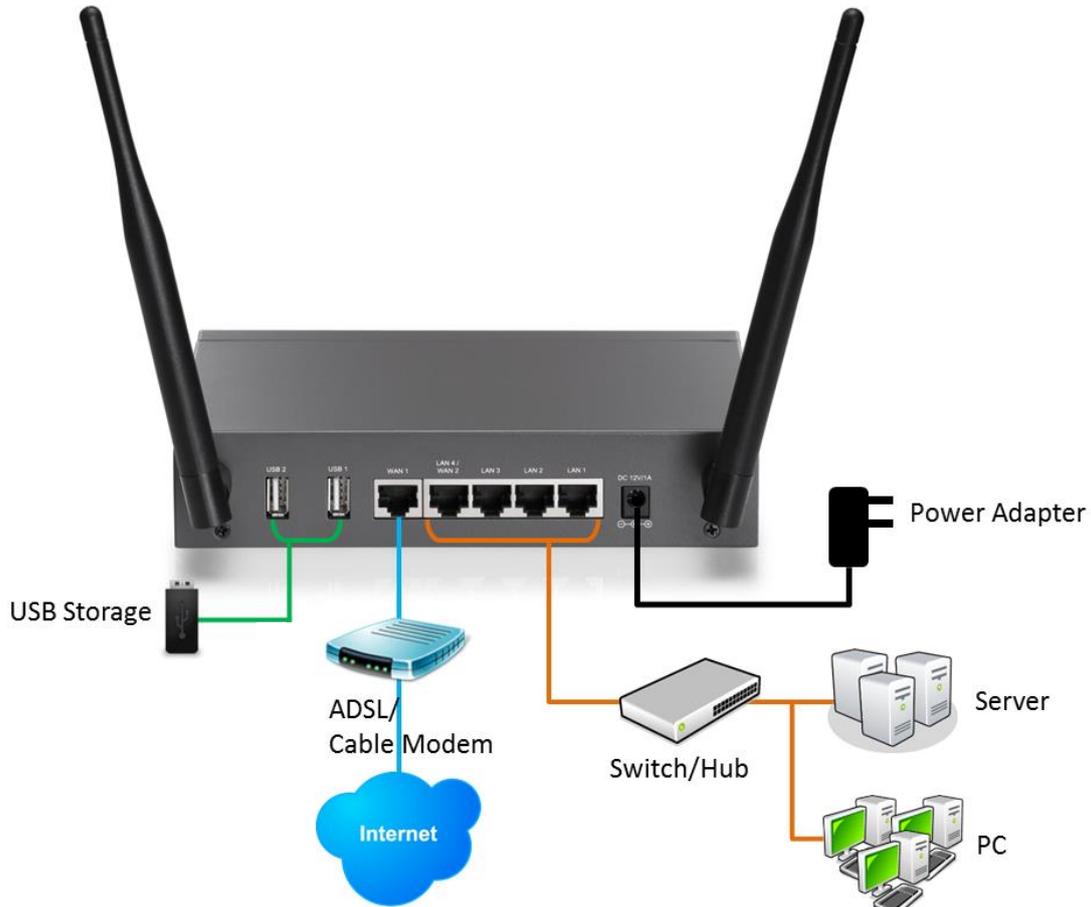
Installing Router on a Wall

The Router has two wall-mount slots on its bottom panel. When mounting the device on a wall, please ensure that the heat dissipation holes are facing sideways as shown in the following picture for safety reasons. is not responsible for damages incurred by insecure wall-mounting hardware.

Specifications

Model Name	ALL-VPN10
CPU	MTK 6856-700MHz
Flash/DRAM	16M/128M
WAN Port	1~2 (10/100)
LAN Port	3~4 (10/100)
USB Port	2
Wireless Antenna	5dBi *2
Operating Frequency	2.4GHz
Frequency Band	2400-2483.5MHz
Operating Channels	11 for 802.11b, 802.11g, 802.11n (H20) 7 for 802.11n(HT40)
Output Power	802.11b: 19.8dBm 802.11g: 22.3dBm 802.11n (HT20): 24.51dbm 802.11n (HT40) 22.07 dbm
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85% non-condensing
Storage Humidity	5% to 90% non-condensing
Power Supply	External Power Adapter 12V1A
Weight	715g
Dimensions	190x130x40mm

3.2 VPN Router Network Connection



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 Mangement” configuration is done.

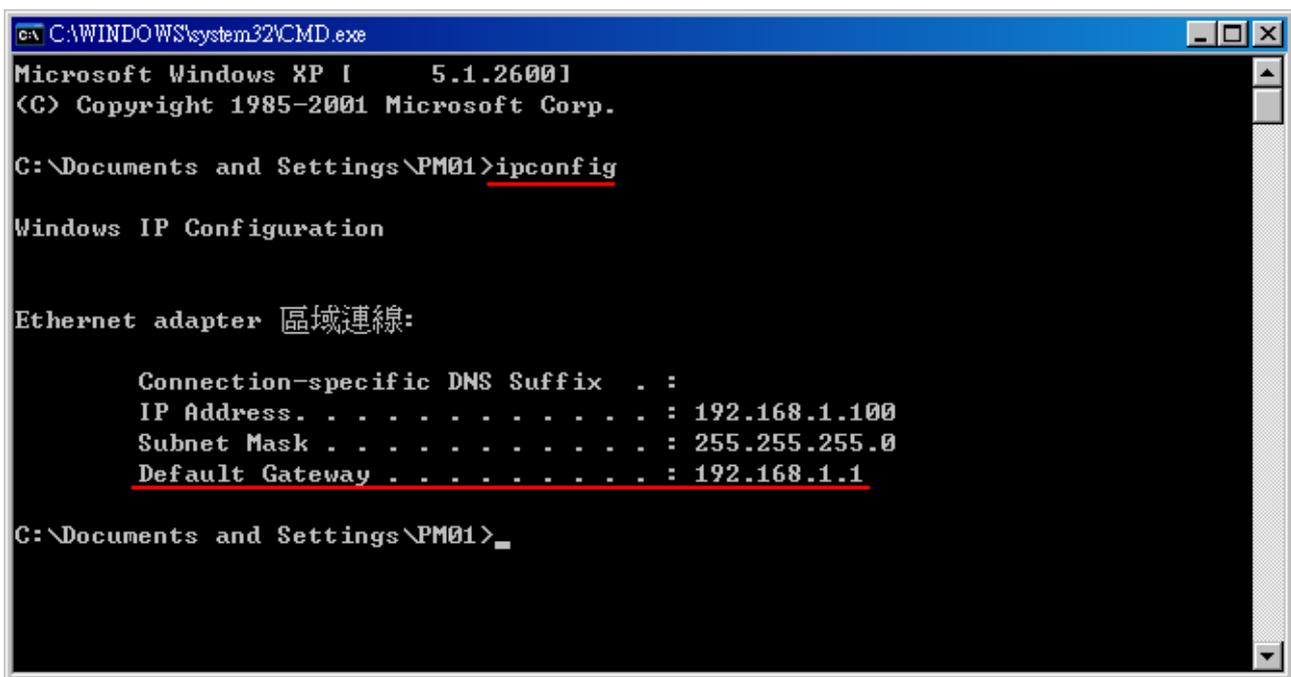
DMZ : The DMZ port can be connected to servers that have legal IP addresses, such as Web servers, mail servers, etc.

Please use only the power supply unit that is delivered with the device.

IV. Login

This chapter is mainly introducing Web- based UI after connecting the device.

First, check up the device's IP address by connecting to DOS through the LAN PC under the device. Go to Start → Run, enter cmd to command 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 the router.



```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [ 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\PM01>ipconfig

Windows IP Configuration

Ethernet adapter 區域連線:

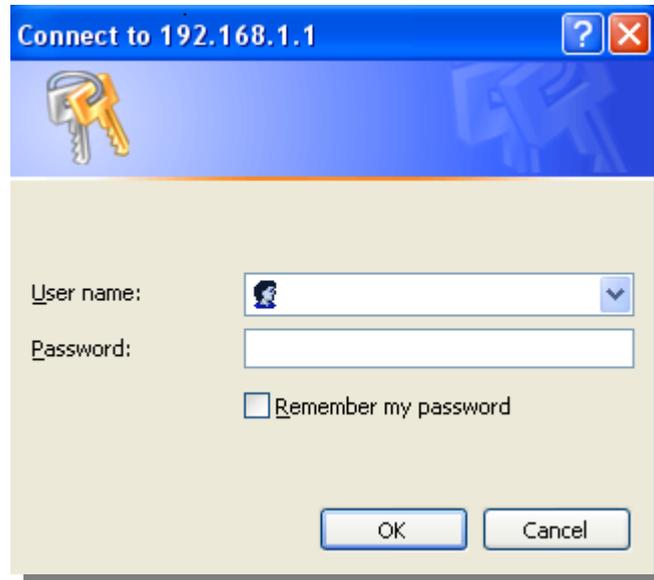
    Connection-specific DNS Suffix . :
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

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:



The device's 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 can not login to the device. Press Reset button for more than 10 sec, all the setting will return to default.

V. V. Device Spec Verification, Status Display and Login Password and Time Setting

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 the device's parameters and status are listed for users' reference.

5.1.1 WAN Status

WAN Status

Interface	WAN 1	WAN 2
WAN IP Address	221.169.231.22	0.0.0.0
Default Gateway	221.169.231.1	0.0.0.0
DNS	139.175.55.244 139.175.252.16	0.0.0.0
Downstream Bandwidth (KBytes/sec)	3	0
Upstream Bandwidth (KBytes/sec)	111	0
DDNS Setup	Dyndns Disabled NOIP Disabled	Dyndns Disabled NOIP Disabled
Quality of Service	0 rules set	0 rules set
Manual Connect	Disconnect Connect	Release Renew

IP Address :	Indicates the current IP configuration for WAN port.
Default Gateway :	Indicates current WAN gateway IP address from ISP.
DNS Server :	Indicates the current DNS IP configuration.
Session :	Indicates the current session number for each WAN in the device.
Downstream Bandwidth :	Indicates the current downstream bandwidth for each WAN.
Upstream Bandwidth :	Indicates the current upstream bandwidth for each WAN.
DDNS :	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
Interface	LAN		
Status	Connect	Enabled	Enabled

Port ID	Internet	Internet
Interface	WAN 1	WAN 2
Status	Connect	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.

Port1 Information

Summary

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

Statistics

Received Packets Count	8761
Received Packets Byte Count	33668
Transmitted Packets Count	33601
Transmitted Packets Byte Count	11233453
Error Packets Count	0

The current port setting status information will be shown in the Port Information Table. Examples: type (10Base-T/100Base-TX), iniferface (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	SN1234567890abcd
IPv6 Address/Prefix Length	fc00::1/7	Firmware Version	v1.0.0.4 (Oct 23 2013 09:02:42)
Working Mode	Gateway	Current Time	Mon Oct 28 2013 06:32:17
System Active Time	3 Days2 Hours54 Minutes28 seconds		

LAN IP/Subnet Mask : Identifies the current device IP address. The default is 192.168.1.1.

Working Mode : Indicates the current working mode. Can be NAT Gateway or Router mode. The default is “NAT Gateway” mode.

System Active Time : Indicates how long the Router has been running.

Serial Number : This number is the Router serial number.

Firmware Version : Information about the Router present software version.

Current Time : Indicates the device present time. Please note: To have the correct time, users must synchronize the device with the remote NTP server first.

5.1.4 Firewall Status

Security Status

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

SPI (Stateful Packet Inspection) : Indicates whether SPI (Stateful Packet Inspection) is on or off. The default 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”.

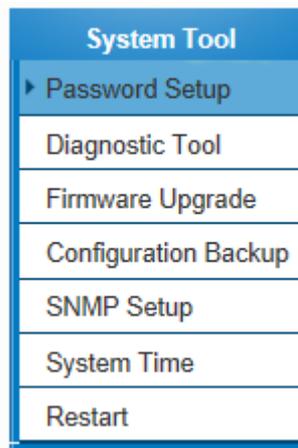
Remote Management: Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is “Off”.

Access Rule : Indicates the number of access rule applied in the device.

5.2 Change and Set Login Password and Time

5.2.1 Password Setting

When you login the device setting window every time, you must enter the password. The default value for the device 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 the device. You can press Reset button for more than 10 sec, the device will return back to default.



▶ Password Setup

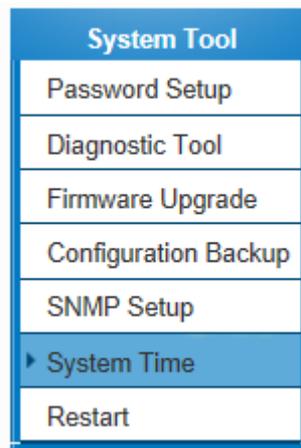
User Name	admin
Password	<input type="text"/>
New User Account	admin
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

User Name :	The default is "admin".
Old Password :	Input the original password. (The default is "admin".)
New User Name :	Input the new user name. i.e.VPN10
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.

5.2.2 Time

The device 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.

Synchronize with external NTP server : The device 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	Berlin (GMT+01:00) ▾
Daylight Saving	<input type="checkbox"/> Enabled from 05 (Month) 25 (Day) to 12 (Month) 25 (Day)
NTP Server	time.nist.gov

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

- Set the local time using Network Time Protocol (NTP) automatically
- Set the local time Manually

<input type="text" value="14"/>	Hours	<input type="text" value="49"/>	Minutes	<input type="text" value="8"/>	seconds
<input type="text" value="3"/>	Month	<input type="text" value="18"/>	Day	<input type="text" value="2164"/>	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.

VI. 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

Host Name :	ALL-VPN10	(Required by some ISPs)
Domain Name :	allnet.de	(Required by some ISPs)

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
 IPv6

LAN Setting

MAC Address 00 - 0E - A0 - AB - CD - EF (Default ff-ff-ff-ff-03)
Device IP Address : 192 . 168 . 1 . 1 Subnet Mask : 255 . 255 . 255 . 0
Multiple Subnet Setting: Disabled

Unified IP Management

WAN Setting

Please choose how many WAN ports you prefer to use : (Default 2)

Interface	Connection Type	Config.
WAN 1	PPPoE	Edit
WAN 2	Obtain an IP automatically	Edit

6.1.1 Host Name and Domain Name

Host Name :	ALL-VPN10	(Required by some ISPs)
Domain Name :	allnet.de	(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 LAN Setting

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.

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

IPv6

LAN Setting

MAC Address 00 - 0E - A0 - AB - CD - EF (Default ff-ff-ff-ff-03)					
Device IP Address : 192 . 168 . 1 . 1			Subnet Mask : 255 . 255 . 255 . 0		
Multiple Subnet Setting: Disabled					

Unified IP Management

Multiple-Subnet Setting :

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

Device IP Address 192 . 168 . 1 . 1

Subnet Mask 255 . 255 . 255 . 0

Multiple Subnet Setting

Multiple Subnet

LAN IP Address

Subnet Mask

Add to list

Delete selected Subnet

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.

6.1.3 WAN Settings

WAN Setting :

▶ WAN Setting

Please choose how many WAN ports you prefer to use : (Default 2)

Interface	Connection Type	Config.
WAN 1	PPPoE	Edit
WAN 2	Obtain an IP automatically	Edit

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) : . . .

EnabledLine-Dropped Scheduling

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

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

Backup Interface :

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 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 disconnection, 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.

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 Connection Type :

WAN IP Address : . . .

Subnet Mask : . . .

Default Gateway : . . .

DNS Server(Required) : . . .

DNS Server(Optional) : . . .

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 :

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 disconnection, 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.

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 Connection Type:

UserName:

Password:

Connect on Demand: Max Idle Time Min.

Keep Alive: Redial Period Sec.

EnabledLine-Dropped Scheduling

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

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

Backup Interface:

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.

<p>Enable Line-Dropped Scheduling</p>	<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: 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 disconnection, 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>
<p>Line-Dropped Period</p>	<p>Input the time rule for disconnection of this WAN service.</p>
<p>Line-Dropped Scheduling</p>	<p>Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.</p>
<p>Backup Interface</p>	<p>Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.</p>

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: WAN1

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.

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

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 disconnection, 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.

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: WAN1

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

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

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.

<p>Enable Line-Dropped Scheduling</p>	<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: 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 disconnection, 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>
<p>Line-Dropped Period</p>	<p>Input the time rule for disconnection of this WAN service.</p>
<p>Line-Dropped Scheduling</p>	<p>Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.</p>
<p>Backup Interface</p>	<p>Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.</p>

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

When you have multiple WAN gateways, you can use Traffic Management and Protocol Binding function to fulfill WAN road balancing, so that we can have highest network bandwidth efficiency.

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	<input type="text" value="Disabled"/>	Import IP Range
	Self-defined Strategy 1	<input type="text" value="Disabled"/>	
	Self-defined Strategy 2	<input type="text" value="Disabled"/>	

Network Service Detection

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

6.2.1 Load Balance Mode

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 ▾	

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.

- **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.

Specify WAN Binding 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.

- **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.

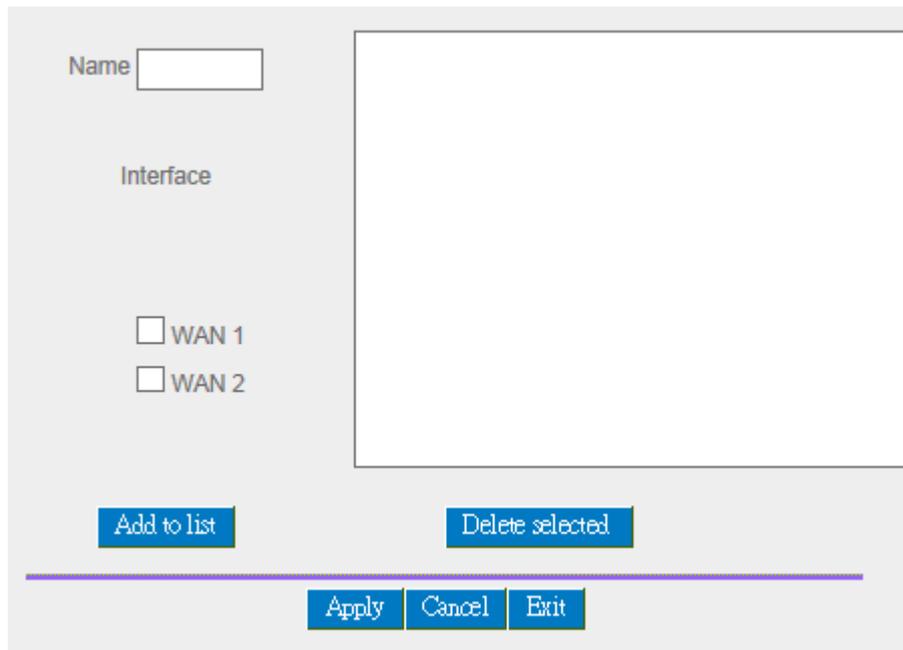
Please refer to the explanations in **6.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding.

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.



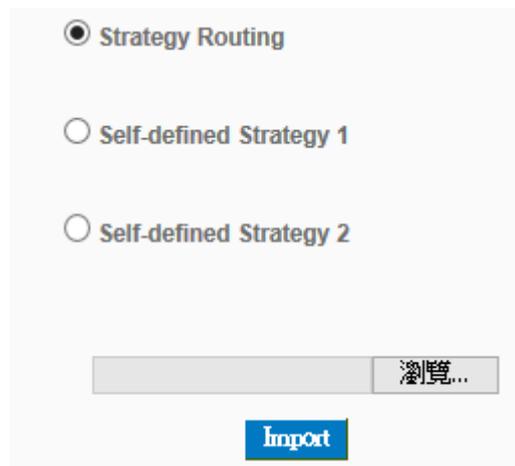
Name:	To define a name for the WAN grouping in the box, such as “Education” etc. The name is for recognizing different WAN groups.
Interface:	Check the boxes for the WANs to be added into this combination.
Add To List:	To add a WAN group to the grouping list.
Delete selected:	To remove selected WANs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

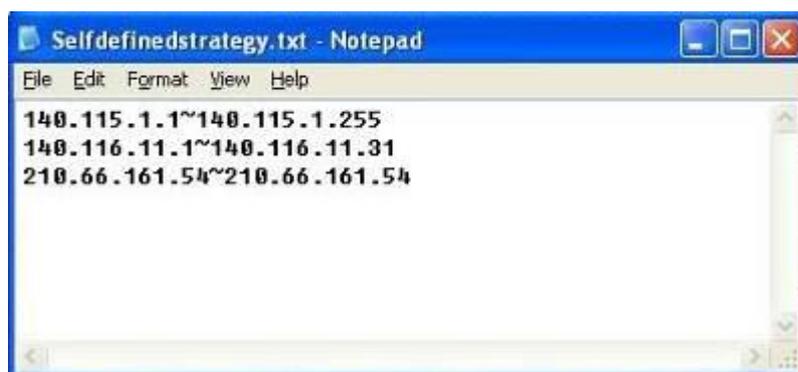
Import Strategy:

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.

6.2.2 Network Service Detection

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 OR ▼ Out bandwidth is over 1 % , regarded as normal.	
<input checked="" type="checkbox"/> Default Gateway	
<input type="checkbox"/> ISP Host	<input type="text"/>
<input type="checkbox"/> Remote Host	<input type="text"/>
<input type="checkbox"/> DNS Lookup Host	<input type="text"/>

Apply Cancel

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:	<p>(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> <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. For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while</p>

	<p>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>
<p>Detecting Feedback Servers:</p>	
<p>Default Gateway:</p>	<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>
<p>ISP Host:</p>	<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>
<p>Remote Host:</p>	<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>
<p>DNS Lookup Host:</p>	<p>This is the detect location for DNS. (Only a web address such as 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). Therefore, in this mode, we recommend assigning one of the connections to the first WAN. When other WANs (WAN2) 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.

6.2.3 Protocol Binding

Interface Configuration

Router allows maximum two 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.

Bandwidth Configuration

When Auto Load Balance mode is selected, the device will select sessions or IP and the WAN bandwidth will 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. The section refers to QoS configuration. Therefore, it should be set in QoS page. Please refer to 8.1 QoS bandwidth configuration.

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"/>

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) 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

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>
Dest. 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</p>

	Class B Network Segment of 210.11.x.x will 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 item:	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 Priority :

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.

Summary <input checked="" type="radio"/> Priority <input type="radio"/> Interface Refresh Close						
Priority	Interface	Service	Source IP	Dest. IP	Enable	Edit
1	WAN 1	[TCP&UDP/1~65535]	192.168.1.200~192.168.1.210	0.0.0.0~0.0.0.0	Enabled	Edit

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 Management” to arrange the list, as described in the following :

Service Name

Protocol v

Port Range to

All Traffic [TCP&UDP/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]
 TELNET [TCP/23~23]
 TELNET Secondary [TCP/8023~8023]

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.
Exit:	To quit this configuration window.

Auto Load Balancing 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 a 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

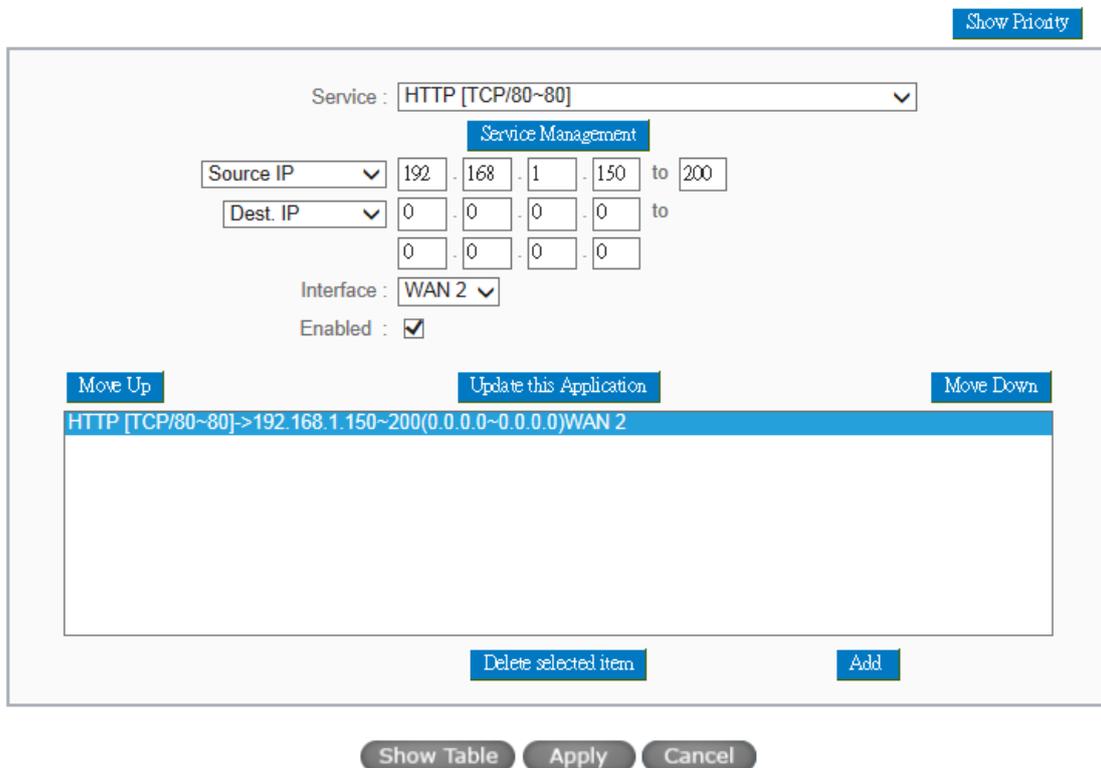
Delete selected item
Add

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



Service : HTTP [TCP/80~80]

Source IP : 192 . 168 . 1 . 150 to 200

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

Interface : WAN 2

Enabled :

HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN 2

Show Table Apply Cancel

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

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](#)

Protocol Binding

[Show Priority](#)

Service : HTTP [TCP/80~80] ▼

[Service Management](#)

Source IP ▼ 192 . 168 . 1 . 150 to 200

Dest. IP ▼ 0 . 0 . 0 . 0 to 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
HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN 2

[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

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

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

Delete selected item
Add

Show Table
Apply
Cancel

VII. Intranet Configuration

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

7.1 Port Management

Port Management

Port Setup
▶ Port Status

Port ID : LAN 1 ▼

▶ **Summary**

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

▶ **Statistics**

Received Packets Count	9159
Received Bytes Count	21530
Transmitted Packets Count	33808
Transmitted Bytes Count	11325728
Error Packets Count	0

Refresh

Summary :

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

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.

7.2 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.

IP/DHCP	
▶ DHCP Setup	
DHCP Status	
IP&MAC binding	
Router Advertisement	

IPv4
IPv6

Enabled DHCP Server

▶ **DHCP Dynamic IP**

Client Lease Time Minutes

DHCP Server	Enabled
IP Range Starts	192.168.1.100
IP Range Ends	192.168.1.149

Unified IP Management

▶ **DNS**

DNS(Required) 1:	0	0	0	0
DNS(Optional) 2:	0	0	0	0

▶ **WINS**

WINS Server 1:	0	0	0	0
WINS Server 2:	0	0	0	0

▶ **DNS Local Database**

Host Name :

IP Address :

Add to list

Delete selected item

Apply
Cancel

Dynamic IP :

Client lease Time :	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.
Range Start :	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 End :	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.

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.

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

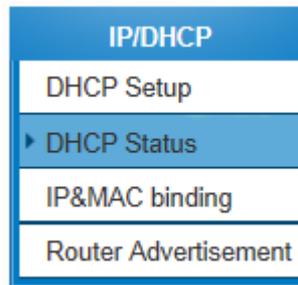
WINS :

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

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.

7.3 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

Status

Subnet	Subnet
DHCP Server	192.168.1.1
Dynamic IP Used	2
Static IP Used	0
DHCP Available	48
Total	50

Client Table

Subnet1

Host Name	IP Address	MAC Address	Client Lease Time	Delete
Nathan-PC	192.168.1.101	00:0f:3d:f1:a1:4e	20 Hours, 39 Minutes, 48 Seconds	
XP_1	192.168.1.102	00:0c:29:ff:78:25	20 Hours, 39 Minutes, 53 Seconds	

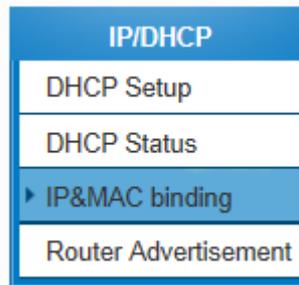
Refresh

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.
DHCP Available :	The amount of IP still available in the DHCP server.
Total :	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.

7.4 IP & MAC Binding

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 : 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

There are two methods for setting up this function :

(1) · 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 :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
MAC Address :	<input type="text"/> - <input type="text"/>
Name :	<input type="text"/>
Enabled :	<input type="checkbox"/>
<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"/>	

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

Apply

Cancel

(2) · IP & MAC Binding

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](#)

Static IP :	There are two ways to input static IP: <ol style="list-style-type: none"> 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				
192.168.1.102	00:0c:29:ff:78:25	<input type="text"/>	<input type="checkbox"/>				
192.168.1.101	00:0f:3d:f1:a1:4e	<input type="text"/>	<input type="checkbox"/>				

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.

VIII. Wireless Network

Wireless function is enabled by default. The WLAN LED will be on after system booting. Client device can find SSID as _AP_1. Please refer to following illustrations to change configuration.



8.1 Basic Configuration

Enabled Wireless Network

Wireless Network

Network Mode :	11bgn Mixed Mode <input type="button" value="v"/>
Country Code :	EUR (Europe) <input type="button" value="v"/>
Frequency Channel :	Auto <input type="button" value="v"/> <input type="button" value="Scanning"/>
WMM Capable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="button" value="Advance"/>
Tx Power :	100 (Range 1-100, Default 100)
Channel Bandwidth :	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40

SSID Summary

No.	Status	SSID	Broadcast SSID	AP Isolation	Security Mode	Access Filter	Guest Access	Edit
1	Enabled	ALL-VPN10_1	Enabled	Disabled	Disable	Disable	Disabled	<input type="button" value="Edit"/>
2	Disabled	ALL-VPN10_2	Enabled	Disabled	Disable	Disable	Disabled	<input type="button" value="Edit"/>
3	Disabled	ALL-VPN10_3	Enabled	Disabled	Disable	Disable	Disabled	<input type="button" value="Edit"/>
4	Disabled	ALL-VPN10_4	Enabled	Disabled	Disable	Disable	Disabled	<input type="button" value="Edit"/>

Enable Wireless Netwrk	Check the box to enable wireless function.
Network Mode	The default value is "11bgn Mixed Mode". "11bgn Mixed Mode", "11b Only", "11g only" and "11n Only" also can be chosen. The default value is recommended.
Country Code	Choose the country where you are.
Frequency Channel	Means the channel of frequency of the wireless LAN.Please choose the channel which is still available to avoid interference. Users can also check "Auto" so that the system will choose a suitable channel automatically.
WMM Capable	WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.
WMM Capable <input type="button" value="Advance"/>	APSD (automatic power-save delivery) APSD is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Direct Link Setup(DLS)

	<p>This function will greatly improve the data transfer rate between WMM-enabled wireless devices.</p> <p>WMM AP Parameter Setting</p> <p>Wifi Multimedia(WMM)</p> <p>APSD Capable : <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>DLS Capable : <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>WMM AP Parameter Setting</p> <table border="1" data-bbox="555 674 1369 891"> <thead> <tr> <th></th> <th>AIFSN</th> <th>CWMin</th> <th>CWMax</th> <th>TXOP</th> <th>ACM</th> <th>Ack Policy</th> </tr> </thead> <tbody> <tr> <td>AC VO</td> <td>1</td> <td>1</td> <td>3</td> <td>47</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC VI</td> <td>1</td> <td>3</td> <td>3</td> <td>94</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC BE</td> <td>3</td> <td>3</td> <td>7</td> <td>0</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC BK</td> <td>7</td> <td>7</td> <td>15</td> <td>0</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p>		AIFSN	CWMin	CWMax	TXOP	ACM	Ack Policy	AC VO	1	1	3	47	<input type="checkbox"/>	<input type="checkbox"/>	AC VI	1	3	3	94	<input type="checkbox"/>	<input type="checkbox"/>	AC BE	3	3	7	0	<input type="checkbox"/>	<input type="checkbox"/>	AC BK	7	7	15	0	<input type="checkbox"/>	<input type="checkbox"/>
	AIFSN	CWMin	CWMax	TXOP	ACM	Ack Policy																														
AC VO	1	1	3	47	<input type="checkbox"/>	<input type="checkbox"/>																														
AC VI	1	3	3	94	<input type="checkbox"/>	<input type="checkbox"/>																														
AC BE	3	3	7	0	<input type="checkbox"/>	<input type="checkbox"/>																														
AC BK	7	7	15	0	<input type="checkbox"/>	<input type="checkbox"/>																														
Tx Power	<p>The default value is 100%. To narrow down covering range, users can input a smaller value.</p>																																			
Channel Bandwidth	<p>20- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p>20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability.</p>																																			
SSID Summary	<p>The status of every SSID will be shown here. Click “Edit” to enter configuration page.</p>																																			

8.2 Security Setting

▶ Select SSID

No. :	1 ▼
Status :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSID :	ALL-VPN10_1
BSSID :	FE:FF:FF:FF:FF:FC
Broadcast SSID :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
AP Isolation :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Guest Access :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

▶ Security Mode

Auth Mode :	Disabled ▼
-------------	------------

▶ WPS Config

WPS :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
-------	---

▶ WDS Config

WDS :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
-------	---

▶ Access Filter

[Show new MAC address](#)

Policy :	Disabled ▼
----------	------------

Add Station MAC : - - - - -

Name :

[Add to list](#)

[Delete selected application](#)

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

8.2.1 Select SSID

Select SSID

No. :	1
Status :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSID :	ALL-VPN10_1
BSSID :	FE:FF:FF:FF:FF:FC
Broadcast SSID :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
AP Isolation :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Guest Access :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

No.	The number of this SSID.
Status	Indicate if this SSID is enabled.
SSID	The name of wireless network. SSID is also called ESSID, which is for recognizing and establishing a wireless network.
BSSID	Indicates the MAC of this SSID.
Broadcast SSID	Check "Enabled" box to reveal SSID in the wireless network. If "Disabled" is checked, wireless client device will not find this SSID. Users have to input SSID manually to connect to this device.
AP Isolation	Enable to feature to make clients connect to this device can not communicate to each other.
Guest Access	Enable to feature so that clients user can only reach internet instead of wired LAN.

8.2.2 Security Mode

provides several security modes. Users need correct key to access wireless network.

Security Mode

Auth Mode :	Disabled Open WEP Shared WEP WEP Auto WPA Enterprise WPA Personal WPA2 Enterprise WPA2 Personal WPA/WPA2 Personal Mixed Mode WPA/WPA2 Enterprise Mixed Mode 802.1X
--------------------	--

1. WEP mode

- Open WEP
- Shared WEP
- WEP Auto

If "Open WEP" or "Shared WEP" is checked, client users need to select the same mode to connect to AP.

If “WEP auto” is checked, client users can choose any security mode.

WEP Security

Default Key :	Key1	
WEP Key1 :	<input type="text"/>	KEY1 Type 64-bit (10 hex digits) ▼
WEP Key2 :	<input type="text"/>	KEY2 Type 64-bit (10 hex digits) ▼
WEP Key3 :	<input type="text"/>	KEY3 Type 64-bit (10 hex digits) ▼
WEP Key4 :	<input type="text"/>	KEY4 Type 64-bit (10 hex digits) ▼

Default Key	Select one of following 4 sets to be security key.
64-bit (10 hex digits)	Input 10 hex digits (0~9, a~f, A~F) as WEP key.
128-bit (26 hex digits)	Input 26 hex digits (0~9, a~f, A~F) as WEP key.
64-bit (5 ASCII)	Input 5 ASCII code (English letter or number) as key.
128-bit (13ASCII)	Input 13 ASCII code (English letter or number) as key.

2. WPA mode

- Personal mode with pre-shared key (PSK)
 - It’s recommended to adopt Personal mode with pre-shared key, such as WPA Personal, WPA2 Personal and WPA/WPA2 Personal Mixed mode. Router and client users only have to share a set of key to ensure security without RADIUS server.
- WPA Personal
- WPA2 Personal
- WPA/WPA2 PersonalMixed mode

Wireless Security

WPA Algorithms :	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> Auto
ReKey Interval :	<input type="text" value="0"/> Seconds (0~4194303)

WPA Algorithms	There are TKIP, AES and Auto can be chosen. Attention! Only AES can achieve 802.11n rate.
ReKey Interval	WPA/WPA2-PSK will rekey in a fixed interval. The interval can be configured.

3. Enterprise Mode

RADIUS server is necessary to use WPA/WPA2 enterprise mode.

- WPA Enterprise
- WPA2 Enterprise
- WPA/WPA2 Enterprise Mixed mode

Wireless Security

WPA Algorithms :	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> Auto		
ReKey Interval :	<input type="text" value="0"/>	Seconds (0~4194303)	
PMK Cache Period :	<input type="text" value="10"/>	Minutes	
Pre-Authentication :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		

RADIUS SERVER

IP Address :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
RADIUS Port :	<input type="text" value="1812"/>
Shared Secret :	<input type="text" value="Allnet"/>
Session Timeout :	<input type="text" value="0"/> seconds (0 or 60~999999)

WPA Algorithms	There are TKIP, AES and Auto can be chosen. Attention! Only AES can achieve 802.11n rate.
ReKey Interval	WPA/WPA2-PSK will rekey in a fixed interval. The interval can be configured.
PMK Cache Period	When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication.
Pre-Authentication	Pre-authentication allows a wireless client to perform authentication with a different AP from the one to which it is currently connected, before moving into the new AP's coverage area. This speeds up roaming.
IP Address	Input RADIUS server IP.
RADIUS Port	Input RADIUS service port.
Shared Secret	Input initial shared key.
Session Timeout	Input a maximum idle time. If the link idles over time, the connection will be terminated.

4. 802.1x Mode

RADIUS server is needed while 802.1x mode is enabled.

RADIUS SERVER

IP Address :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
RADIUS Port :	<input type="text" value="1812"/>
Shared Secret :	<input type="text" value="Allnet"/>
Session Timeout :	<input type="text" value="0"/> seconds (0 or 60~999999)

IP Address	Input RADIUS server IP.
------------	-------------------------

RADIUS Port	Input RADIUS service port.
Shared Secret	Input initial shared key.
Session Timeout	Input a maximum idle time. If the link idles over time, the connection will be terminated.

8.2.3 WPS Config

Users can enable WPS function when using WPA Personal, WPA2 Personal and WPA/WPA2 Personal Mixed Mode. When WPS is enabled, the mode will continue for 2 minutes. If there is no connection established in two minutes, this connection will be stopped.

▶ WPS Config

WPS :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
AP PIN Code :	48392969 <input type="button" value="Generate"/>
WPS Mode :	<input type="radio"/> PIN <input type="text"/> <input checked="" type="radio"/> PBC

1. Use personal PIN code to configure WPS

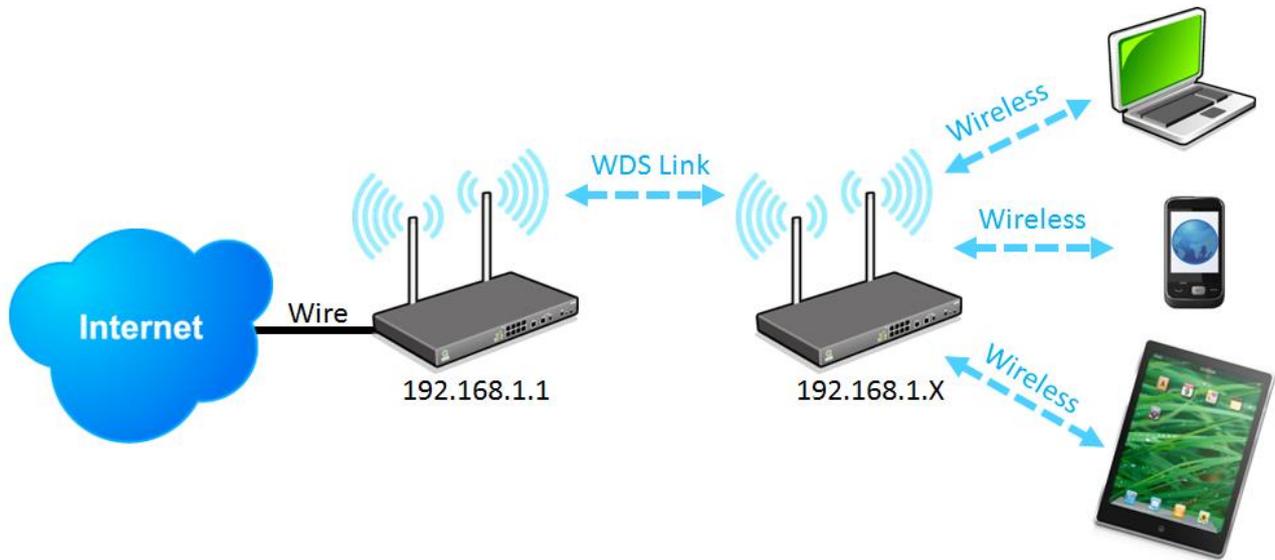
- (1) Enable WPS.
- (2) Input wireless client device PIN code. AP PIN code should be also written in client device.
- (3) Click "Connect" to establish connection.
- (4) Check if WPS connection is established successfully on client device.

2. Use PBC to configure WPS

- (1) Enable WPS.
- (2) Check "PBC" and click "connect" to establish connection. Uses can also push the WPS button on front panel for 5 seconds.
- (3) Check if WPS connection is established successfully on client device.

8.2.4 WDS Config

WDS is the abbreviation of Wireless Distribution System. The system will transmit packets to other WDS devices in the wireless network to extend covering range..



Two devices should be set in the same subnet as figure above.

Configurations of two devices should be the same.

Basic Setting

Wireless Network

Network Mode :	11bgn Mixed Mode
Country Code :	EUR (Europe)
Frequency Channel :	Auto <input type="button" value="Scanning"/>
WMM Capable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="button" value="Advance"/>
Tx Power :	100 (Range 1-100, Default 100)
Channel Bandwidth :	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40

※Under WDS mode, channel bandwidth should be “20”.

Security Mode

Security Mode

Auth Mode :	Disabled
-------------	----------

WDS should be enabled on both devices. MACs of each other should be inputed on both sides. There could be variation on the quantity of AP supported on different devices.

(1) Input AP MAC into blank.

▶ WDS Config

WDS :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
AP MAC :	<input type="text"/> - <input type="text"/>
AP MAC :	<input type="text"/> - <input type="text"/>
AP MAC :	<input type="text"/> - <input type="text"/>
AP MAC :	<input type="text"/> - <input type="text"/>

※ If WEP mode is enabled, system will arrange 4 sets of key for those MACs. Make sure the order is correct.

(2) Or check "Scanning" to select existing AP and then click "Submit".

Scan List							Submit	Select All	Refresh	Close
Enable	Channel	SSID	BSSID	Security	Signal	Network Mode				
<input type="checkbox"/>	2		74:d0:2b:dd:83:d4	WPA2PSK/AES	31	11b/g/n				
<input type="checkbox"/>	2		5c:d9:98:a7:19:a4	WPA1PSKWPA2PSK/AES	68	11b/g/n				
<input type="checkbox"/>	6	Lily	00:17:16:05:4f:10	WPA1PSKWPA2PSK/AES	42	11b/g/n				
<input type="checkbox"/>	7	FAE	00:17:16:05:50:10	WPA2PSK/AES	13	11b/g/n				

8.2.5 Access Filter

For additional security of wireless access, the Access Control facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface.

[▶ Access Filter](#)

Show new MAC address

Policy : Disabled ▾

Add Station MAC : - - - - -

Name :

Add to list

Delete selected application

Policy	Deny: Connection from the disabled MAC list will be denied. Allow: Only MAC listed in "Enabled"list can establish connection.
Add Station MAC	MAC Address: Input MAC into the policy. Users can find MAC address such as "00:11:22:33:44:55" from client device and input into the blanks.

8.3 Station List

Station List provides the knowledge of connecting wireless clients.

Station List

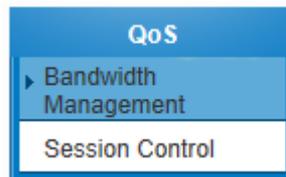
No.	MAC Address	DHCP IP	Host Name	SSID	Rate
-----	-------------	---------	-----------	------	------

Refresh

MAC Address	The MAC address of client device.
DHCP IP	The IP address allocated from system.
Host Name	The host name of client device.
SSID	SSID of client device.
Rate	The quality of Wifi signal (%).

IX. 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.



9.1 Bandwidth Management

▶ The Maximum Bandwidth Provided by ISP

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

▶ Quality of Service

Interface : WAN 1 WAN 2

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

Source IP ▼ : . . . to / Group : ▼

. . .

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

Enabled :

Add to list

Delete selected item

Show Table Apply Cancel

9.1.1 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"/>

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 unit of calculation in this example is Kbit. Some software indicates the downstream/upstream speed with the unit KB. $1\text{KB} = 8\text{Kbit}$.

9.1.2 QoS

To satisfy the bandwidth requirements of certain users, the device enables users to set up QoS: Rate Control and Priority Control. Users can select only one of the above QoS choices.

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

Interface : WAN 1 WAN 2

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

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 ~ 149". The rule will control IP addresses from 192.168.1.100 to 149. 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 C.

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.</p> <p>The maximum bandwidth will not exceed the limit set up under this rule.</p> <p>Attention! The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.</p>
Bandwidth sharing :	<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 example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.</p> <p>Attention: 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. 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>
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 :

Below to the left is "Show Table" button. Click it, a dialog as below will pop up. Users can select "Rule" or "Interface" button to display the configured rules. Click "Refresh" to renew the table and "Close" to close it. For reconfiguring the rule, click "Edit".

Summary								
QoS Type	Application/Service	IP Address	Upstream/Downstream	Mini. Rate (Kbit/sec)	Max. Rate (Kbit/sec)	Bandwidth sharing	Enabled	Interface (WAN)

Example 1. How to set up the maximum download speed to 50 Kbit for the FTP protocol on all WAN interfaces ?

Please refer to the following as a setup example. Click before both WAN1 and WAN2; then choose "FTP [TCP/21~21]" in Service; for IP Address, put your LAN IP range (e.g.192.168.1.1~254); in "Direction" part, open the dropdown box and choose Downstream. Import 2Kbit/Sec in Mini. Rate, which guarantees the minimum bandwidth for FTP downloading. And import 50Kbit/Sec in Max. Rate for a maximum limitation. Choose "Share total bandwidth with all IP addresses" in "Bandwidth sharing" method, which means that the whole LAN users share a maximum 50Kbits/Sec download speed on the FTP protocol no matter how many users are using in intranet. Click "Enable" and "Add to list", then this rule is successfully added.

Interface : WAN 1 WAN 2

Service : FTP [TCP/21~21] ▼

Service Management

IP Address ▼ : 192 . 168 . 1 . 1 to 254

Direction : Downstream ▼

Mini. Rate : 2 Kbit/sec Max. Rate : 50 Kbit/sec

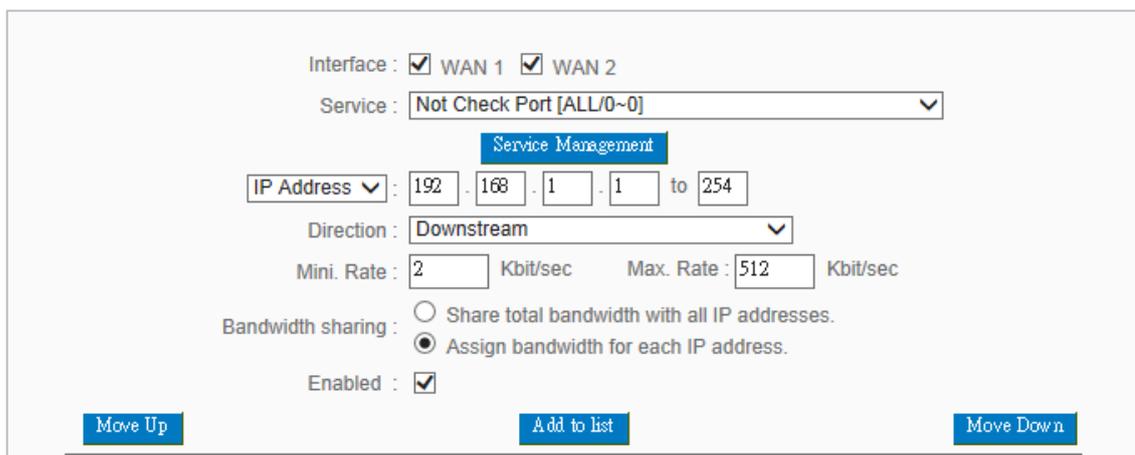
Bandwidth sharing : Share total bandwidth with all IP addresses.
 Assign bandwidth for each IP address.

Enabled :

Move Up Add to list Move Down

Example 2. How to set up the maximum download speed of each WAN to 512Kbit/Sec for each LAN user? One by one IP to set up?

No need to set up one by one. Below is the example. Click both WAN1 and WAN2; then choose “No Check Port[TCP&UDP /0~0]” in Service; for IP Address, put your LAN IP range (e.g.192.168.1.1~254); in "Direction" part, open the dropdown box and choose Downstream. Import 2Kbit/Sec in Mini. Rate, which guarantees the minimum bandwidth. And import 512Kbit/Sec in Max. Rate for a maximum limitation. Choose “Assign bandwidth for each IP address” in “Bandwidth sharing” method, which ensures each IP a minimum 2Kbits/Sec download speed . Click “Enable” and “Add to list”, then this rule is successfully added.



Interface : WAN 1 WAN 2

Service : Not Check Port [ALL/0~0]

Service Management

IP Address ▼ : 192 . 168 . 1 . 1 to 254

Direction : Downstream

Mini. Rate : 2 Kbit/sec Max. Rate : 512 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

Attention! The action rule priority of the QoS bandwidth management is from the bottom to the top rule, therefore you have to remove the rule what you want to implement first to the bottom.

9.2 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

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.

<p>When single IP exceed __ :</p>	<p><input checked="" type="radio"/> block this IP to add new session 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 connection 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 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.</p>
<p>Apply :</p>	<p>Click "Apply" to save the configuration.</p>
<p>Cancel :</p>	<p>Click "Cancel" to leave without making any change.</p>

Exempted Service Port or IP Address

▶ Exempted Service Port or IP Address

Service : ▼

Service Management

Source IP ▼ : - - - to

Enabled :

Maximum connections limit : Unlimited
 Not exceed

Add to list

Delete selected item

<p>Service Port :</p>	<p>Choose the service port.</p>
-----------------------	---------------------------------

Source IP :	Input the IP address range or IP group.
Enabled :	Activate the rule.
Add to list :	Add this rule to the list.
Delete seleted 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.

9.3 Smart QoS

The smart QoS function enables the administrators to constrain the bandwidth occupied automatically without any configuring.

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)

Downstream (WAN 1 : Kbit/sec WAN 2 : Kbit/sec)

Penalty mechanism

Enabled QoS :	Choose to apply QoS function.
When the usage of any WAN's bandwidth is over than __%, 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.
If any 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.
Enabled 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 IP :	The IPs which are under penalty mechanism will be shown on the list.

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.

X. Firewall

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

10.1 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
Block WAN Request	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Remote Management	<input type="radio"/> Disabled <input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS Port <input type="text" value="8080"/>
Local Management	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS Port <input type="text" value="80"/>
Multicast Pass Through	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Prevent ARP Virus Attack	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Router sends ARP <input type="text" value="5"/> times per-second.

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 Through :	There are many audio and visual streaming media on the network. Broadcasting 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.
Show Blocked IP :	 <p>Show the blocked IP list and the remained blocked time.</p>
Restricted WEB Features :	It supports the block that is connected through: Java, Cookies, Active X, and HTTP Proxy access.
Apply :	Click "Apply" to save the configuration.
Cancel :	Click "Cancel" to leave without making any change.

10.2 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.

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.

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

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			

[Add New Rule](#) [Restore Default Rules](#)

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.

Edit :	Define the network access rule item
--------	-------------------------------------

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

10.2.1 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

Action :	<p>Allow: Permits the pass of packets compliant with this control rule</p> <p>Deny: Prevents the pass of packets not compliant with this control rule</p>
Service :	From the drop-down menu, select the service that users grant or do not give permission.
Service Management :	<p>If the service that users wish to manage does not exist in the drop-down menu, press – Service Management to add the new service.</p> <p>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.</p>
Log :	<p>No Log : There will be no log record.</p> <p>Create Log when matched : Event will be recorded in the log.</p>
Source 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.

Example 1. : How to block TCP135-139 virus port?

Firstly, Add TCP 135-139 port in "Add new service port" (Please refer to the chapter of how to add a new service port), then have the configuration as below step :

Action : Forbid

Service Port : TCP135-139

Source Interface : ANY (Meaning to block all traffic from intranet to internet and all attack from internet to intranet through the service port.)

Source IP : ANY (Meaning to block all traffic from intranet to internet and all attack from internet to intranet through the service port.)

Dest. IP : ANY (Meaning to block all traffic from intranet to internet and all attack from internet to intranet through the service port.)

▶ Service

Action :	Deny ▼
Service :	TCP 135-139 [TCP/135~139] ▼ Service Management
Log :	No log ▼
Source Interface :	ANY ▼

Source IP :	ANY ▼		
Dest. IP :	ANY ▼		

Example 2. : How to forbid intranet IP range from 192.168.1.200 to 230 to access service port 80?

Action : Forbid

Service Port : TCP 80

Source Interface : LAN (Meaning to service port 80 which blocks the traffic from intranet to internet.)

Source IP : 192.168.1.200~192.168.1.230

Dest. IP : ANY (Meaning to any service port 80 which blocks the traffic from intranet to internet among 192.168.1.200~230.)

▶ Service

Action :	Deny ▼
Service :	HTTP [TCP/80~80] ▼ Service Management
Log :	No log ▼
Source Interface :	LAN ▼

Source IP :	Range ▼	192 . 168 . 1 . 200	to	192 . 168 . 1 . 230
Dest. IP :	ANY ▼			

10.3 Content 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 Domain Keywords

Scheduling

Apply this rule Always (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

Apply
Cancel

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 v :
 .
 .
 .
 to

Group v IP Grouping

Add to list

Delete selected domain

Add :	Enter the websites to be controlled such as www.playboy.com
Add to list :	Click "Add to list" to create a new website to be controlled.
Delete selected item :	Click to select one or more controlled websites and click this option to delete.

Website Blocking by Keywords :

- Block Forbidden Domains
- Accept Allowed Domains

-
- Forbidden Domains Enabled
 - Enable Website Blocking by Domain Keywords

Website Blocking by Domain Keywords

Keywords

Add

Exception IP address . . . to

Group Add to list

Delete selected keywords

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

Allowed Domains

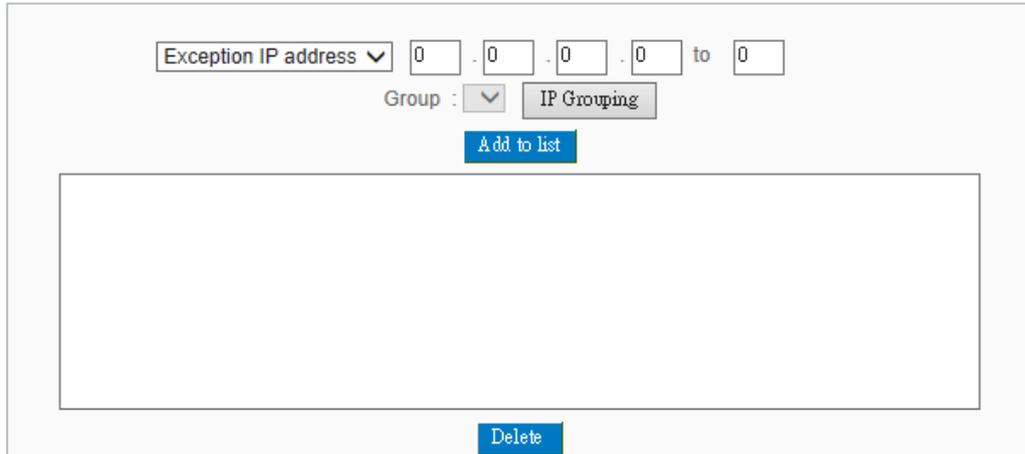
Add :

Enabled :	Activate the function. The default setting is "Disabled."
Add :	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.

Exception IP

Here IP/IP ranges are exempted from “Accept Allowed Domain” through this method.

▶ Exception

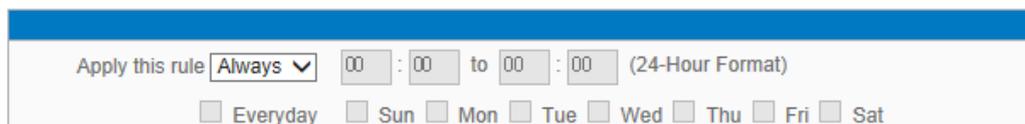


- Exception IP address Input unrestricted IP/IP Range
- Add to list : Click this button to add new unrestricted IPs
- Delete selected item : Select out one/more unrestricted IPs, click this button to delete them

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



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.)

XI. L7 Management



11.1 L7 Filter

(1) Rule list:

[L7 Block Application](#)

Jump to Page entries per page

Priority	Enabled	Name	Time	Exception	Source IP Address	Edit	Delete
				Exception			
					Add New Rule		

Below are the steps for rule setting with an example in the enterprise:

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Rule Name :

Step 2: Choose the application

Rule Name :

Category	Item
Instant Messenger	All
P2P Software	Gadu-Gadu
Online Game	Google Talk
Web Objects	ICQ
File Format	MSN
Stocks Software	QQ/TM
Social Network Website	Skype(Voice)
Online Video Website	Tlen.pl
Media Player	WebQQ
Blog	WebWW
Application Define	Yahoo!Messenger

※Figures are used for reference. Please visit the official website for the actual application support list.

(1) After choosing [Category], the [Item] column will show the corresponding list.

Hint:

- Directly click on the applications to put them effective.
- Cancel the application by double clicks.
- Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.
- Items could be choosing in multiple categories.

(2) Click  to drop the applications into the right column.

Category ▲	Item ▲	Delete
Instant Messenger	Google Talk	
Instant Messenger	ICQ	
Instant Messenger	QQ/TM	

Step 3: Make sure the time setting is correct to make the rule in effective only during the set time.

All time is set as the default. The time frame could be modified in the following settings.

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

Step 4: Set exceptional users (IP or QQ number)**These settings will apply to all rules of this application**

- Exception QQ Number
- Exception Source IP Address

- Administrator can set IP address or QQ numbers (if QQ is blocked) in the exceptional user setting.
- Please note that the exceptional user setting will be applied to all the rules in the application.

For example, if there is a Google Talk rule with no exceptional IP, when adding a new Google Talk rule with the exceptional IP 192.168.1.100, 192.168.1.100 could use Google Talk anyway no matter applied to the original rule or the new rule.

Step 5: Click  to save the rule setting.

11.2 L7 VIP Priority Channel

L7 Management

Application Status

L7 Blocking

▶ L7 VIP Priority Channel

L7 QoS

(1) Rule List:

▶ **Summary**

Enhanced L7 VIP

Jump to /Page entries per page

No.	Enabled	Name	Interface	VIP Application	IP Range/Group	Time	Edit	Delete
<input type="button" value="Add New Rule"/>								

(2) Add New Rule: Click

▶ **Basic Setting**

Rule Name :

interface : WAN 1 WAN 2

▶ **Set Application or IP as VIP**

VIP Application

VIP Source IP/Group

▶ **Scheduling**

Apply this rule : to : (24-Hour Format)

Everyday Sun Mon Tue Wed Thu Fri Sat

Step1: Basic Setting**Basic Setting**

Rule Name :	<input type="text"/>
interface :	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Select one WAN as VIP. For example, only the traffic of president room on WAN1 and WAN2 is VIP, traffic on other WAN ports is not VIP.

Hint:

If users want traffic only run on VIP WAN, users can also configure “L7 Application Binding”.

Step2: Set Application or IP as VIP**▶ Set Application or IP as VIP** **VIP Application** **VIP Source IP/Group**

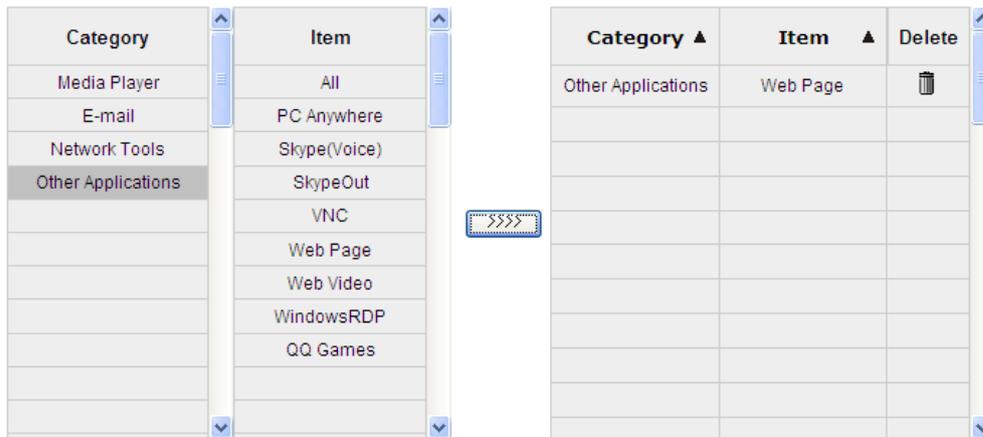
- Set application as VIP. For instance, [Webpage] is selected. When the system recognizes the IP is using webpage service, the system will give VIP priority.
- Set source IP/Group as VIP. For instance, if [General Manager Room] IP group is chosen, they will have VIP priority no matter what application is used.
- Set VIP application and source IP/Group at the same time. If [Webpage] and [General Manager Room] are configured at the same time, it means when general manager room use webpage service, the system will give them VIP bandwidth. But VIP bandwidth will not allowed when they use other network service.

Take a community for an example:

The community will ensure VIP authority when internal users browse webpage, the administrator should check [VIP Application] and [webpage] at Item column.

Set Application or IP as VIP

VIP Application



※Figures are used for reference. Please visit the official website for the actual application support list.

After choosing [Category], the [Item] column will show the corresponding list.

Hint :

Directly click on the applications to put them effective.

Cancel the application by double clicks.

Click [Choose All] to put all applications into effective, and click unnecessary items for cancel.

Items could be chosen in multiple categories.

Click  to drop the applications into the right column.

Step 3: Make sure the time setting is correct to make the rule in effective only during the set time.

Always is set as the default. The time frame could be modified in the following settings.

Scheduling

Apply this rule Always ▾	<input type="text"/> : <input type="text"/> to <input type="text"/> : <input type="text"/> (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

Apply **Cancel**

Step 4: Click **Apply** to save the rules.

11.3 L7 QoS

L7 Management

Application Status

L7 Blocking

L7 VIP Priority Channel

▶ L7 QoS

(1) Rule List :

▶ **The Maximum Bandwidth Provided by ISP**

Interface	Upstream Bandwidth (Kbit/sec)	Remnant guarantee Upstream Bandwidth (Kbit/sec)	Downstream Bandwidth (Kbit/sec)	Remnant guarantee Downstream Bandwidth (Kbit/sec)
WAN 1	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 2	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>

▶ **Summary**

Jump to /Page entries per page

Priority	Enabled	Name	Interface	IP Range/Group	Upstream/Downstream	Bandwidth	Time	Edit	Delete
<input type="button" value="Add New Rule"/>									

The Maximum Bandwidth provided by ISP : This table is relative to general QoS function.

The Maximum Bandwidth Provided by ISP

Interface	Upstream Bandwidth (Kbit/sec)	Remnant guarantee Upstream Bandwidth (Kbit/sec)	Downstream Bandwidth (Kbit/sec)	Remnant guarantee Downstream Bandwidth (Kbit/sec)
WAN 1	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 2	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>	<input type="text" value="10000"/>

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

Filling WAN Upstream/Downstream bandwidth with realistic broadband network bandwidth which user applying by

ISP, QoS Bandwidth control is according to the bandwidth number that user filling to calculate. Click [Apply](#) to save the set-up.

Bandwidth unit is kbit, some of the software applications display by KB, 1KB=8kbit.

Calculating bandwidth utility of QoS rule: minimize of bandwidth × IP set-up number. For example, IP range is 192.168.1.101~110, minimize bandwidth by each IP is 500kbit/sec, the total bandwidth utility of QoS rule is 500kbit/sec × 10(by IP) = 5000kbit/sec.

Remnant guarantee Bandwidth = Bandwidth – QoS Policy. The Remnant guarantee displays as a negative number in red when the bandwidth of QoS Policy is over the WAN bandwidth.

[Show QoS Table](#)

: Display the QoS Policy, including the L7 QoS and general QoS. The L7 QoS has a higher priority

then the general QoS if both overlapping.

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

Add New Rule

(2) Add New Rule : Click

Add Restrict Rule

Rule Name :

Category		Category ▲	Item ▲	Delete
P2P Software				
Online Game				
Media Player				
FTP Data				
WebMail				
Other Applications				

>>>>

Application Define

Quality of Service

Interface :	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2
Source IP/Group :	Range <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> to <input type="text"/>
Bandwidth :	Mini. Rate : <input type="text"/> Kbit/sec Max. Rate : <input type="text"/> Kbit/sec
Upstream/Downstream :	<input type="text"/> Downstream
Bandwidth sharing :	<input type="radio"/> Share total bandwidth with all IP addresses. <input checked="" type="radio"/> Assign bandwidth for each IP address.

Scheduling

Apply this rule <input type="text"/> Always	<input type="text"/> : <input type="text"/> to <input type="text"/> : <input type="text"/> (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

Apply **Cancel**

Step 1: Name the rule

The name of the rule will be shown on the list, so administrator could name the rule by users or usages.

Rule Name :

Step 2: Choose the application

Step 3: QoS Configuration

Quality of Service

Interface :	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2
Source IP/Group :	Range <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> to <input type="text"/>
Bandwidth :	Mini. Rate : <input type="text"/> Kbit/sec Max. Rate : <input type="text"/> Kbit/sec
Upstream/Downstream :	<input type="text"/> Downstream <input type="text"/>
Bandwidth sharing :	<input type="radio"/> Share total bandwidth with all IP addresses. <input checked="" type="radio"/> Assign bandwidth for each IP address.

Interface	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Source IP/Group	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 ~ 149". The rule will control IP addresses from 192.168.1.100 to 149.
Upstream/Downstream	Upstream : Means the upload bandwidth for Intranet IP. Downstream : Means the download bandwidth for Intranet IP.
Bandwidth sharing	<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 example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.</p> <p>※Attention: 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. 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>

Step 4: Make sure the time setting is correct to make the rule in effective only during the set time.

All time is set as the default. The time frame could be modified in the following settings.

▶ **Scheduling**

Apply this rule <input type="text" value="Always"/> ▼	<input type="text"/> : <input type="text"/> to <input type="text"/> : <input type="text"/> (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

Step 5: Click  to save the rule setting.

11.4 Application Define

When you set up the L7 Management rules, not only you can select the application that is defined by , but also you can add your own L7 applications by the URL, destination IP address or the port number.

You can see the Application Define feature on the Application Status Table or on the APP List of all L7 Management features.

※Application Status

Application Define

Jump to Page entries per page

Category ▲	Application ▲	L7 Blocking	L7 VIP Priority Channel	L7 QoS
<div style="border: 1px solid #0070C0; padding: 2px; display: inline-block;">Add New Rule</div>				

※Figures are used for reference. Please visit the official website for the actual application support list.

※Each function of L7 Management APP List

▶ Add Rule

Rule Name :

<table border="1" style="width: 100%; border-collapse: collapse; background-color: #f0f0f0;"> <thead> <tr> <th style="width: 30%;">Category ▲</th> <th style="width: 70%;">Item ▲</th> </tr> </thead> <tbody> <tr><td>Instant Messenger</td><td></td></tr> <tr><td>P2P Software</td><td></td></tr> <tr><td>Online Game</td><td></td></tr> <tr><td>Web Objects</td><td></td></tr> <tr><td>File Format</td><td></td></tr> <tr><td>Stocks Software</td><td></td></tr> <tr><td>Social Network Website</td><td></td></tr> <tr><td>Online Video Website</td><td></td></tr> <tr><td>Media Player</td><td></td></tr> <tr><td>FTP Data</td><td></td></tr> <tr><td>Blog</td><td></td></tr> </tbody> </table>	Category ▲	Item ▲	Instant Messenger		P2P Software		Online Game		Web Objects		File Format		Stocks Software		Social Network Website		Online Video Website		Media Player		FTP Data		Blog		<div style="border: 1px solid #ccc; padding: 2px 10px;">>>>></div>	<table border="1" style="width: 100%; border-collapse: collapse; background-color: #f0f0f0;"> <thead> <tr> <th style="width: 30%;">Category ▲</th> <th style="width: 30%;">Item ▲</th> <th style="width: 10%;">Delete ▲</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>	Category ▲	Item ▲	Delete ▲																														
Category ▲	Item ▲																																																										
Instant Messenger																																																											
P2P Software																																																											
Online Game																																																											
Web Objects																																																											
File Format																																																											
Stocks Software																																																											
Social Network Website																																																											
Online Video Website																																																											
Media Player																																																											
FTP Data																																																											
Blog																																																											
Category ▲	Item ▲	Delete ▲																																																									

Application Define

※Figures are used for reference. Please visit the official website for the actual application support list.

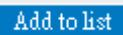
Application Define-Add New Rule



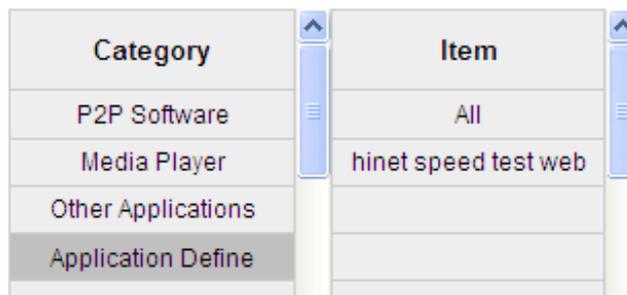
Step 1 : Name the Application

Step 2 : Define the application by the URL, destination or the port number. The definable parameter as below :

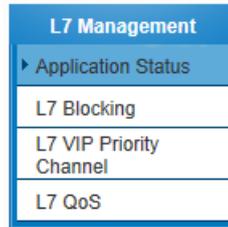
Dest. IP	If only a single IP is to be restricted, input this IP address, such as "100.100.100.105". The rule will control only the IP 100.100.100.105. If an IP range is to be controlled, input the range, such as "100.100.100.105~ 200".
Dest. IP Group	Apply the Dest. IP Group from the [Group Management] function.
Domain Name	Use Domain Name to define the application, for example, input the "speed.hinet.net" such as http://speed.hinet.net.
Service Port	Set up the TCP \ UDP port number or apply the port group from the [Group Management] function.

Step 3 : Click  to add your own L7 application to the list right side to finish the setting.

Step 4: Apply your own application to the L7 management; you can see your own L7 application on the 'Application Define'.



11.5 Applicatios Status



The Administrator can check the whole applied applications from the Application Status function, including the ID of the policies.

Application Status Application Define

1 ↓ 2 → Jump to 1 /Page 3 → 10 entries per page

Category ▲	Application ▲	L7 Blocking	L7 VIP Priority Channel	L7 QoS
Social Network Website	Google+	4 → 1	--	--
Social Network Website	Facebook	1	--	--

Add New Rule

※Figures are used for reference. Please visit the official website for the actual application support list.

1	Sorting and ordering the applications	Sorting the applications or ordering the applications by the name.
2	Jump to 1 /Page	Jump to the specific page.
3	10 entries per page	Identify the lines in one page.
4	L7 VIP Priority Channel	Display policy which made by the application, presses the ID to edit the policy.

XII. VPN (Virtual Private Network)

10.1. VPN

VPN

- ▶ Summary
- Gateway to Gateway
- Client to Gateway
- PPTP Setup
- VPN Pass Through

▶ Summary

VPN Tunnel Number : 0 Tunnel(s) Used 10 Tunnel(s) Available

▶ VPNTunnel(s) Status

Jump to 1 / Page 5 entries per page

No.	Account ID	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Control	Config.
-----	------------	--------	------------------------	----------------	-----------------	-------------------	---------	---------

▶ VPNGroup Status

Group Name	ConnectedTunnel (s)	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote ClientStatus	Control	Config.
------------	------------------------	------------------------	----------------	------------------	------------------------	---------	---------

Add Tunnel(s)

10.1.1. Add a New VPN Tunnel

The device supports Gateway to Gateway tunnel or Client to Gateway tunnel.

The VPN tunnel connections are done by 2 VPN devices via the Internet. When a new tunnel is added, the setting page for Gateway to Gateway or Client to Gateway will be displayed.

Gateway to Gateway :

Click "Add" to enter the setting page of Gateway to Gateway.

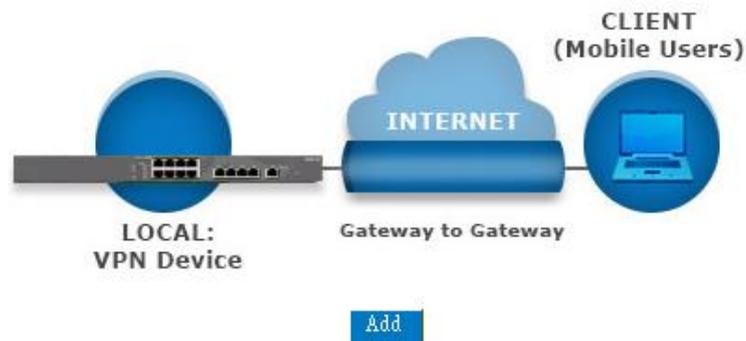
▶ Gateway to Gateway



Client to Gateway :

Click "Add" to enter the setting page of Client to Gateway.

▶ Client to Gateway



10.1.1.1. Gateway to Gateway Setting

▶ Gateway to Gateway

Tunnel(s) No.	1
Tunnel(s) Name :	
Interface:	WAN 1 ▾
Enabled :	<input checked="" type="checkbox"/>

The following instructions will guide users to set a VPN tunnel between two devices.

Tunnel No. :	Set the embedded VPN feature, please select the Tunnel number.
Tunnel Name :	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion. Note: If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.
Interface :	From the pull-down menu, users can select the Interface for this VPN tunnel.
Enabled :	Click to activate the VPN tunnel. This option is set to activate by default. Afterwards, users may select to activate this tunnel feature.

Local Group Setup :

▶ Local VPN Group Setting

Local Security Gateway Type:	IP Only ▾
IP Address:	221 . 169 . 231 . 22
Local Security Group Type:	Subnet ▾
IP Address:	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0

This Local Security Gateway Type must be identical with that of the remote type (Remote Security Gateway Type).

Local Security GatewayType :	This local gateway authentication type comes with five operation modes, which are: IP only IP + Domain Name (FQDN) Authentication
------------------------------	---

IP + E-mail Addr. (USER FQDN) Authentication
Dynamic IP + Domain Name (FQDN) Authentication
Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name

(1) IP only:

If users decide to use **IP only**, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Local Security Gateway Type:	IP Only
IP Address:	221 . 169 . 231 . 22

(2) IP + Domain Name(FQDN) Authentication:

If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.

Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address:	221 . 169 . 231 . 22
Domain Name:	

(3) IP + E-mail Addr. (USER FQDN) Authentication.

If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Local Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address:	221 . 169 . 231 . 22
E-mail:	

(4) Dynamic IP + Domain Name(FQDN) Authentication:

If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and

	<p>respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.</p> <table border="1" data-bbox="571 427 1385 501"> <tr> <td>Local Security Gateway Type:</td> <td>Dynamic IP + Domain Name(FQDN) Authentication ▾</td> </tr> <tr> <td>Domain Name:</td> <td><input type="text"/></td> </tr> </table> <p>(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.</p> <p>If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; If users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.</p> <table border="1" data-bbox="571 862 1385 936"> <tr> <td>Local Security Gateway Type:</td> <td>Dynamic IP + E-mail(User FQDN) Authentication ▾</td> </tr> <tr> <td>E-mail:</td> <td><input type="text"/> @ <input type="text"/></td> </tr> </table>	Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication ▾	Domain Name:	<input type="text"/>	Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication ▾	E-mail:	<input type="text"/> @ <input type="text"/>		
Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication ▾										
Domain Name:	<input type="text"/>										
Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication ▾										
E-mail:	<input type="text"/> @ <input type="text"/>										
<p>Local Security Group Type :</p>	<p>This option allows users to set the local VPN connection access type. The following offers a few items for local settings. Please select and set appropriate parameters:</p> <p>1. IP address</p> <p>This option allows the only IP address which is entered to build the VPN tunnel.</p> <table border="1" data-bbox="571 1234 1385 1339"> <tr> <td>Local Security Group Type:</td> <td>IP Address ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/></td> </tr> </table> <p>Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.</p> <p>2. Subnet</p> <p>This option allows local computers in this subnet can be connected to the VPN tunnel.</p> <table border="1" data-bbox="571 1637 1385 1787"> <tr> <td>Local Security Group Type:</td> <td>Subnet ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/></td> </tr> <tr> <td>Subnet Mask:</td> <td><input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/></td> </tr> </table> <p>Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.</p>	Local Security Group Type:	IP Address ▾	IP Address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/>	Local Security Group Type:	Subnet ▾	IP Address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/>	Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Local Security Group Type:	IP Address ▾										
IP Address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/>										
Local Security Group Type:	Subnet ▾										
IP Address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/>										
Subnet Mask:	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>										

Remote Group Setup :

Remote VPN Group Setting

Remote Security Gateway Type:	IP Only
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Remote Security Group Type:	Subnet
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	255 . 255 . 255 . 0

This remote gateway authentication type (Remote Security Gateway Type) must be identical to the remotely-connected local security gateway authentication type (Local Security Gateway Type).

<p>Remote Security Gateway Type :</p>	<p>This remote gateway authentication type comes with five operation modes, which are:</p> <ul style="list-style-type: none"> IP only-Authentication by use of IP only IP + Domain Name (FQDN) Authentication, -IP + Domain name IP + E-mail Addr. (USER FQDN) Authentication, -IP + Email address Dynamic IP + Domain Name (FQDN) Authentication, -Dynamic IP address + Domain name Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name <p>(1) IP only:</p> <p>If users select the IP Only type, entering this IP allows users to gain access to this tunnel.</p> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>IP Only</td> </tr> <tr> <td>IP Address</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> </table> <p>If the IP address of the remote client is unknown, choose IP by DNS Resolved, allowing DNS to translate IP address. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.</p> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>IP Only</td> </tr> <tr> <td>IP by DNS Resolved</td> <td><input type="text"/></td> </tr> </table> <p>(2) IP + Domain Name(FQDN) Authentication:</p> <p>If users select IP + domain name, please enter IP address and the domain</p>	Remote Security Gateway Type:	IP Only	IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Remote Security Gateway Type:	IP Only	IP by DNS Resolved	<input type="text"/>
Remote Security Gateway Type:	IP Only								
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>								
Remote Security Gateway Type:	IP Only								
IP by DNS Resolved	<input type="text"/>								

name to be verified. FQDN refers to the combination of host name and domain name. Users may enter any name that corresponds to the domain name of FQDN. This IP address and domain name must be identical to those of the remote VPN security gateway setting type to establish successful connection.

Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name:	<input type="text"/>

If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translate the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP by DNS Resolved	<input type="text"/>
Domain Name:	<input type="text"/>

(3) IP + E-mail Addr. (USER FQDN) Authentication:

If users select IP address and E-mail type, entering the IP address and the E-mail allows users to gain access to this tunnel.

Remote Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
E-mail:	<input type="text"/> @ <input type="text"/>

If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translated the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

Remote Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP by DNS Resolved	<input type="text"/>
E-mail:	<input type="text"/> @ <input type="text"/>

(4) Dynamic IP + Domain Name(FQDN) Authentication:

If users use dynamic IP address to connect with the device, users may select the combination of the dynamic IP address, host name and domain

	<p>name.</p> <div data-bbox="572 383 1366 456"> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>Dynamic IP + Domain Name(FQDN) Authentication ▾</td> </tr> <tr> <td>Domain Name:</td> <td><input type="text"/></td> </tr> </table> </div> <p>(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.</p> <p>If users use dynamic IP address to connect with the device, users may select this type to link to VPN. When the remote VPN gateway requires connection to facilitate VPN connection, the device will start authentication and respond to the VPN tunnel connection; Please enter the E-Mail to the empty space.</p> <div data-bbox="572 842 1366 916"> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>Dynamic IP + E-mail(User FQDN) Authentication ▾</td> </tr> <tr> <td>E-mail:</td> <td><input type="text"/> @ <input type="text"/></td> </tr> </table> </div>	Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication ▾	Domain Name:	<input type="text"/>	Remote Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication ▾	E-mail:	<input type="text"/> @ <input type="text"/>		
Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication ▾										
Domain Name:	<input type="text"/>										
Remote Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication ▾										
E-mail:	<input type="text"/> @ <input type="text"/>										
<p>Remote Security Group Type :</p>	<p>This option allows users to set the remote VPN connection access type. The following offers a few items for remote settings. Please select and set appropriate parameters:</p> <p>(1) IP address</p> <p>This option allows the only IP address which is entered to build the VPN tunnel.</p> <div data-bbox="572 1240 1366 1344"> <table border="1"> <tr> <td>Remote Security Group Type:</td> <td>IP Address ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> </table> </div> <p>Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.2.1 can establish connection.</p> <p>(2) Subnet</p> <p>This option allows local computers in this subnet can be connected to the VPN tunnel.</p> <div data-bbox="572 1585 1366 1729"> <table border="1"> <tr> <td>Remote Security Group Type:</td> <td>Subnet ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> <tr> <td>Subnet Mask:</td> <td>255 . 255 . 255 . 0</td> </tr> </table> </div> <p>Reference: When this VPN tunnel is connected, only computers with the session of 192.168.2.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.</p>	Remote Security Group Type:	IP Address ▾	IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Remote Security Group Type:	Subnet ▾	IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Subnet Mask:	255 . 255 . 255 . 0
Remote Security Group Type:	IP Address ▾										
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>										
Remote Security Group Type:	Subnet ▾										
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>										
Subnet Mask:	255 . 255 . 255 . 0										

IPSec Setup

IPSec Setting

Keying Mode:	IKE with Preshared Key ▾
Phase1 DHGroup :	Group 1 ▾
Phase1 Encryption:	DES ▾
Phase1 Authentication:	MD5 ▾
Phase1 SA Life Time:	0 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DHGroup :	Group 1 ▾
Phase2 Encryption:	DES ▾
Phase2 Authentication:	MD5 ▾
Phase2 SA Life Time:	0 seconds
Preshared Key:	<input type="text"/>

If

there is any encryption mechanism, the encryption mechanism of these two VPN tunnels must be identical in order to create connection. And the transmission data must be encrypted with IPSec key, which is known as the encryption "key". The device provides the IKE automatic encryption mode- IKE with Preshared Key (automatic). By using the drop down menu, select the desired encryption mode as illustrated below.

Encryption Management Protocol :

When users set this VPN tunnel to use any encryption and authentication mode, users must set the parameter of this exchange password with that of the remote.

Use IKE Protocol :

Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the key will not be able to get the Phase 2 key in such a short period of time.

- **Perfect Forward Secrecy:** When users check the PFS option, don't forget to activate the PFS function of the VPN device and the VPN Client as well.
- **Phase 1/ Phase 2 DH Group:** This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.

- **Phase 1/ Phase 2 Encryption:** This option allows users to set this VPN tunnel to use any encryption mode. Note that this parameter must be identical to that of the remote encryption parameter: DES (64-bit encryption mode), 3DES (128-bit encryption mode), AES (the standard of using security code to encrypt information). It supports 128-bit, 192-bit, and 256-bit encryption keys.
- **Phase 1/Phase 2 Authentication:** This authentication option allows users to set this VPN tunnel to use any authentication mode. Note that this parameter must be identical to that of the remote authentication mode: "MD5" or "SHA1".
- **Phase 1 SA Life Time:** The life time for this exchange code is set to 28800 seconds (or 8hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Phase2 SA Life Time:** The life time for this exchange code is set to 3600 seconds (or 1hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Preshared Key :** For the Auto (IKE) option, enter a password of any digit or characters in the text of "Pre-shared Key" (the example here is set as test), and the system will automatically translate what users entered as exchange password and authentication mechanism during the VPN tunnel connection. This exchange password can be made up of up to 30 characters.

Advanced Setting- for IKE Protocol Only

▶ Advanced

Aggressive Mode
 Keep-Alive
 NetBIOS Broadcast
 NAT Traversal
 Dead Peer Detection(DPD) Enable Automatic Version Check Every seconds
 Heart Beat, Remote Host
 Enable Automatic Version Check Every seconds, Retry count
 Tunnel Backup :
 Remote Gateway :
 Backup Interface :

The advanced settings include Main Mode and Aggressive mode. For the Main mode, the default setting is set to VPN operation mode. The connection is the same to most of the VPN devices.

- **Aggressive Mode:** This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
- **Use IP Header Compression Protocol:** If this option is selected, in the connected VPN tunnel, the device supports IP Payload Compression Protocol.
- **Keep Alive:** If this option is selected, VPN tunnel will keep this VPN connection. This is mostly used to connect the remote node of the branch office and headquarter or used for the remote dynamic IP address.
- **AH hash calculation:** For AH (Authentication Header), users may select MD5/DSHA-1.
- **NetBIOS Broadcast:** If this option is selected, the connected VPN tunnel allows the passage of NetBIOS broadcast packet. This facilitates the easy connection with other Microsoft network; however, the traffic using this VPN tunnel will increase.
- **Dead Peer Detection (DPD):** If this option is selected, the connected VPN tunnel will regularly transmit HELLO/ACK message packet to detect whether there is connection between the two ends of the VPN tunnel. If one end is disconnected, the device will disconnect the tunnel automatically and then create new connection. Users can define the transmission time for each DPD message packet, and the default value is 10 seconds.
- **Heart Beat :** VPN Tunnel Heart Beat Detection function ◦

If this option is selected, the system will sent ICMP ACK packet to the remote host with VPN tunnel regularly; the remote host will also send an ICMP ACK reply packet toward the originator.

If there is still no received ICMP ACK reply after exceeding the setting retry, the Heart Beat originator will terminate this VPN tunnel.

Under this situation, if you are the VPN tunnel initiator, the system will try to reconnect the tunnel; if you are the passive party, the system will wait for the initiator to establish the tunnel again.

Remote Host	The remote end point for the Heart Beat Detection. It is always sensible to select an end point for the Heart Beat detection; the end point should be a strong and stable server which is able to send reply quickly. We suggest using the LAN IP address of the VPN remote end point device as the target of the Heart Beat detection.
<hr/>	
Interval	The default time for the Heart Beat interval is 30 seconds. The system will send back an ICMP echo request in every 30 seconds after the VPN tunnel is established.
<hr/>	
Retry	The default retry times are 5. The system will terminate the VPN tunnel if the

Heart Beat is still failure over the retry default.

The VPN Heart Beat detection and DPD features are both used to provide a stabile VPN solution for customers. The difference between them is that we can use the Heart Beat detection in a non IPSec protocol. With the Heart Beat detection, we can monitor the VPN tunnel and make sure whether the tunnel exists and smooth or not. However, with the DPD feature, it is only available under the IPSec protocol.

10.1.1.2. Client to Gateway Setting

The following describes how an administrator builds a VPN tunnel between devices. Users can set this VPN tunnel to be used by one client at the client end. If it is used by a group of clients, the individual setting for remote clients can be reduced. Only one tunnel will be set and used by a group of clients, which allows easy setting.

Situation in Tunnel :

▶ Client to Gateway

Tunnel(s) VPN Group

Tunnel(s) No.	1
Tunnel(s) Name :	<input type="text"/>
Interface:	WAN 1 ▼
Enabled :	<input checked="" type="checkbox"/>

Tunnel No. :	Set the embedded VPN feature, please select the Tunnel number.
Tunnel Name :	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion.
	Note: If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.
Interface :	Users may select which port to be the node for this VPN channel. They can be applied for VPN connections.
Enabled :	Click to Enable to activate the VPN tunnel. This option is set to Enable by default. After users set up, users may select to activate this tunnel feature.

Local Group Setup

This local gateway authentication type (Local Security Gateway Type) must be identical with that of the remote type (Remote Security Gateway Type).

Local Security Gateway Type :	<p>This local gateway authentication type comes with five operation modes, which are:</p> <p>IP only - Authentication by the use of IP only IP + Domain Name (FQDN) Authentication, -IP + Domain name IP + E-mail Addr. (USER FQDN) Authentication, -IP + Email address Dynamic IP + Domain Name (FQDN) Authentication, -Dynamic IP address + Domain name Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name</p> <p>(1) IP only:</p> <p>If users decide to use IP only, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #0070c0; color: white; padding: 2px;">Local Security Gateway Type:</td> <td style="padding: 2px;">IP Only ▼</td> </tr> <tr> <td style="background-color: #0070c0; color: white; padding: 2px;">IP Address:</td> <td style="padding: 2px;"> <input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/> </td> </tr> </table> </div> <p>(2) IP + Domain Name(FQDN) Authentication:</p> <p>If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #0070c0; color: white; padding: 2px;">Local Security Gateway Type:</td> <td style="padding: 2px;">IP + Domain Name(FQDN) Authentication ▼</td> </tr> <tr> <td style="background-color: #0070c0; color: white; padding: 2px;">IP Address:</td> <td style="padding: 2px;"> <input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/> </td> </tr> <tr> <td style="background-color: #0070c0; color: white; padding: 2px;">Domain Name:</td> <td style="padding: 2px;"><input style="width: 100%;" type="text"/></td> </tr> </table> </div> <p>(3) IP + E-mail Addr. (USER FQDN) Authentication.</p> <p>If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further</p>	Local Security Gateway Type:	IP Only ▼	IP Address:	<input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/>	Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication ▼	IP Address:	<input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/>	Domain Name:	<input style="width: 100%;" type="text"/>
Local Security Gateway Type:	IP Only ▼										
IP Address:	<input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/>										
Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication ▼										
IP Address:	<input style="width: 20px;" type="text" value="221"/> . <input style="width: 20px;" type="text" value="169"/> . <input style="width: 20px;" type="text" value="231"/> . <input style="width: 20px;" type="text" value="22"/>										
Domain Name:	<input style="width: 100%;" type="text"/>										

	<p>settings.</p> <div data-bbox="571 383 1396 488"> <table border="1"> <tr> <td>Local Security Gateway Type:</td> <td>IP + E-mail(User FQDN) Authentication</td> </tr> <tr> <td>IP Address:</td> <td>221 . 169 . 231 . 22</td> </tr> <tr> <td>E-mail:</td> <td><input type="text"/> @ <input type="text"/></td> </tr> </table> </div> <p>(4) Dynamic IP + Domain Name(FQDN) Authentication:</p> <p>If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.</p> <div data-bbox="571 904 1396 981"> <table border="1"> <tr> <td>Local Security Gateway Type:</td> <td>Dynamic IP + Domain Name(FQDN) Authentication</td> </tr> <tr> <td>Domain Name:</td> <td><input type="text"/></td> </tr> </table> </div> <p>(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.</p> <p>If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; if users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.</p> <div data-bbox="571 1391 1332 1456"> <table border="1"> <tr> <td>Local Security Gateway Type:</td> <td>Dynamic IP + E-mail(User FQDN) Authentication</td> </tr> <tr> <td>E-mail:</td> <td><input type="text"/> @ <input type="text"/></td> </tr> </table> </div>	Local Security Gateway Type:	IP + E-mail(User FQDN) Authentication	IP Address:	221 . 169 . 231 . 22	E-mail:	<input type="text"/> @ <input type="text"/>	Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication	Domain Name:	<input type="text"/>	Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication	E-mail:	<input type="text"/> @ <input type="text"/>
Local Security Gateway Type:	IP + E-mail(User FQDN) Authentication														
IP Address:	221 . 169 . 231 . 22														
E-mail:	<input type="text"/> @ <input type="text"/>														
Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication														
Domain Name:	<input type="text"/>														
Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication														
E-mail:	<input type="text"/> @ <input type="text"/>														
<p>Local Security Group Type :</p>	<p>This option allows users to set the local VPN connection access type. The following offers a few items for local settings. Please select and set appropriate parameters:</p> <p>1. IP address</p> <p>This option allows the only IP address which is entered to build the VPN tunnel.</p> <div data-bbox="577 1765 1380 1865"> <table border="1"> <tr> <td>Local Security Group Type:</td> <td>IP Address</td> </tr> <tr> <td>IP Address:</td> <td>192 . 168 . 1 . 0</td> </tr> </table> </div> <p>Reference: When this VPN tunnel is connected, computers with the IP</p>	Local Security Group Type:	IP Address	IP Address:	192 . 168 . 1 . 0										
Local Security Group Type:	IP Address														
IP Address:	192 . 168 . 1 . 0														

address of 192.168.1.0 can establish connection.

2. Subnet

This option allows local computers in this subnet to be connected to the VPN tunnel.

Local Security Group Type:	Subnet <input type="button" value="v"/>
IP Address:	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0

Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

Remote Group Setup :

Remote Security Gateway Type:	IP Only ▼
IP Address ▼	<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>

This remote gateway authentication type (Remote Security Gateway Type) must be identical to the remotely-connected local security gateway authentication type (Local Security Gateway Type).

<p>Remote Security Gateway Type :</p>	<p>This local gateway authentication type comes with five operation modes, which are:</p> <ul style="list-style-type: none"> IP only IP + Domain Name (FQDN) Authentication IP + E-mail Addr. (USER FQDN) Authentication Dynamic IP + Domain Name (FQDN) Authentication Dynamic IP + E-mail Addr. (USER FQDN) Authentication <p>(1) IP only:</p> <p>If users decide to use IP only, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #0070C0; color: white; padding: 2px;">Remote Security Gateway Type:</td> <td style="padding: 2px;">IP Only ▼</td> </tr> <tr> <td style="background-color: #0070C0; color: white; padding: 2px;">IP Address ▼</td> <td style="padding: 2px;"> <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> </td> </tr> </table> </div> <p>(2) IP + Domain Name(FQDN) Authentication:</p> <p>If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #0070C0; color: white; padding: 2px;">Remote Security Gateway Type:</td> <td style="padding: 2px;">IP + Domain Name(FQDN) Authentication ▼</td> </tr> <tr> <td style="background-color: #0070C0; color: white; padding: 2px;">IP Address ▼</td> <td style="padding: 2px;"> <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> </td> </tr> <tr> <td style="background-color: #0070C0; color: white; padding: 2px;">Domain Name:</td> <td style="padding: 2px;"><input style="width: 100%; height: 20px;" type="text"/></td> </tr> </table> </div>	Remote Security Gateway Type:	IP Only ▼	IP Address ▼	<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>	Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication ▼	IP Address ▼	<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>	Domain Name:	<input style="width: 100%; height: 20px;" type="text"/>
Remote Security Gateway Type:	IP Only ▼										
IP Address ▼	<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>										
Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication ▼										
IP Address ▼	<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>										
Domain Name:	<input style="width: 100%; height: 20px;" type="text"/>										

(3) IP + E-mail Addr. (USER FQDN) Authentication.

If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Remote Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
E-mail:	<input type="text"/> @ <input type="text"/>

(4) Dynamic IP + Domain Name(FQDN) Authentication:

If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.

Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name:	<input type="text"/>

(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.

If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; if users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.

Remote Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication
E-mail:	<input type="text"/> @ <input type="text"/>

IPsec Setup

▶ IPsec Setting

Keying Mode:	IKE with Preshared Key ▼
Phase1 DHGroup :	Group 1 ▼
Phase1 Encryption:	DES ▼
Phase1 Authentication:	MD5 ▼
Phase1 SA Life Time:	0 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DHGroup :	Group 1 ▼
Phase2 Encryption:	DES ▼
Phase2 Authentication:	MD5 ▼
Phase2 SA Life Time:	0 seconds
Preshared Key:	<input type="text"/>

If there is any encryption mechanism, the encryption mechanism of these two VPN tunnels must be identical in order to create connection. And the transmission data must be encrypted with IPsec key, which is known as the encryption "key". The device provides the IKE automatic encryption mode- IKE with Preshared Key (automatic). By using the drop down menu, select the desired encryption mode as illustrated below.

Encryption Management Protocol :

When users set this VPN tunnel to use any encryption and authentication mode, users must set the parameter of this exchange password with that of the remote.

IKE Protocol :

Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the key will not be able to get the Phase 2 key in such a short period of time.

- **Perfect Forward Secrecy:** When users check the PFS option, don't forget to activate the PFS function of the VPN device and the VPN Client as well.

- **Phase 1/ Phase 2 DH Group:** This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
- **Phase 1/ Phase 2 Encryption:** This option allows users to set this VPN tunnel to use any encryption mode. Note that this parameter must be identical to that of the remote encryption parameter: DES (64-bit encryption mode), 3DES (128-bit encryption mode), AES (the standard of using security code to encrypt information). It supports 128-bit, 192-bit, and 256-bit encryption keys.
- **Phase 1/Phase 2 Authentication:** This authentication option allows users to set this VPN tunnel to use any authentication mode. Note that this parameter must be identical to that of the remote authentication mode: "MD5" or "SHA1".
- **Phase 1 SA Life Time:** The life time for this exchange code is set to 28800 seconds (or 8hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Phase2 SA Life Time:** The life time for this exchange code is set to 3600 seconds (or 1hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
- **Preshared Key :** For the Auto (IKE) option, enter a password of any digit or characters in the text of "Pre-shared Key" (the example here is set as test), and the system will automatically translate what users entered as exchange password and authentication mechanism during the VPN tunnel connection. This exchange password can be made up of up to 30 characters.

Advanced Setting- for IKE Protocol Only

▶ Advanced

Aggressive Mode
 Keep-Alive
 NetBIOS Broadcast
 NAT Traversal
 Dead Peer Detection(DPD) Enable Automatic Version Check Every seconds
 Heart Beat, Remote Host
 Enable Automatic Version Check Every seconds, Retry count
 Tunnel Backup :
 Remote Gateway :
 Backup Interface :

The advanced settings include Main Mode and Aggressive mode. For the Main mode, the default setting is set to VPN operation mode. The connection is the same to most of the VPN devices.

- Aggressive Mode: This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
- Use IP Header Compression Protocol: If this option is selected, in the connected VPN tunnel, the device supports IP Payload Compression Protocol.
- Keep Alive: If this option is selected, VPN tunnel will keep this VPN connection. This is mostly used to connect the remote node of the branch office and headquarter or used for the remote dynamic IP address.
- AH hash calculation: For AH (Authentication Header), users may select MD5/DSHA-1.
- NetBIOS Broadcast: If this option is selected, the connected VPN tunnel allows the passage of NetBIOS broadcast packet. This facilitates the easy connection with other Microsoft network; however, the traffic using this VPN tunnel will increase.
- Dead Peer Detection (DPD): If this option is selected, the connected VPN tunnel will regularly transmit HELLO/ACK message packet to detect whether there is connection between the two ends of the VPN tunnel. If one end is disconnected, the device will disconnect the tunnel automatically and then create new connection. Users can define the transmission time for each DPD message packet, and the default value is 10 seconds
- Heart Beat : VPN Tunnel Heart Beat Detection function ◦

If this option is selected, the system will sent ICMP ACK packet to the remote host with VPN tunnel regularly; the remote host will also send an ICMP ACK reply packet toward the originator.

If there is still no received ICMP ACK reply after exceeding the setting retry, the Heart Beat originator will terminate this VPN tunnel.

Under this situation, if you are the VPN tunnel initiator, the system will try to reconnect the tunnel; if you are the passive party, the system will wait for the initiator to establish the tunnel again.

Remote Host	The remote end point for the Heart Beat Detection. It is always sensible to select an end point for the Heart Beat detection; the end point should be a strong and stable server which is able to send reply quickly. We suggest using the LAN IP address of the VPN remote end point device as the target of the Heart Beat detection.
--------------------	---

Interval	The default time for the Heart Beat interval is 30 seconds. The system will send back an ICMP echo request in every 30 seconds after the VPN tunnel is
-----------------	--

established.

Retry	The default retry times are 5. The system will terminate the VPN tunnel if the Heart Beat is still failure over the retry default.
--------------	--

The VPN Heart Beat detection and DPD features are both used to provide a stabile VPN solution for customers. The difference between them is that we can use the Heart Beat detection in a non IPSec protocol. With the Heart Beat detection, we can monitor the VPN tunnel and make sure whether the tunnel exists and smooth or not. However, with the DPD feature, it is only available under the IPSec protocol.

10.1.2. PPTP Server

It supports the PPTP of Window XP/ 2000 to create point-to-point tunnel protocol for single- device users to create VPN connection.

Enable PPTP Server

PPTP encryption Setup

Use MPPE encryption

PPTP IP Address Range

IP Range Starts: 192.168.1.150
IP Range Ends: 192.168.1.154

[Unified IP Management](#)

New User Account

User(s) Defined

User Name :

New Password :

Confirm Password :

IP Address : Automatically
 Assign IP Address : . . .

[Add to list](#)

[Delete selected users](#)

Connection List

Tunnel(s) Used Tunnel(s) Available

User Name	Remote Address	PPTP IP Address
-----------	----------------	-----------------

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

Enabled PPTP Server :	When this option is selected, the point-to-point tunnel protocol PPTP server can be enabled.
PPTP IP Address Range :	Please enter PPTP IP address range so as to provide the remote users with an entrance IP into the local network. Enter Range Start: Enter the value into the last field. Enter Range End: Enter the value into the last field.
User name :	Please enter the name of the remote user.

Password : Confirm Password :	Enter the password and confirm again by entering the new password.
Add to list :	Add a new account and password.
Delete selected item :	Delete Selected Item.
Connection List	All PPTP Status:Displays all successfully connected users, including username, remote IP address, and PPTP address.

10.1.3. VPN Pass Through

▶ VPN Pass Through

IPSec Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
PPTP Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
L2TP Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

IPSec Pass Through :	If this option is enabled , the PC is allowed to use VPN- IPSec packet to pass in order to connect to external VPN device.
PPTP Pass Through :	If this option is enabled , the PC is allowed to use VPN- PPTP packet to pass in order to connect with external VPN device.
L2TP Pass Through :	If this option is enabled , the PC end is allowed to use VPN- L2TP packet to pass in order to connect with external VPN device.

After modification, push **“Apply”** button to save the network setting or push **“Cancel”** to keep the settings unchanged.

10.2. QVM VPN Function Setup

The QVM-series device provides three major convenient functions:

1. **Smart Link IPSec VPN:** Easy VPN setup replaces the conventional complicated VPN setup process by entering **Server IP, User Name, and Password.**
2. **Central Control Feature:** Displays a clear VPN connection status of all remote ends and branches. Its central control screen allows setup from remote into external client ends.
3. **VPN Disconnection Backup:** Solves data transmission problem arising from failed ISP connection with remote ends or the branches.

Select QVM feature as Client mode :

▶ Setup Mode

Smart Link VPN Server Setup ▼

▶ Smart Link VPN Server

Account ID:	<input style="width: 100%;" type="text"/>
Password:	<input style="width: 100%;" type="password"/>
Confirm Password:	<input style="width: 100%;" type="password"/>
IP Address:	<input style="width: 25px;" type="text" value="192"/> <input style="width: 25px;" type="text" value="168"/> <input style="width: 25px;" type="text" value="1"/> <input style="width: 25px;" type="text" value="0"/>
Subnet Mask:	<input style="width: 25px;" type="text" value="255"/> <input style="width: 25px;" type="text" value="255"/> <input style="width: 25px;" type="text" value="255"/> <input style="width: 25px;" type="text" value="0"/>
VPN Hub Function:	<input type="checkbox"/>
Active:	<input type="checkbox"/>
<input style="background-color: #0070C0; color: white; padding: 5px 15px;" type="button" value="Add to list"/>	

▶ Client Table

No.	Account ID	Status	Interface	Start Time	End Time	Duration	Control	Delete

Account ID :	Must be identical to that of the server account ID.
Password :	Must be identical to that of the server password.
Confirm Password :	Please enter the password and confirm again.
QVM VPN(IP Address or Dynamic Domain Name) :	Input QVM VPN Server IP address or domain name.
Status :	Displays QVN connection status.
Keep Alive: Redial Period <input type="text" value="5"/> Mins :	This function is to set re- connect duration if QVM contention drops. The range is 1~60 mins.
QVM Backup Tunnel :	You can input at most 3 backup IP addresses or domain names for backup. Once the connection is dropped, the function will be automatically enabled to backup the VPN connection and ensure data transition security.
Advanced Function : Change QVM Client's Service Port :	In some environment, port 443 has been used, for example, E-Mail Forwarding. To avoid the conflict with QVM, QVM port can be changed to other encryption ports, such as 10443.

After modification, press **"Apply"** to save the network setting or press **"Cancel"** to keep the settings unchanged.

XIII. Advanced Function

11.1 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 : ...

Interface : ANY ▼

Enabled :

Add to list

Delete selected application

Show Table
Apply
Cancel

11.1.1 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.

11.1.2 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://211.243.220.43>.

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] ▼

Service Management

IP Address :

Interface : ANY ▼

Enabled :

Add to list

Delete selected application

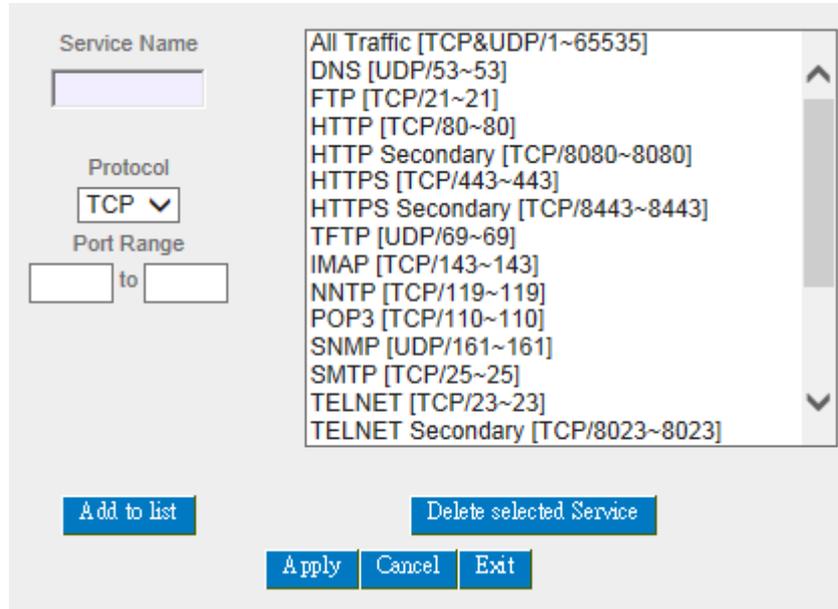
Show Table
Apply
Cancel

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.
Enabled :	Activate this function.
Service Port 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 :



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 such as 500~500 or 2300~2310, etc.
Add to list :	Add the service to the service list. It supports up to 100 rules.
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.

11.2 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 Function (Automatically mapping) : Yes NO

▶ UPnP Setup

Service :

Name or IP Address :

Enabled :

Service Management
Add to list

Delete selected application

Show Table
Apply
Cancel

- 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.
- Cancel:** Click "Cancel" to leave without making any change.

11.3 Routing

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

IPv4

IPv6

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 ▾

Static Routing

Dest. IP : . . .

Subnet Mask : . . .

Default Gateway : . . .

Metric :

Interface : LAN ▾

Add to list

Delete selected item

Show Table
Apply
Cancel

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 :

Metric :

Interface : LAN

Dest. IP :	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.
Subnet Mask :	
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.

11.4 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:

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 Seleted 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 !

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. 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.

10.5 DDNS- Dynamic Domain Name Service

DDNS supports the dynamic web address transfer for NOIP DDNS、DynDNS. This is for VPN 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, dydns or NOIP ddns .

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	Dydns Disabled NOIP Disabled	Dydns:--- NOIP:---	Edit
WAN 2	Dydns Disabled NOIP Disabled	Dydns:--- NOIP:---	Edit

* The UI might vary from model to model, depending on different product lines.

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:	Not Updated.	

No-IP.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:	Not Updated.	

* The UI might vary from model to model, depending on different product lines.

Interface	This is an indication of the WAN port the user has selected.
DDNS	Check either of the boxes before DynDNS and NOIPD DNS 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.ddns.org.cn as a user name for DDNS.
Password	The password which is set up for DDNS.
Dynamic Domain Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org
WAN 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.

11.6 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	00-0E-A0-AB-CD-F0	Edit
WAN 2	00-0E-A0-AB-CD-F1	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 -0E -A0 -AB -CD -F0
MAC Address from this PC	<input type="radio"/>

Default 00-0E-A0-AB-CD-F0

Apply
Cancel

11.7 USB Storage

By using FTP Client software or SAMBA, users are able to access the files stored in the USB Storage device (FAT32/NTFS) after being inserted to the USB port on the router.

The USB LED notification will light up after the storage device has been inserted into the USB port. The status of the USB Storage settings can be seen after logging in to the router.



▶ Status

Port ID	USB Mass Storage	Disk Capacity	Free Capacity	Disconnect
USB1				Link Down
USB2	Generic Mass Storage	3.91 GB	3.36 GB	Disconnect

Status :

Link Down : The USB port does not detect the device or there are no devices plugged into the port.

Disconnect : An USB Storage device is plugged into the port, clicking on “Disconnect” will disconnect the device.

11-7-1 FTP Service

The FTP Service functionality is enabled by default, only the setup of an user account is required to use the service. Please use an FTP Client software to use the service.

- The FTP Server IP is the same as the Router IP.
- The default service port is 21.

▶ General Setting



(1) User Account setup

🔑 User Management

User Name :

Password :

Access Policy : Read-Only ▾

Enabled :

[Add to list](#)

john=>Read-Only
sam=>Read-Only
tina=>Read-Write

[Delete select Account](#)

- User name : User name of the account for both FTP and SAMBA Services.
- Password : Password of the account for both FTP and SAMBA Services. Must contain at least 5 characters.
- Access Policy :
 - read only : User can only read the files in the USB Storage device.
 - read-write : User can add, read, or delete the files stored in the device.
- Enabled : Check this box to enable the rule.

(2) Guest Account Setup

Guest Access
 Read-Write
 Read-Only
 Disabled

Guest Access is for providing guests (username: Guest) access to the files within the USB Storage without requiring a password. The default setting for this function is disabled. There are only two permissions for this function.

- read only : Users can only read from the storage device.
- read-write : Users can add, read, or delete the files stored in the device.

(3) Advanced Settings

Simultaneous FTP Connections	<input type="text" value="10"/>
FTP Server Charset	<input type="text" value="UTF-8"/> ▼

- Simultaneous FTP Connection : Total number of client connections the FTP Server can accept at the same time.
- FTP Service Charset : FTP Server Character set, the selections are UFT8, GB2312 and BIG5.

11-7-2 SAMBA

SAMBA Service functionality is enabled by default, only the setup of an user account is required to use the service.

Network Place (Samba) Enabled Disabled

(1) User Account Setup

➤ User Management

User Name :

Password :

Access Policy : ▼

Enabled :

Add to list

john=>Read-Only
sam=>Read-Only
tina=>Read-Write

Delete select Account

- User name : User name of the account for both FTP and SAMBA Services.
- Password : Password of the account for both FTP and SAMBA Services. Must contain at least 5 characters.
- Access Policy :
 - read only : Users can only read from the storage device.
 - read-write : Users can add, read, or delete the files stored in the device.
- Enabled : Check this box to enable the rule.

(2) Guest Account Setup

Guest Access Read-Write Read-Only Disabled

Guest Access is for providing guests (username: Guest) access to the files within the USB Storage without requiring a password. The default setting for this function is disabled. There are only two permissions for this function.

- read only : Users can only read from the storage device.
- read-write : Users can add, read, or delete the files stored in the device.

(3) Advanced Settings

Host Name	ALL-VPN10
Work Group	workgroup

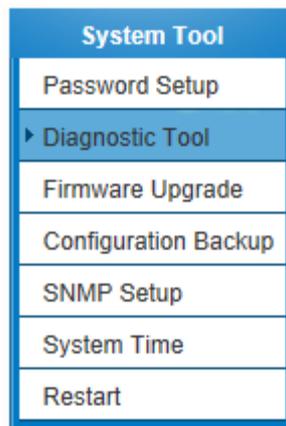
- Host Name : The name for the router.
- Work Group : The name of the workgroup to join or show in the network.

XIV. 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.

12.1 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

Look up domain name

DNS Lookup

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

DNS Lookup Ping

Look up domain name

Name: www.allnet.de
 Address: 212.18.29.151

Ping

DNS Lookup Ping

Ping host or IP address

Status **Test Succeeded**

Packets: 4/4 transmitted,3/4 received,25 % loss

Round Trip Time: Minimum = 352.5 ms
Maximum = 738.5 ms
Average = 538.2 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 192.168.5.20. Press "Go" to start the test. The result will be displayed on this screen.

12.2 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.

Note !

Please read the warning before firmware upgrade.

Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.



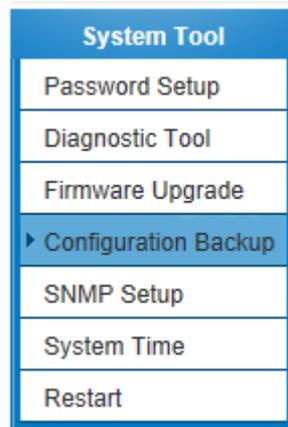
Firmware Upgrade



- 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 : v1.0.0.4 (Oct 23 2013 09:02:42)

12.3 Configuration Backup



▶ Import Configuration File

Import

▶ Export Configuration File

Export

Import Configuration File :

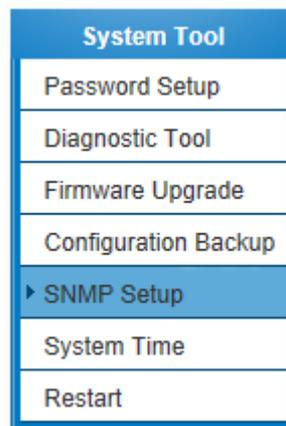
This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to import the file.

Export Configuration File :

This feature allows users to backup all parameter settings. Click "Export" and select the location to save the "config.exp" file.

12.4 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	ALL-VPN10
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

* The UI might vary from model to model, depending on different product lines.

Enabled :	Activate SNMP feature. The default is activated.
System Name :	Set the name of the device such as .
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.

12.5 System Recover

Users can restart the device with System Recover button.



▶ Restart

Restart Router

▶ Factory Default

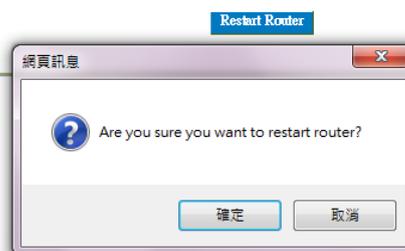
Return to Factory Default Setting

System Recover

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

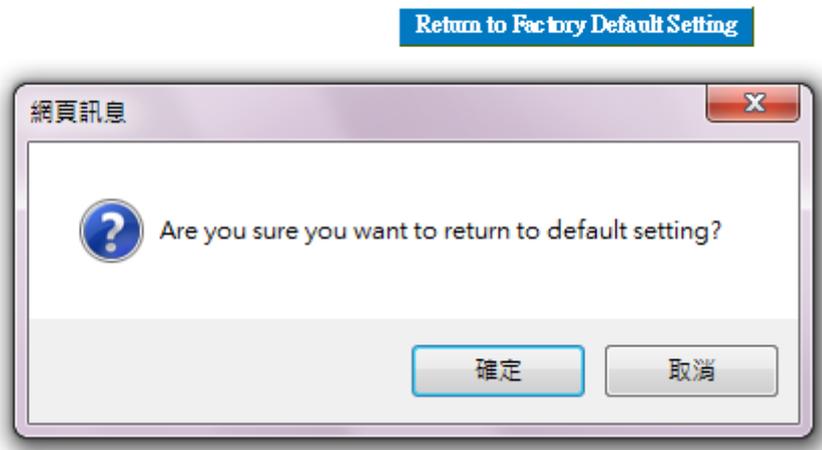
▶ Factory Default



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.

▶ Factory Default

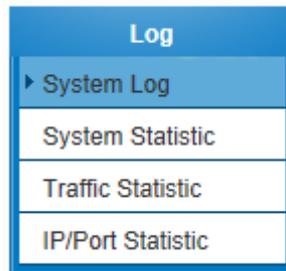


XV. Log

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.

13.1 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

▶ Email

E-mail Alert

Mail Server : Name or IP Address

Send E-mail to : E-mail Address

Log Queue Length : entries

Log Time Threshold : Minutes

[Email Log Now](#)

▶ 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

Enable :	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

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.

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.

System Error Message :	Provides the system log with all kinds of error messages. For example, wrong settings, occurrence of abnormal functions, system reactivation, disconnection of PPPoE and so on.
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.
Configuration Change :	When the system settings are changed, this message will be sent back to 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.

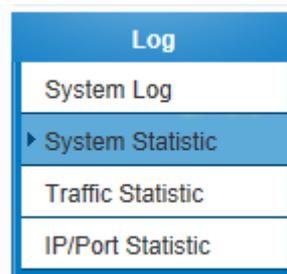
View System Log :

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: Mon Oct 28 08:50:22 2013		<input type="button" value="All Log"/> <input type="button" value="Refresh"/> <input type="button" value="Close"/>
Time ▲	Event-Type	Message
Jan 1 01:00:26 1970	System Log	ALL-VPN10 : System is up
Jan 1 01:00:26 1970	Kernel	kernel: PROC INIT OK!
Jan 1 01:00:28 1970	System Log	PPTP Server: pptp server is up.
Jan 1 01:16:53 1970	System Log	WAN1 connection is up : 192.168.3.105/255.255.255.0 gw 192.168.3.1 on eth1
Sep 30 03:58:04 2013	System Log	User admin login success from 192.168.1.100
Sep 30 04:00:24 2013	System Log	/sbin/usbinkctl: Succeeded to initialize usb2
Sep 30 04:07:46 2013	System Log	/sbin/usbinkctl: Succeeded to remove usb2
Sep 30 04:08:02 2013	System Log	/sbin/usbinkctl: Succeeded to initialize usb2
Sep 30 04:17:14 2013	System Log	WAN1 connection is up : 192.168.3.109/255.255.255.0 gw 192.168.3.1 on eth1

13.2 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 (%).



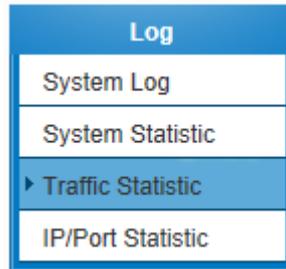
System Statistic

Interface	WAN 1	WAN 2	LAN
Device Name	eth1	eth2	eth0
Status	Connect	Enabled	---
Device IP Address	221.169.231.22	0.0.0.0	192.168.1.1
MAC Address	00-0E-A0-AB-CD-F0	00-0E-A0-AB-CD-F1	00-0E-A0-AB-CD-EF
Subnet Mask	255.255.255.255	0.0.0.0	255.255.255.0
Default Gateway	221.169.231.1	0.0.0.0	---
DNS	139.175.55.244 139.175.252.16	0.0.0.0	---
Network Service Detection	Test Succeeded	Test Failed	---
Received Packets	47	0	10
Transmitted Packets	2	0	33
Total Packets	50	0	44
Received Packets KBytes	6585	0	1406
Transmitted Packets KBytes	73337	0	11287
Total Packets KBytes	79922	0	12694
Received KBytes/Sec	2	0	<1
Transmitted KBytes/Sec	112	0	<1
Error Packets	0	0	0
Dropped Packets	0	0	0
Sessions	0	0	---
New Sessions/Sec	0	0	---
Upstream Bandwidth Usage	9	0	---
Downstream Bandwidth Usage	0	0	---

Refresh

13.3 Traffic Statistic

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



Traffic Statistic

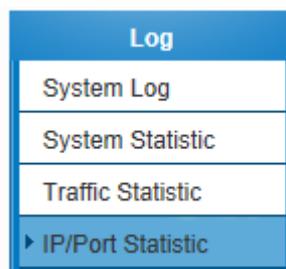
Traffic Type : ▾

Enabled Traffic Statistic

Source IP	KBytes/sec	%
-----------	------------	---

13.4 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 IP Address : 192 168 1 100 Search

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

Refresh

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 IP Address : 192 168 1 100 Search

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

Refresh

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 : 80 Search

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

Refresh

XVI. Log out

On the top right corner of the web- based UI, there is a Logout button. Click on it to log out of the web- based UI. To enter next time, open the Web browser and enter the IP address, user name and password to log in.





Appendix I : Technical Support Information

Official Website

<http://www.allnet.de>

Support :

E- mail : support@allnet.de

Appendix II Federal Communication Commission Interference Statement

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.

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

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

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

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

Radiation Exposure Statement:

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 60950-1: 2006+A11: 2009+A1: 2010+A12: 2011

Safety of Information Technology Equipment

EN 300 328 V1.7.1: 2006

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1: 2008

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1 2009

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems.

This device is a wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

ALLNET GPL Code Statement

This ALLNET product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

<http://www.allnet.de/gpl.html>

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

Written offer for GPL and LGPL source code

Where such specific license terms entitle you to the source code of such software, ALLNET will provide upon written request via e-mail and/or traditional paper mail the applicable GPL and LGPL source code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Email:

support@allnet.de

**CE-Declaration of Conformity**

For the following equipment:

Germering, 11th of October, 2013

VPN/Firewall WLAN-N WAN Router**ALL-VPN10**

The safety advice in the documentation accompanying the products shall be obeyed.
The conformity to the above directive is indicated by the CE sign on the device.

The Allnet ALL-VPN10 conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

EN301489-1 V1.9.2 (2011-09)

EN301489-17 V2.2.1 (2012-09)

EN55022:2010+AC:2011, Class B

EN61000-3-2:2006+A1:2009+A2:2009, Class A

EN610003-3:2008

EN61000-4-2:2009

EN61000-4-3:2006+A1:2008+A2:2010

EN61000-4-4:2012

EN61000-4-5:2006

EN61000-4-6:2009

EN61000-4-11:2004

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET Computersysteme GmbH

Maistraße 2

82110 Germering

Germany

Germering, 11.10.2013


Wolfgang Marcus Bauer
CEO