ALL0360

Wireless LAN Controller

User Manual

Content

II. Multi- WAN ALL0360 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 ALL0360 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 ALL0360 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. Logout

2.2 Setting Flow Chart

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

#	Setting	Content	Purpose
1	Hardware installation	Configure the network to meet user's demand.	Install ALL0360 hardware based on user physical requirements.
2	Login	Login the device with Web Browser.	Login ALL0360 web-based UI.
3	Verify device specification	Verify Firmware version and working status.	Verify ALL0360 specification, Firmware version and working status.
	Set password and time	Set time and re-new password.	Modify the login password considering safe issue. Synchronize the ALL0360 time with WAN.
4	Set WAN connection	Verify WAN connection setting, bandwidth allocation, and protocol binding.	Connect to WAN. Configure bandwidth to optimize data transmission.
5	Set LAN connection: physical port and IP address settings	Set mirror port and VLAN. Allocate and manage LAN IP.	Provide mirror port, port management and VLAN setting functions. Support Static/DHCP IP allocation to meet different needs. IP group will simplize the management work.
6	Set QoS bandwidth management: avoid bandwidth occupation	Restrict bandwidth and session of WAN ports, LAN IP and application.	To assure transmission of important information, manage and allocate the bandwidth further to achieve best efficiency.

7	Set Firewall: prevent attack and improper access to network resources	Block attack, Set Access rule and restrict Web access.	Administrators can block BT to avoid bandwidth occupation, and enable access rules to restrict employee accessing internet improperly or using MSN, QQ and Skype during working time. They can also protect network from Worm or ARP attacking.
8	Advanced Settings:DMZ/Forwarding, UPnP, DDNS, MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone
9	Management and maintenance settings: Syslog, SNMP, and configuration backup	Monitor ALL0360 working status and configuration backup.	Administrators can look up system log and monitor system status and inbound/outbound flow in real time.
11	Logout	Close configuration window.	Logout ALL0360 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 ALL0360 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 off: System self-test is completed successfully.
LAN/WAN/DMZ: 10M- Speed	Off	Ethernet is running at 10Mbps.
LAN/WAN/DMZ: 100M- Speed	Amber	Ethernet is running at 100Mbps.
LAN/WAN/DMZ: 1000M- Speed	Green	Ethernet is running at 1000Mbps.
WAN/DMZ:	Green	Green LED on: WAN is connected and gets the IP address. Green LED Blinking: Packets are transmitting through Ethernet port. Green LED off: WAN can not get the IP address.
LAN	Green	Green LED on: LAN is connected. Green LED Blinking: Packets are transmitting through Ethernet port.
USB	Green	Green LED on: USB is connected and the device is supported. Green LED Blinking: Packets are transmitting through USB port.

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.

System Built-in Battery

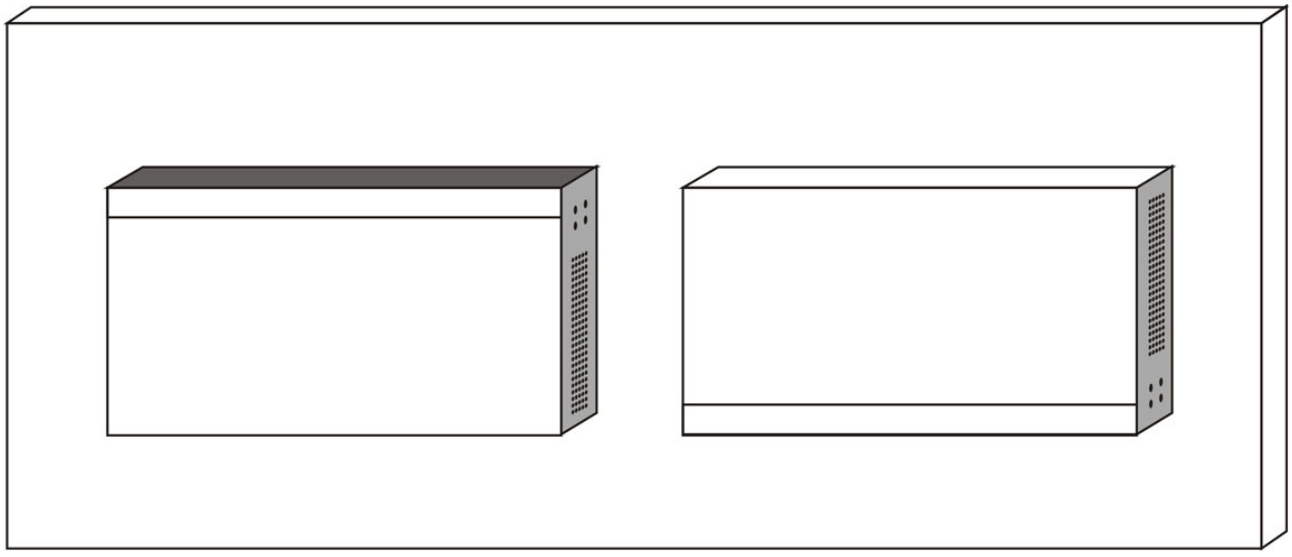
A system timing battery is built into ALL0360. The lifespan of the battery is about 1~2 years. If the battery life is over or it can not be charged, ALL0360 will not be able to record time correctly, nor synchronize with internet NTP time server. Please contact your system supplier for information on how to replace the battery.

Attention!

Do not replace the battery yourself; otherwise irreparable damage to the product may be caused.

Wall-Mount Placement

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



3.2 ALL0360 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.

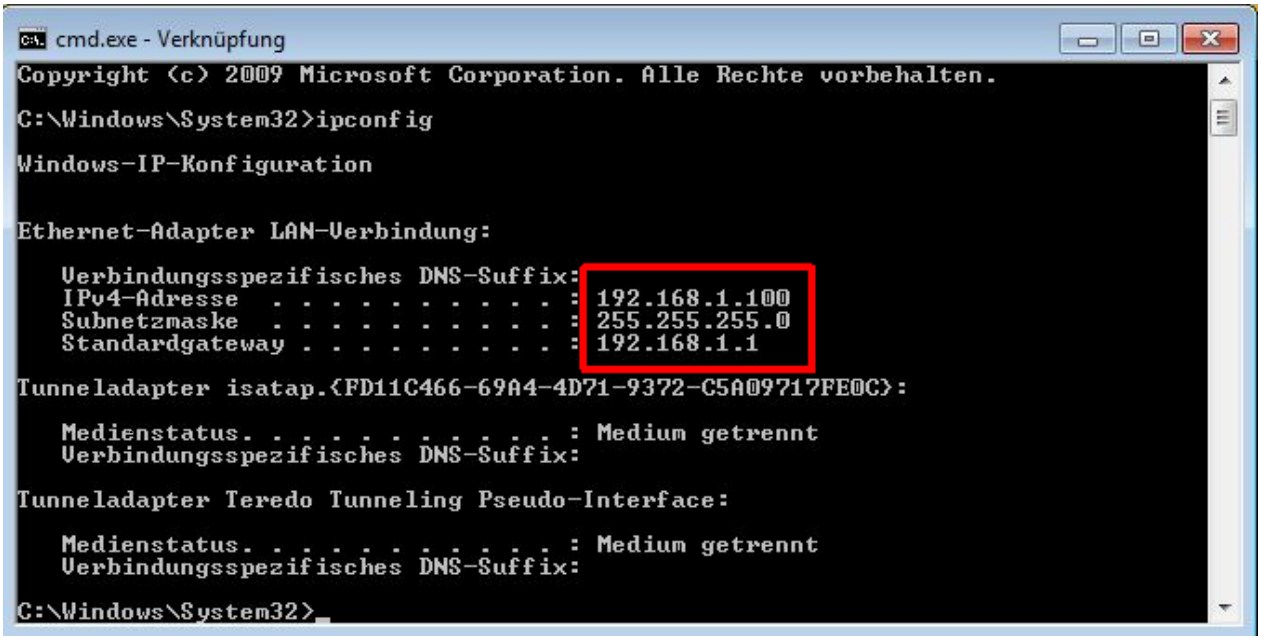
LAN Connection: The LAN port can be connected to a Switching Hub or directly to a PC. Users can use servers for monitoring or filtering through the port after "Physical Port Mangement" configuration is done.

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

IV. Login ALL0360

This chapter is mainly introducing Web-based UI after connecting ALL0360.

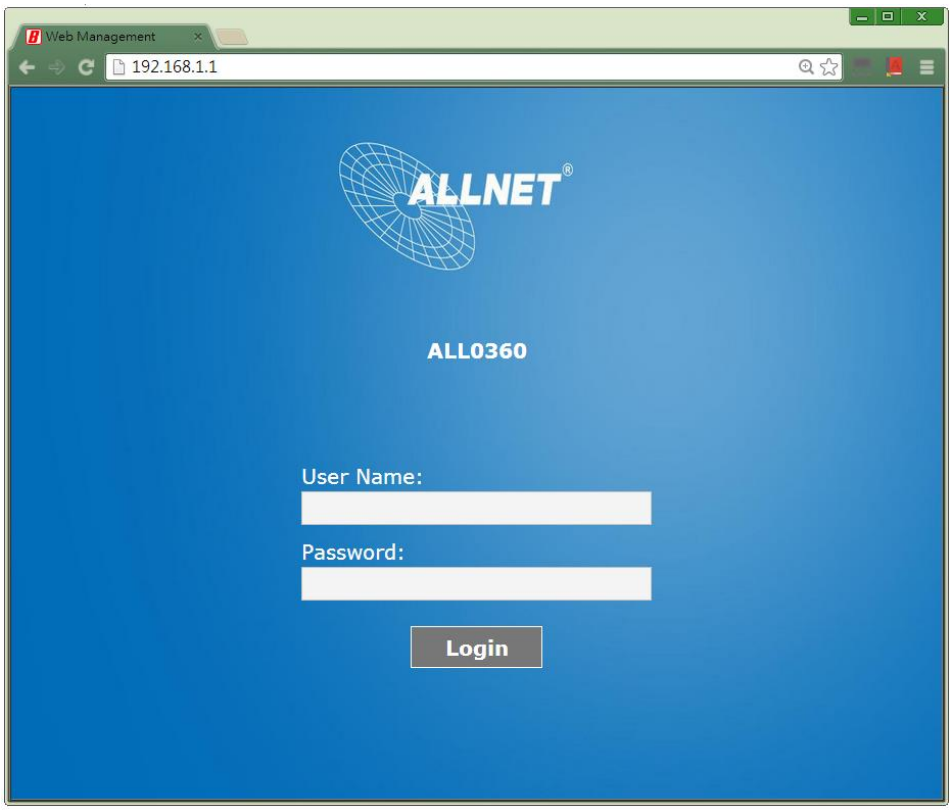
First, check up ALL0360 IP address by connecting to DOS through the LAN PC under ALL0360. Go to Start → Run, enter **cmd** to commend DOS, and enter **ipconfig** for getting Default Gateway address, as the graphic below, 192.168.1.1. Make sure Default Gateway is also the default IP address of ALL0360.



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:



ALL0360 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 ALL0360. Press Reset button for more than 10 sec, all the setting will return to default.

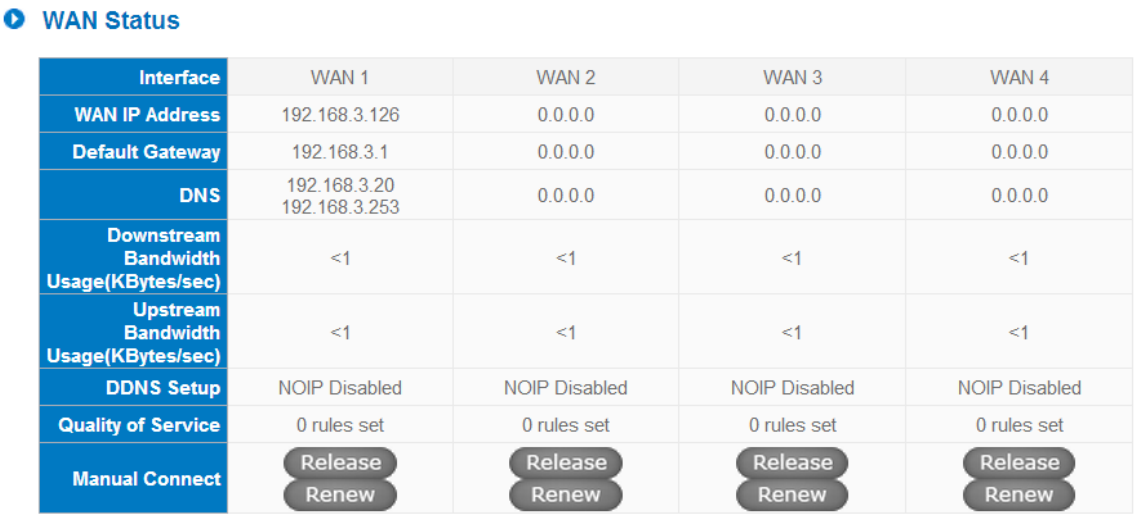
V. Device Spec Verification, Status Display and Login Password and Time Setting

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 ALL0360 parameters and status are listed for users' reference.

5.1.1 WAN Status



WAN Status

Interface	WAN 1	WAN 2	WAN 3	WAN 4
WAN IP Address	192.168.3.126	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	192.168.3.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS	192.168.3.20 192.168.3.253	0.0.0.0	0.0.0.0	0.0.0.0
Downstream Bandwidth Usage(KBytes/sec)	<1	<1	<1	<1
Upstream Bandwidth Usage(KBytes/sec)	<1	<1	<1	<1
DDNS Setup	NOIP Disabled	NOIP Disabled	NOIP Disabled	NOIP Disabled
Quality of Service	0 rules set	0 rules set	0 rules set	0 rules set
Manual Connect	Release Renew	Release Renew	Release Renew	Release Renew

WAN 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 ALL0360.
Downstream Bandwidth Usage(%):	Indicates the current downstream bandwidth usage(%) for each WAN.
Upstream Bandwidth Usage(%):	Indicates the current upstream bandwidth usage(%) for each WAN.
DDNS:	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.

5.1.2 Physical Port Status

Physical Port Status

Port ID	1
Interface	LAN
Status	Connect

Port ID	Internet	Internet	Internet	Internet
Interface	WAN 1	WAN 2	WAN 3	WAN 4
Status	Connect	Enabled	Enabled	Enabled

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

WAN 1 Information

Summary

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

Statistics

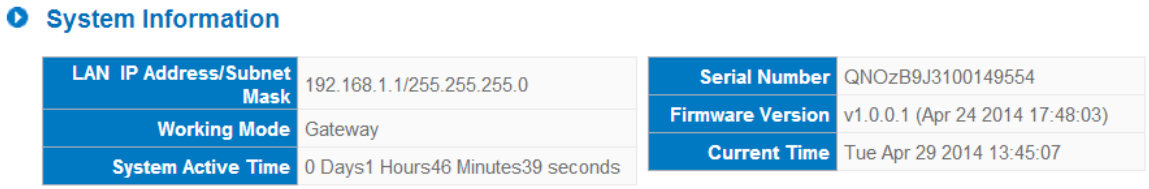
Received Packets Count	282810
Received Packets Byte Count	156558097
Transmitted Packets Count	238132
Transmitted Packets Byte Count	143336359
Error Packets Count	0

Refresh Close

The current port setting status information will be shown in the Port Information Table. Examples: type (10Base-T/100Base-TX/1000Base-T), 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 tabble also shows statistics of Receive/ Transmit Packets, Receive/Transmit Packets Byte Count as well as Error Packets Count.

5.1.3 System Information



Device IP Address/ Subnet Mask: Identifies the current device IP address and subnet mask. The default is 192.168.1.1 and 255.255.255.0

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

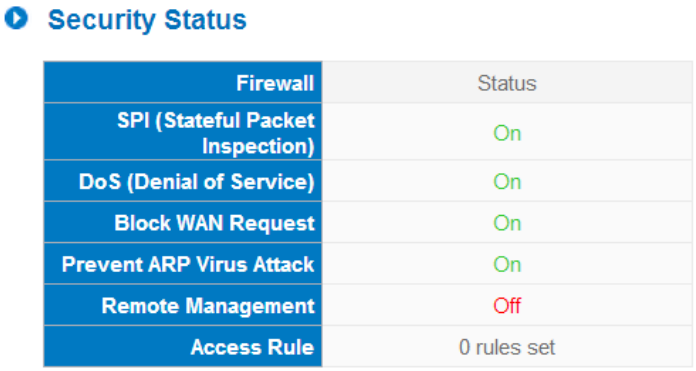
System active time: Indicates how long the device has been running.

Serial Number: This number is the device serial number.

Firmware Version:Information about the device present software version.

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

5.1.4 Firewall Status



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".

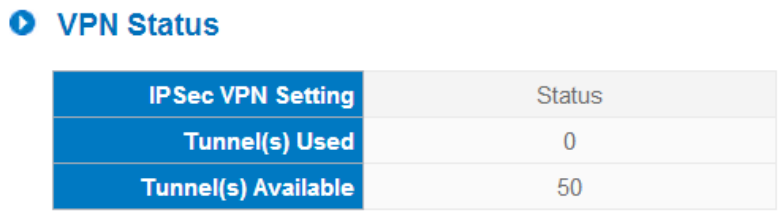
Block WAN Request:Indicates that denying the connection from Internet is activated. The default configuration is “On”.

Prevent ARP Virus Attack:Indicates that preventing Arp virus attack is acitvated. 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 ALL0360.

5.1.5 VPN Status

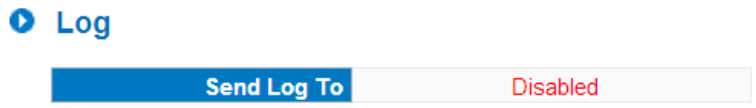


VPN Setting Status: Indicates VPN setting information in ALL0360.

Tunnel(s) Used:Indicates number of tunnels that have been configured in VPN (Virtual Private Network).

Tunnel(s) Available:Indicates number of tunnels that are available for VPN (Virtual Private Network).

5.1.6 Log Setting Status

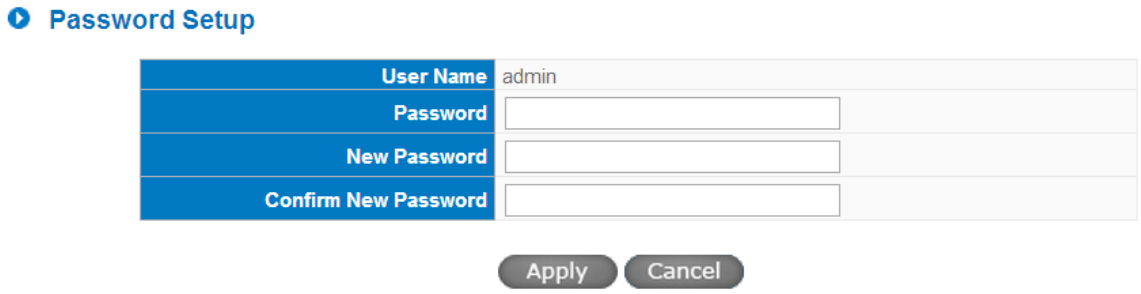


Syslog Server: Indicates if Syslog Server is Enabled or Disabled.

5.2 Change and Set Login Password and Time

5.2.1 Password Setting

When you login ALL0360 setting window every time, you must enter the password. The default value for ALL0360 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 ALL0360. You can press Reset button for more than 10 sec, ALL0360 will return back to default.



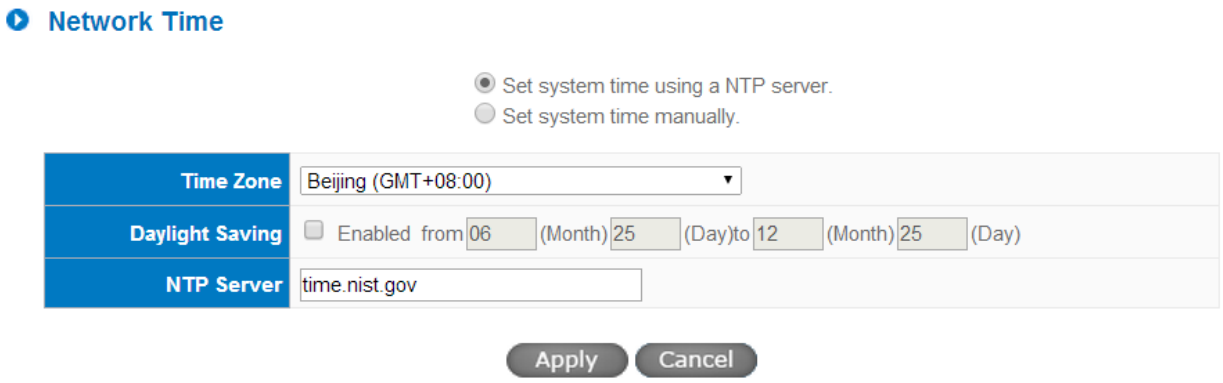
User Name:	The default is "admin".
Old Password:	Input the original password.（The default is "admin".）
New User Name:	Input the new user name. i.e.Allnet
New Password:	Input the new password.
Confirm New Password:	Input the new password again for verification.
Apply:	Click **"Apply"** to save the configuration.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

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

5.2.2 Time

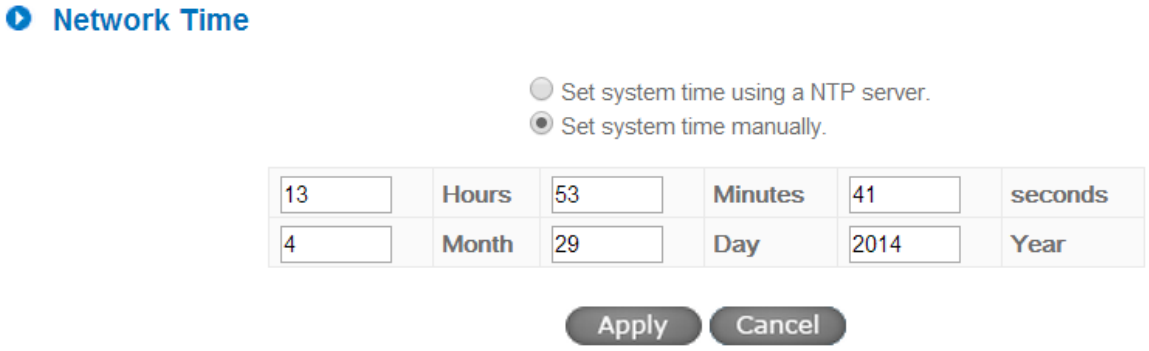
ALL0360 can adjust time setting. Users can know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources. You can either select the embedded NTP Server synchronization function or set up a time reference.

Synchronize with external NTP server: ALL0360 has embedded NTP server, which will update the time spontaneously.



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.
External 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.



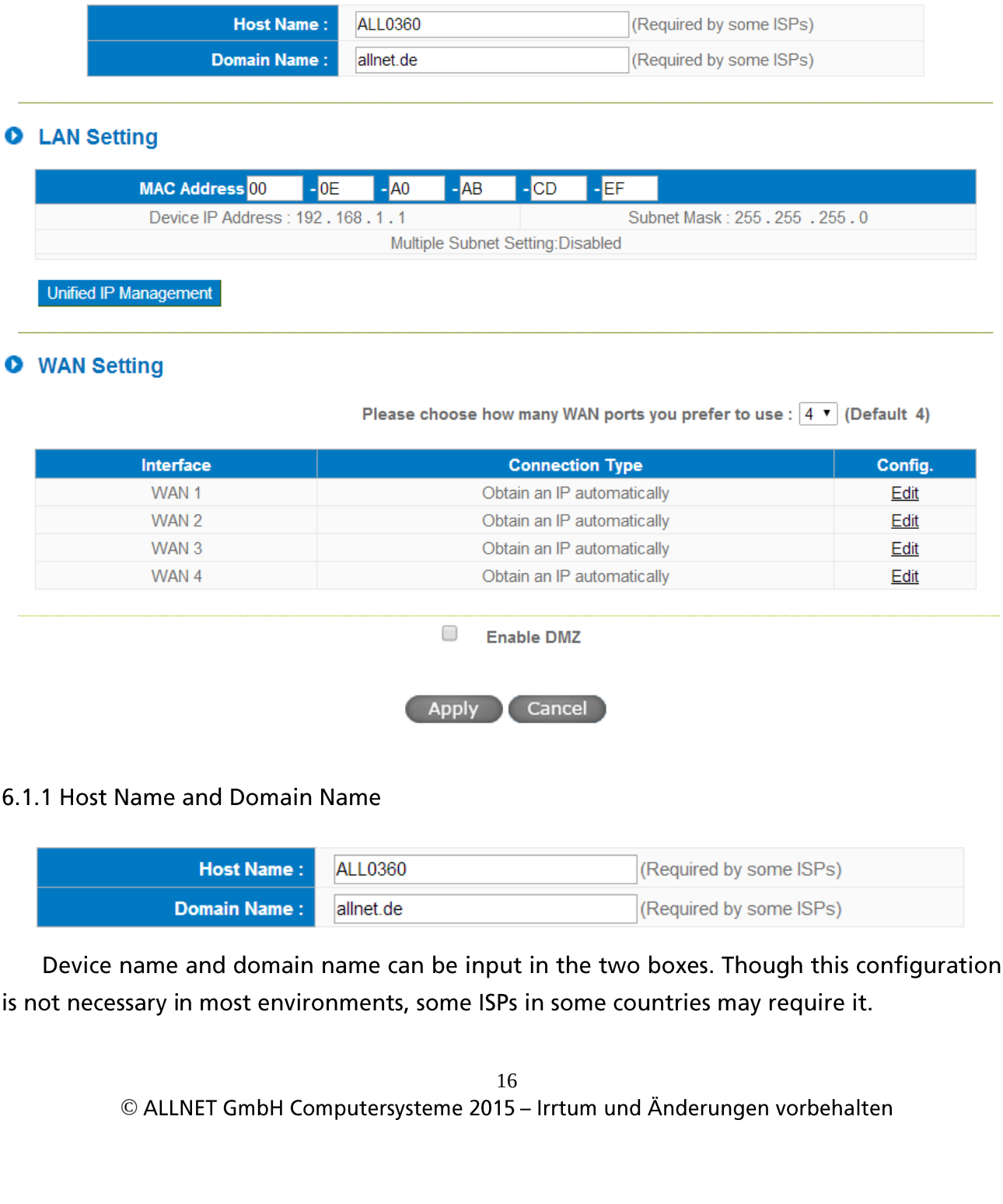
After the changes are completed, click **"Apply"** to save the configuration. Click **"Cancel"** to leave without making any change. This action will be effective before "Apply" to save the

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

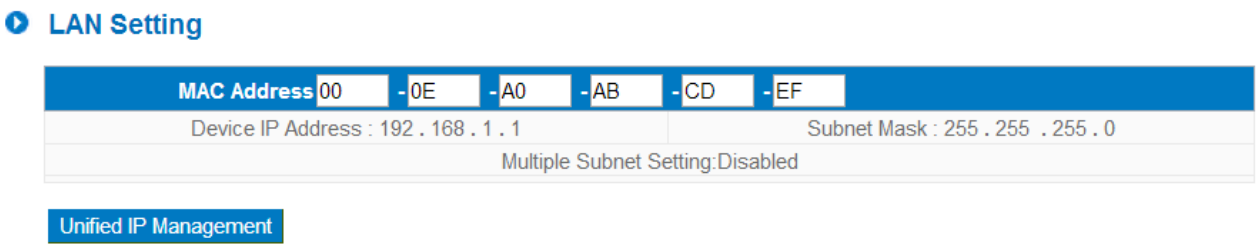


6.1.1 Host Name and Domain Name

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

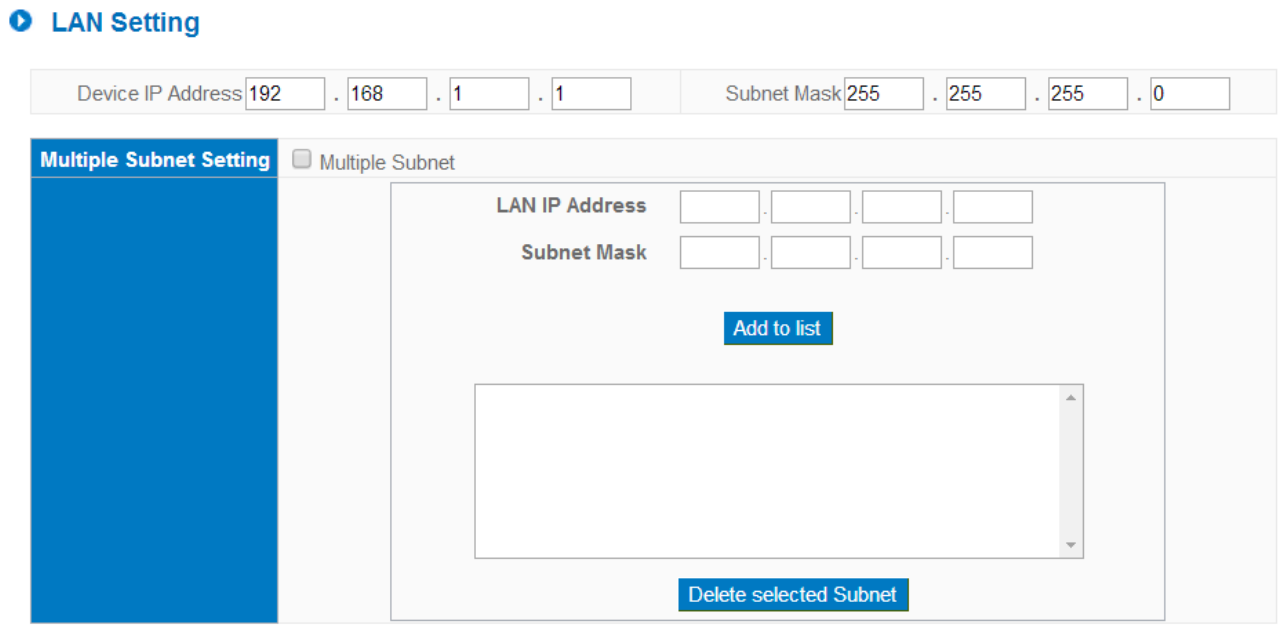
LAN setting is shown and can be configured in this page. The LAN MAC can be modified. When a new router replaces an old one, LAN MAC can be changed as MAC of the original device. Gateway ARP binding with LAN PCs won't need to be configured again. Click "Unified IP Management" to setup.



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.

Unified IP Management

LAN IP and IP segment group (DHCP) can be configured here.



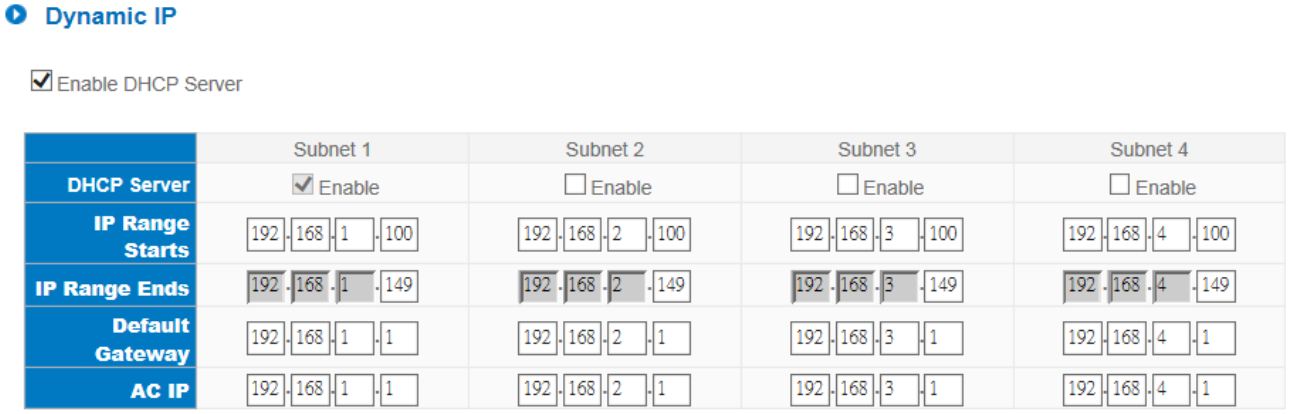
LAN Setting

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.

Multiple-Subnet Setting:

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

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.



Dynamic IP

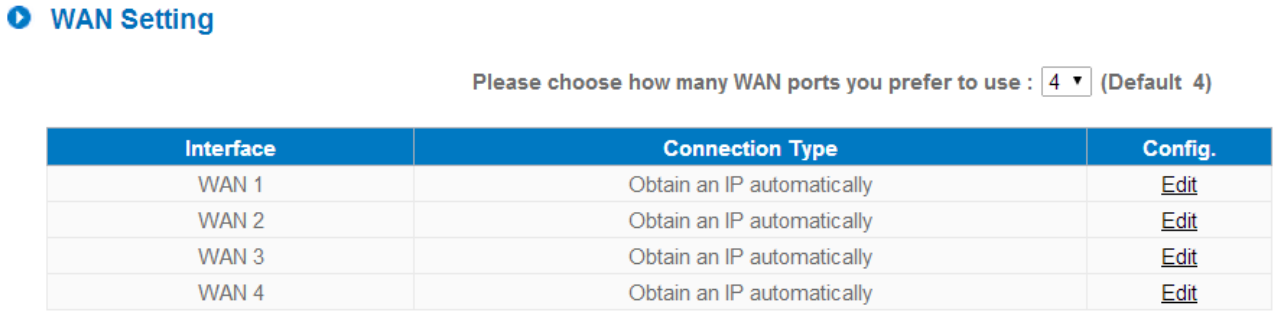
There are four set of Class C DHCP server. The defaults are enable. LAN PCs can get IP automatically without configured and recorded.

IP Range Start: The four default IP segments initial from 192.168.1.100, 192.168.2.100, 192.168.3.100, 192.168.4.100. Users can configure according actual demand.

IP Range End: The four default IP segments end at 192.168.1.149, 192.168.2.149, 192.168.3.149, 192.168.4.149. It means there are 50 IPs in one of segments. Users can configure according actual demand.

6.1.3 WAN & DMZ Settings

WAN Setting:



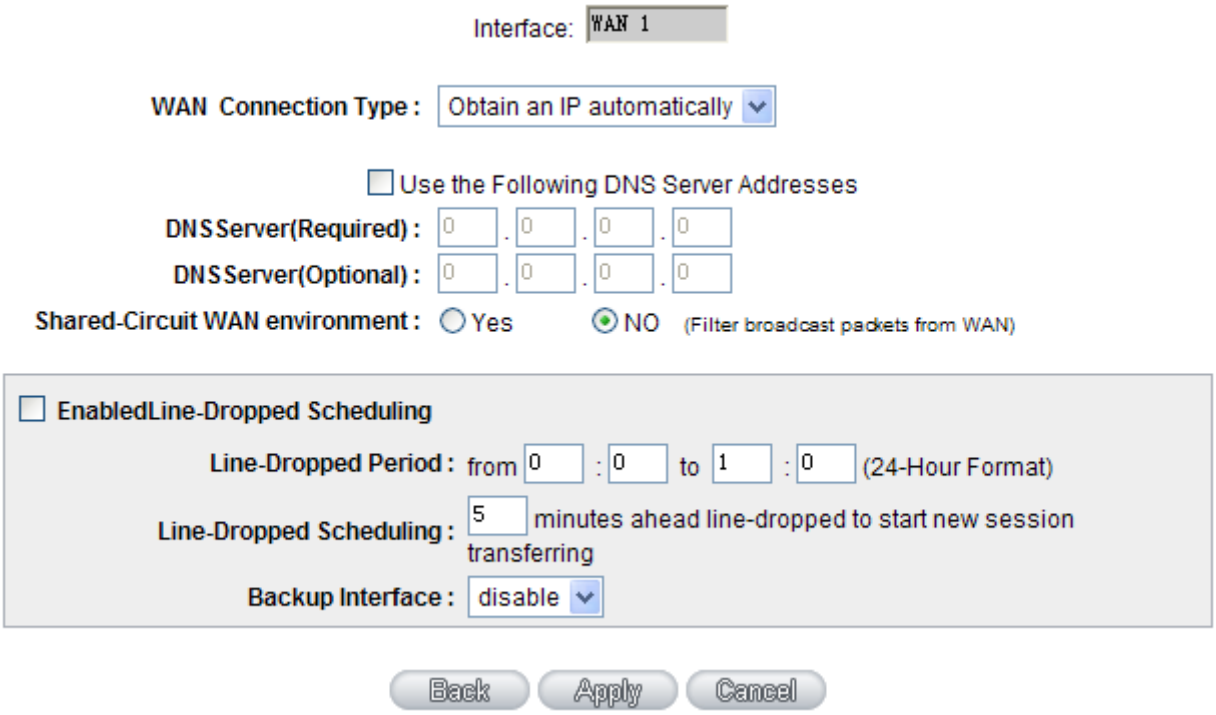
Interface: An indication of which port is connected.

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.



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.

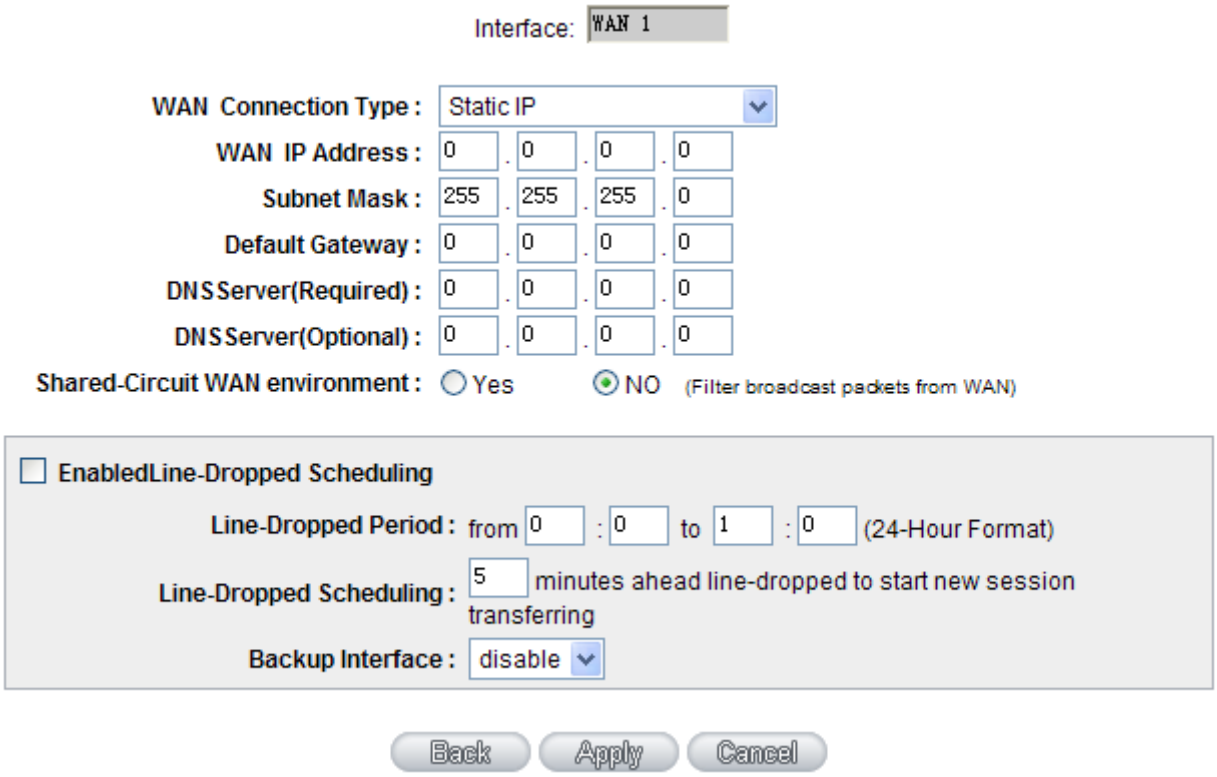
Enable Line-Dropped Scheduling: The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the 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.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select “Enabled” to filter broadcast packets. The default is “Disabled”.
MTU:	MTU is abbreviation of Maximum Transmission Unit. “Auto” and “Manual” can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is “Auto”.

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

Static IP

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



WAN IP address: Input the available static IP address issued by ISP.

Subnet Mask: Input the subnet mask of the static IP address issued by ISP, such as:

Issued eight static IP addresses: 255.255.255.248

Issued 16 static IP addresses: 255.255.255.240

Default Gateway: Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.

DNS Server: Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.

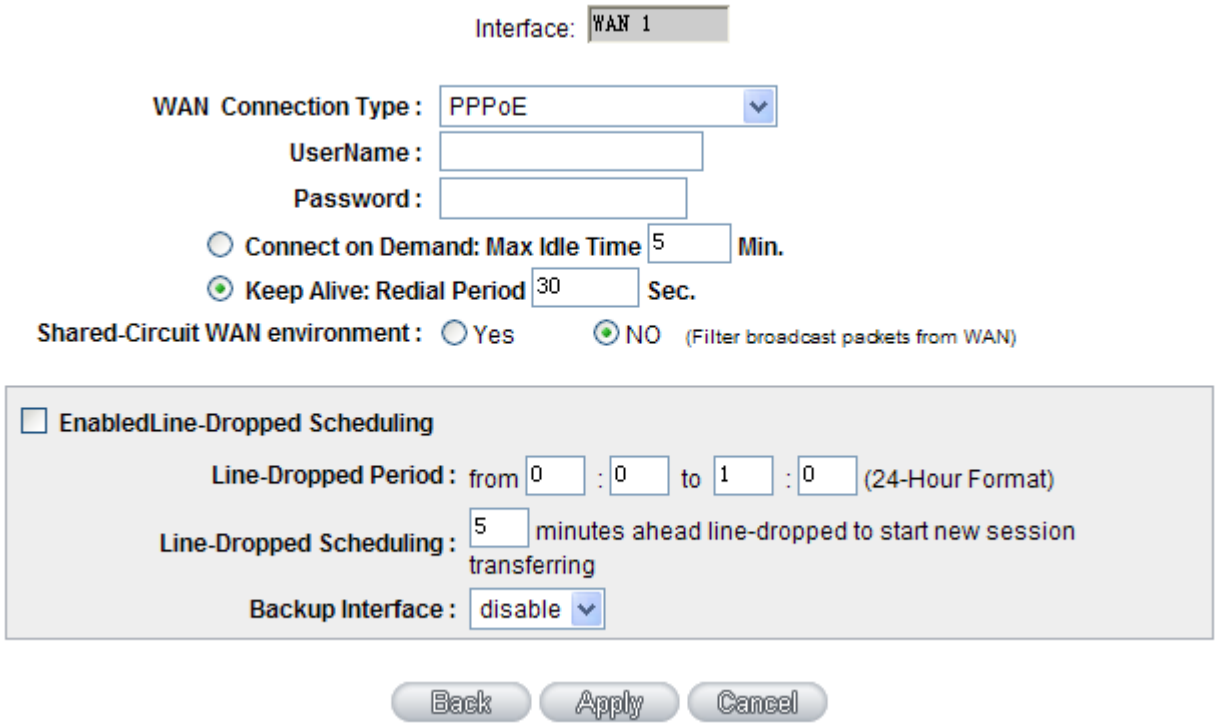
Enable Line-Dropped Scheduling:	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the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

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

PPPoE

This option is for an ADSL virtual dial-up connection (suitable for ADSL PPPoE). Input the user connection name and password issued by ISP. Then use the PPP Over-Ethernet software built into the device to connect with the Internet. If the PC has been installed with the PPPoE

dialing software provided by ISP, remove it. This software will no longer be used for network connection.



User Name: Input the user name issued by ISP.

Password Input the password issued by ISP.

Connect on Demand: This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break-off resulting from no packet transmissions is five minutes).

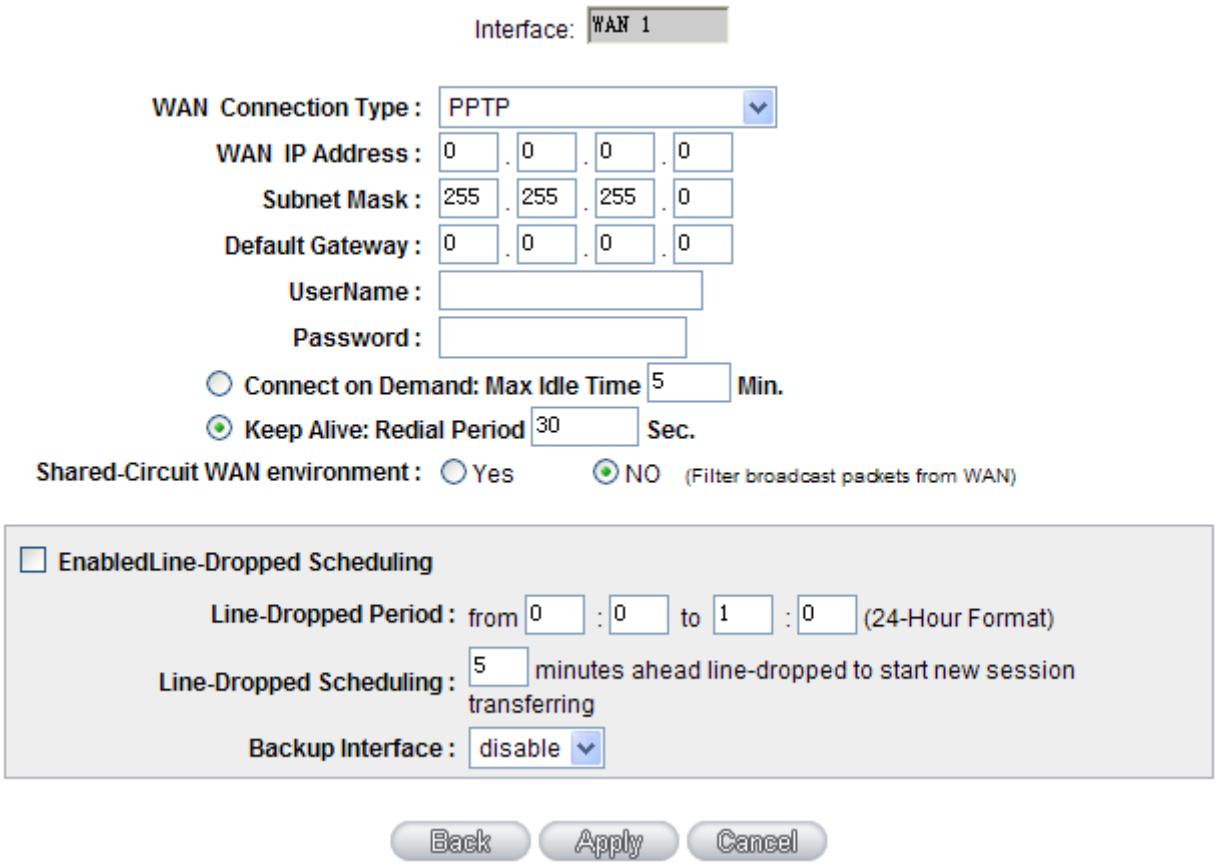
Keep Alive: This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is disconnected. It also enables a user to set up a time for redialing. The default is 30 seconds.

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

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

PPTP

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



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 the disconnection of this WAN service.

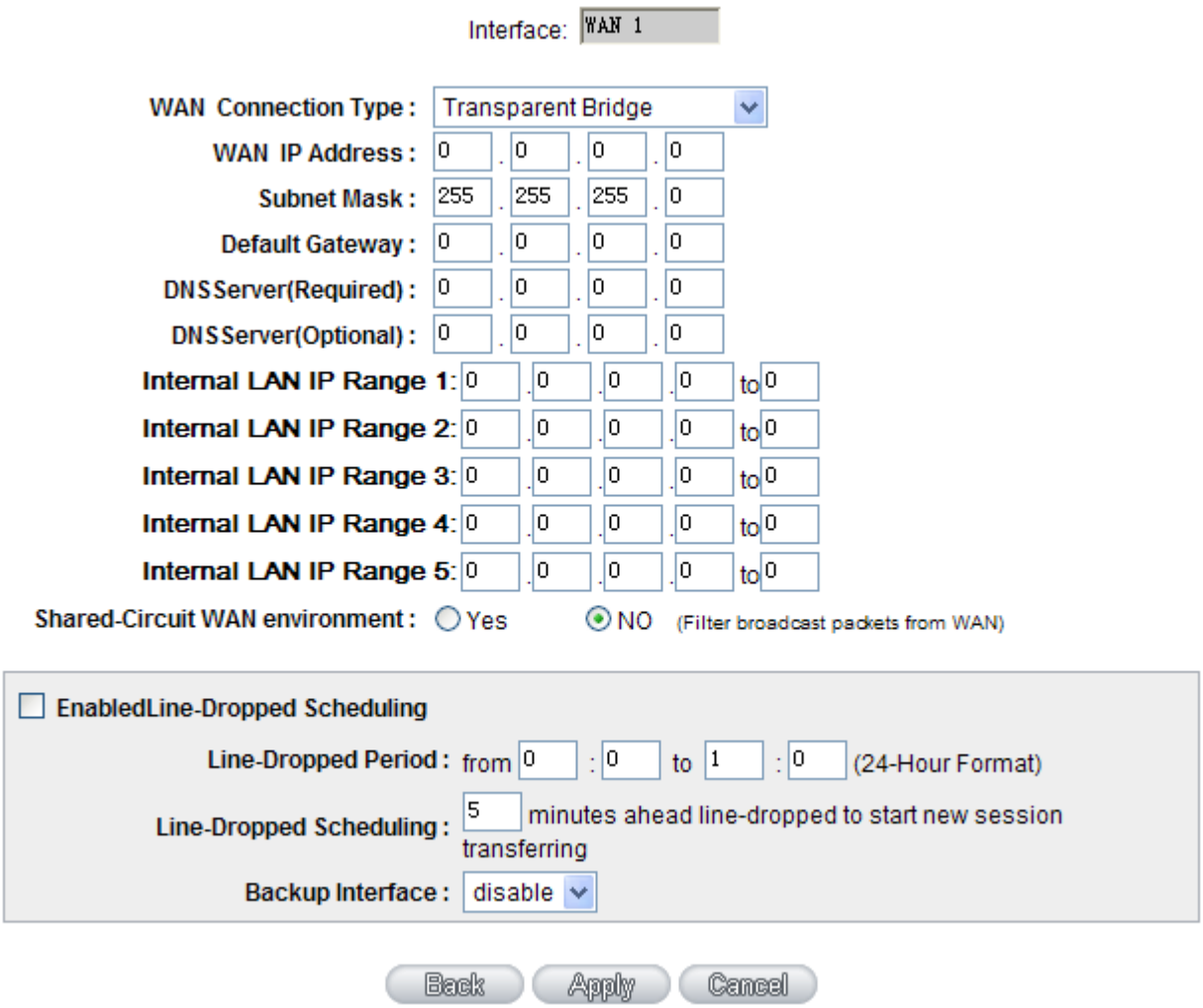
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs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

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

Transparent Bridge

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

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



WAN IP Address:	Input one of the static IP addresses issued by ISP.
Subnet Mask:	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway Address:	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
DNS Server:	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.

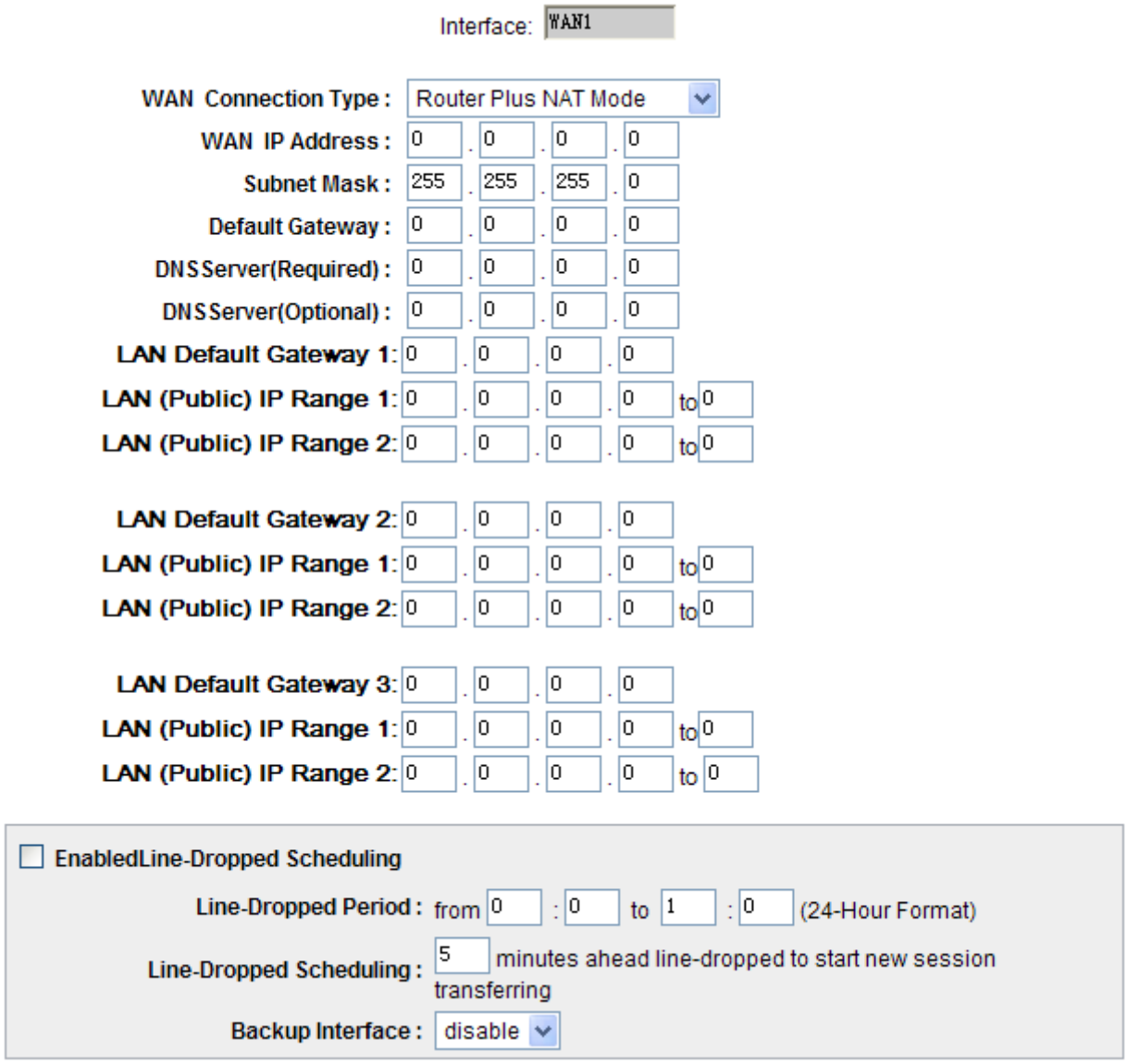
Internal LAN IP Range:	Input the available IP range issued by ISP. If ISP issued two discontinuous IP address ranges, users can input them into **Internal LAN IP Range 1** and **Internal LAN IP Range 2** respectively.
Enable Line-Dropped Scheduling:	The WAN disconnection schedule will be activated by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

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

Router Plus NAT Mode:

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

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



WAN IP address Enter the public IP address.

Subnet mask Enter the public IP address subnet mask.

WAN default gateway Enter the WAN default gateway, which provided by your ISP.

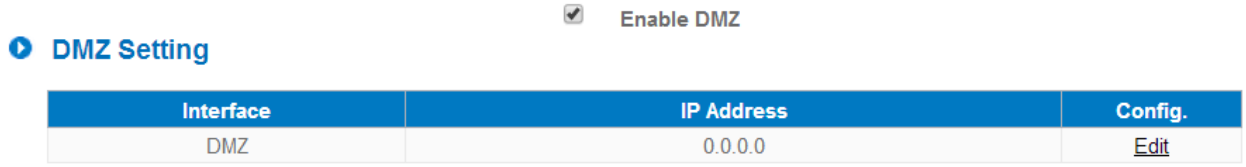
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
Intranet routing default gateway	Enter one of IP addresses that provide by the ISP as your default gateway.
Intranet IP addresses range	Enter your IP addresses range, which IP addresses are provided by ISP. If you have multiple IP ranges, you need setup group1 and group 2. You can also setup the default gateway and IP range in the group 2.
Enable Line-Dropped Scheduling	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of 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.

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

DMZ Setting

For some network environments, an independent Configurable DMZ port may be required

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



IP address: Indicates the current default static IP address.

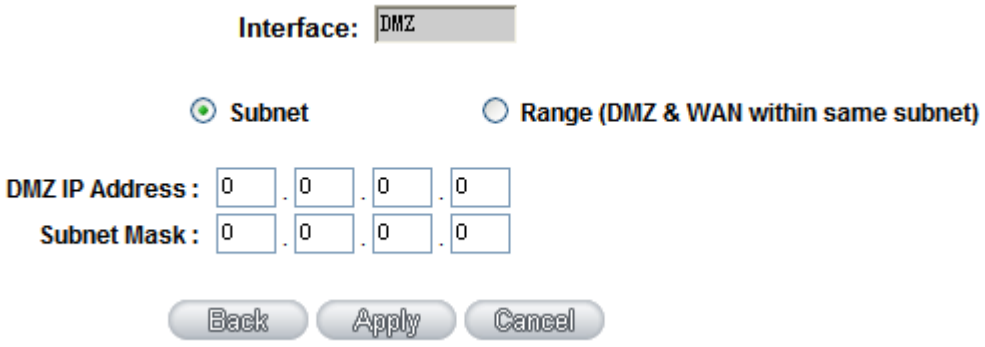
Config.: Indicates an advanced configuration modification: Click **Edit** to enter the advanced configuration page.

The DMZ configuration can be classified by Subnet and Range:

Subnet:

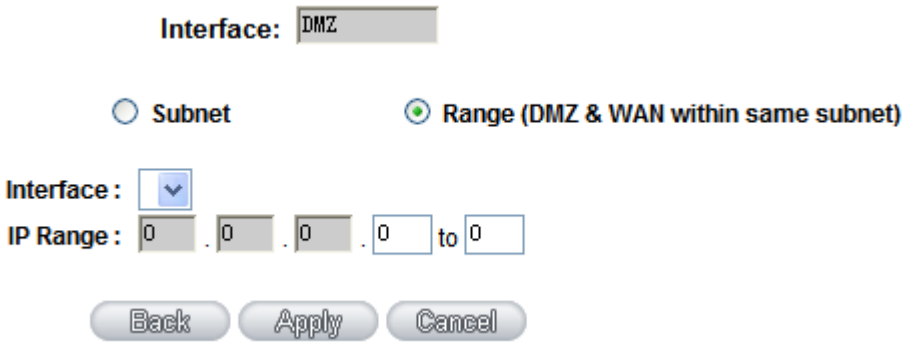
The DMZ and WAN located in different Subnets

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



Range:

DMZ and WAN are within same Subnet

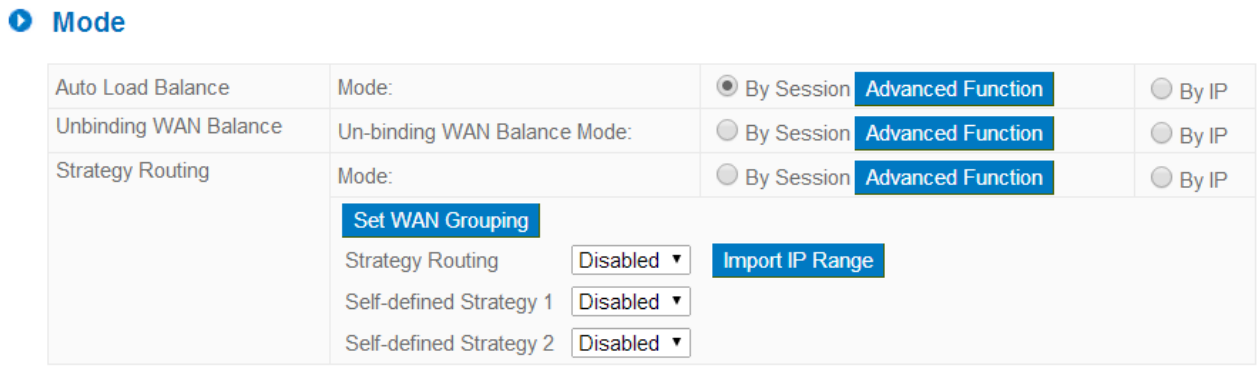


IP Range: Input the IP range located at the DMZ port.

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

6.2 Multi- WAN Setting

6.2.1 Load Balance Mode



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.

Exclusive 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.

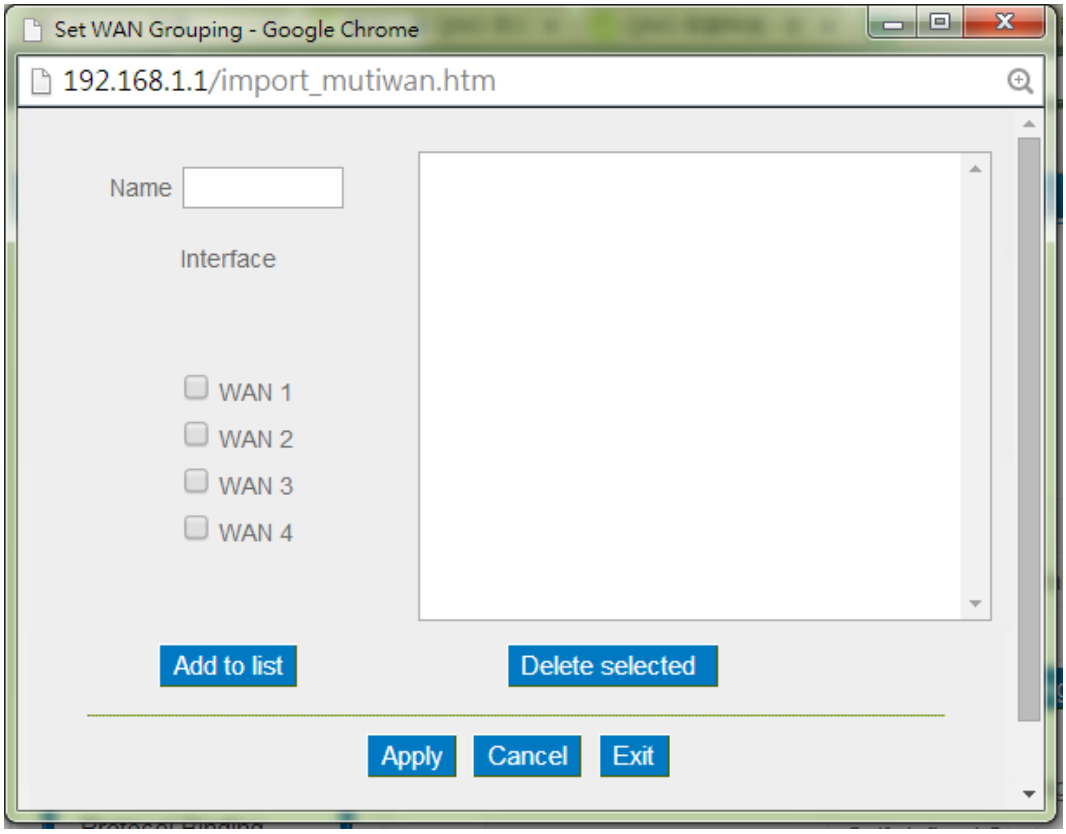
Please refer to the explanations in **6.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding.

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.



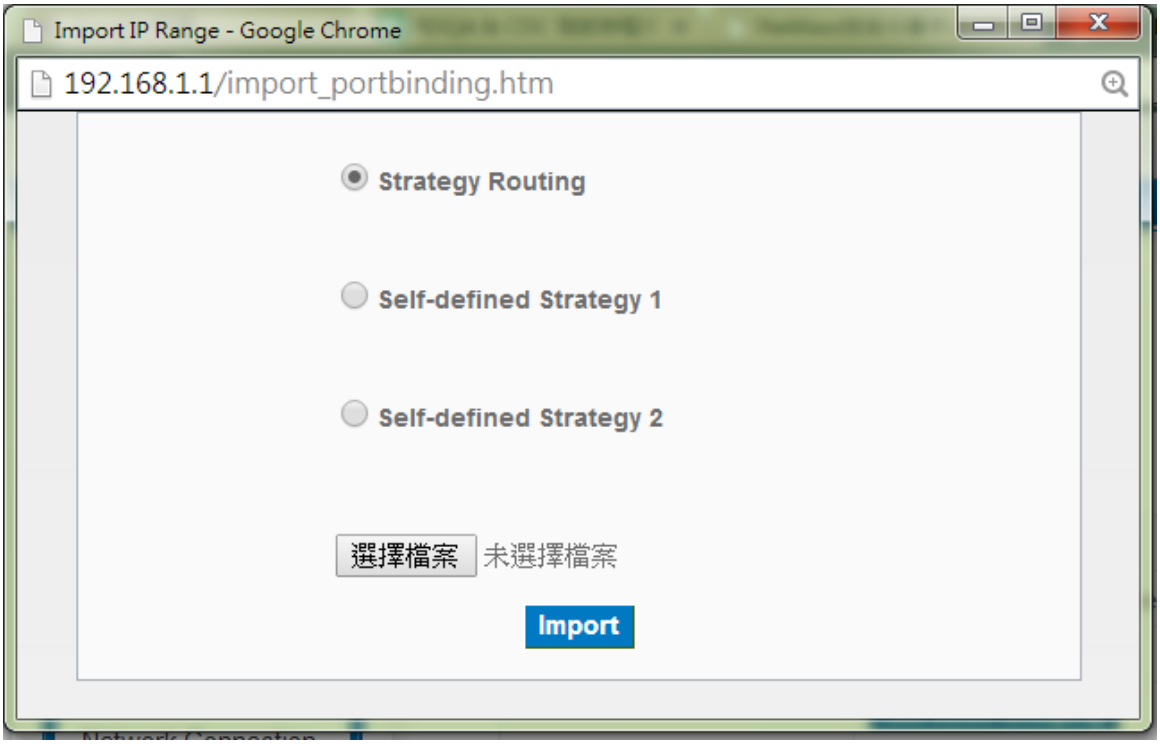
Name:	To define a name for the WAN grouping in the box, such as "Education" etc. The name is for recognizing different WAN groups.
Interface:	Check the boxes for the WANs to be added into this combination.
Add To List:	To add a WAN group to the grouping list.
Delete selected Item:	To remove selected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

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

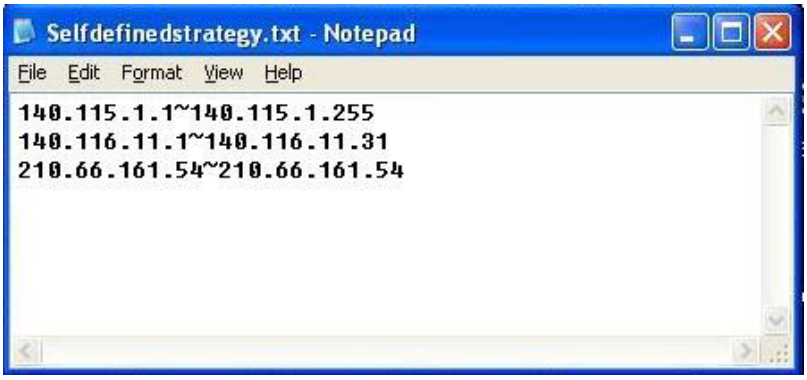
Import Strategy:

A division of traffic policy can be defined by users too. In the "Import Strategy" window,

select the WAN or WAN group (ex. WAN 1) to be assigned and click the “Import IP Range” button; the dialogue box for document importation will be displayed accordingly. A policy document is an editable text document. It may contain a destination IP users designated. After the path for document importation has been selected, click “Import”, and then at the bottom of the configuration window click “Apply”. The device will then dispatch the traffic to the assigned destination IP through the WAN (ex. WAN 1) or WAN grouping users designated to the Internet.



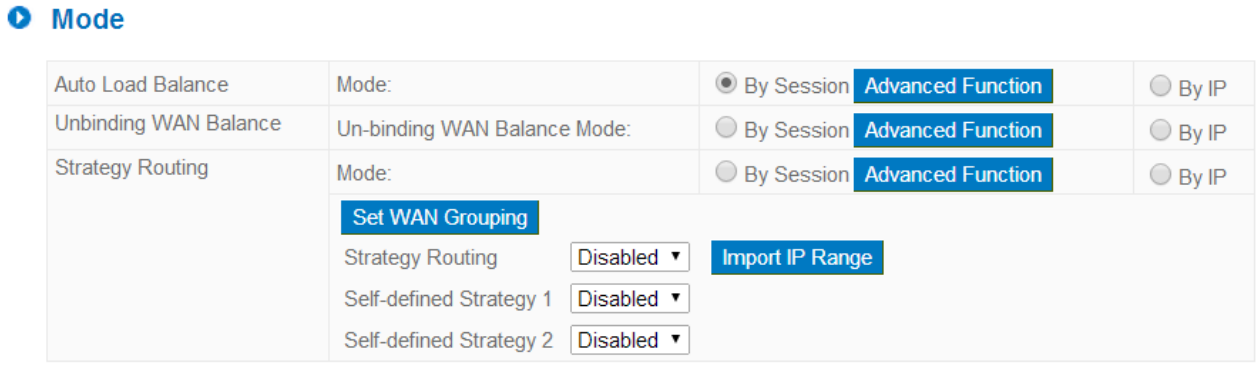
To build a policy document users can use a text-based editor, such as Notepad, which is included with Windows system. Follow the text format in the figure below to key in the destination IP addresses users want to assign. For example, if the destination IP address range users want to designate is 140.115.1.1 ~ 140.115.1.255, key in 140.115.1.1 ~ 140.115.1.255 in Notepad. The next destination IP address range should be keyed in the next line. Attention! Even if only one destination IP address is to be assigned, it should follow the same format. For example, if the destination IP address is 210.66.161.54, it should be keyed in as 210.66.161.54~210.66.161.54. After the document has been saved (the extension file name is .txt), users can import the IP range of self-defined strategy.



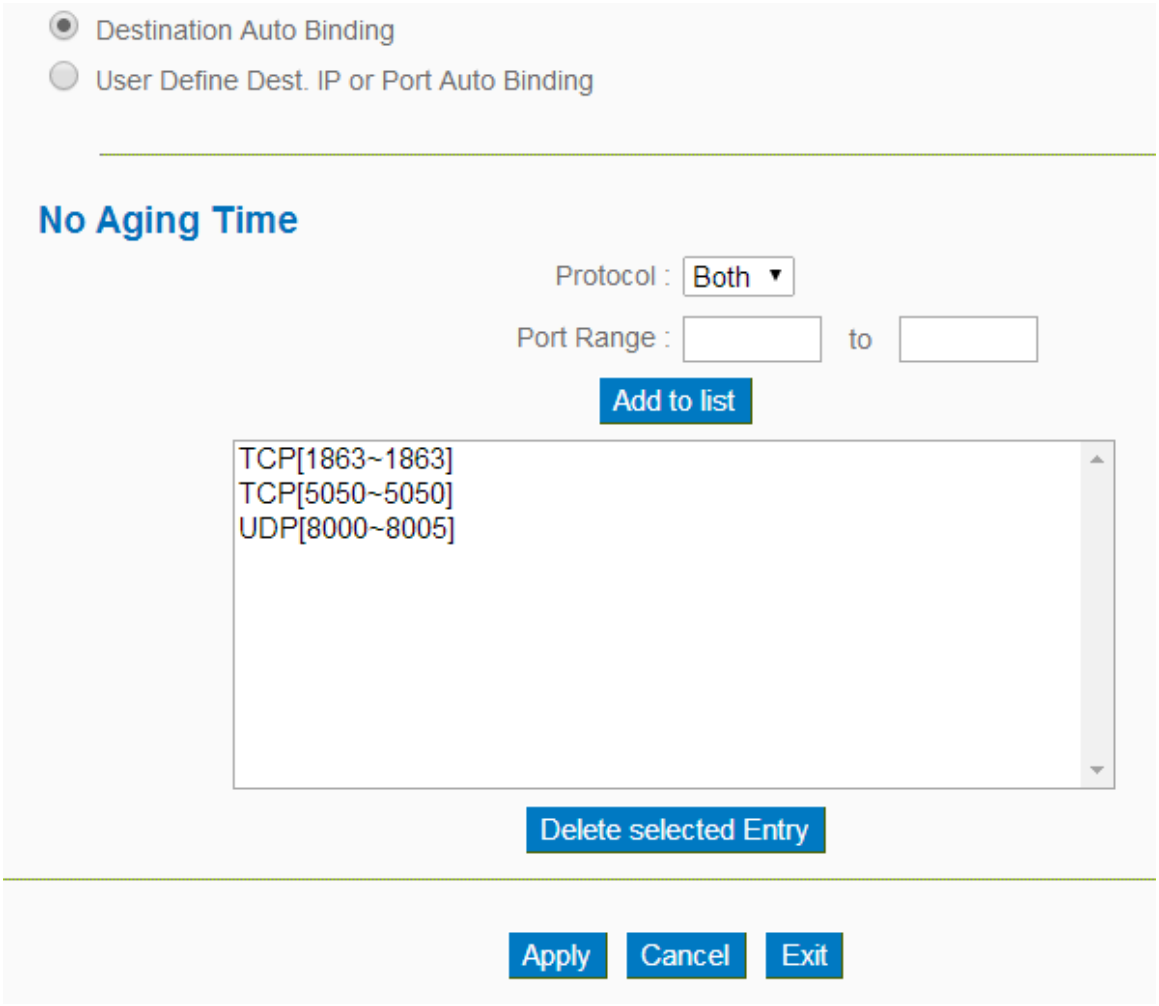
Session Balance Advanced Function

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

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



Click “Advanced Function” to enter the setting window:



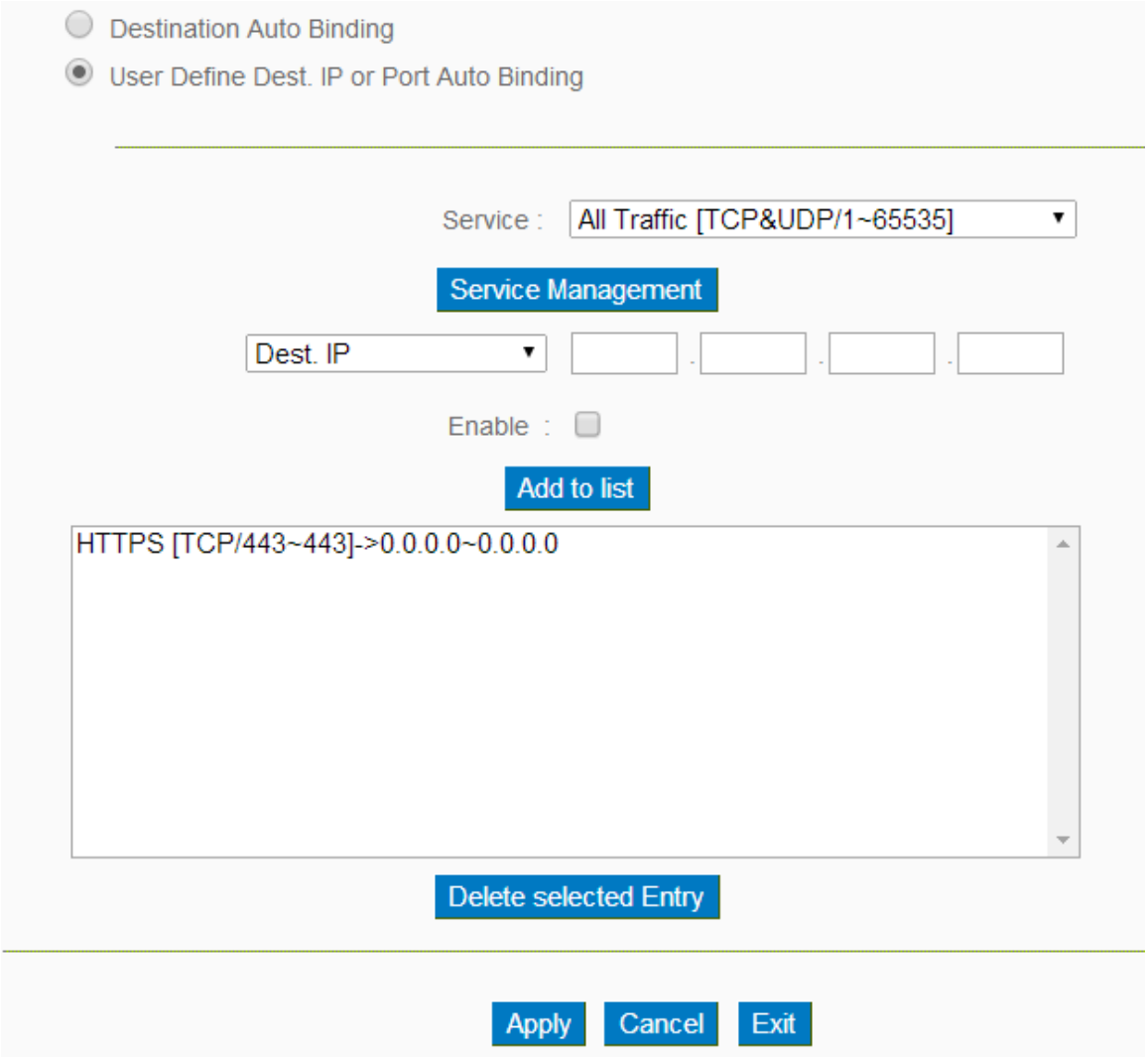
Destination Auto Binding Indicates that the session will be connected with the same WAN IP when the destination IP is in the same Class B range. For example, there are WAN1-1 200.10.10.1 and WAN2- 200.10.10.2, and two intranet IP addresses. When 192.168.1.100 visits Internet 61.222.81.100 for the first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

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

Note!

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

User Define Dis. Or Port Auto Binding	Indicates that the intranet IP will connect through the same WAN IP when the service ports are self- defined. You can self- define the service ports and destination IP. (If the destination IP is set as 0.0.0.0 to 0, this represents that the destination is to any IP range.) **Note!** You can only choose either **Destimation Auto Binding or User Define Dis.** Or **Port Auto Binding**.
Take default rules for example:	



When any intranet IP connects with TCP443 port or any destination (0.0.0.0 to 0 represents any destination), it will go through the same WAN IP. As for which WAN will be selected, this follows the first- chosen WAN IP distributed by the original session balance mechanism. For example, there are two intranet IP- 192.168.100.1 and 192.168.100.2. When these intranet IPs first connects with TCP443 port, 192.168.100.1 will go through WAN1, and 192.168,100.2 will go through WAN2. Afterwards, 192.168.100.1 will go through WAN1 when there are TCP443 port connections. 192.168.100.2 will go through WAN2 when there are TCP443 port connections.

This rule is by default. You can delete or add rules to meet your connection requirement.

6.2.2 Network Detection Service

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

Network Service Detection

	Interface	WAN 1
☑	Enable	
	Retry count	5
	Retry timeout	30 seconds
	When Fail	Remove the Connection
☑	When In OR Out bandwidth is over 1 %, regarded as normal.	
☑	Default Gateway	
☐	ISP Host	
☐	Remote Host	
☐	DNS Lookup Host	

Interface: Select the WAN Port that enables Network Service Detection.

Retry: This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured "Retry Times", it will be judged as "External Connection Disconnected".

Retry Timeout: Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.

When Fail: (1) **Generate the Error Condition in the System Log:** If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections.

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 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.

(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.

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.

Detecting Feedback Servers:

Default Gateway: 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.

ISP Host: 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)

Remote Host: 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).
DNS Lookup Host:	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.

Note !

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

6.2.3 Protocol Binding

WAN Setting:

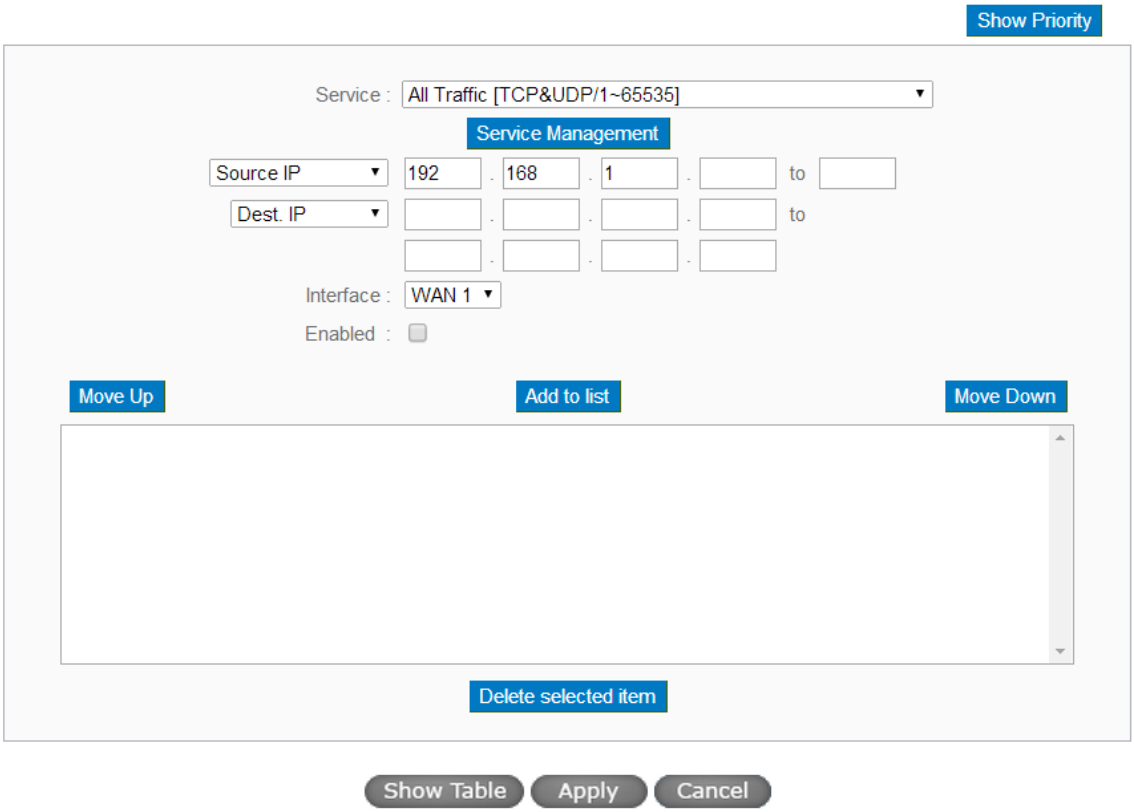
Protocol Binding

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

Note !

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

Protocol Binding



Service: 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.
Option List for Service Management: Click the button to enter the Service Port configuration page to add or remove default

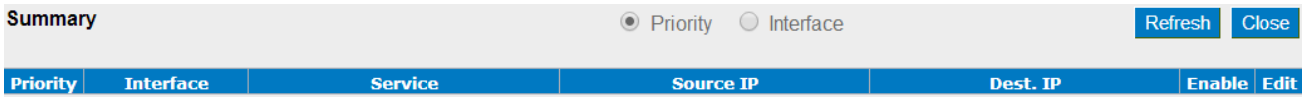
	Service Ports on the option list.
Source IP:	Users can assign packets of specific Intranet virtual IP to go through a specific WAN port for external connection. In the boxes here, input the Intranet virtual IP address range; for example, if 192.168.1.100~150 is input, the binding range will be 100~150. If only specific Service Ports need to be designated, while specific IP designation is not necessary, input "0" in the IP boxes.
Destination IP:	In the boxes, input an external static IP address. For example, if connections to destination IP address 210.11.1.1 are to be restricted to WAN1, the external static IP address 210.1.1.1 ~ 210.1.1.1 should be input. If a range of destinations is to be assigned, input the range such as 210.11.1.1 ~ 210.11.255.254. This means the Class B Network Segment of 210.11.x.x will be restricted to a specific WAN. If only specific Service Ports need to be designated, while a specific IP destination assignment is not required, input "0" into the IP boxes.
Interface:	Select the WAN for which users want to set up the binding rule.
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Delete selected application:	To remove the rules selected from the Service List.
Moving Up & Down:	The priority for rule execution depends on the rule order in the list. A rule located at the top will be executed prior to those located below it. Users can arrange the order according to their priorities.

Note !

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

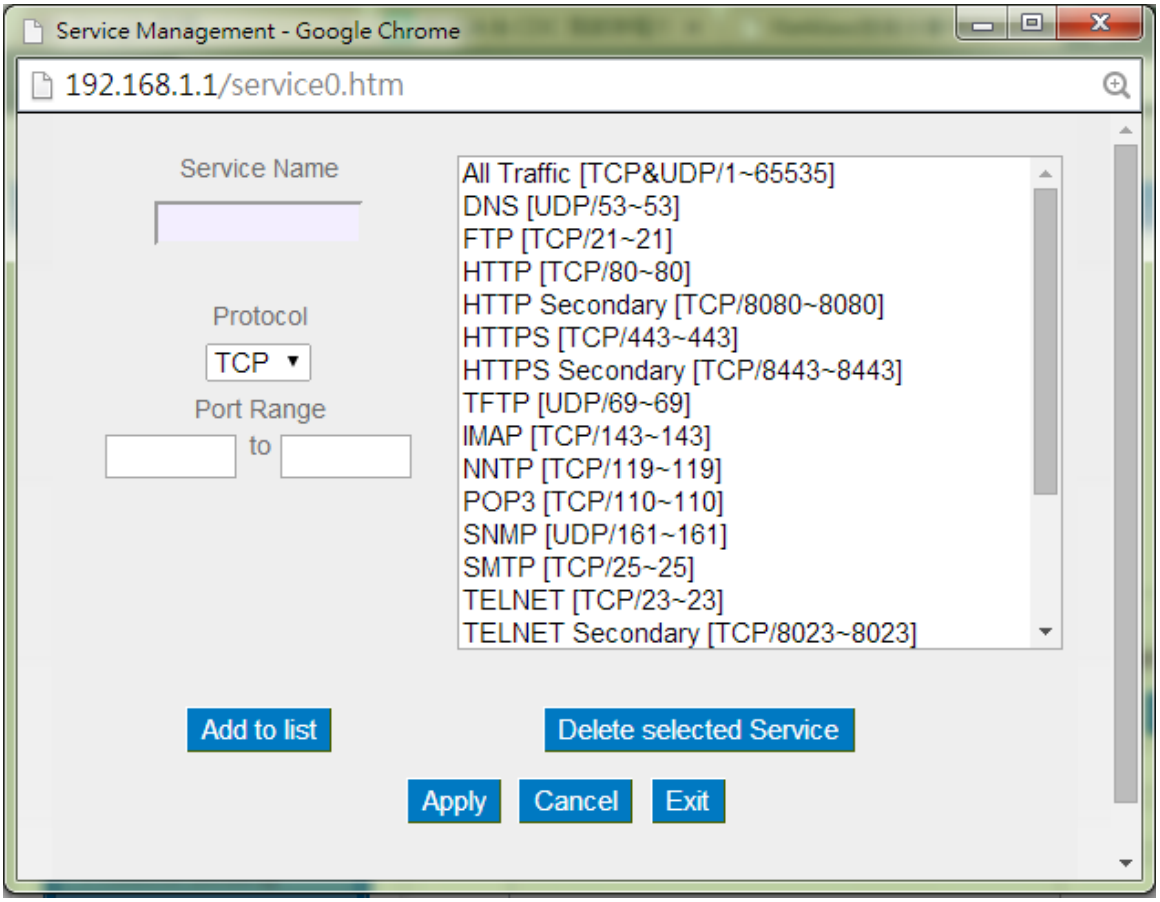
Show Table:

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



Add or Remove Service Port

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



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.

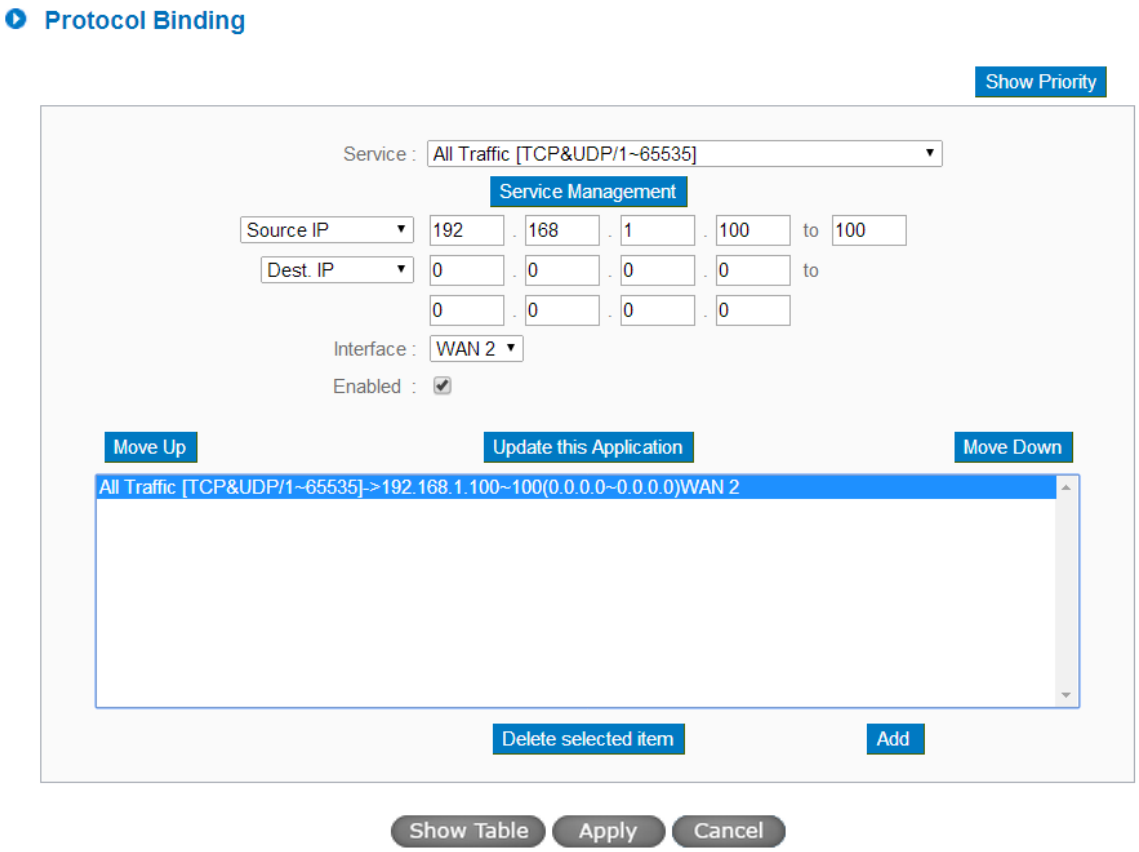
Port range:	In the boxes, input the range of Service Ports users want to add.
Add To List:	Click the button to add the configuration into the Services List. Users can add up to 100 services into the list.
Delete selected service:	To remove the selected activated Services.
Apply:	Click the "**Apply**" button to save the modification.
Cancel:	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.
Close:	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.

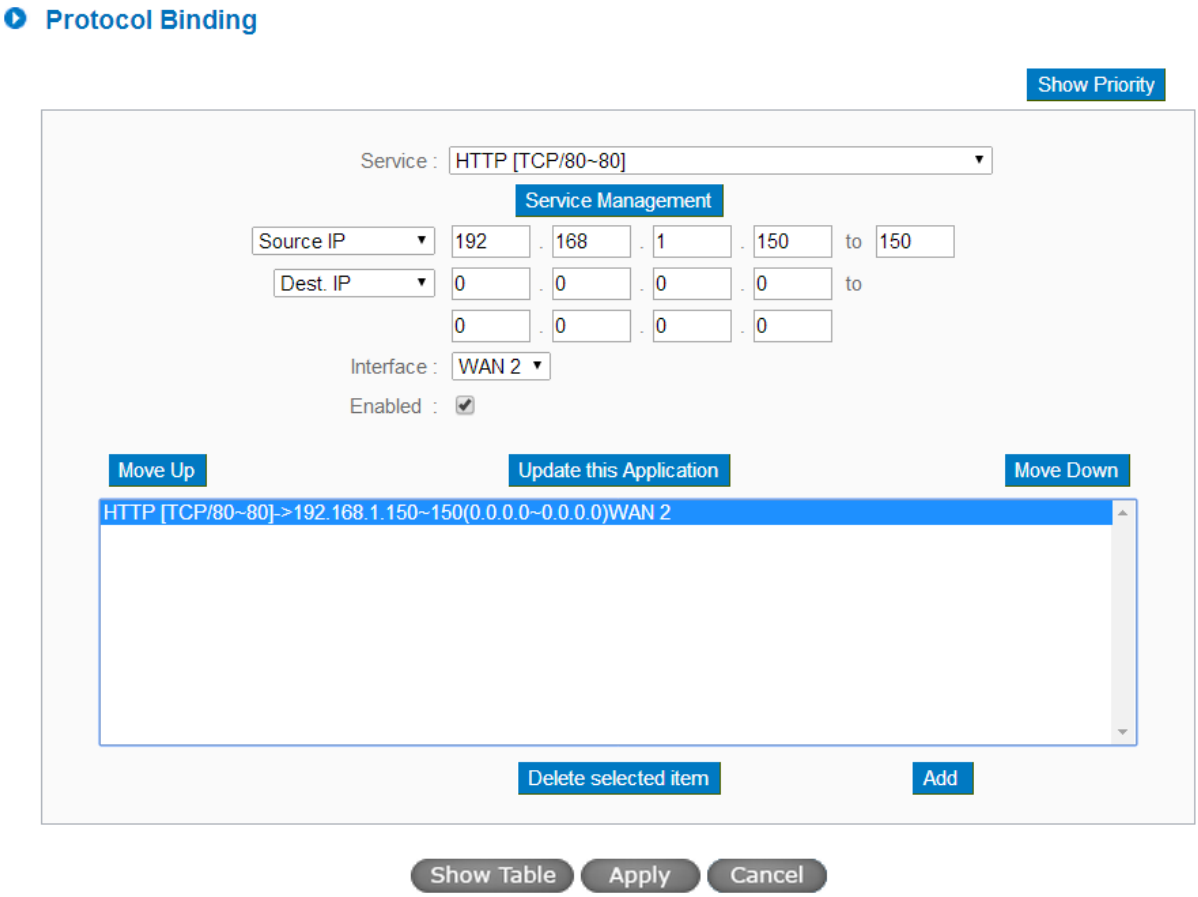
Example 1:How do I set up Auto Load Balance Mode to assign the Intranet IP 192.168.1.100 to WAN2 for the Internet?

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.



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?

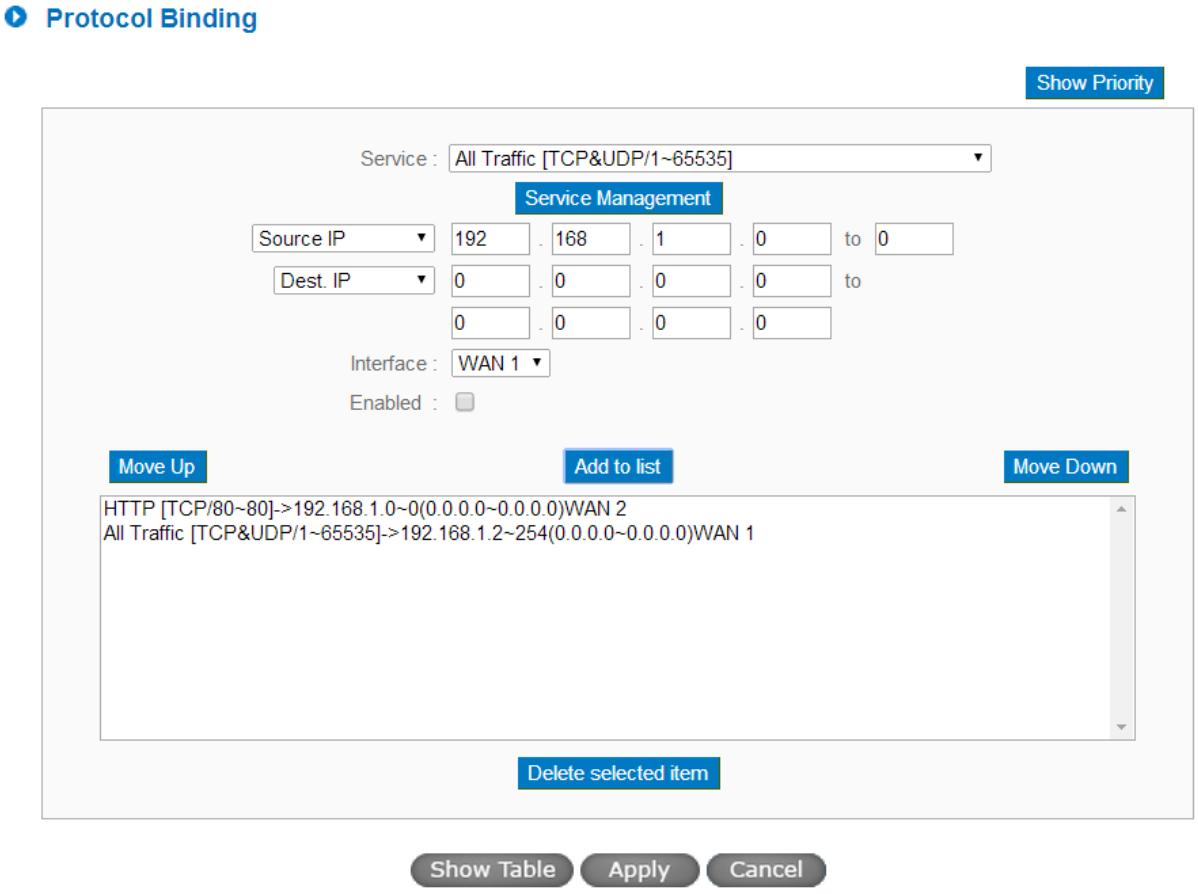
As in the figure below, select "HTTP [TCP/80~80]" from the pull-down option list "Service", and then in the boxes for "Source IP" input "192.168.1.150" to "200". Retain the original numbers "0.0.0.0" in the boxes of "Destination IP" (which means to include all Internet IP addresses). Select WAN2 from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



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.



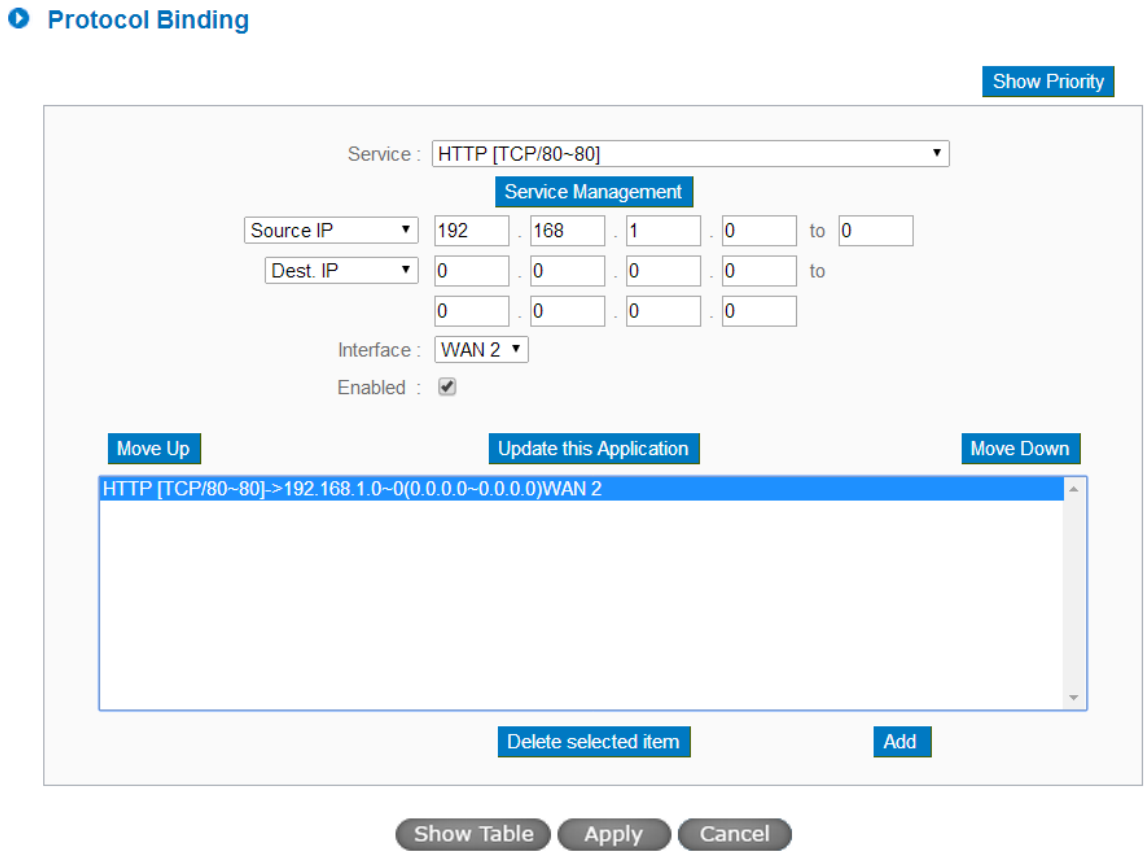
Configuring "Assigned Routing Mode" for load Balance:

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

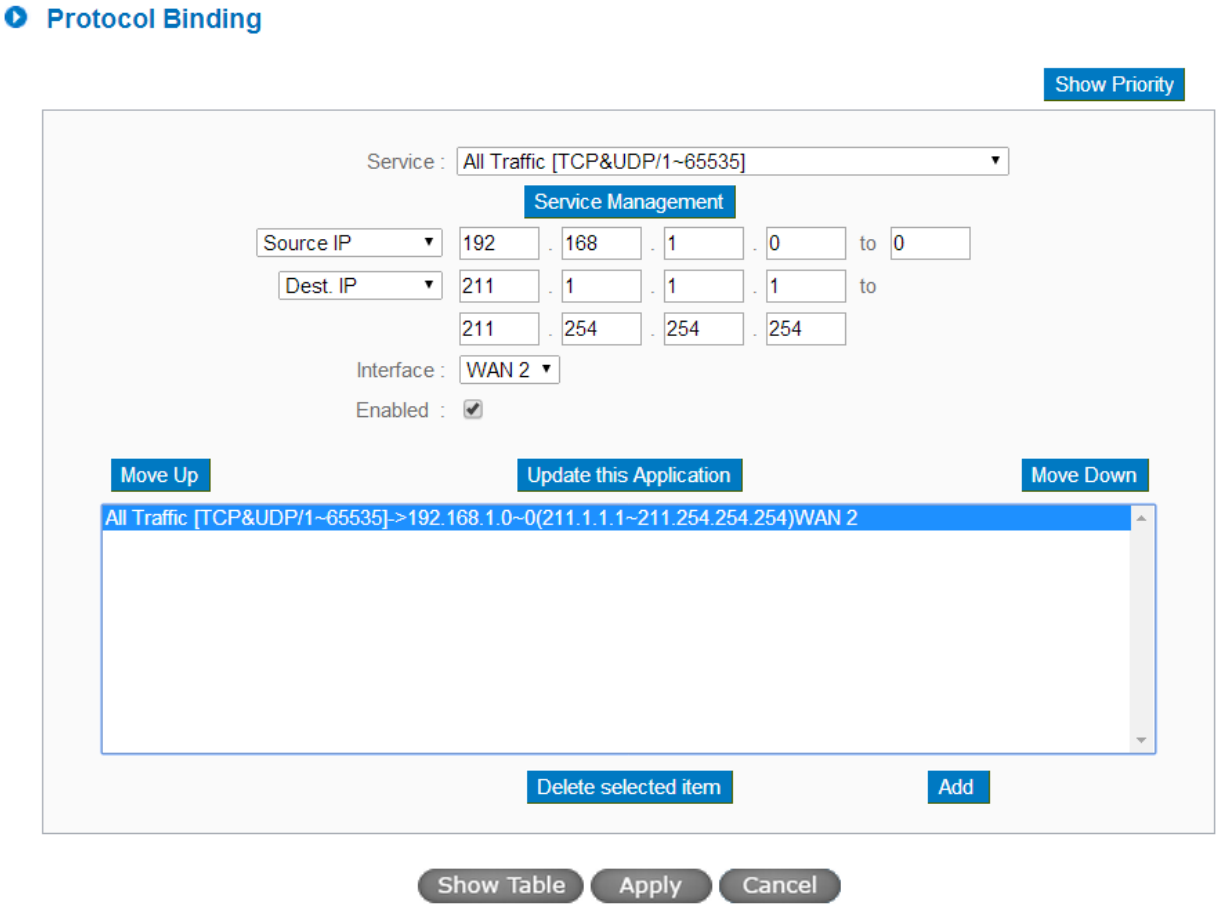
"Service", and then in the boxes of "Source IP" input "192.168.1.0 ~ 0" (which means to include all Intranet IP addresses). Retain the original numbers "0.0.0.0" in the boxes of "Destination IP" (Which means to include all Internet IP addresses). Select WAN2 from the pull-down option list "Interface", 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.



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?

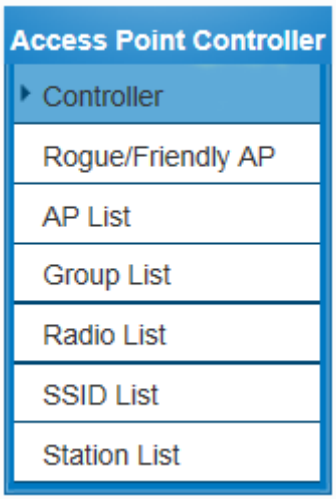
As in the following figure, there are two rules to be configured. The first rule: Select "All Port [TCP&UDP/1~65535]" from the pull-down option list "Service", and then in the boxes of "Source IP" input "192.168.1.0 ~ 0" (which means to include all Intranet IP addresses). In the boxes for "Destination 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.



VII. Access Point Controller (APC)

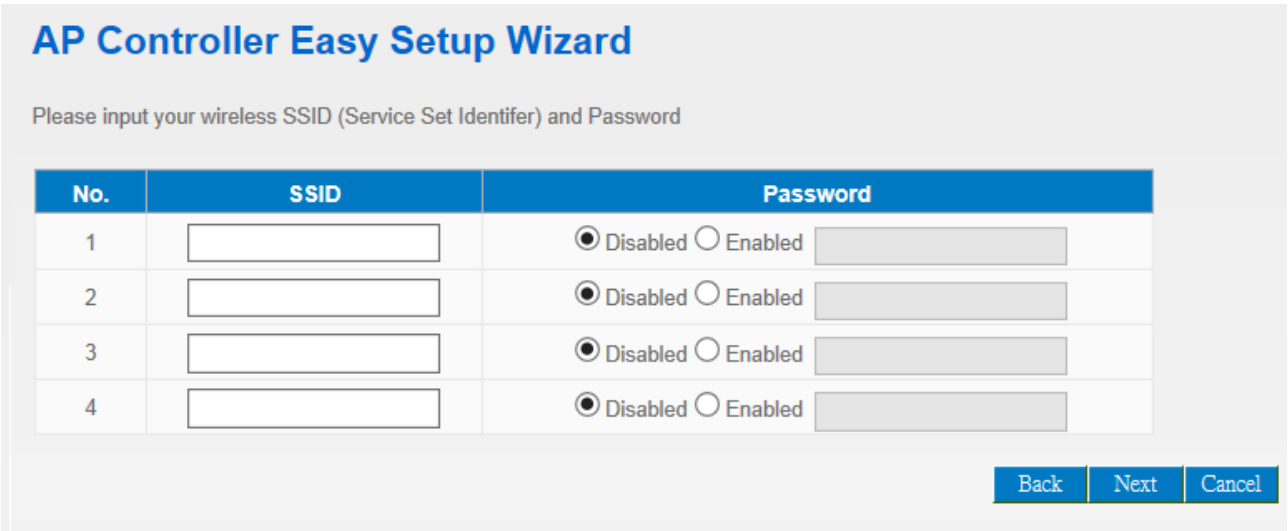
The Access Point Controller (APC) function can simultaneously manage multiple APs through a unified central interface, including modify wireless settings, import configuration files, firmware upgrades and AP restart. We can also monitor the wireless network status through the Web interface as well.



7.1 Easy Setup Wizard

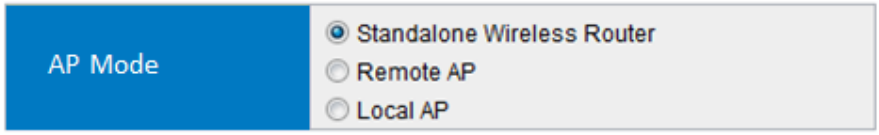
The Easy Setup Wizard in Controller page can help you finish local AP settings through some simple steps.

Follow the steps from the Wizard by entering the SSID and Password you choose

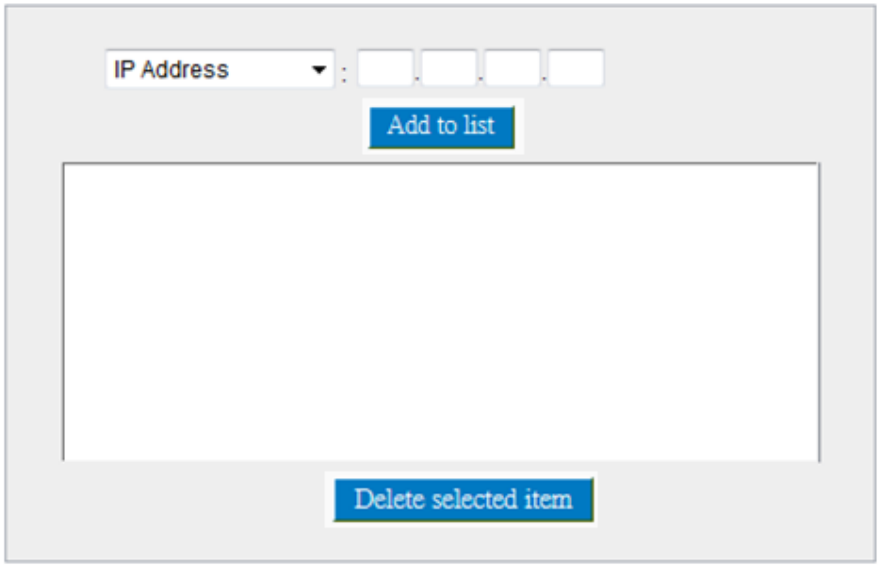


When done, put the AP into Local AP Mode.

AP Mode



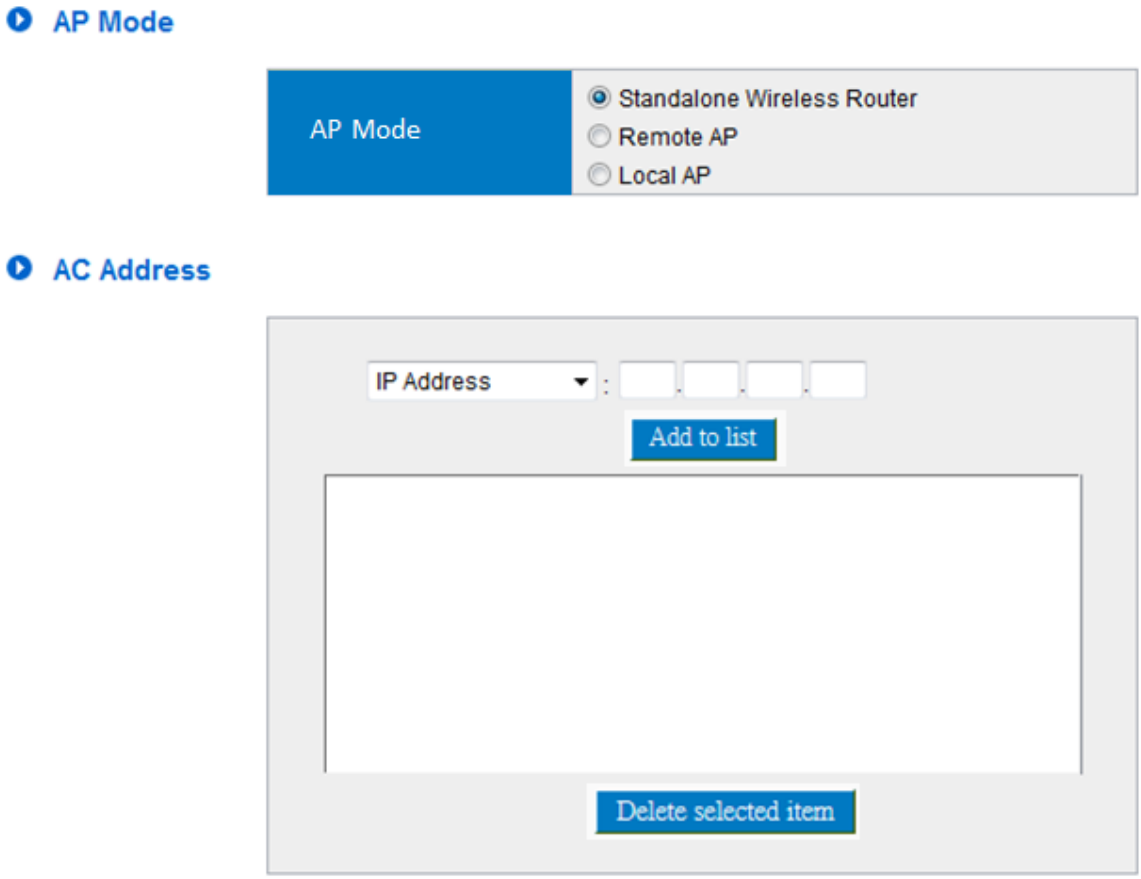
AC Address



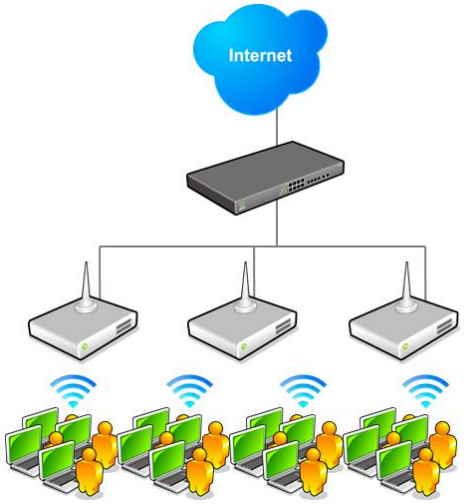
The AP will automatically restart, then connect the LAN port of AP to a LAN port of the APC, and the wireless settings will be configured to the AP.

7.2 Local and Remote AP Modes

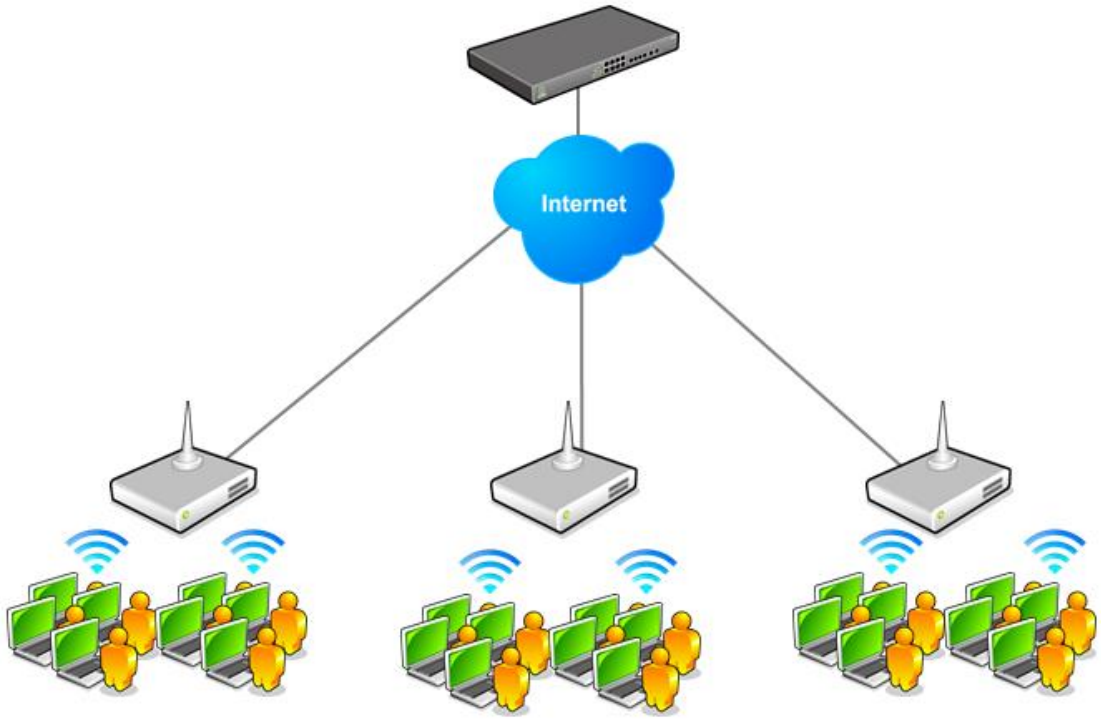
Some AP can be configured as Local AP or Remote AP. The AP will automatically restart after changing Modes.



Under Local AP Mode, the AP is connected to one of the APC's LAN ports. While in this mode, the NAT will not be functional, and the UI will only allow the changing of the AP modes



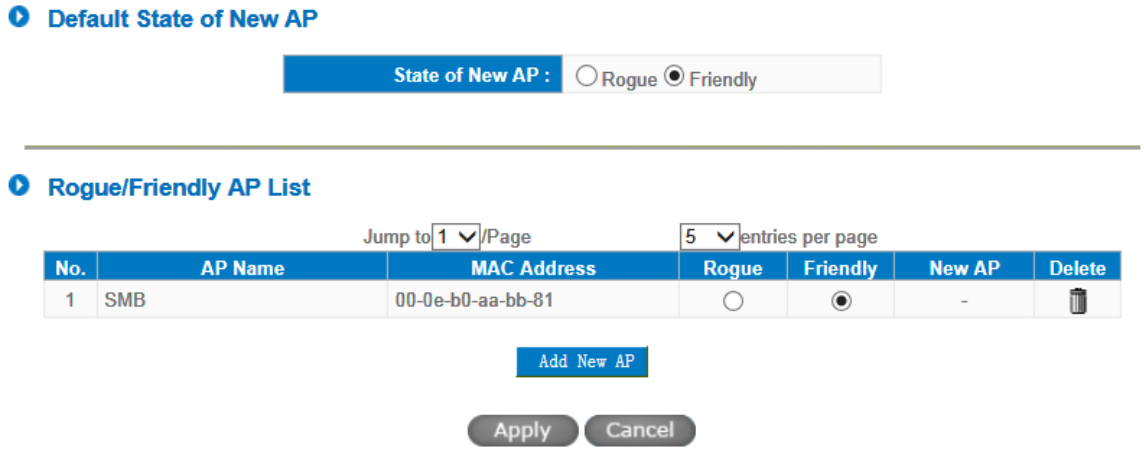
Under Remote AP Mode, the NAT feature will still be operational in translating IPs. While in this mode, the AP and its UI, is functionally the same as a standalone AP, the only difference being the configurations and modifications of setting are done through the APC. When configuring the AP to Remote AP Mode, the IP Address of the APC must be entered.



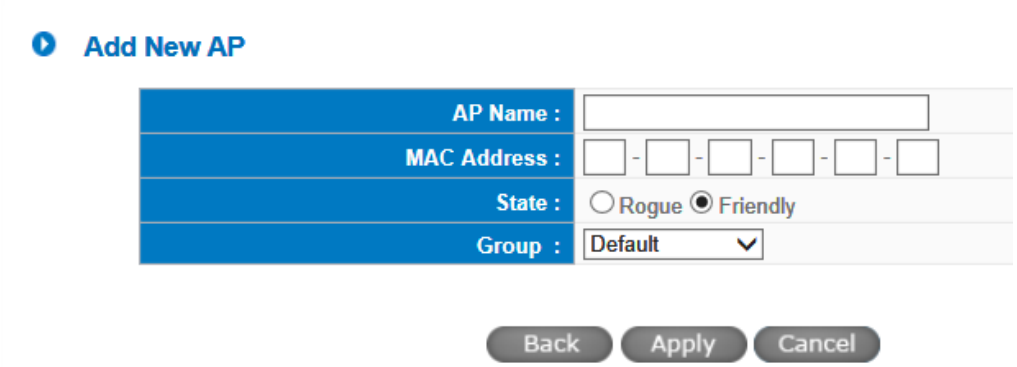
Please reference the AP User's Manual for other settings related to Remote AP Mode.

Rogue/Friendly AP

Here, settings for new AP connections to be a considered as either Rogue or Friendly AP can be configured. The AP will search then attempt to connect with the Controller. If the Controller is set to Friendly then a connection will be established and basic settings will be applied to the AP. However, if the Controller is set Rogue, then no further action will be carried out.

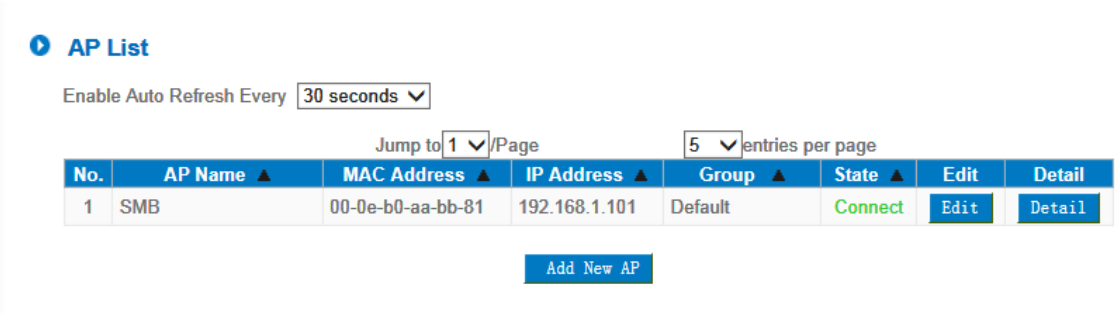


New APs can also be added manually through the AP's MAC Address by clicking the Add New AP button.



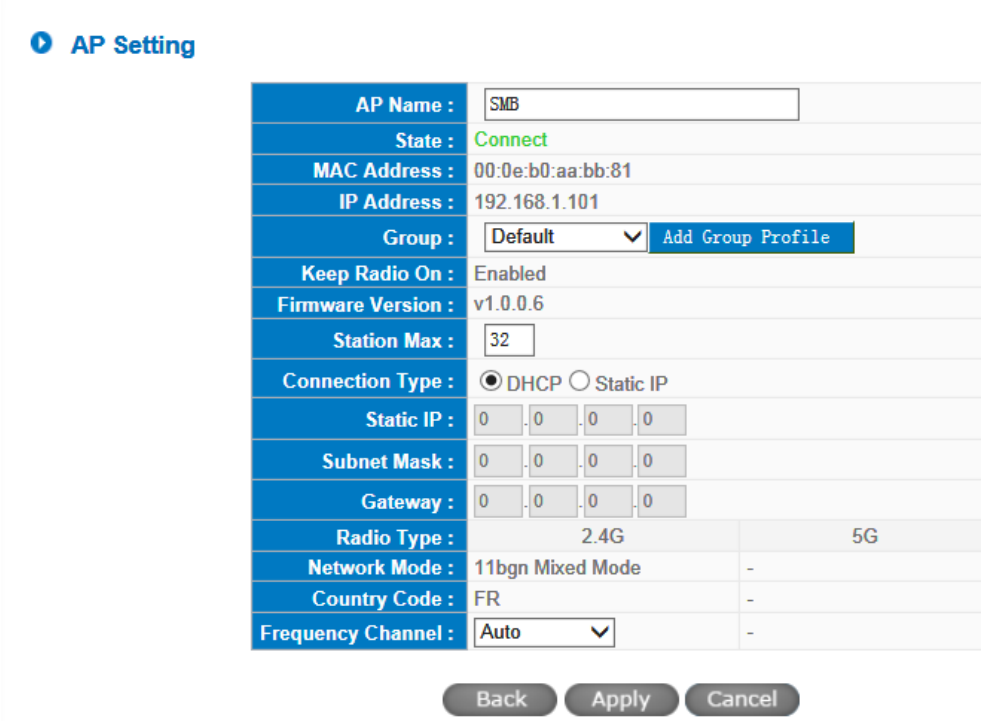
AP List

This List shows the connected APs' MAC/IP Address, Group association and Status. As well as changing a specific AP's settings.

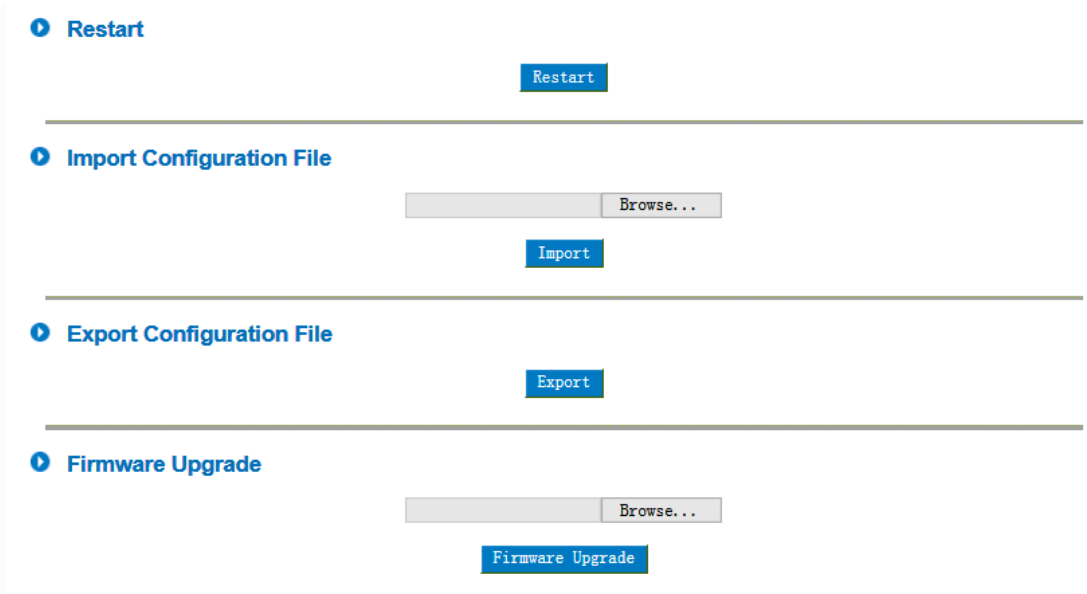


Note: Enabling Auto Refresh here will refresh the page automatically every selected time period. The options for Auto Refresh are: Disabled, 30 seconds, 1 minute and 5 minutes.

A specific AP's settings can also be changed by using the Edit button.

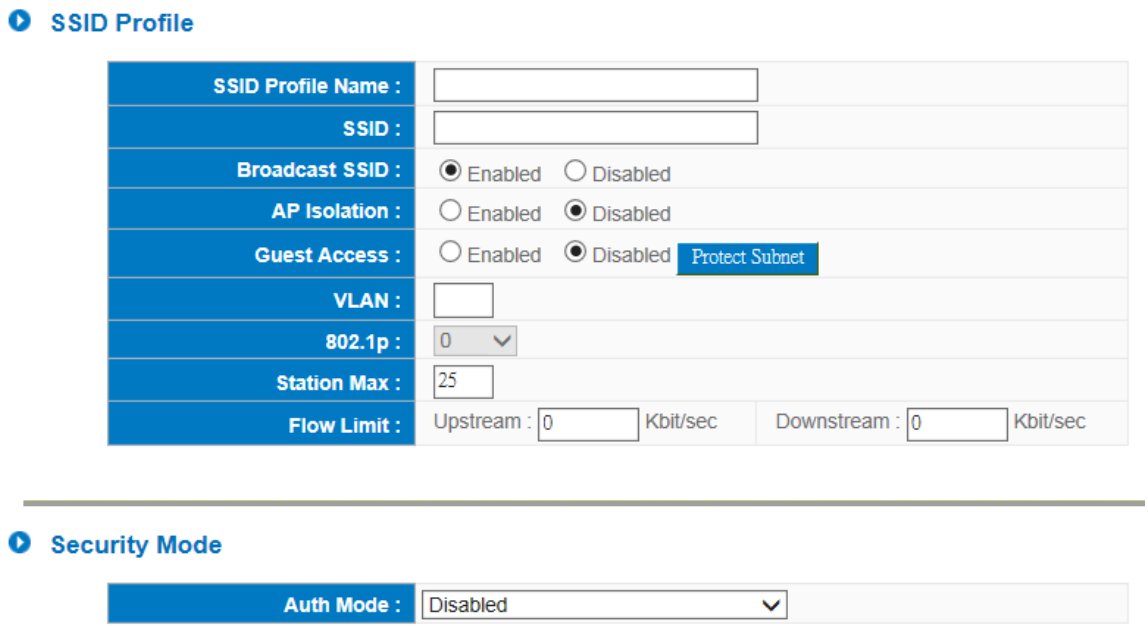


Config file Import/Export, AP Restart and Firmware Upgrade can be done here also.

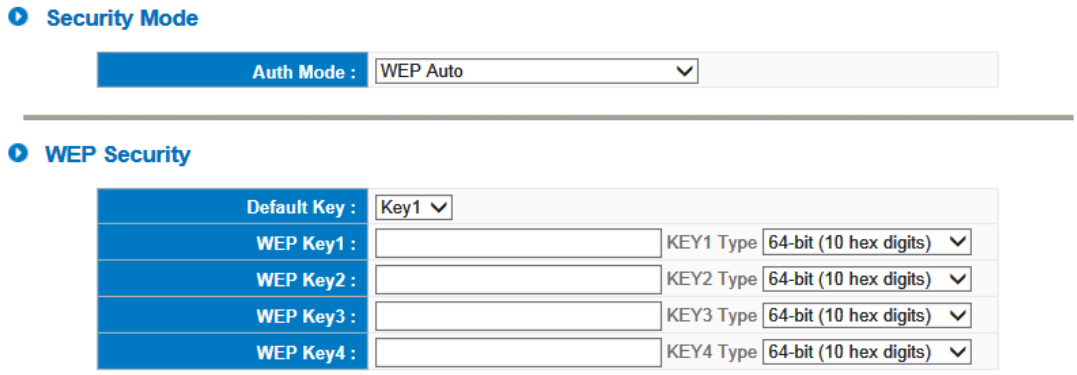


7.3 Adding a SSID List

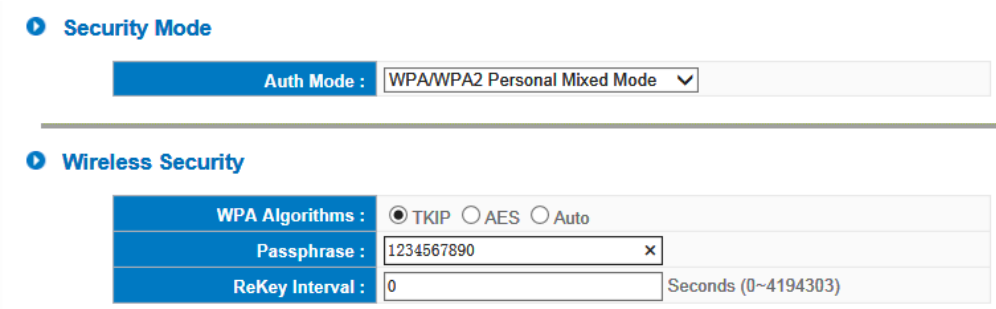
SSID Profile settings page



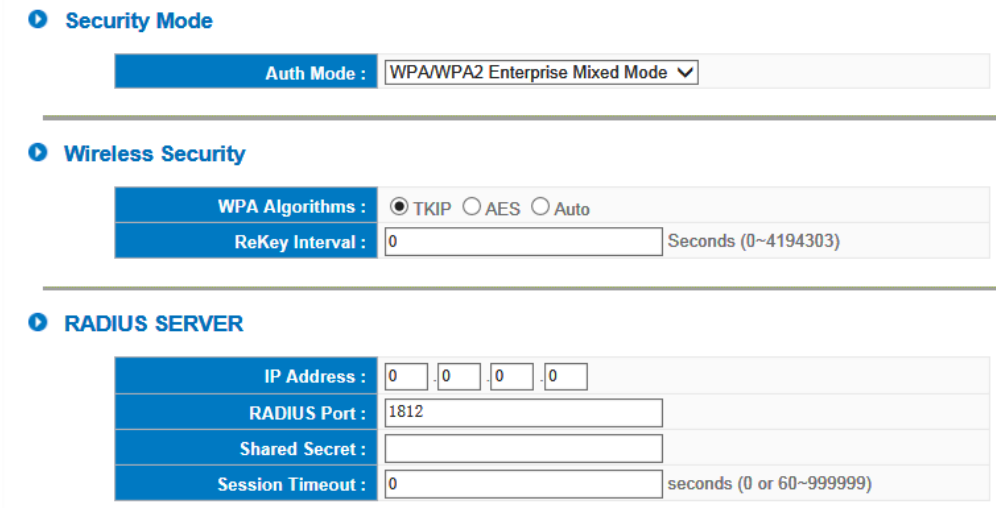
- **SSID Profile Name**
- **SSID Name**
- **Broadcast SSID:** if enabled, the SSID name will be broadcasted to all clients. When Broadcast SSID is disabled, clients will have to manually enter SSID name to connect to this network.
- **AP Isolation:** when enabled, any wireless clients of this SSID will not be able to see other wireless clients, ***but can still connect to LAN clients or resources.***
- **Guest Access:** when enabled, any wireless client of this SSID can *only* connect to the Internet. ***Note: to effectively block wireless clients from accessing internal network PCs/resources, Protect Subnet must be used and the internal network IP range also entered.***
- **VLAN:** the 802.1q VLAN Tag ID of this SSID.
- **802.1p:** the 802.1p value of this SSID.
- **Station Max:** the maximum number of clients that can connect to this SSID on this device.
- **Flow Limit:** the upload and download limits of this SSID's clients.
- **Security Mode:** the authentication and encryption methods of this SSID.
  - **Disabled:** does not require users to enter a password when connecting to SSID.
  - **Open WEP, Shared WEP or WEP Auto:** uses WEP to authenticat users. 64-bit or 128-bit keys can be selected, along with either ASCII or HEX digits.



- **WPA, WPA2 and WPA/WPA2 Personal:** uses WPA to authenticate users and either TKIP or AES algorithms must be chosen. Personal authentications require an 8-63 characters Passphrase.

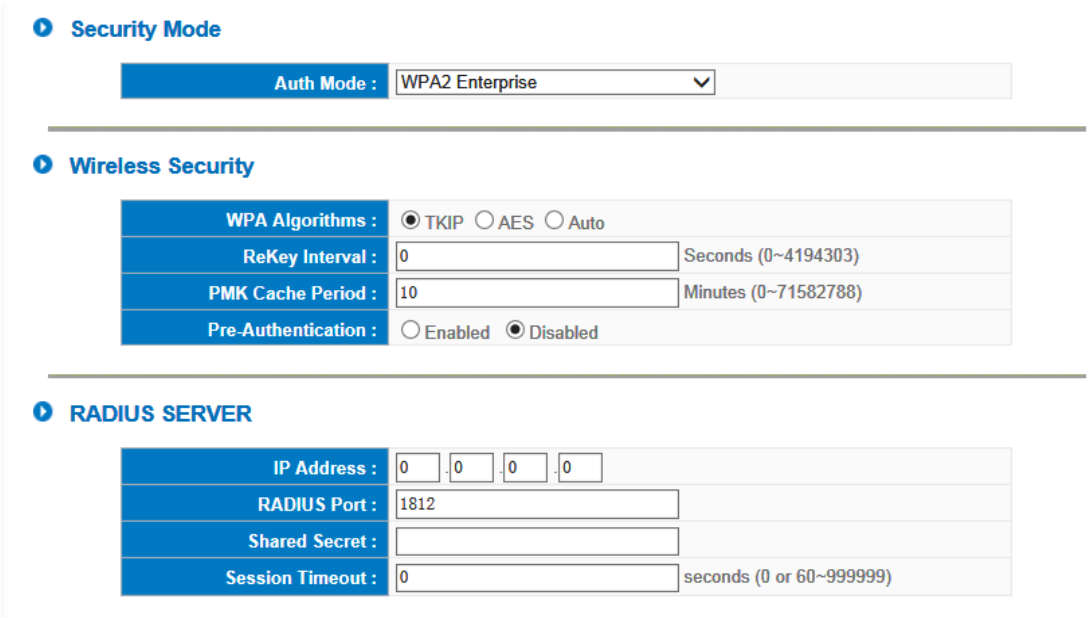


- **WPA, WPA2 and WPA/WPA2 Enterprise:** along with either TKIP or AES algorithms, Enterprise also requires a RADIUS server with additional settings, such as, IP Address and Port number of the RADIUS server, Shared Secret and Session Timeout.

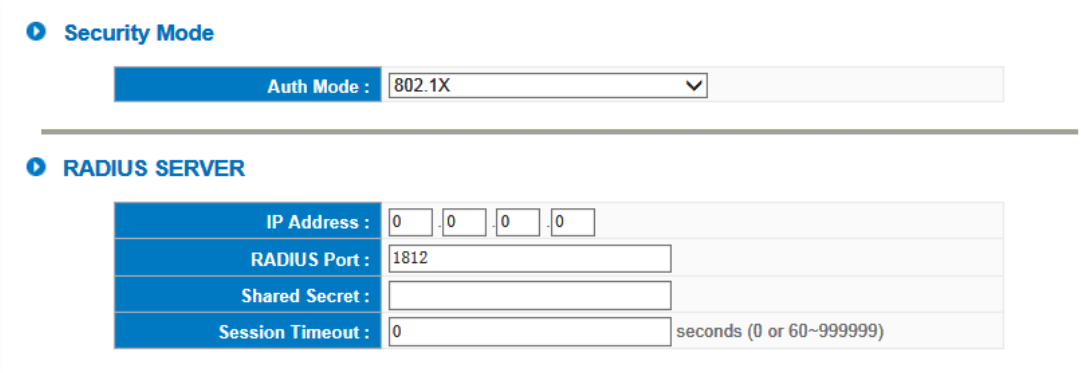


When WPA2 Enterprise is being used, PMK Cache Period and Pre-Authentication can be set and enabled which will speed up the switching time of roaming between Wi-Fi connections

for users.

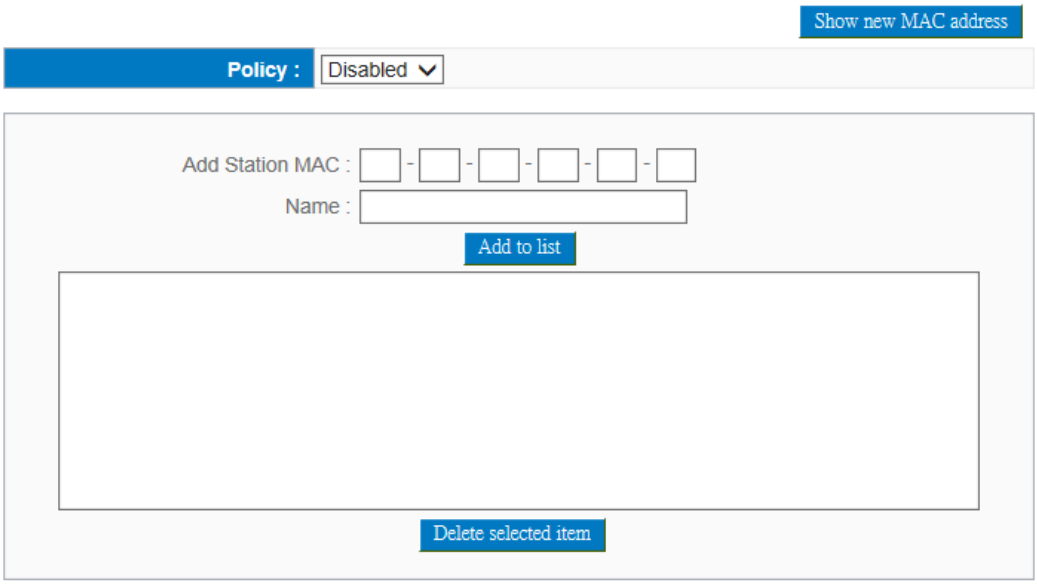


- **802.1X:** 802.1X authentication method will be used. Just like Enterprise mode, a RADIUS server with additional settings, such as, IP Address and Port number of the RADIUS server, Shared Secret and Session Timeout are required.

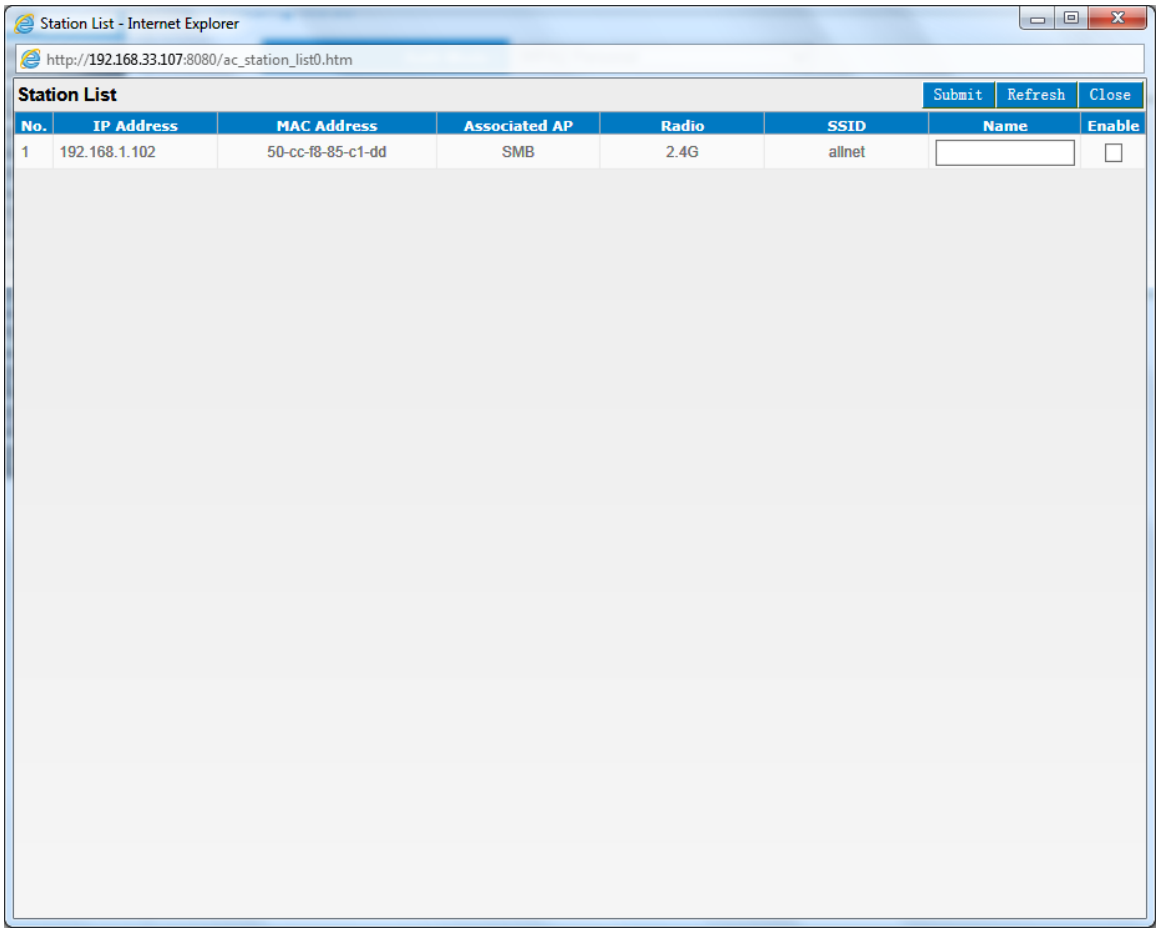


- **Access Filter:** black list or white list settings for this SSID.

Access Filter

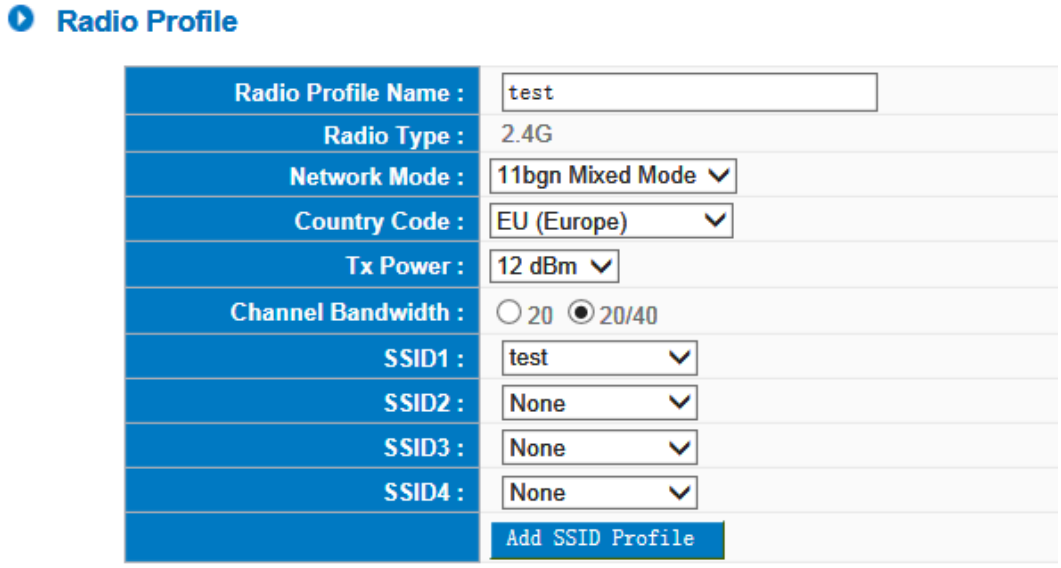


- **Show new MAC Address:** displays a list of connected clients, from here a particular device can be added to the Access Filter by entering a Name, placing a check under Enable then Submit.



7.4 Adding a Radio List

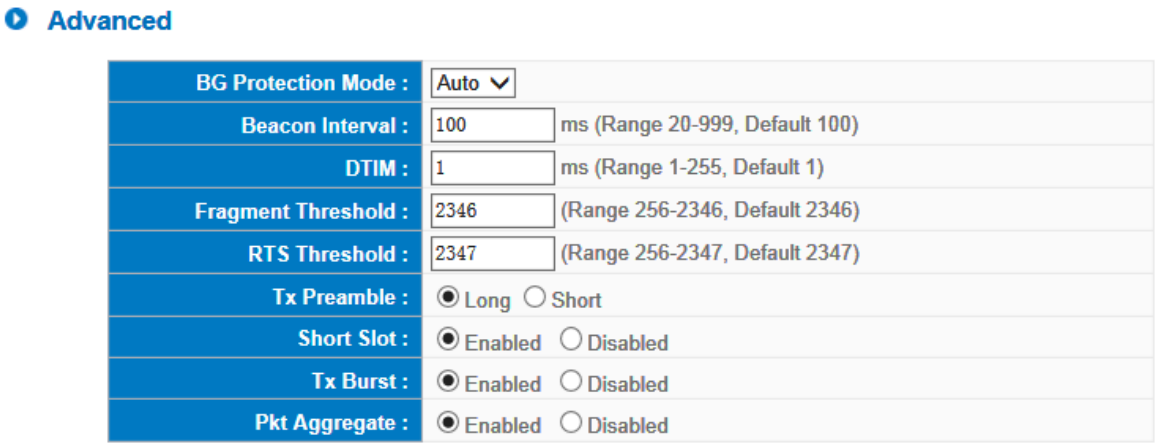
Radio Profile settings page:



- Radio Profile Name
- Radio Type
- Network Mode: choose between the different 802.11 modes.
- Country Code: choose your country or the same country that uses the same wireless channels, some wireless channels are not availiable in certain countries.
- Tx Power
- Channel Bandwidth: this is available only when a Network Mode with 802.11n is selected. You can choose whether to use the 20MHz channel only or both 20/40MHz (auto switching) channels.
- SSID 1~4: choose the SSID that should be used by this Radio Profile.
- **Advanced**

Note: Advanced settings can easily affect your Wi-Fi's stability; do not change any settings if you are unsure of its effects!

- **BG Protection Mode:** in a network environment where 802.11b and 802.11g are both used at the same time, enabling this feature can increase the stablility of the wireless signal.
- **Beacon Interval:** change the transmission beacon interval time
- **DTIM:** change the Delivery Traffic Indication Map time
- **Fragment Threshold:** setting for the Fragment Threshold size value
- **RTS Threshold:** setting for the RTS Threshold size value
- **Tx Preamble:** setting for Tx Preamble signal length
- **Short Slot:** enable or disable whether when collision occurs to use a shorter waiting time
- **Tx Burst:** enable to disable the transmission rate enhancement feature
- **Pkt Aggregate:** enable or disable packet aggregation feature



- **WiFi Multimedia (WMM)**

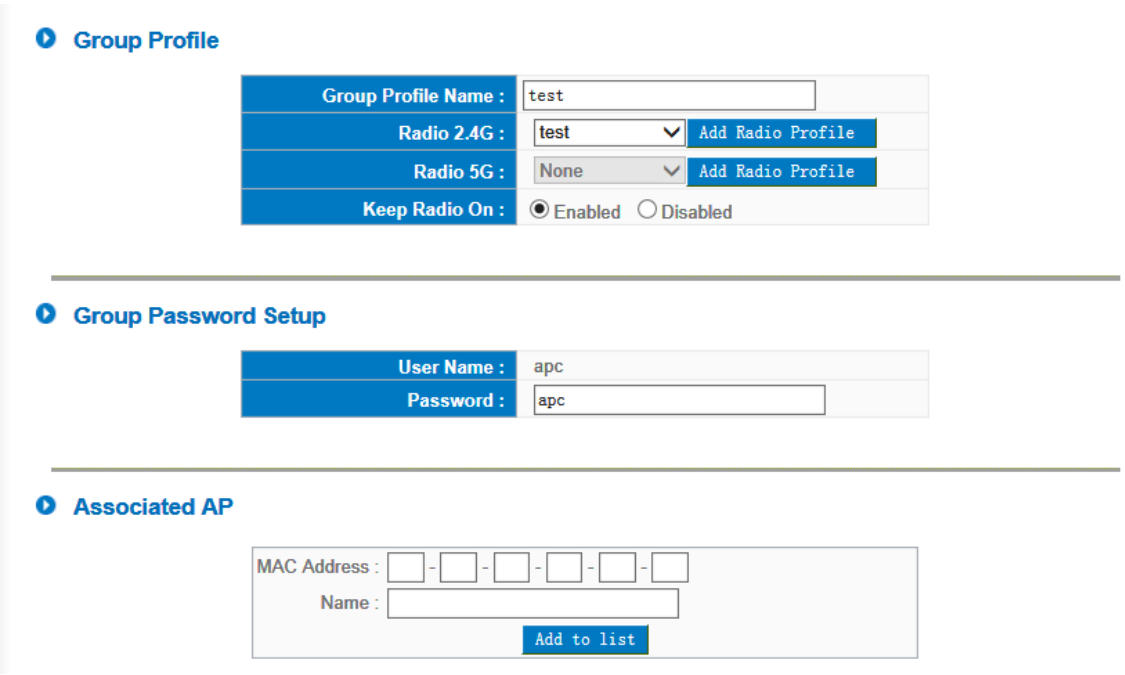
- **APSD Capable:** whether to enable Automatic Power Save Delivery feature.
- **DLS Capable:** whether to enable Direct Link Setup.
- **WMM Capable:** whether to enable WiFi Mulitmedia feature.

Wifi Multimedia(WMM)

APSD Capable :	○ Enabled ◉ Disabled
DLS Capable :	○ Enabled ◉ Disabled
WMM Capable :	○ Enabled ◉ Disabled

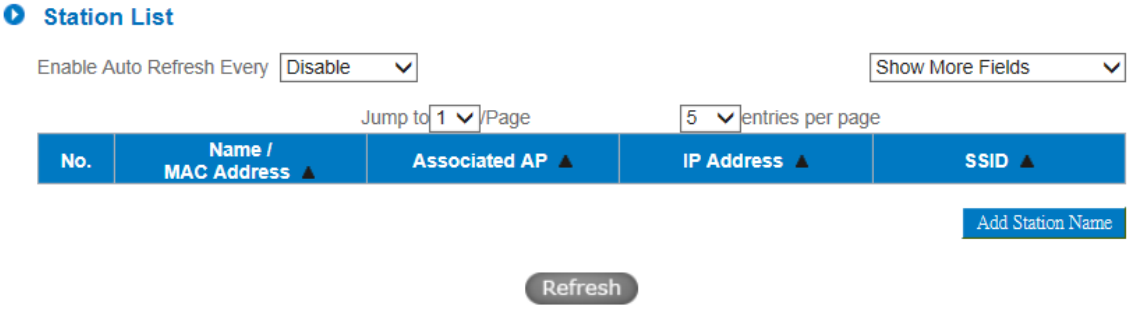
7.5 Adding a Group List

Group Profile settings page:



- **Radio:** choose the Radio Profile this group will use.
- **Keep Radio On:** if enabled, when AP loses its connection with the APC, it will keep its wireless radio on and provides local wireless connection.
- **Group Password Setup:** setup an AP group password, default username and password is “apc”.
- **Associated AP:** the APs associated with the Group, can be added manually or by using the tables below.

7.6 Station List

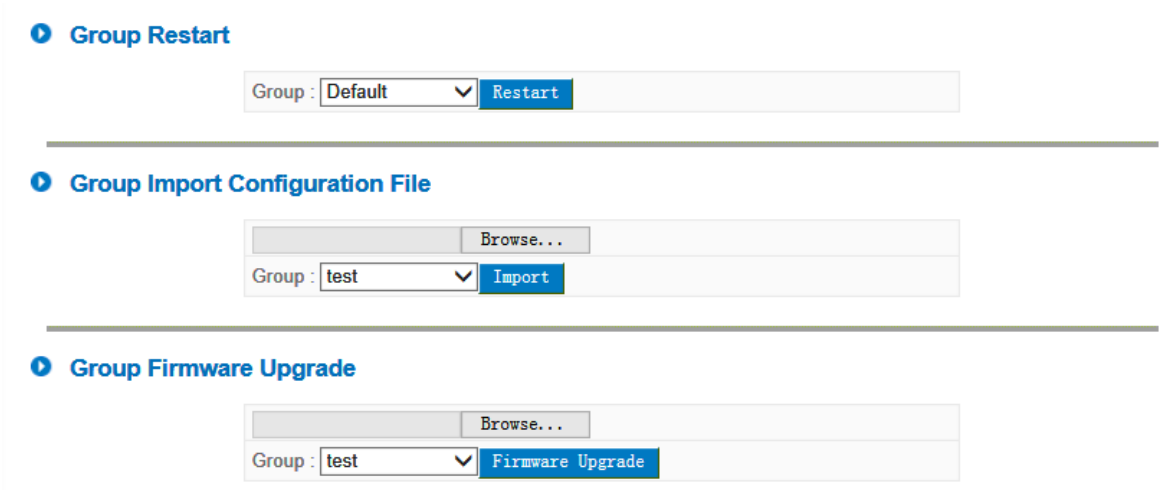


- **Enable Auto Refresh Every:** auto refreshes this list on every selected intervals
- **Show More Fields:** select or de-select the fields to show in the table below

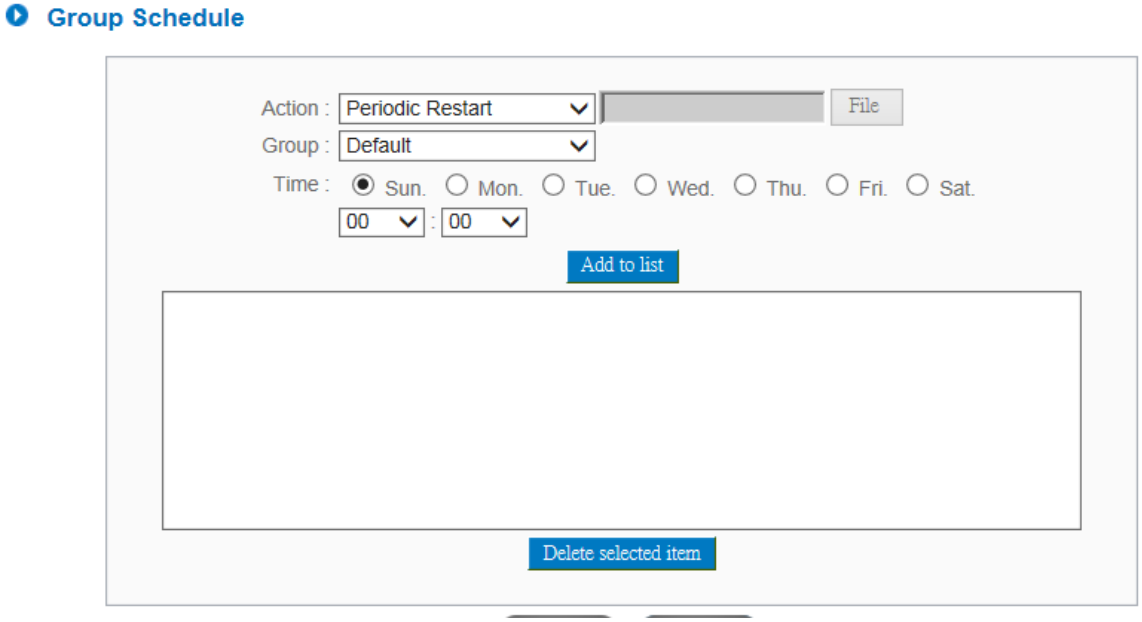
- **Add Station Name:** manually enter the Name and MAC Address of a station, Station Names will be shown in Station List instead of MAC Address.

7.7 Group Management

You can restart, import configuration file, or firmware upgrade a group of APs in the Group List page.



The Group Schedule section allows the above functions to be performed in a specific time within a weekly.



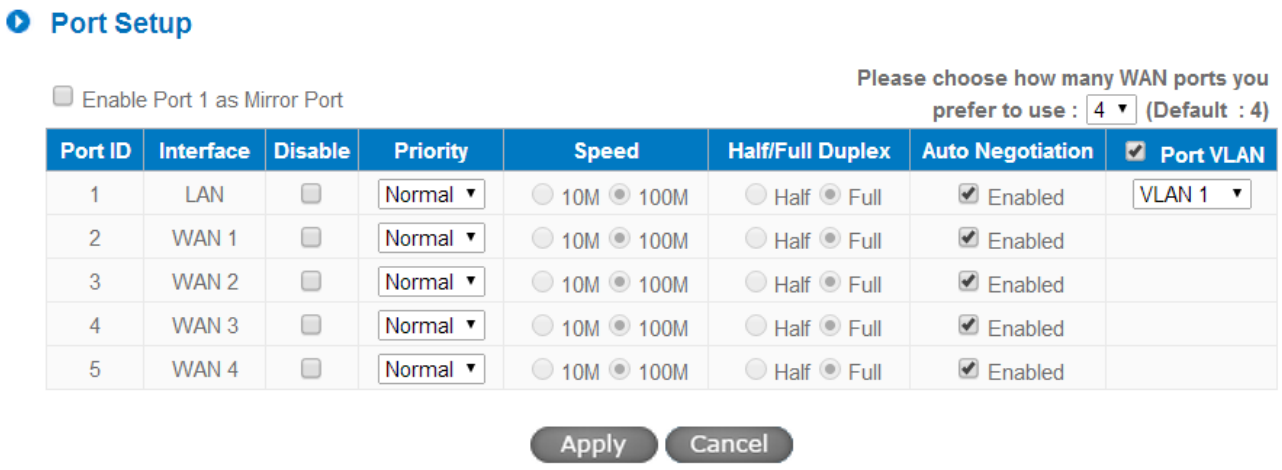
Scheduled actions will be executed at specified the day and time, with the results recorded in System Log. The executed schedule will then be removed from the list except for Periodic Restart, which will not be removed after execution.

VIII. Port Management

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

8.1 Setup

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



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

Disabled: This feature allows users turn on/off the Ethernet port. If selected, the Ethernet port will be shut down immediately and no connection can be made. The default value is "on".

Priority: This feature allows users to set the high/low priority of the packet delivery for the Ethernet port. If it is set as High, the port has the first priority to deliver the packet. The default value is “Normal”.

Speed: This feature allows users to select the network hardware connection speed for the Ethernet port. The options are 10Mbps and 100Mbps.

Duplex Status: This feature allows users to select the network hardware connection speed working mode for the Ethernet. The options are full duplex and half duplex.

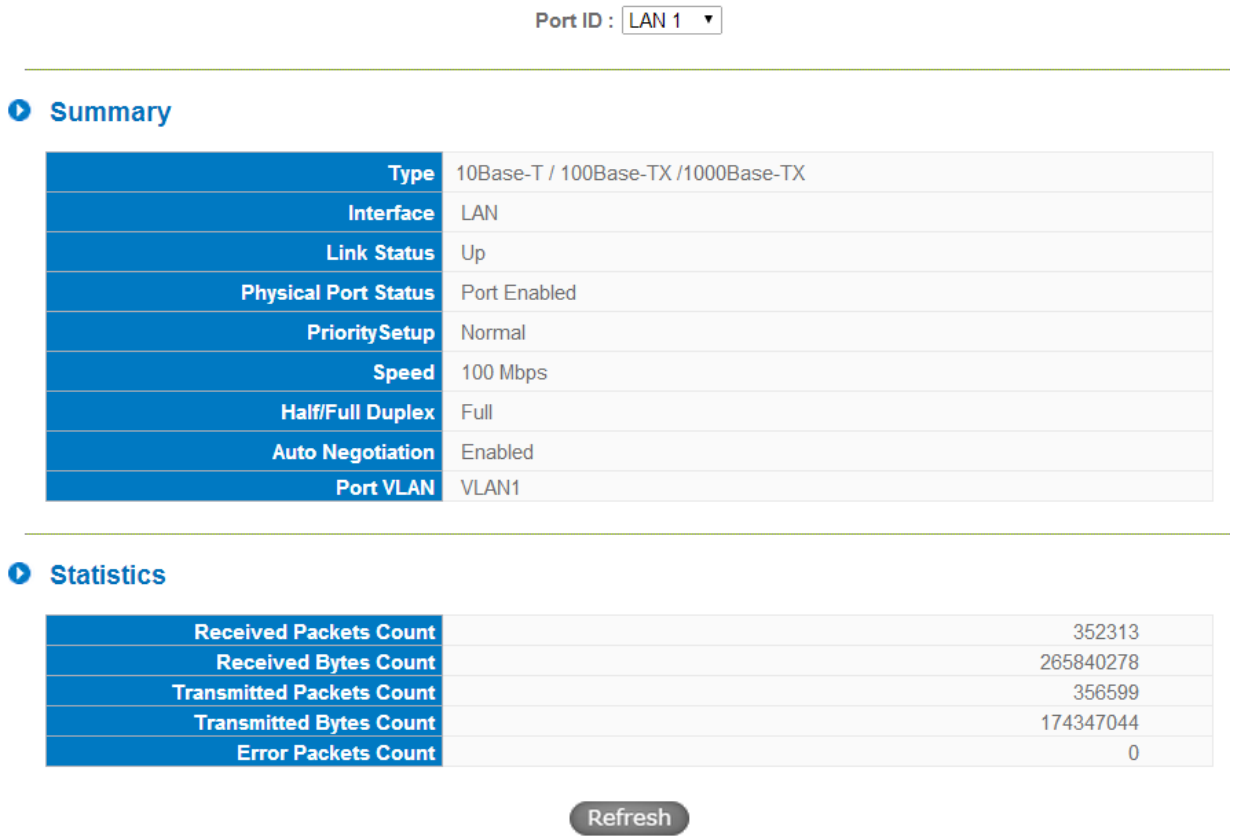
Auto Neg.: The Auto-Negotiation mode can enable each port to automatically adjust and gather the connection speed and duplex mode. Therefore, if Enabled Auto-Neg. selected, the ports setup will be done without any manual setting by administrators.

VLAN: This feature allows administrators to set the LAN port to be one or more disconnected network sessions. All of them will be able to log on to the Internet through the device.

Members in the same network session (within the same VLAN) can see and communicate with each other. Members in different VLAN will not know the existence of other members.

VLAN All: Set VLAN All port to be the public area of VLAN so that it can be connected to other VLAN networks. A server should be constructed for the intranet so that all VLAN group can visit this server. Set one of the network ports as VLAN All. Connect the server to VLAN All so that computers of different VLAN groups can be connected to this server. Moreover, the port where the administrator locates must be set as VLAN All so that it can be connected to the entire network to facilitate network management.

8.2 Port Status



Summary:

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

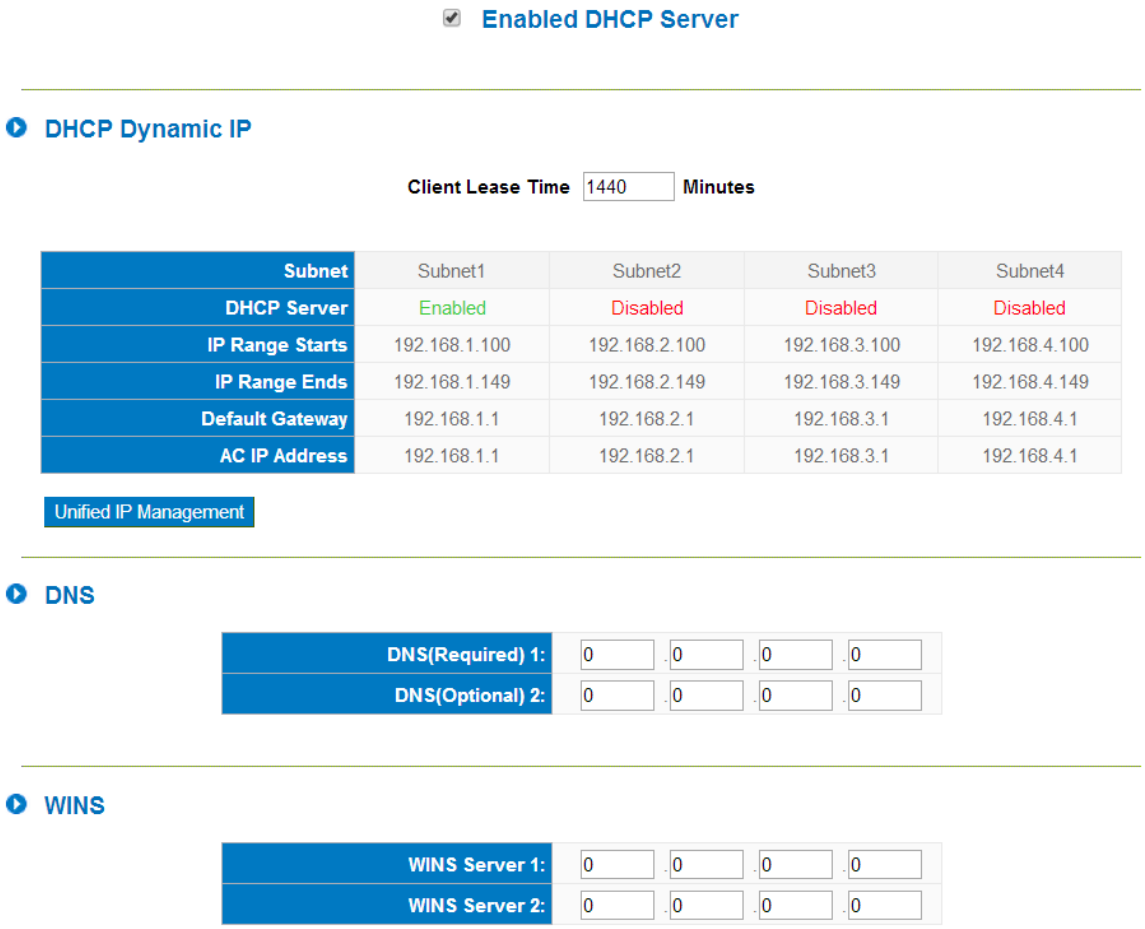
Statistics:

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

8.3 IP/ DHCP

With an embedded DHCP server, it supports automatic IP assignation 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.



Dynamic IP:

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

DNS (Domain Name Service):

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

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.

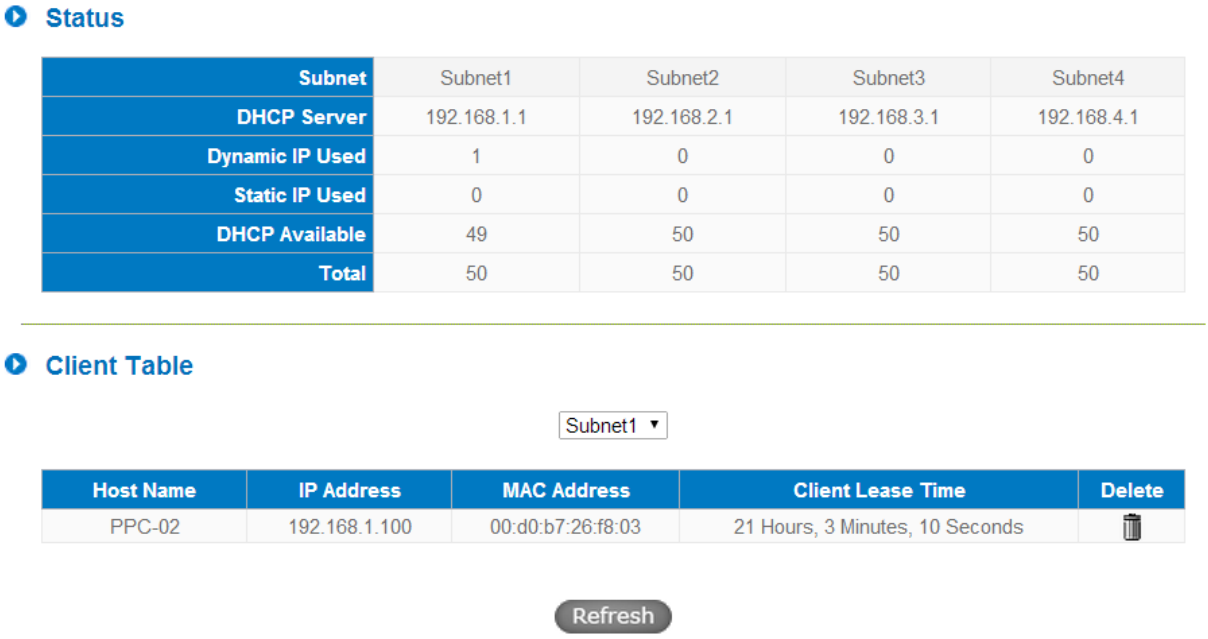
WINS Server: Input the IP address of WINS.

Apply: Click **"Apply"** to save the network configuration modification.

Cancel: Click **"Cancel"** to leave without making any changes.

8.4 DHCP Status

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



DHCP Server: This is the current DHCP IP.

Dynamic IP Used: The amount of dynamic IP leased by DHCP.

Static IP Used: The amount of static IP assigned by DHCP.

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

Total IP: The total IP which the DHCP server is configured to lease.

Host Name: The name of the current computer.

IP Address: The IP address acquired by the current computer.

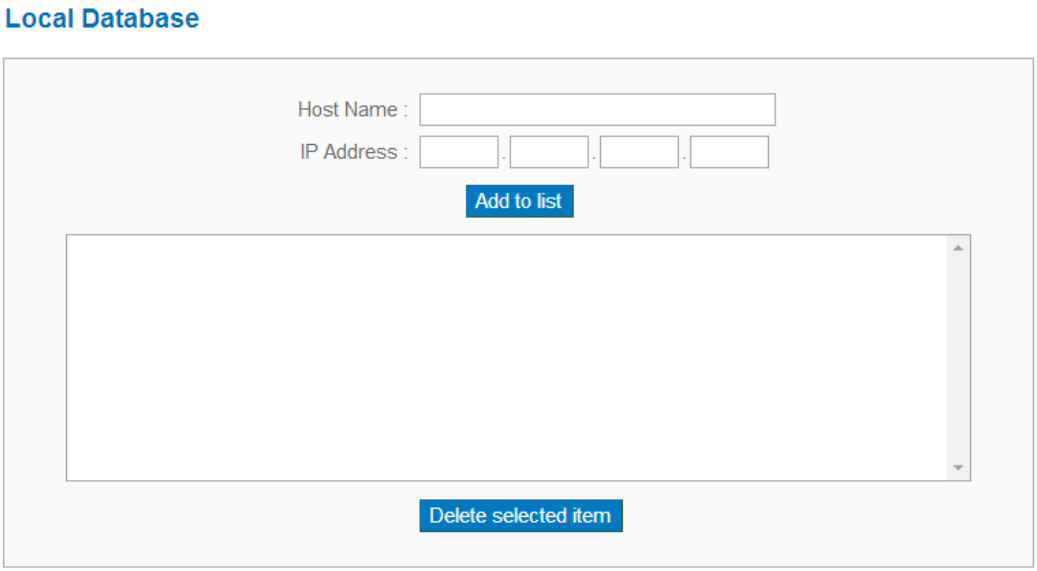
MAC Address: The actual MAC network location of the current computer.

Client Lease Time: The lease time of the IP released by DHCP.

Delete: Remove a record of an IP lease.

DNS Local Database(Future)

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

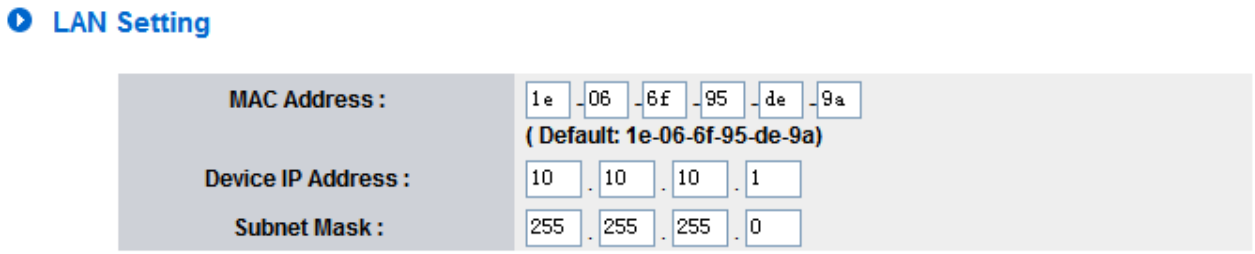


Host Domain Name	Enter the website host domain name. i.e. www.google.com
IP Address	Enter the corresponding IP address of the host domain above.
Add to Llist	Add the items into the list below.
Delete selected item	Delete the items chosen.

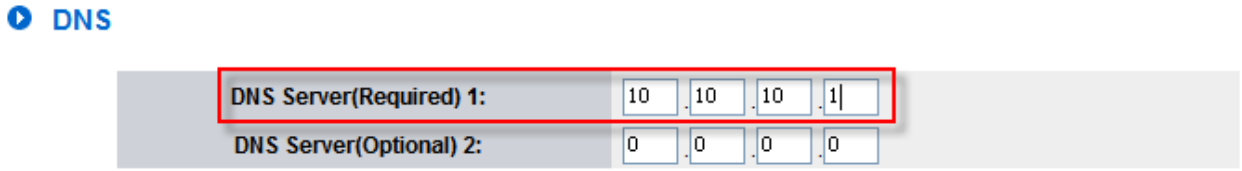
※ Note!

(1) Users MUST enable DCHP server service to enable DNS local database.

(2) Users must set DHCP server DNS IP address as the router LAN IP. For example, LAN is 10.10.10.1, as shown in the following figure.



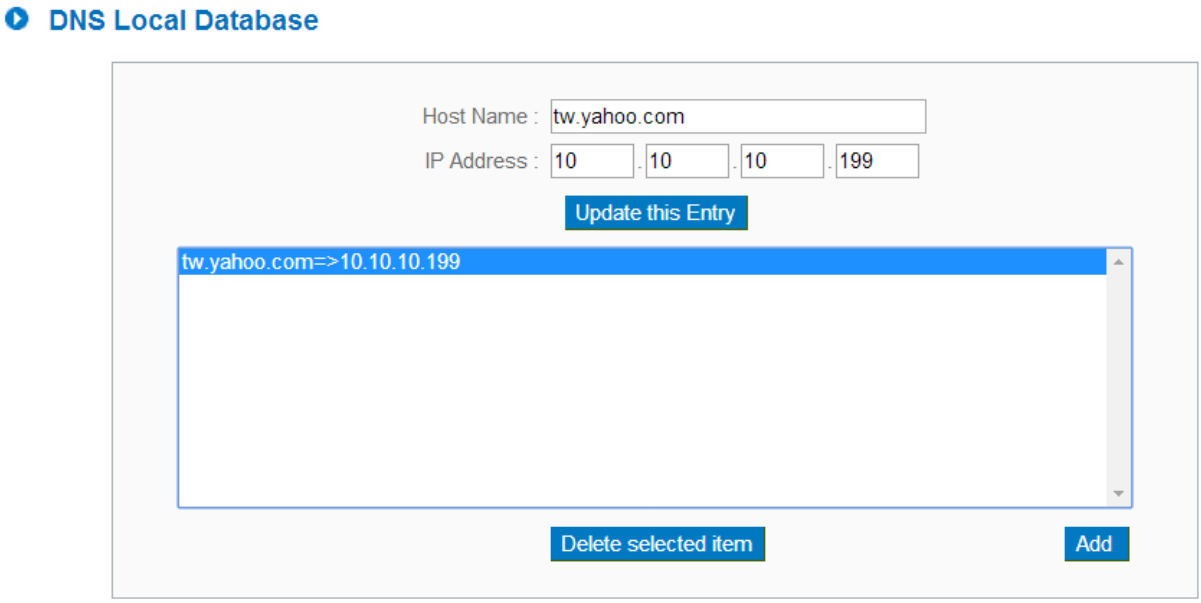
Therefore, DCHP DNS IP address must be 10.10.10.1 to make DNS local database in effect.



(3) After enabling DNS local database, if there is no host domain names in the list, the router will still use ISP DNS server or internal DNS server for lookup.

Test if DNS local database is effective:

Assumed tw.yahoo.com IP address is 10.10.10.199, as the following figure.



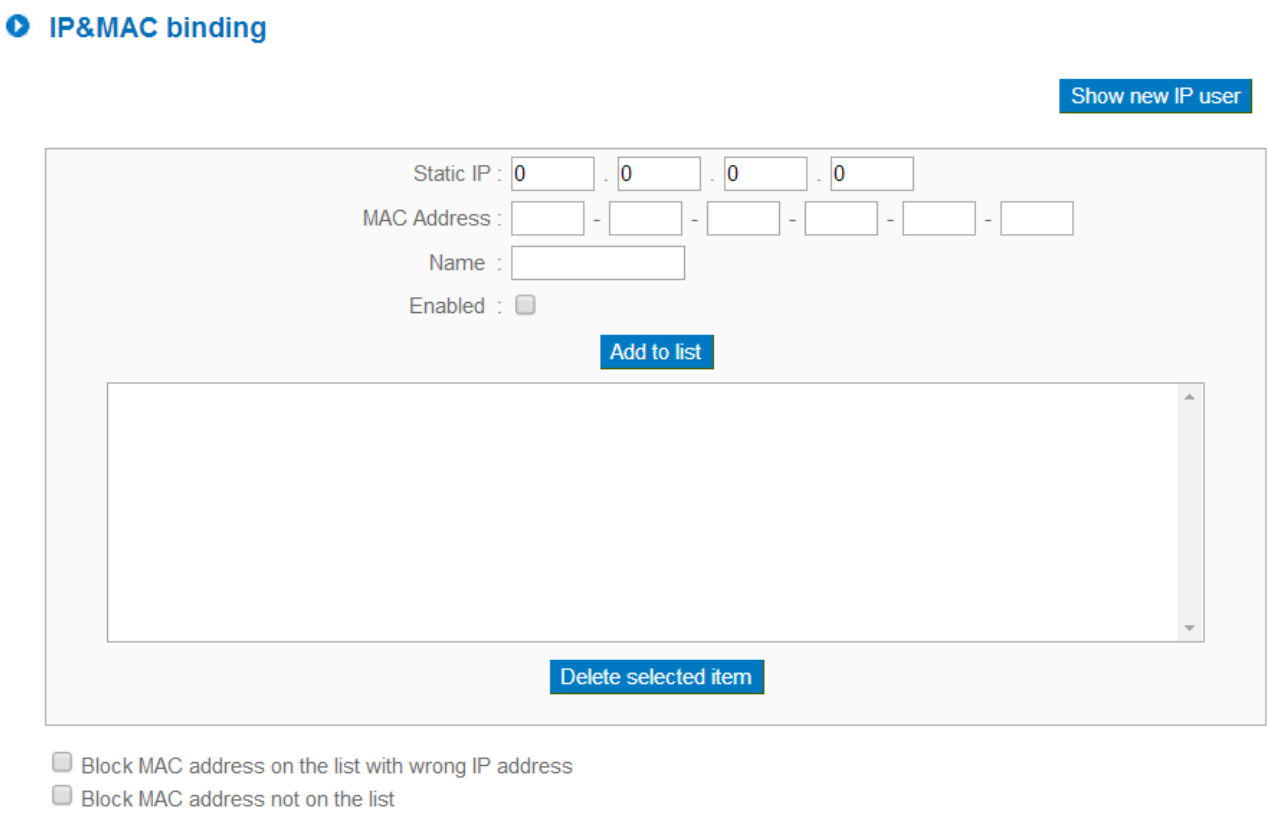
(1) System Tool => Diagnostic => DNS Name Lookup

(2) Enter tw.yahoo.com for lookup.

(3) The IP is 10.10.10.199, confirming the corresponding IP in DNS local database.

8.5 IP & MAC Binding

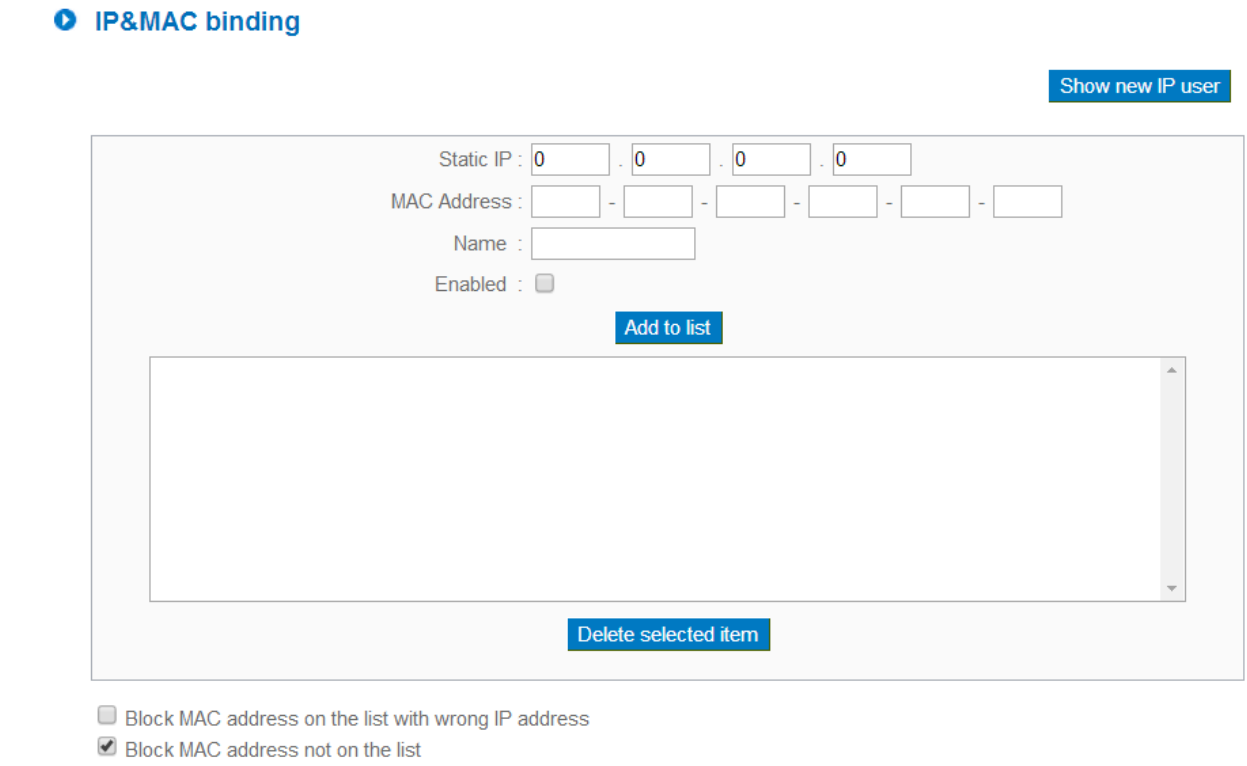
Administrators can apply IP & MAC Binding function to make sure that users can not add extra PCs for Internet access or change private IP addresses.



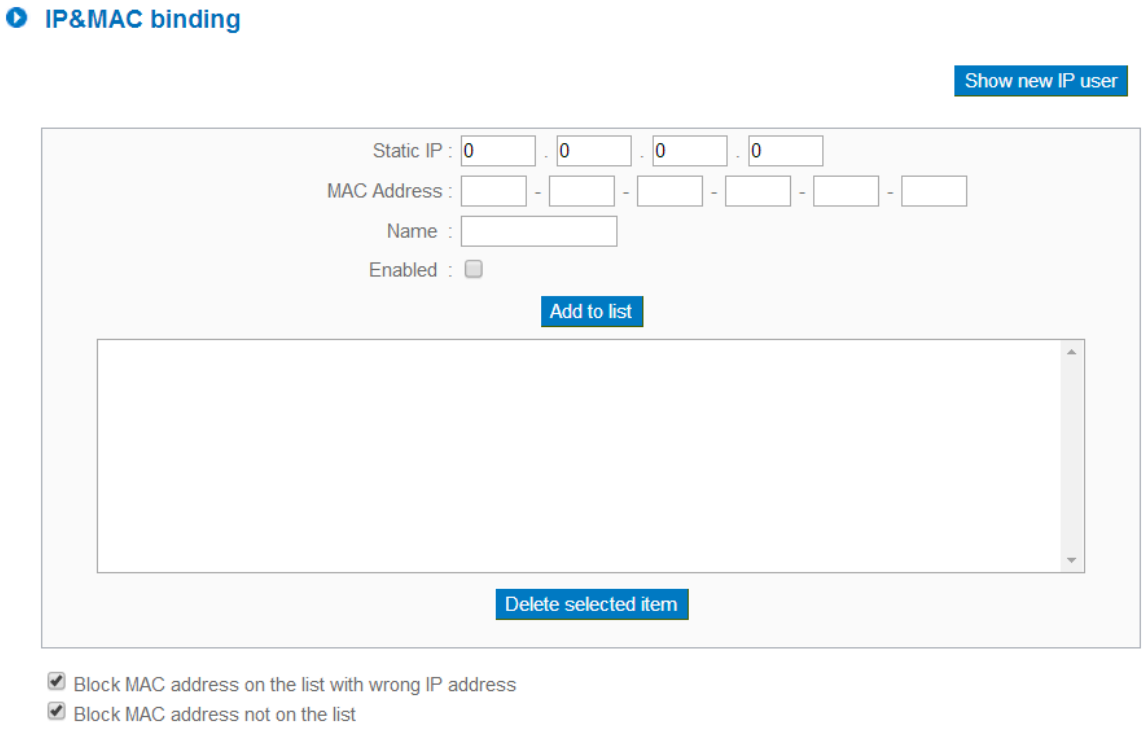
There are two methods for setting up this function:

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

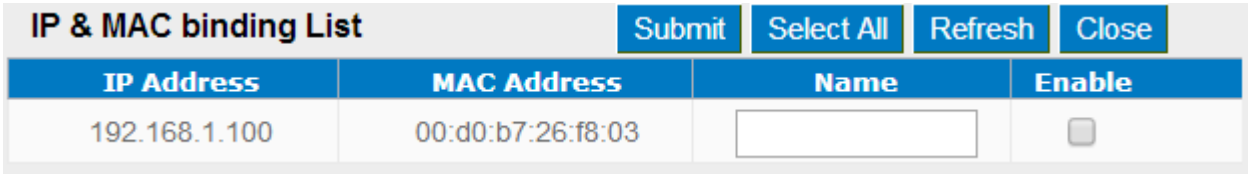


Static IP:	There are two ways to input static IP: 1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a specific assigned IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty. 2. If users want DHCP to assign a static IP for a PC every single time, users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

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

Show New IP user:

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

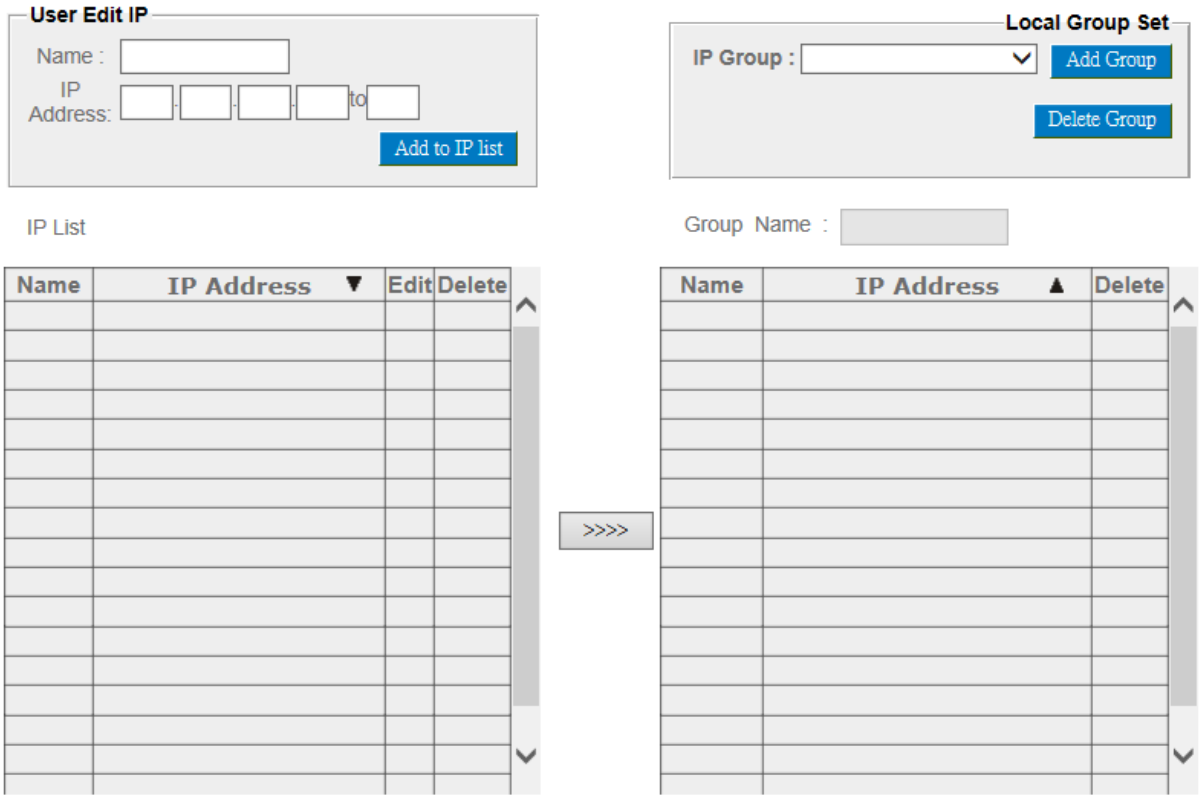


Name:	Input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
Enabled:	Choose the item to be bound.
Apply:	Activate the configuration.
Select All:	Choose all items on the list for binding.
Refresh:	Refresh the list.
Close:	Close the list.

8.6 IP Grouping

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

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

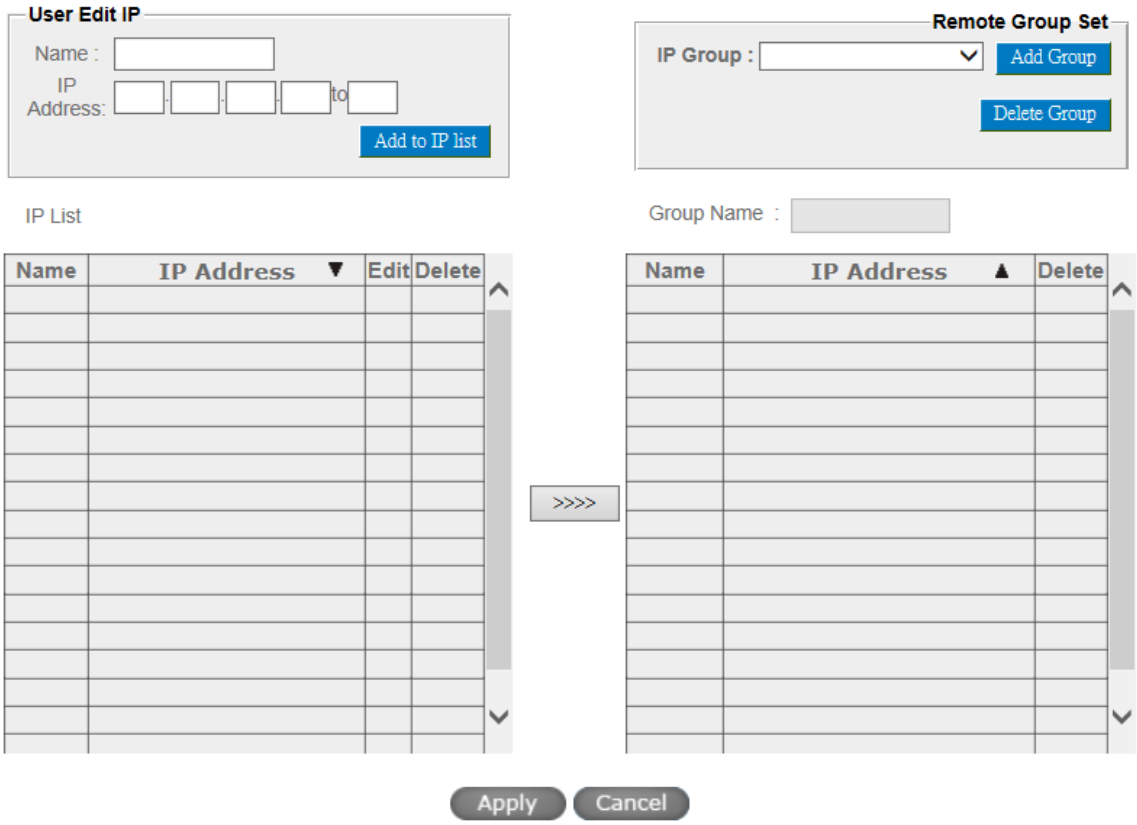


User Edit IP	The IP list will show the list which learns the IP addresses automatically on the left under side. You can also modify IP addresses manually.
Name	Input the name of IP address (or range) showed below.
IP Address	Input IP address (or range). For example, 192.168.1.200 ~ 250.

Add to IP List	After setting name and IP address, push this button to add the information into the IP list below. If this IP (or range) is already in the list, you can not add it again.
Local Group Set	You can choose from the IP list on the left side to set up a local IP group.
IP Group	Choose IP Group that you would like to modify. If you would like to add new groups, please push "Add new group" button.
Group Name	When you add new groups, please note if the group name is in the column.
Delete Group	Choose the group that you would like to delete from the pull- down list, and push the "Delete Group" button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
 **button**	You can choose several IPs from IP list on the left side, and push this button to have them added into the group the right side.
Delete 	Delete self- defined IP or IP range.
Apply	Click **"Apply"** to save the network configuration modification
Cancel	Click **"Cancel"** to leave without making any changes.

Remote IP Group Management:

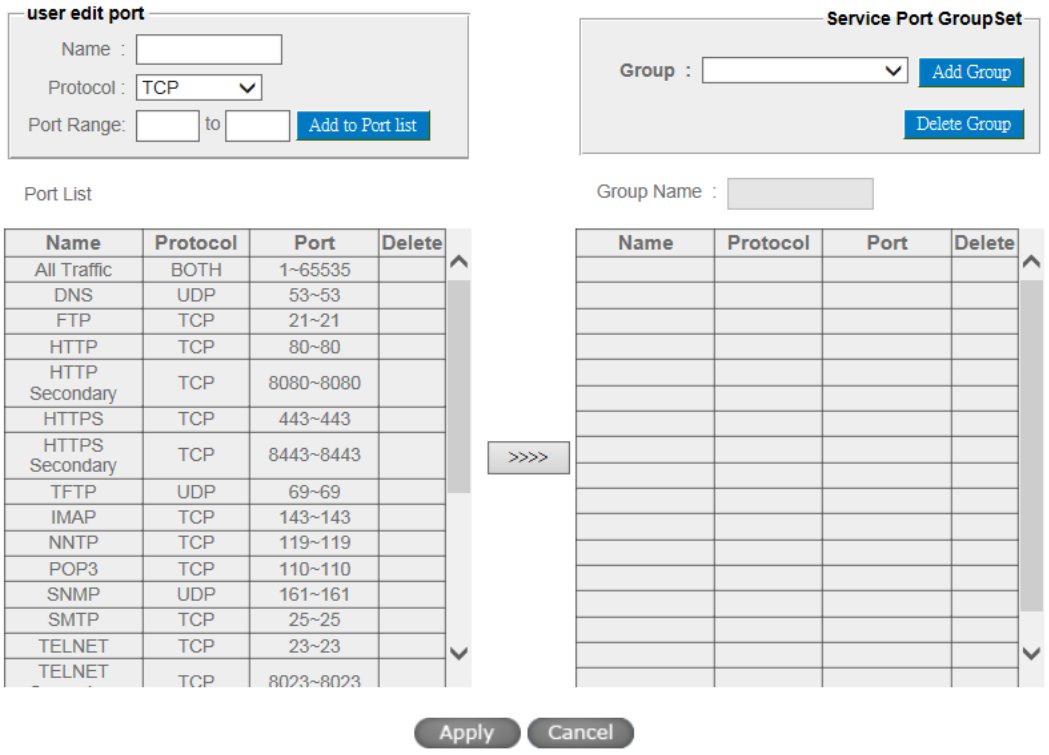
Basically, Remote IP Group setups are exactly the same as Local IP Group setups. However, remote IP group does not have automatically learning functions. Instead, you need to define addresses, ranges and groups manually. For example, 220.130.188.1 to 200 (range).



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

8.7 Port Group Management

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



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

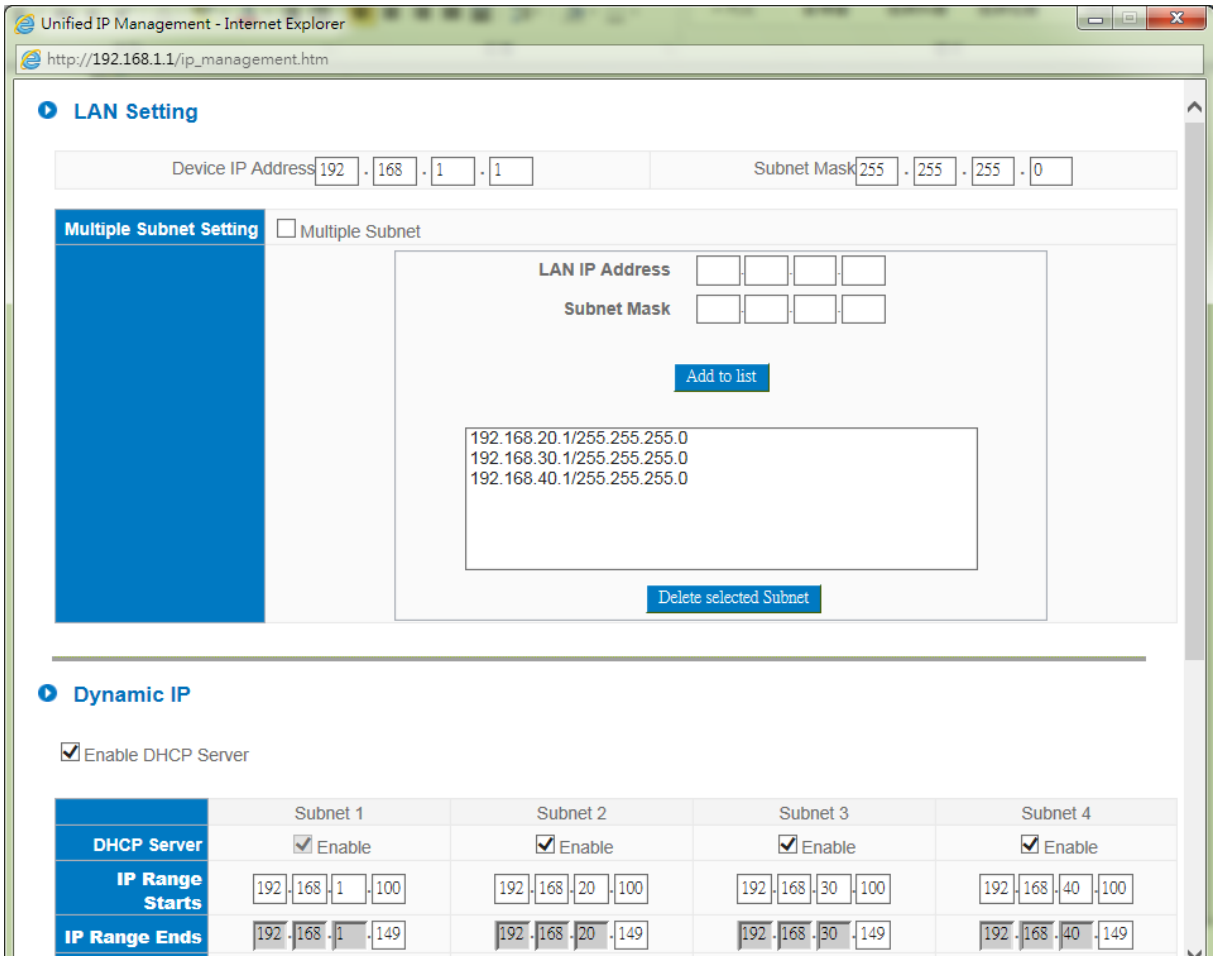
Delete	Delete self- defined port or port range.
Apply	Click **"Apply"** to save the network configuration modification
Cancel	Click **"Cancel"** to leave without making any changes.

8.8 802.1q

8.8.1 DHCP by VLAN

The DHCP server is able to assign different subnets to different VLANs. Users can assign LAN subnets into several VLANs and assign different DHCP subnets to them. Detailed configuration steps are as follows.

Enable Multiple Subnets in the LAN Setting, as well as, the DHCP server of the corresponding subnet.



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

In the VLAN Status page, choose Port-Based mode and configure different LAN ports as

different VLANs.

Port Setup

Enable Port 1 as Mirror Port

Please choose how many WAN ports you prefer to use : 3 (Default : 4)

Port ID	Interface	Disable	Priority	Speed	Half/Full Duplex	Auto Negotiation	Port VLAN
1	LAN	☐	Normal	10M 100M	Half Full	Enabled	VLAN 1
2	LAN	☐	Normal	10M 100M	Half Full	Enabled	VLAN 2
3	WAN 1	☐	Normal	10M 100M	Half Full	Enabled	
4	WAN 2	☐	Normal	10M 100M	Half Full	Enabled	
5	WAN 3	☐	Normal	10M 100M	Half Full	Enabled	

Apply Cancel

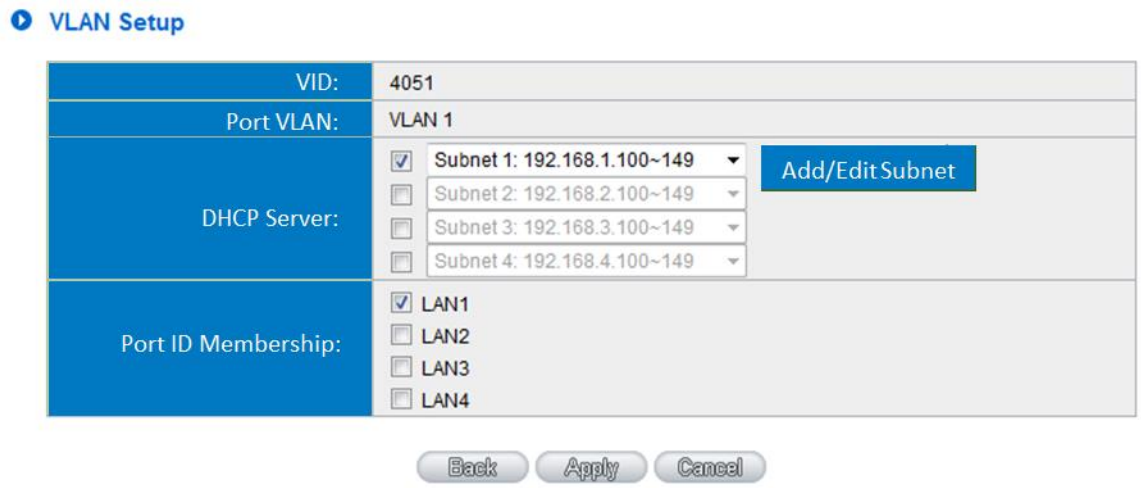
* The UI might vary from model to model, depending on different product lines.

Go to 802.1q VLAN Setting page and for VID 4051, click the Edit button. In DHCP Server and Port ID Membership, choose Subnet 1 and LAN 1 respectively.

VLAN Summary

VID	Interface	Enabled	Subnet Setting	DHCP Server	Port ID Membership	Edit	Delete
4001	LAN	☑	Subnet1	LAN 1, LAN 2, LAN 3, LAN 4			
4051	LAN	☑	Subnet1	LAN 1		Edit	
4052	LAN	☑	N/A	LAN 2		Edit	
4053	LAN	☑	N/A	LAN 3		Edit	
4054	LAN	☑	N/A	LAN 4		Edit	
4081	WAN	☑	N/A	WAN 1			
4082	WAN	☑	N/A	WAN 2			
4083	WAN	☑	N/A	WAN 3			
4084	WAN	☑	N/A	WAN 4			

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



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

Repeat the above steps for VID 4052, 4053 and 4054. When all done, different DHCP Subnets are now set to different LAN Ports for each VID.

8.8.2 802.1Q VLAN Settings

The 802.1q standard make that different network devices with the same VLAN ID can communicate with each other. To configure 802.1q VLAN, you need to know the following technical words :

VID: VLAN ID. Each VLAN has a different VID, and they are not able to transfer packets to other VLANs. When multiple ethernet ports are configured with the same VID, packets are transfered between these ports only. In 802.1q standard, packets in VLAN will be attached a specific VLAN tag in its header.

PVID: Port VLAN ID. An ethernet port can be members of multiple VLANs, and it can choose one of the VID as its PVID. When a INCOMING packet does not have 802.1q tag, the network device will use the PVID as its VID. But if the packet already has 802.1q tag, it will be untouched.

Tagged/Untagged: This is used to determine an OUTGOING packet will keep 802.1q tag or not. If tagged is set, the tags will be kept, and untagged means that tag will be removed.

Below are two examples illustrating practical applications of 802.1q.

8.8.2.1 Forward WAN packets with different VLAN tags to different WAN ports

The ISP uses different VID for different usage through its line. VID 500 is used for internet, VID 400 for VoIP and VID 600 for IPTV. 802.1q VLAN can be used to meet the requirements of this situation, the steps of configuration are as follows.

(1) Under VLAN Status page, switch VLAN Mode to Tagged-Based.

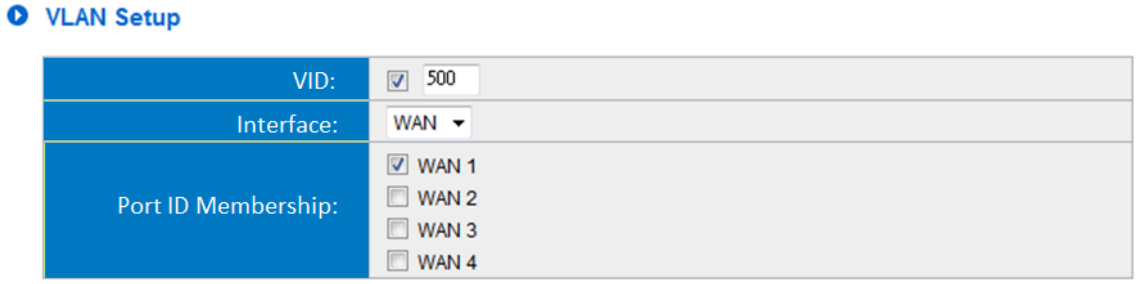
VLAN Status

VLAN Mode : Tagged-Based

Port ID	Interface	Connect Mode	PVID	VID Membership	Config.
1	LAN	Untagged	4001	VID4001	Edit
2	LAN	Untagged	4001	VID4001	Edit
3	LAN	Untagged	4001	VID4001	Edit
4	LAN	Untagged	4001	VID4001	Edit
5	WAN 1	Untagged	4081	VID4081	Edit
6	WAN 2	Untagged	4082	VID4082	Edit
7	WAN 3	Untagged	4083	VID4083	Edit
8	WAN 4	Untagged	4084	VID4084	Edit

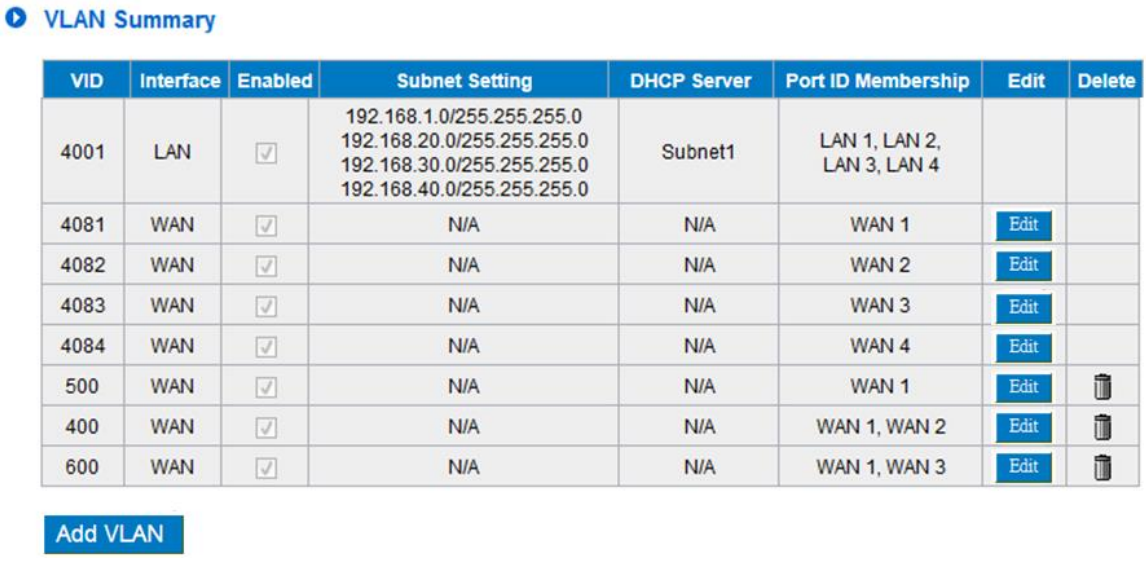
* The UI might vary from model to model, depending on different product lines.

(2) Go to 802.1q VLAN Setting, add a new VLAN with a ID tag of 500, switch the Interface to WAN and Port ID Membership on WAN 1. Click Apply when done.



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

(3) Follow the previous steps in adding VID 400 (Port ID Membership of WAN 1 and 2) and VID 600 (Port ID Membership of WAN 1 and 3). The VLAN Summary page should look like the picture below if done correctly.



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

(4) Go back to VLAN Setup page, Edit WAN 1. Change the Connect Mode to “Tagged” and PVID to “VID 500”. Click Apply when done.

VLAN Setup

Port ID:	5
Interface:	WAN1
Connect Mode:	Tagged
PVID:	VID500
VID Membership:	☑ VID4081 (Default) ☐ VID4082 ☐ VID4083 ☐ VID4084 ☑ VID500 ☑ VID400 ☑ VID600

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

(5) Follow the previous steps for configuring PVID 400 and 600 on WAN 2 and 3 respectively. But keep the Connect Mode as Untagged. When finished, the VLAN Status page should look like the picture below.

VLAN Status

VLAN Mode : Tagged-Based

Port ID	Interface	Connect Mode	PVID	VID Membership	Config.
1	LAN	Untagged	4001	VID4001	Edit
2	LAN	Untagged	4001	VID4001	Edit
3	LAN	Untagged	4001	VID4001	Edit
4	LAN	Untagged	4001	VID4001	Edit
5	WAN 1	Tagged	500	VID4081, VID500, VID400, VID600	Edit
6	WAN 2	Untagged	400	VID4082, VID400	Edit
7	WAN 3	Untagged	600	VID4083, VID600	Edit
8	WAN 4	Untagged	4084	VID4084	Edit

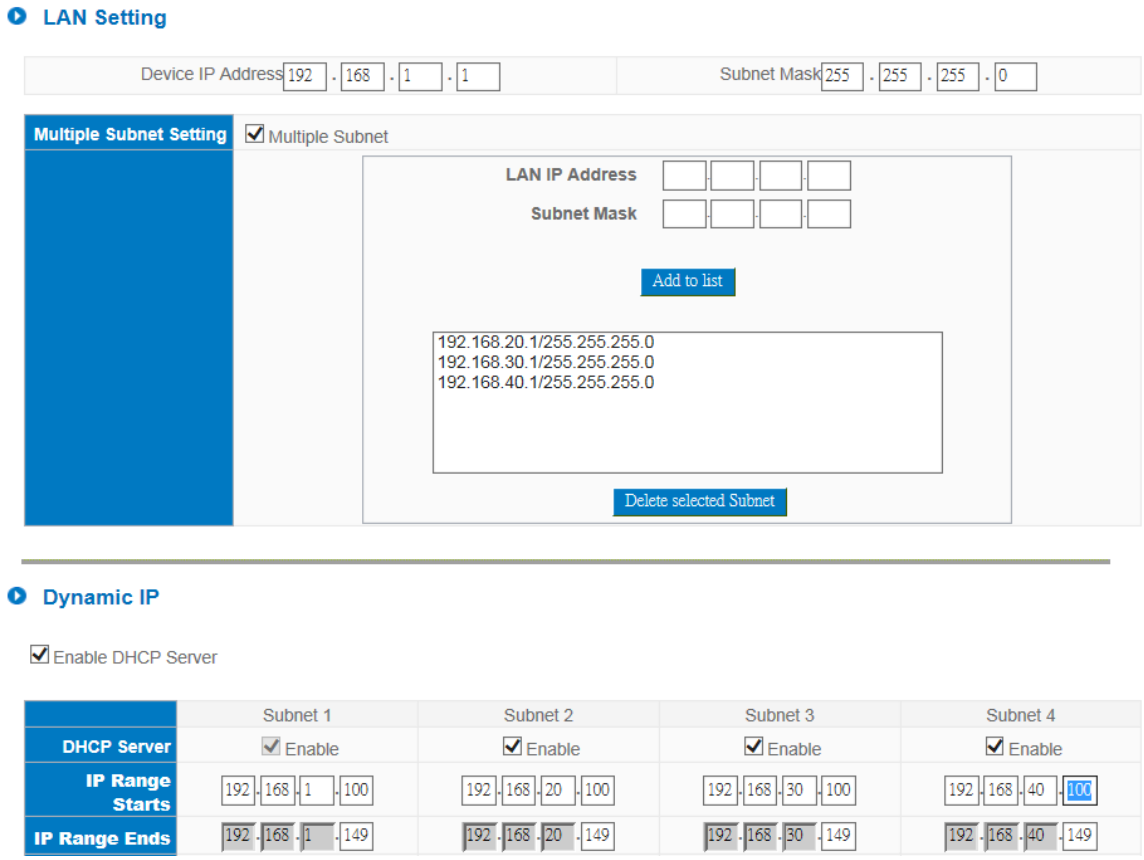
* The UI might vary from model to model, depending on different product lines.

(6) After completing the setup, connect the ISP line to WAN 1, VoIP to WAN 2 and IPTV to WAN3.

8.8.2.2 Attach a VLAN Tag to specific destination subnet

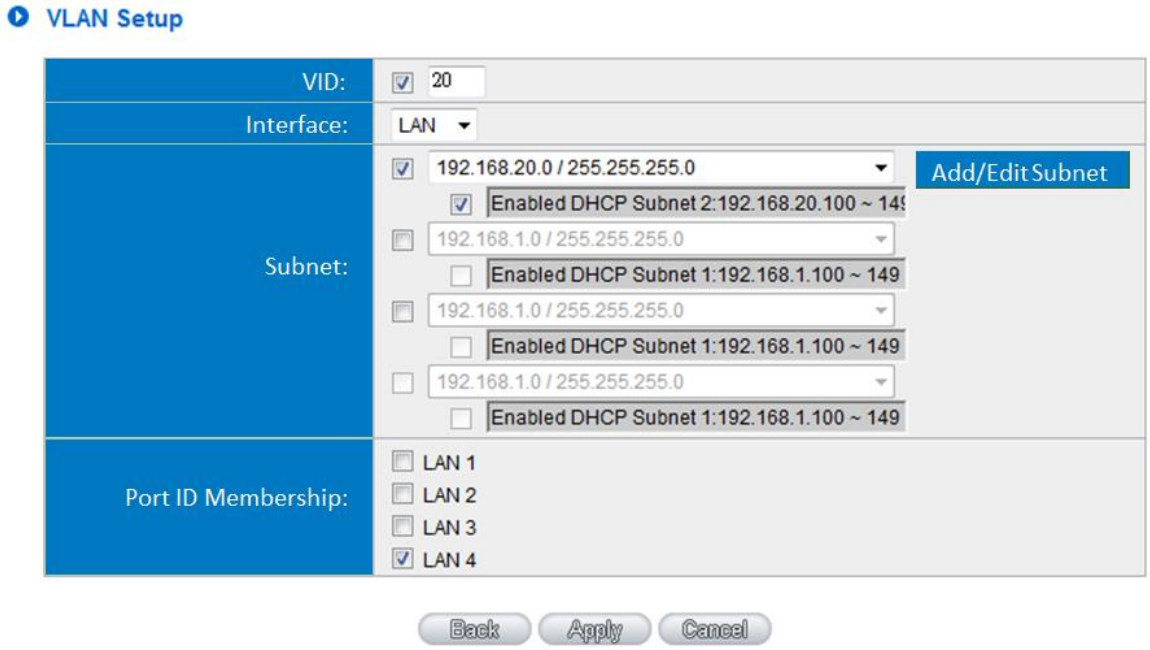
A common practice for businesses is to divide its internal network into VLANs and using switches, according to different departments. As an example, subnet 192.168.20.X using VID 100 for Technical Support Department, and subnet 192.168.30.0 for Sales Department. The configuration steps are as follows.

(1) Enable Multiple Subnets in the LAN Setting, as well as, the DHCP server of the corresponding subnet.



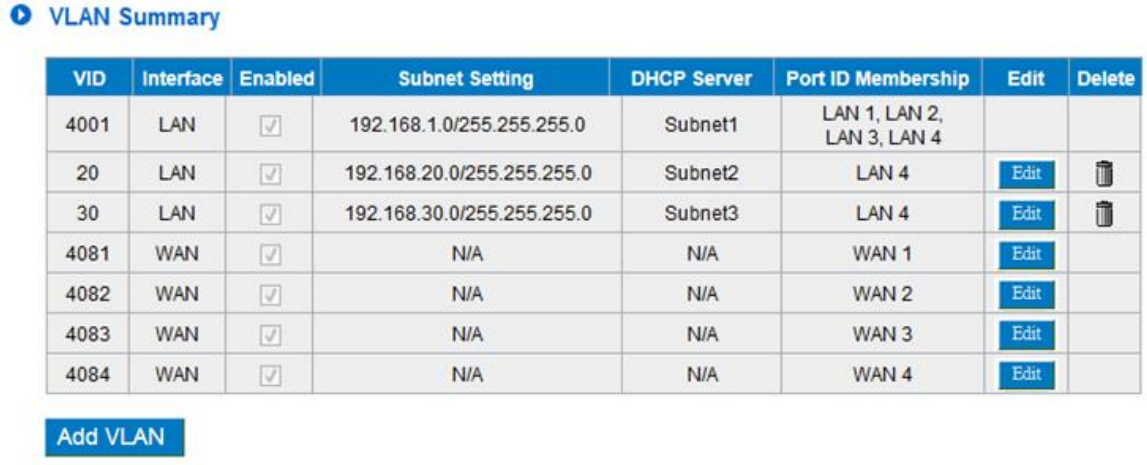
* The UI might vary from model to model, depending on different product lines.

(2) Go to 802.1q VLAN Settings; add a new VID 20, Interface as LAN, Subnet as 192.168.20.0/255.255.255.0. If DHCP is needed then the box should be checked. Finally, set Port ID Membership as LAN 4.



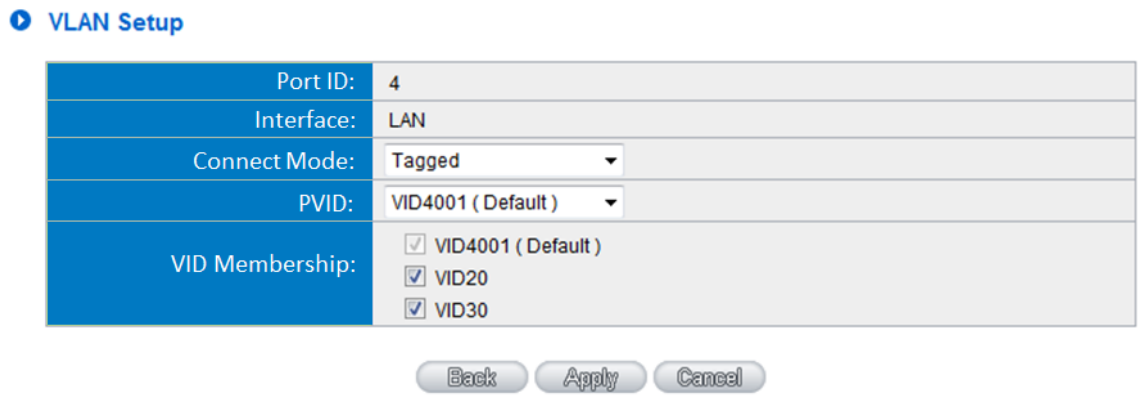
* The UI might vary from model to model, depending on different product lines.

(3) Use the same steps as above to setup VID 30 for 192.168.12.0/255.255.255.0, and Port ID Membership as LAN 4. The VLAN Summary page should look the same as the picture below.



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

(4) Go to the VLAN Status page and Edit LAN4, change Connect Mode to Tagged and apply.



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

When configurations are complete, connect the switch to the router's LAN 4 Port. VID 20 tags will be added to packets sent to destination 192.168.20.x, and VID 30 tags to 192.168.30.x destination packets.

IX. QoS (Quality of Service)

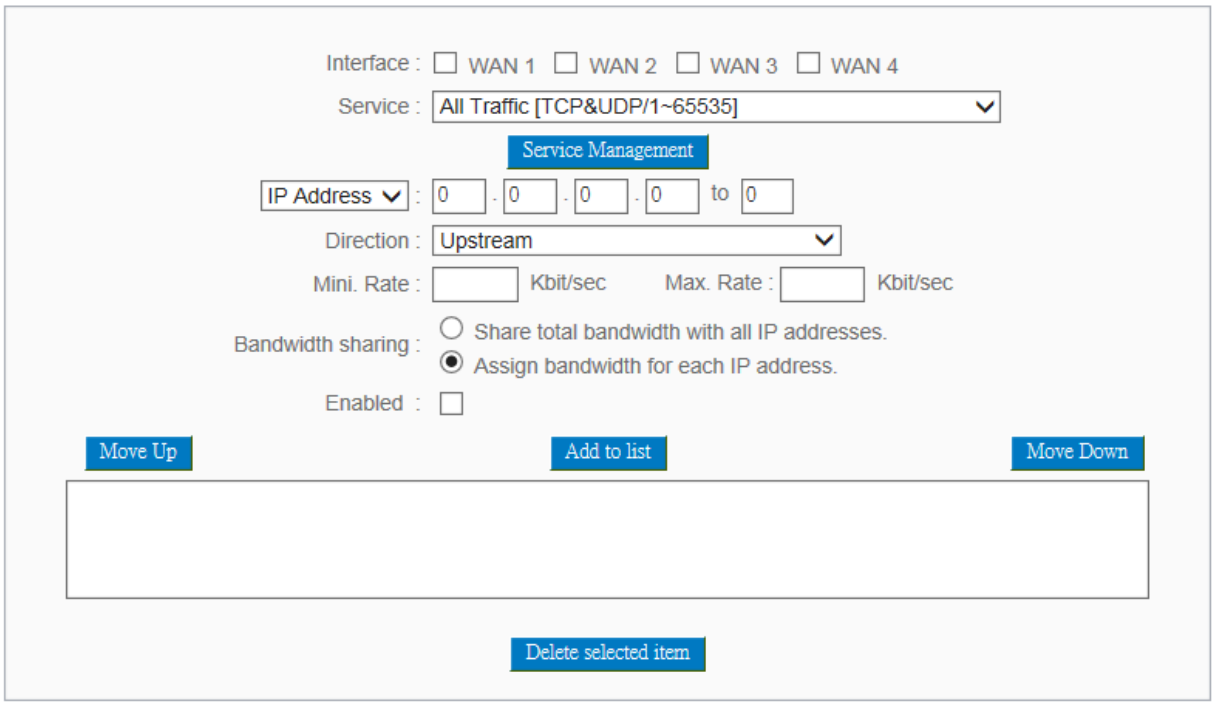
QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IP addresses to save bandwidth or provide priority to specific applications or services, and also to enable other users to share bandwidth, as well as to ensure stable and reliable network 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 Bandwidth (Kbit/sec)	Remnant guarantee Upstream Bandwidth (Kbit/sec)	Downstream Bandwidth (Kbit/sec)	Remnant guarantee Downstream Bandwidth (Kbit/sec)
WAN 1	10000	10000	10000	10000
WAN 2	10000	10000	10000	10000
WAN 3	10000	10000	10000	10000
WAN 4	10000	10000	10000	10000

Quality of Service



8.1.1 The Maximum Bandwidth provided by ISP

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	10000	10000	10000	10000
WAN 2	10000	10000	10000	10000
WAN 3	10000	10000	10000	10000
WAN 4	10000	10000	10000	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 1024Kbit/50=20Kbit/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. 1KB = 8Kbit.

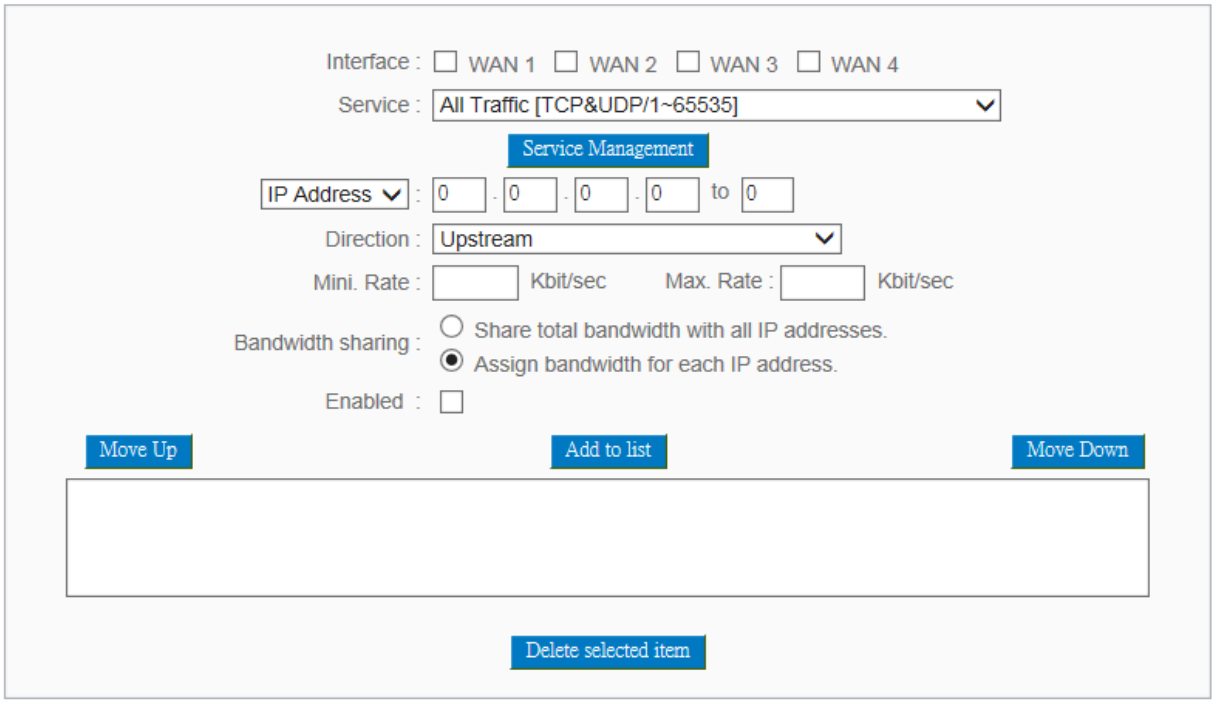
8.1.2 QoS

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: Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.

Service Port: Select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select "All (TCP&UDP) 1~65535". If only FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.

IP Address: This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 150". The rule will control IP addresses from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input "0" in the boxes of IP address. This means all Intranet IP addresses will be restricted. QoS can also control the range of Class B.

Direction:

Upstream: Means the upload bandwidth for Intranet IP.

Downstream: Means the download bandwidth for Intranet IP.

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.

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.

Min. & Max. Rate: (Kbit/Sec)

The minimum bandwidth: The rule is to guarantee minimum available bandwidth.

The maximum bandwidth: This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule.

Attention! The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.

Bandwidth Assign Type:

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).

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.

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.

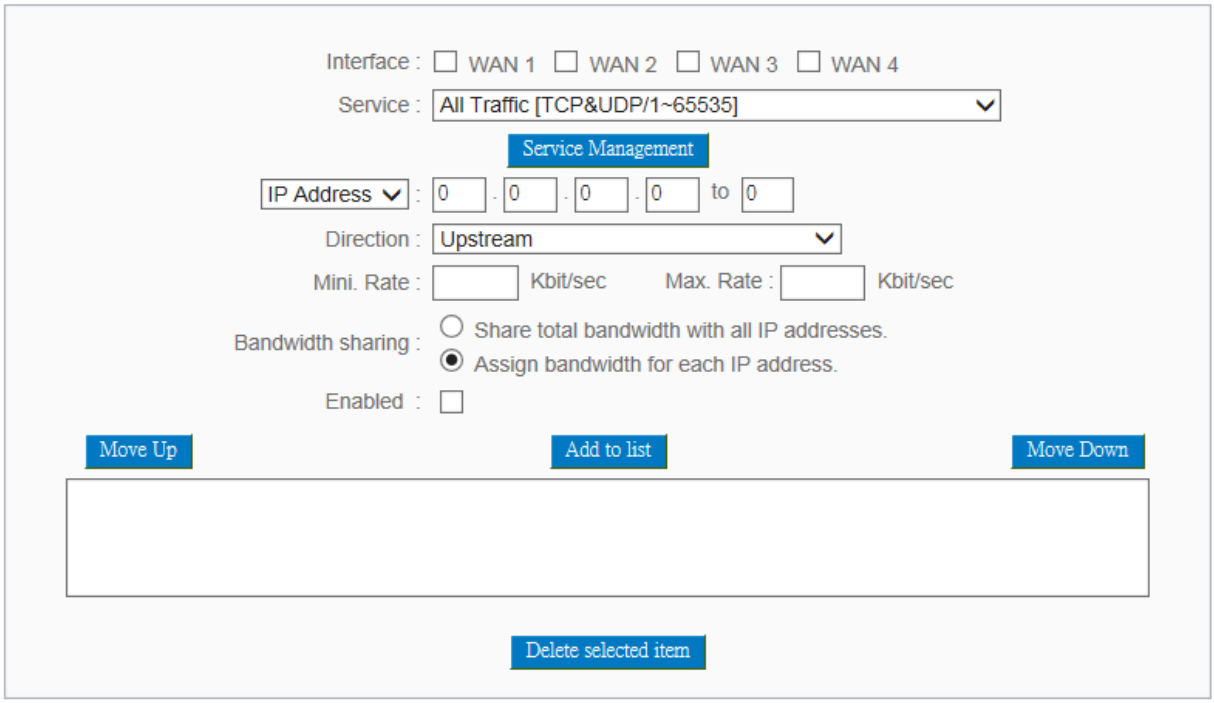
Enable:	Activate the rule.
Add to list:	Add this rule to the list.
Move up & Move down:	QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. 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:

Priority Control:

The Router will distribute the bandwidth as 60% (the highest) and 10% (the lowest). If you set the service port 80 as "High" priority, the router will give 60% bandwidth to the port 80. In the other hand, if you give the port 21 as "Low" priority, the device will only give it 10% bandwidth. The remained 30% bandwidth will be shared by the other service.

Quality of Service



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 FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.

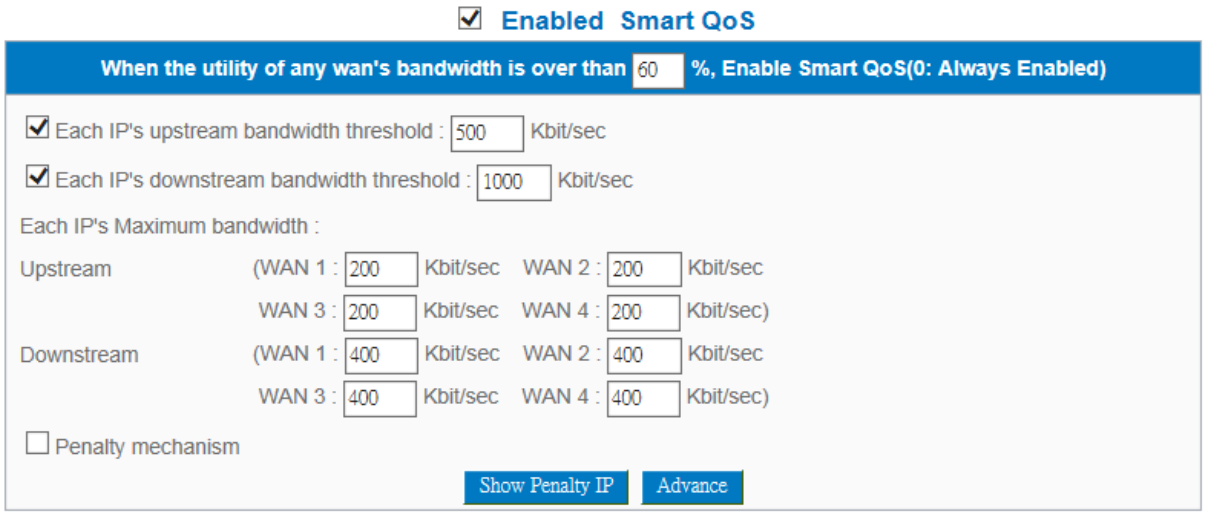
Direction: Upstream: Means the upload bandwidth for Intranet IP.
Downstream: Means the download bandwidth for Intranet IP.
Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server.
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.

Enabled: Activate the rule.

Add to list: Add this rule to the list.

Delete Selected items:	Remove the rules selected from the Service List.
Show Table:	This will display all the Priority 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.

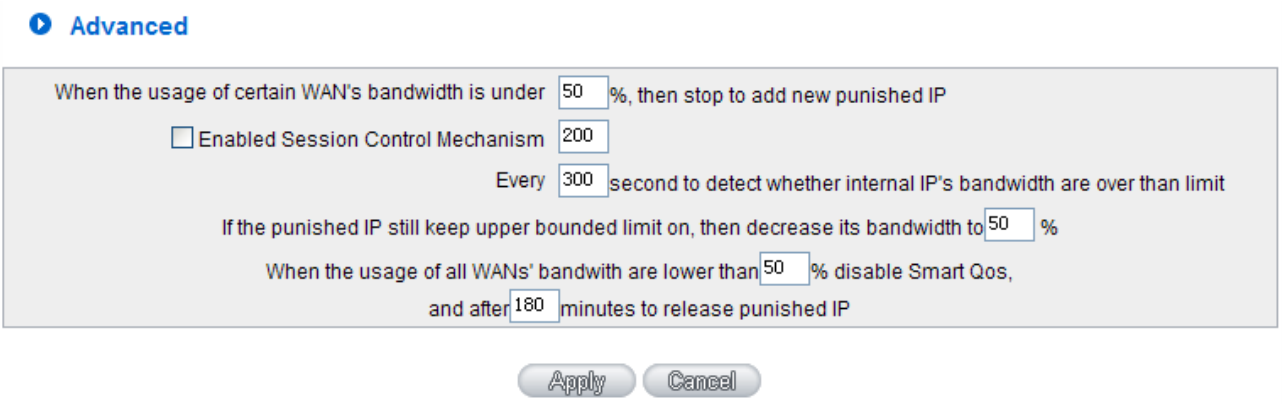
8.1.3 Smart QoS



Enabled QoS:	Choose to apply QoS function.
When the usage of any WAN's bandwidth is over___%, Enable Smart QoS	Input the required rate value into the column. The default is 60%.
Each IP's upstream bandwidth threshold (for all WAN):	Input the max. upstream rate for intranet IPs.
Each IP's downstream bandwidth threshold (for all WAN) :	Input the max. downstream rate for intranet IPs.
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 List:	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.



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

When the usage of certain WAN's bandwidth is under __%, will stop to punish the IP which is over the limit. While the bandwidth is over the certain percentage, penalty mechanism will be actived.

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

Detect usage of internal IP's bandwidth every __ secend.

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

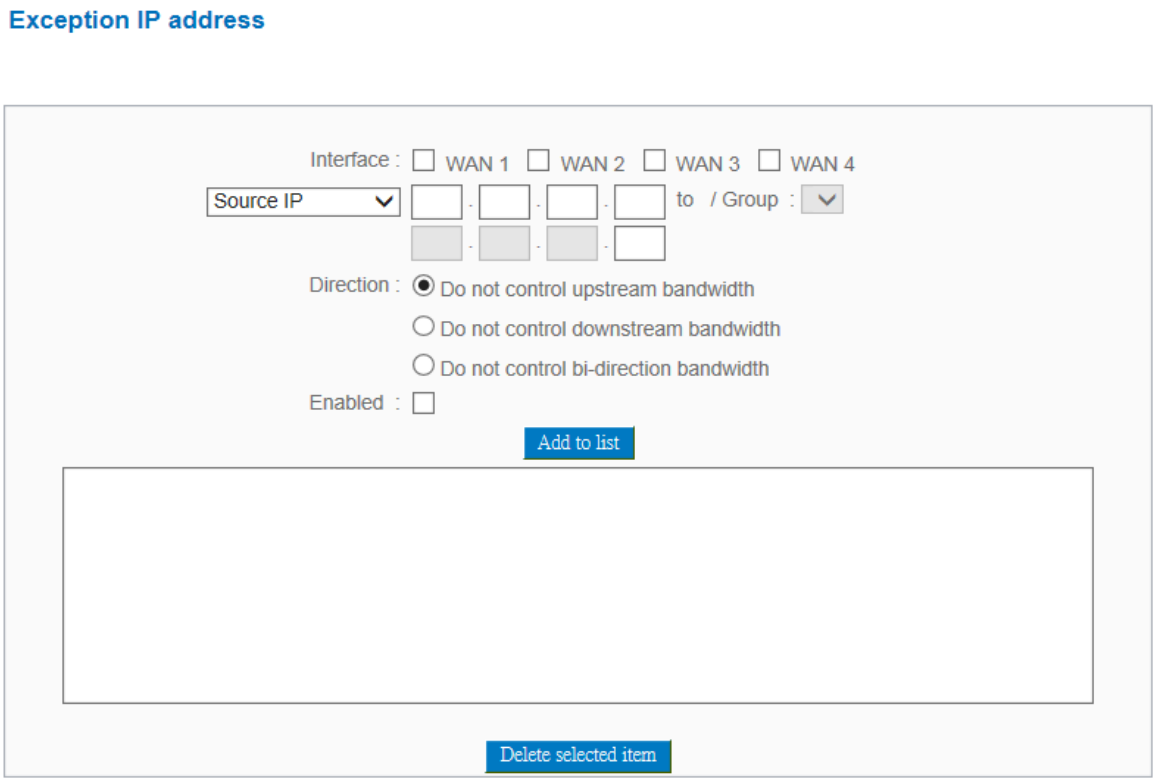
If the punished IP still keep over the limit, the limit badwidth will be decrase to __%.

When the usage of all WANs' bandwith are lower than__% disable Smart Qos, and after__minutes to release punished IP

Smart QoS will be disabled when the usage of bandwidth is lower than __%. Punished IP will be released after __minute.

8.1.4 Exception IP address

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



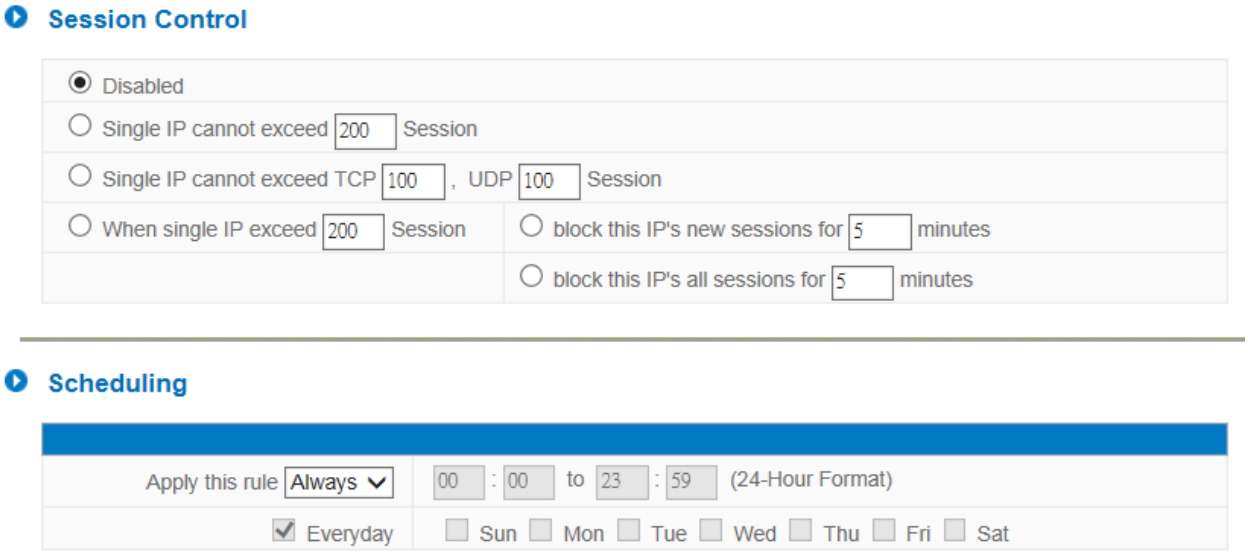
WAN	Select WAN ports.
Source IP	Enter the exempted IP range, or select the exempted IP group.
Do not control Direction	Select do not control upload, download, or both of them.
Enabled	Enable this policy.
Add to List	Add this policy into the exempted list.
Delete Selected item	Delete selected list.
Apply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

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.

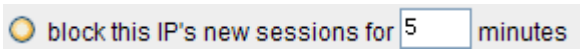
Session Control and Scheduling:



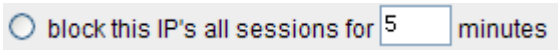
Disabled: Disable Session Control function.

Single IP cannot exceed __ session: This option enables the restriction of maximum external sessions to each Intranet PC. When the number of external sessions reaches the limit, to allow new sessions to be built, some of the existing sessions must be closed. For example, when BT or P2P is being used to download information and the sessions exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.

When single IP exceed __:



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.



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.

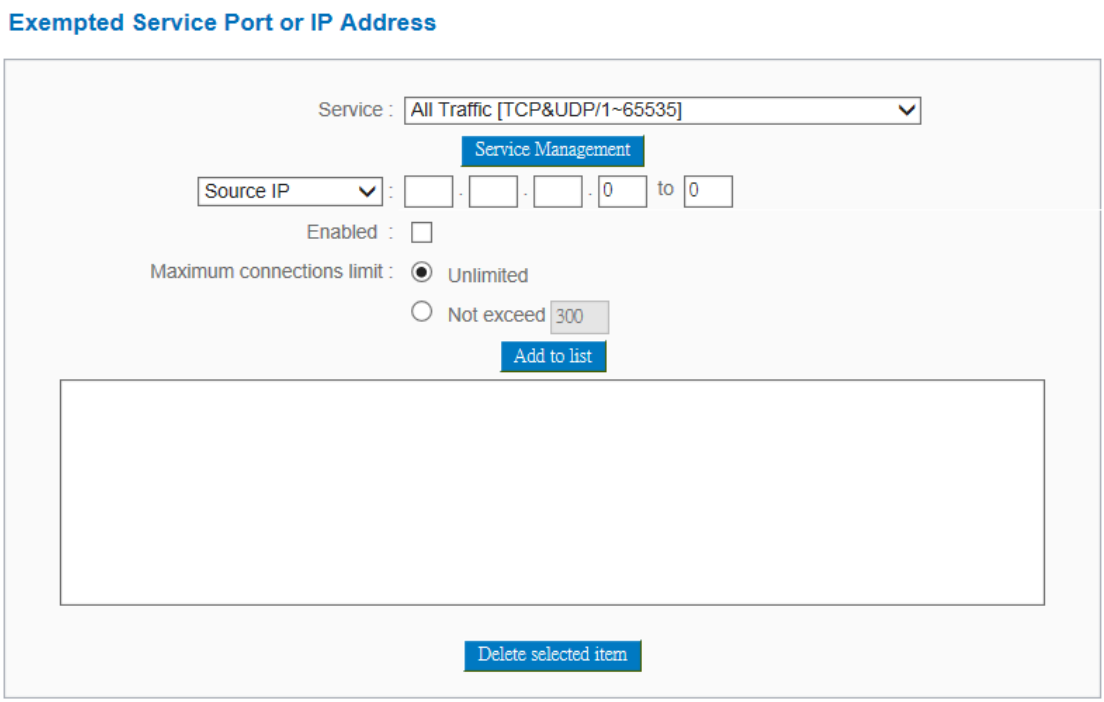
Scheduling: If "**Always**" is selected, the rule will be executed around the clock.

If "**From**…" is selected, the rule will be executed according to the configured time range. For example, if the time control is from Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.

Apply: Click **"Apply"** to save the configuration.

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

Exempted Service Port or IP Address



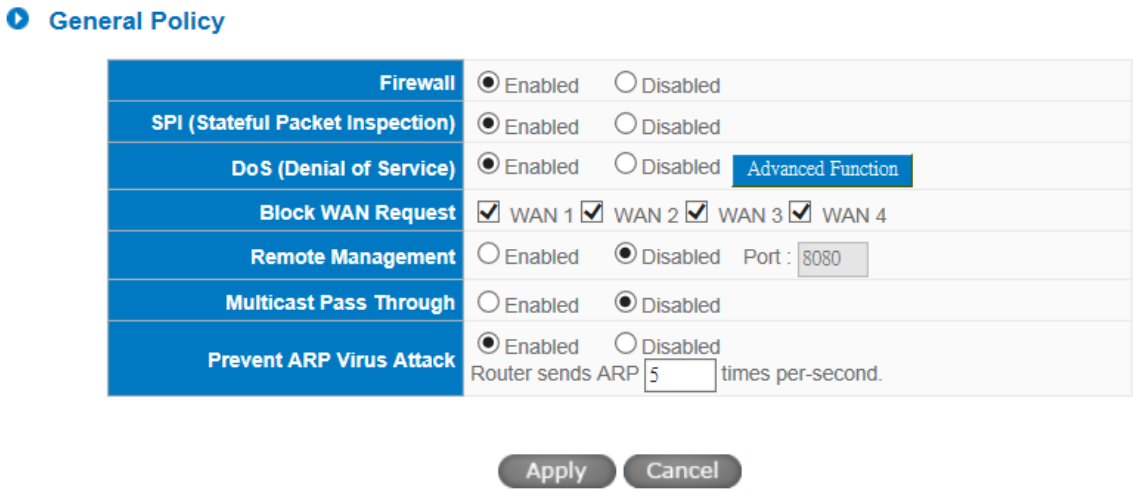
Service Port:	Choose the service port.
IP Address:	Input the IP address range or IP group.
Enabled:	Activate the rule.
Add to list:	Add this rule to the list.
Delete seleted item:	Remove the rules selected from the Service List.
Apply:	Click **"Apply"** to save the configuration.
Cancel:	Click **"Cancel"**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

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.



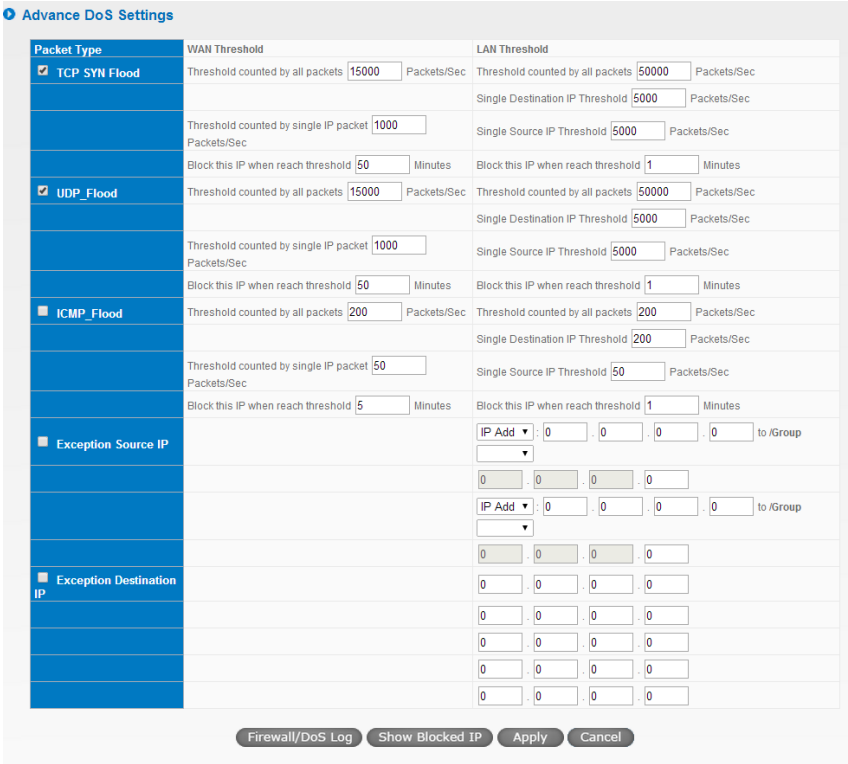
Firewall: This feature allows users to turn on/off the firewall.

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.

Advanced Setting



Packet Type: This device provides three types of data packet transmission: TCP-SYN-Flood, UDP-Flood and ICMP-Flood.

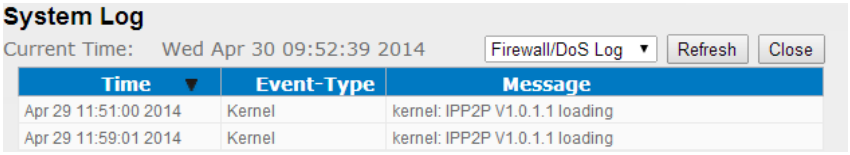
WAN Threshold: When all packet values from external attack or from single external IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes OBJ 176). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.

LAN Threshold: When all packet values from internal attack or from single internal IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.

Exempted Source IP: Input the exempted source IP.

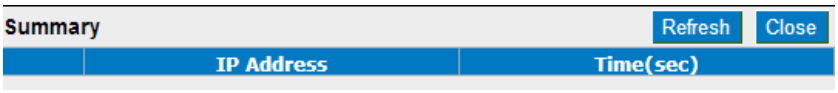
Exempted Dest. IP: Input the exempted Destination IP addresses.

Firewall/DoS Log



Show the Firewall/Log.

Show Blocked IP:



Show the blocked IP list and the remained blocked time.

Restricted WEB Features: It supports the block that is connected through: Java, Cookies, Active X, and HTTP Proxy access.

Don't Block Java / ActiveX / Cookies Proxy to Trusted Domain: If this option is activated, users can add trusted network or IP address into the trust domain, and it will not block items such as Java/ActiveX/Cookies contained in the web pages from the trust domains.

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.

9.2.1 Default Rule

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

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

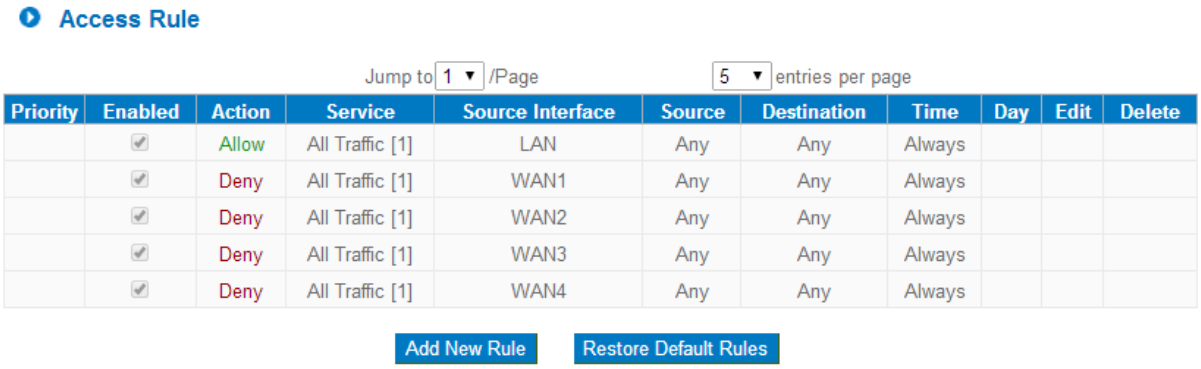
Users may define access rules and do more than the default rules. However, the following four extra service items are always on and are not affected by other user-defined settings.

* HTTP Service (from LAN to Device) is on by default (for management)

* DHCP Service (from LAN to Device) is set to on by default (for the automatic IP retrieval)

* DNS Service (from LAN to Device) is on by default (for DNS service analysis)

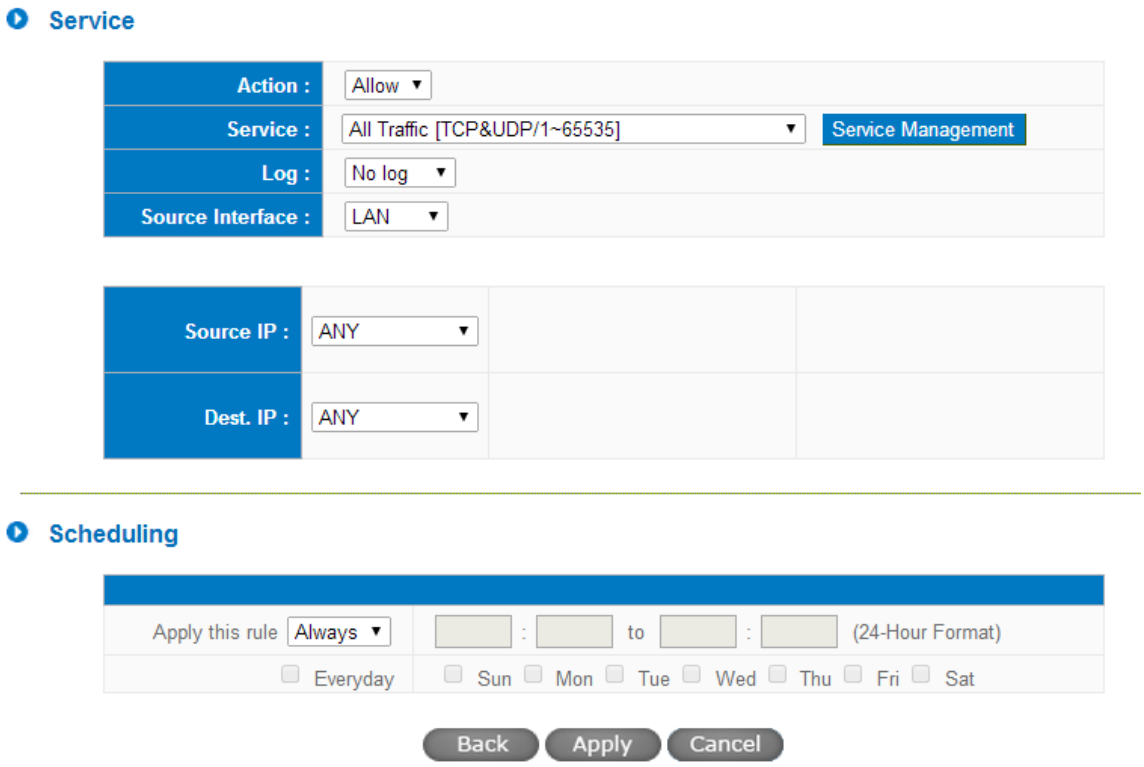
* Ping Service (from LAN to Device) is on by default (for connection and test)



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
Return to Default Rule:	Restore all settings to the default values and delete all the self-defined settings.

9.2.2 Add New Access Rule



Action: Allow: Permits the pass of packets compliant with this control rule.

Deny: Prevents the pass of packets not compliant with this control rule.

Service Port: From the drop-down menu, select the service that users grant or do not give permission.

Service Port Management: If the service that users wish to manage does not exist in the drop-down menu, press – Service Management to add the new service.

From the pop-up window, enter a service name and communications protocol and port, and then click the "Add to list" button to add the new service.

Log: No Log: There will be no log record.

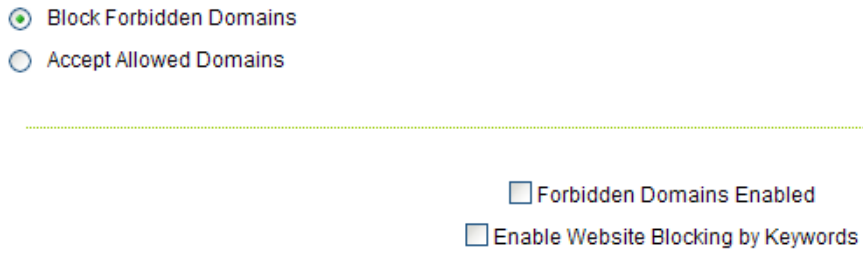
Create Log when matched: Event will be recorded in the log.

Interface: Select the source port whether users are permitted or not (for example: LAN, WAN1, WAN2 or Any). Select from the

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

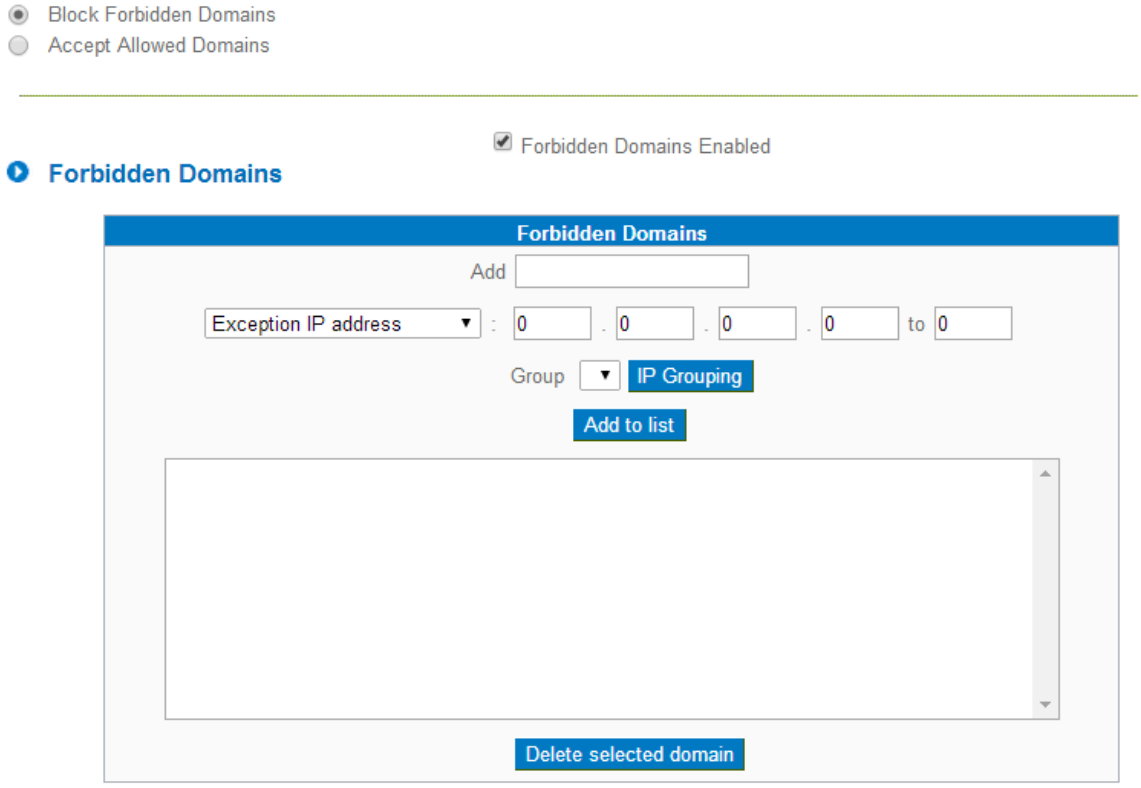
10.3 Content Filter

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 Domain

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



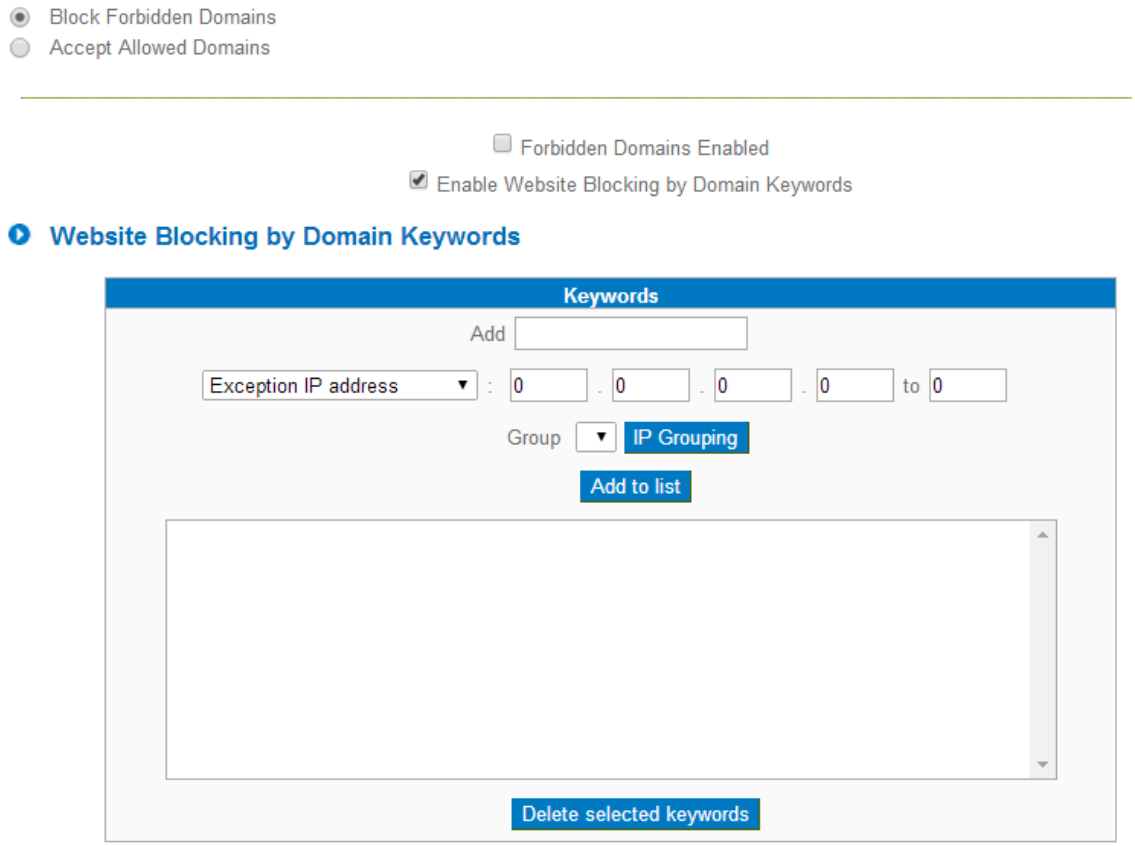
Domain Name: Enter the websites to be controlled such as www.playboy.com

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:



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.

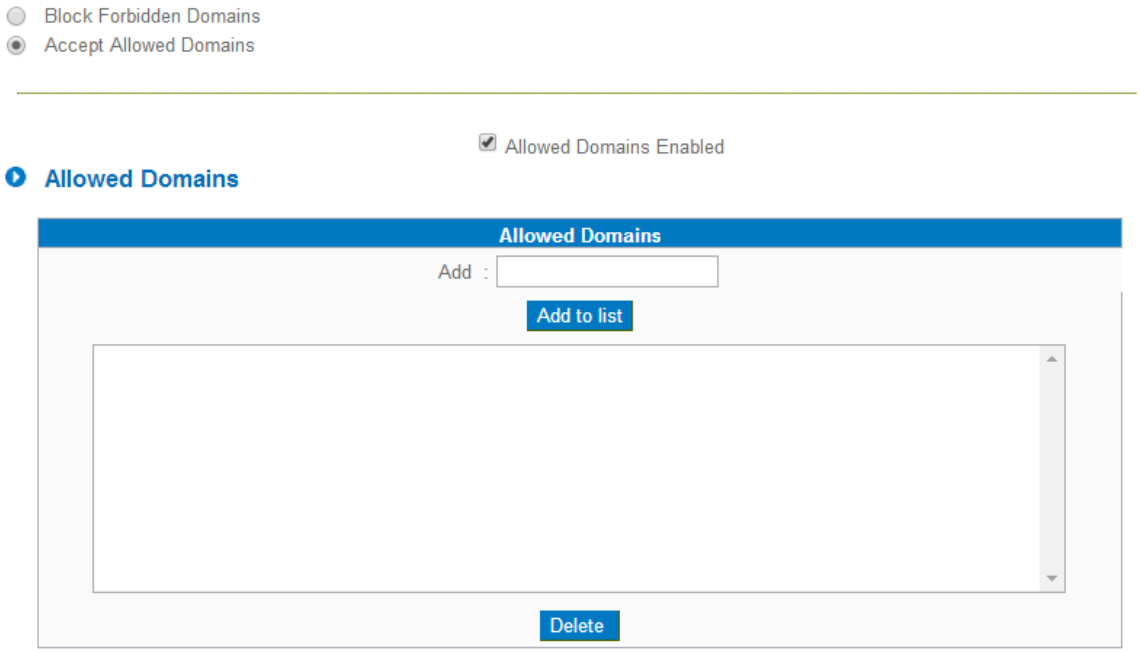
Delete selected item: Delete the service item content from the list

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.



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

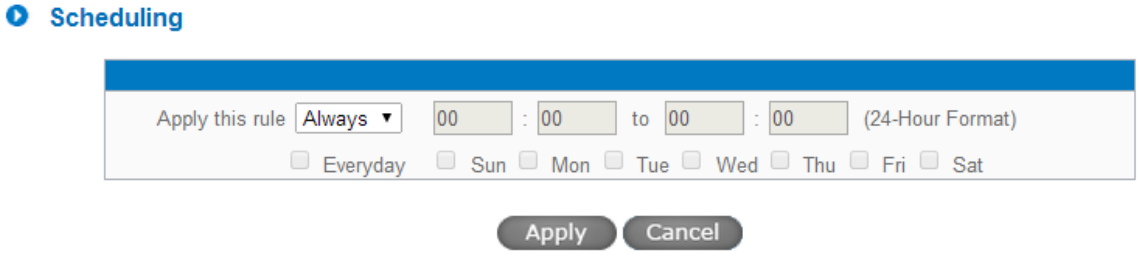
Domain Name: Input the allowed domain name, etc. www.google.com

Add to list: Add the rule to list.

Delete selected item: Users can select one or more rules and click to delete.

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.

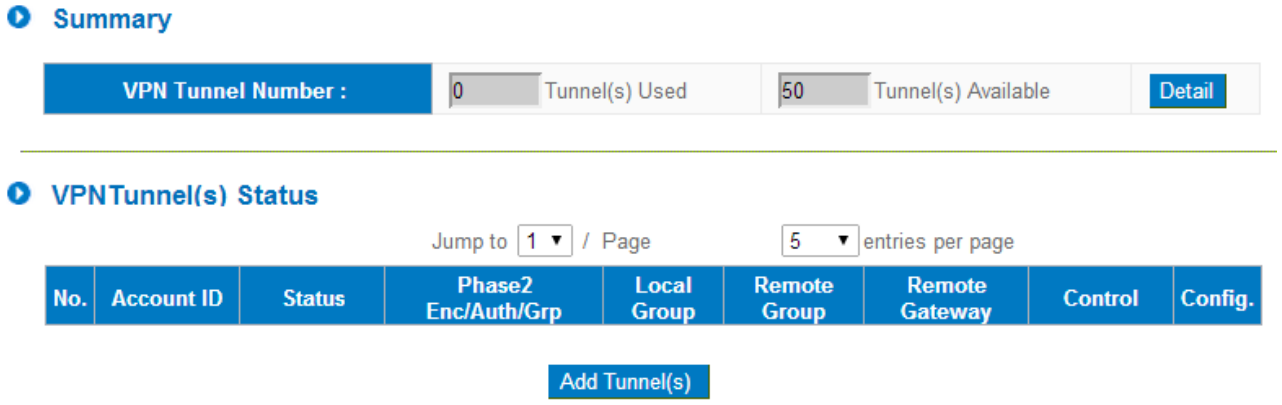


Always: Select **"Always"** to apply the rule on a round-the-clock basis. Select **"from",** and the operation will run according to the defined time.

...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. VPN (Virtual Private Network)



11.1. Add a New VPN Tunnel

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

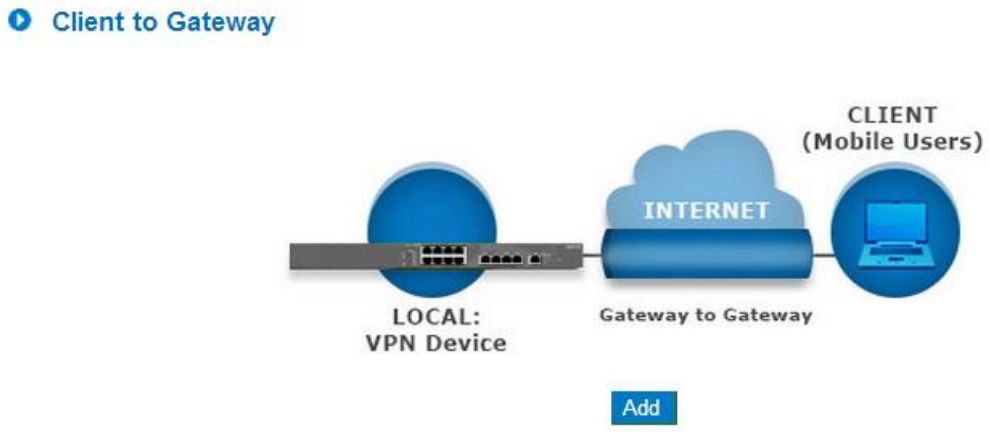
The VPN tunnel connections are done by 2 VPN devices via the Internet. When a new tunnel is added, the setting page for Gateway to Gateway or Client to Gateway will be displayed.

Gateway to Gateway:

Click “Add” to enter the setting page of Gateway to Gateway.

Client to Gateway:

Click “Add” to enter the setting page of Client to Gateway.



10.1.1. Gateway to Gateway Setting

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.

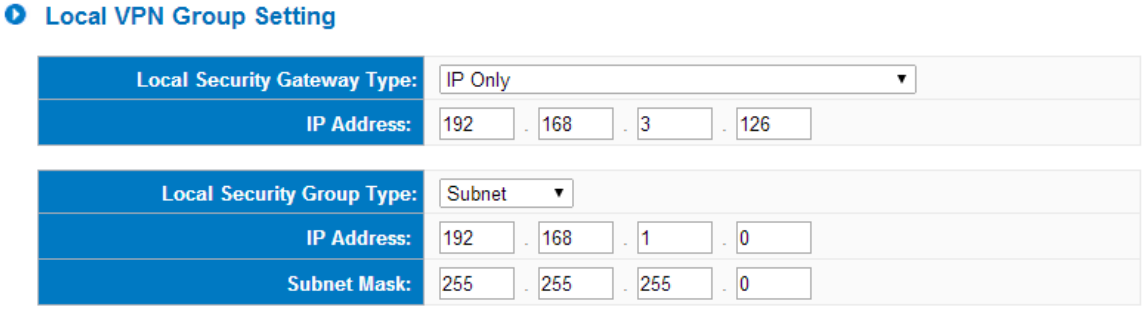
Tunnel Name: Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion.

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:



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

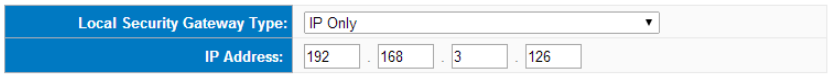
Local Security Gateway Type:

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

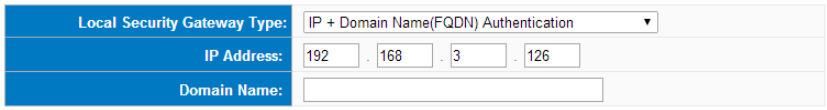
(1) IP only:

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.



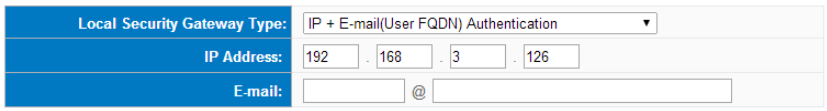
(2) IP + Domain Name(FQDN) Authentication:

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.



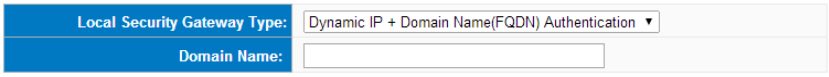
(3) IP + E-mail Addr. (USER FQDN) Authentication.

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.



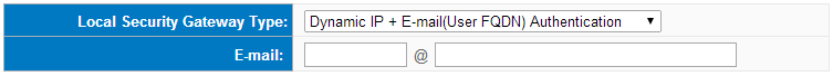
(4) Dynamic IP + Domain Name(FQDN) Authentication:

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.



(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.



Local Security Group Type:

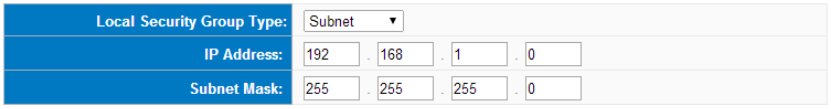
This option allows users to set the local VPN connection access type. The following offers a few items for local settings. Please select and set appropriate parameters:

1. **IP address**
   This option allows the only IP address which is entered to build the VPN tunnel.

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

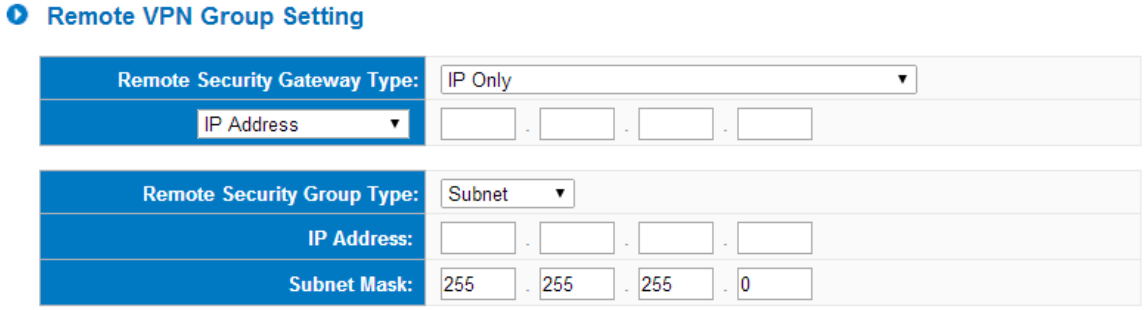
2. Subnet

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



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:



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).

Remote Security Gateway Type:

This remote gateway authentication type comes with five operation modes, which are:
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

(1) IP only:

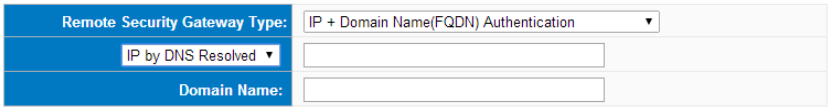
If users select the IP Only type, entering this IP allows users to gain access to this tunnel.

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.

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

If users select IP + domain name, please enter IP address and the domain 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.

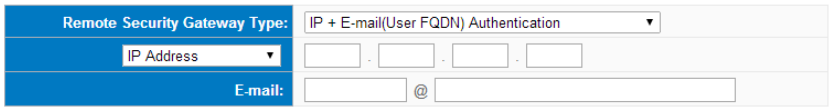
If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translate the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.



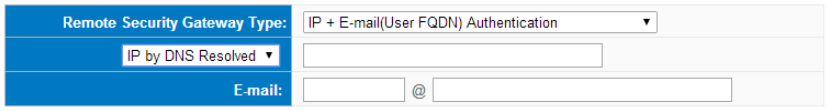
(3) IP + E-mail Addr. (USER FQDN) Authentication:

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.

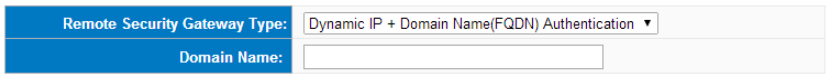


If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translated the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.



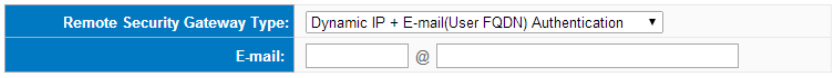
(4) Dynamic IP + Domain Name(FQDN) Authentication:

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 name.



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

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.

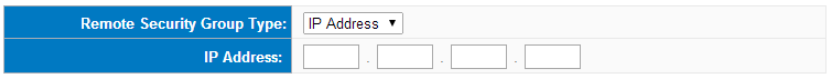


Remote Security Group Type:

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:

(1) **IP address**

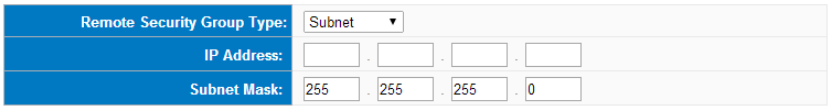
This option allows the only IP address which is entered to build the VPN tunnel.



Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.2.1 can establish connection.

(2) **Subnet**

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



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.

IPSec Setup

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 following two encrypted Key Managements. They are Manual and IKE automatic encryption mode- IKE with Preshared Key (automatic). By using the drop down menu, select the desired encryption mode as illustrated below.

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	☑
Phase2 DHGroup :	Group 1
Phase2 Encryption:	DES
Phase2 Authentication:	MD5
Phase2 SA Life Time:	0 seconds
Preshared Key:	

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. Setting methods include Auto (IKE) or Manual. To do the settings, select any one from the two options.

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	☑
Phase2 DHGroup :	Group 1
Phase2 Encryption:	DES
Phase2 Authentication:	MD5
Phase2 SA Life Time:	0 seconds
Preshared Key:	

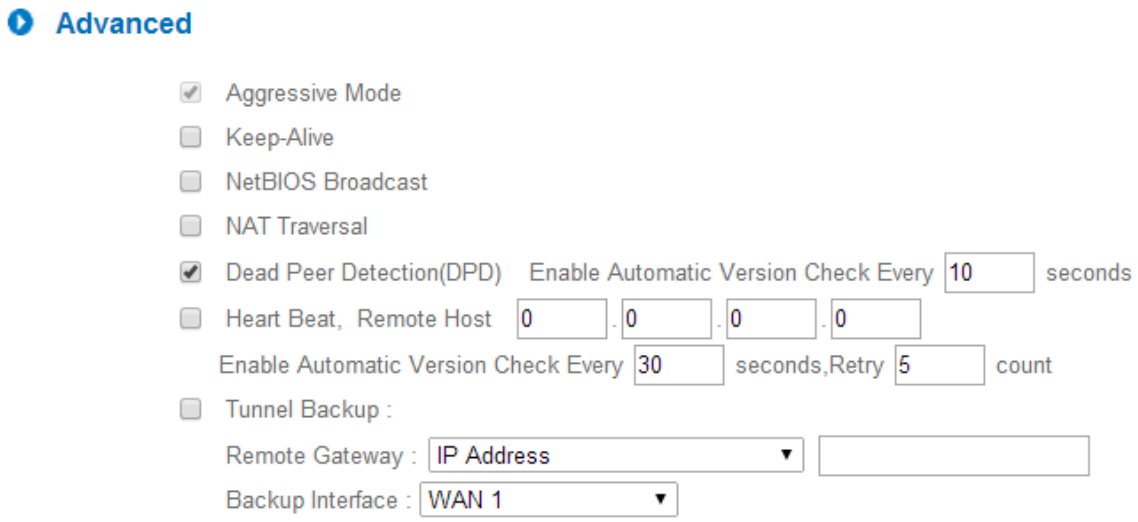
Use IKE Protocol:

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



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.
- 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.
- 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.

- VPN Tunnel backup:

VPN tunnel backup can be configured in Advanced settings under IPSec Settings. If configured, the VPN connection will be preserved as when the primary VPN Tunnel is broken, the VPN connection will revert to the backup settings.

VPN Tunnel backup requires two settings:

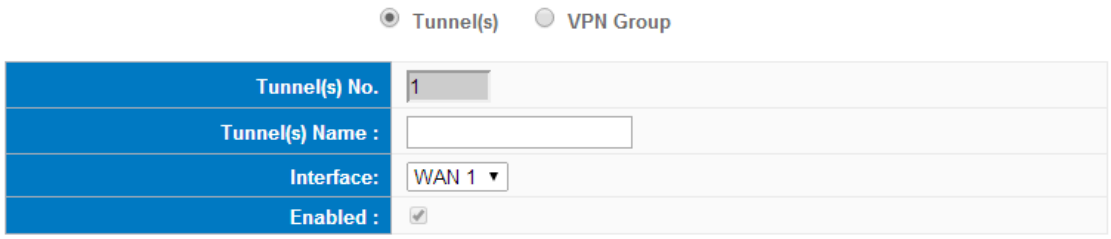
Remote Gateway: select and input IP or hostname of remote gateway. If the remote gateway uses FQDN or E-mail authentication methods, choose “Same with Primary tunnel Setup”.
Backup Interface: the interface that the backup tunnel will use, can either be

wired or USB connection.

10.1.2. 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 or by a group of clients (Group VPN,future) 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.

（1）Situation in Tunnel:



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

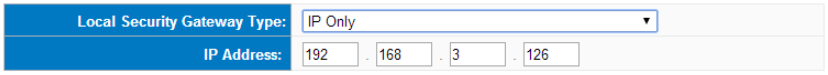
This local gateway authentication type (Local Security Gateway Type) must be identical with that of the remote type (Remote Security Gateway Type).

Local Security Gateway Type:

This local gateway authentication type comes with five operation modes, which are:
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

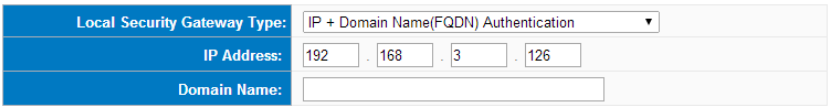
(1) IP only:

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.



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

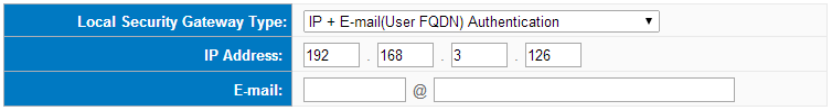
If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com.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



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

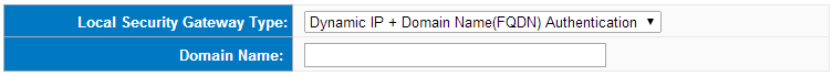
If users select IP address and E-mail, enter the IP address

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.



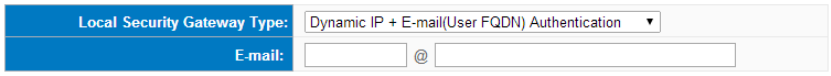
(4) Dynamic IP + Domain Name(FQDN) Authentication:

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.



(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.



Local Security Group Type:

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:

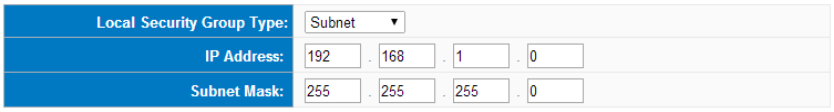
1. **IP address**

   This option allows the only IP address which is entered to build the VPN tunnel.

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

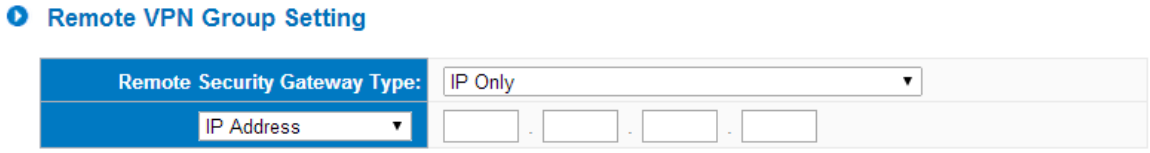
2. Subnet

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



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:



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).

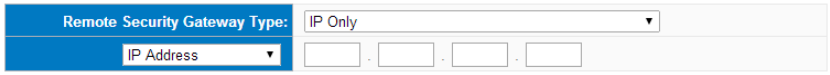
Remote Security Gateway Type:

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

(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.

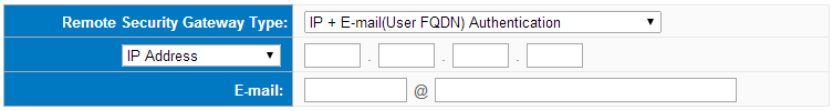


(2) IP + Domain Name(FQDN) Authentication:

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.

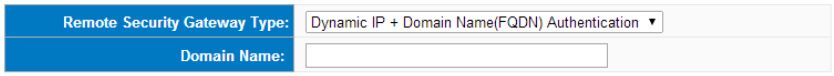
(3) IP + E-mail Addr. (USER FQDN) Authentication.

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.



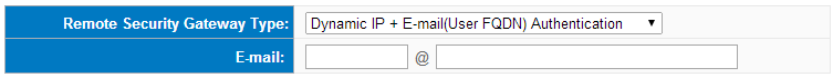
(4) Dynamic IP + Domain Name(FQDN) Authentication:

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.

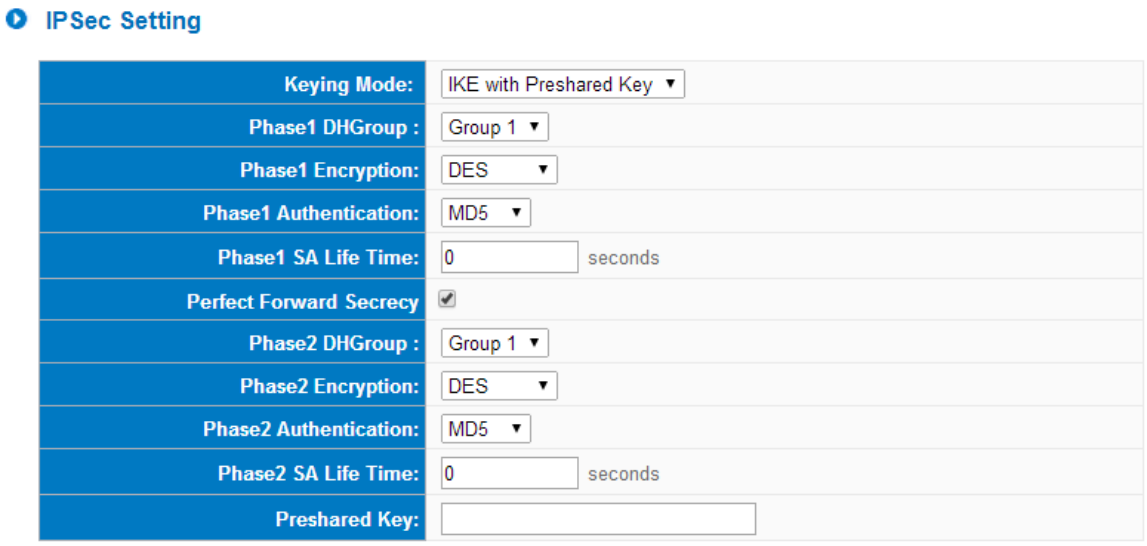


(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.

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.



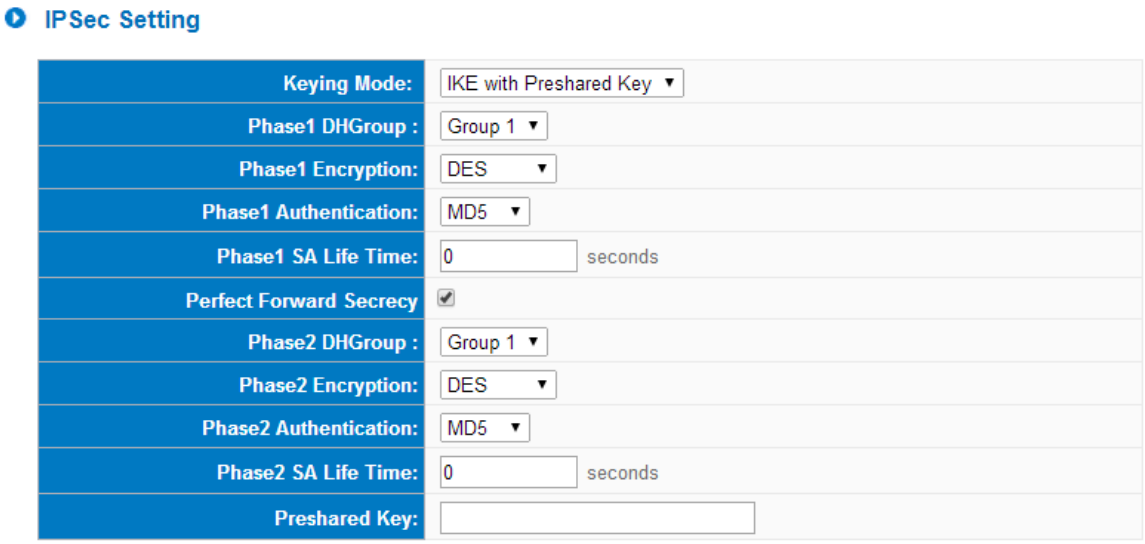
IPSec Setup



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 following two encrypted Key Managements. They are Manual and 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. Setting methods include Auto (IKE) or Manual. To do the settings, select any one from the two options.



IKE Protocol:

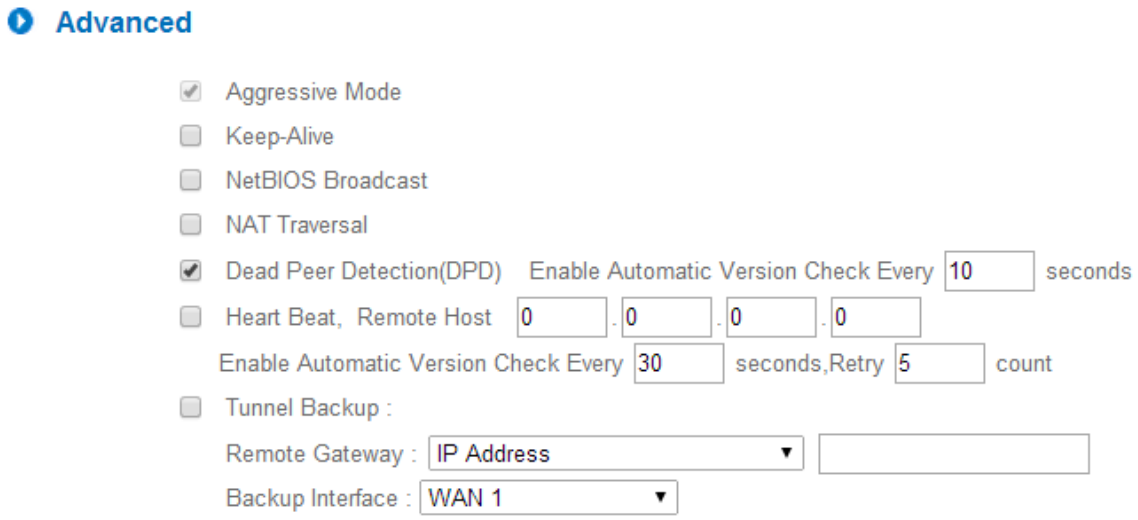
Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the 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 Preshareed Key Only



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.
- 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.
- 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.

- VPN Tunnel backup:

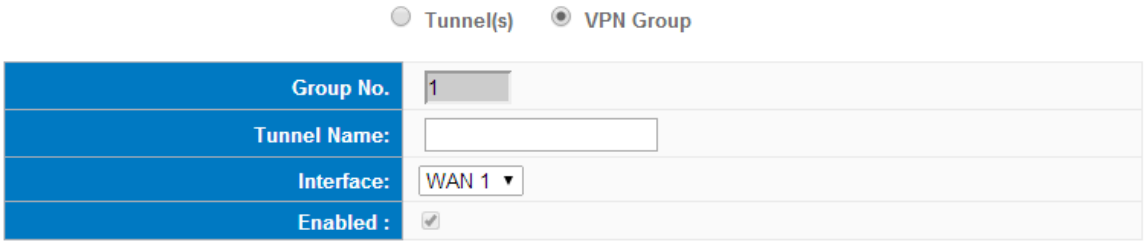
  VPN tunnel backup can be configured in Advanced settings under IPSec Settings. If configured, the VPN connection will be preserved as when the primary VPN Tunnel is broken, the VPN connection will revert to the backup settings.

  VPN Tunnel backup requires two settings:

  Remote Gateway: select and input IP or hostname of remote gateway. If the remote gateway uses FQDN or E-mail authentication methods, choose "Same with Primary tunnel Setup".

  Backup Interface: the interface that the backup tunnel will use, can either be wired or USB connection.

Situation in Group VPN:



Group No.: Two Group VPN settings at most.

Group 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 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 list, users can select the Interface for this VPN tunnel.

Enabled: Click to **Enabled** the VPN tunnel. This option is set to Enabled by default. After the set up, users may select to activate this tunnel feature.

Local Group Setup:

Local Security Group Type:

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:

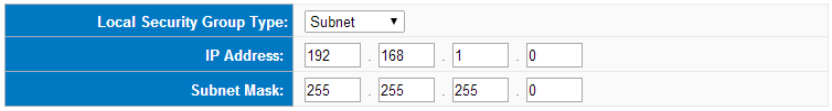
3. **IP address**

   This option allows the only IP address which is entered to build the VPN tunnel.

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

4. Subnet

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



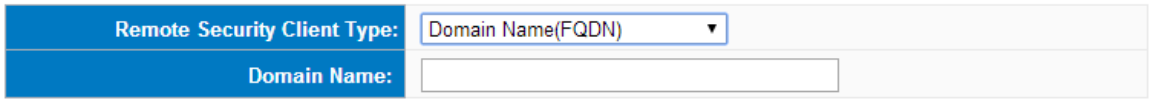
Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

5. IP Range

This option allows connection only when IP address range which is entered after the VPN tunnel is connected.

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 ~254 can establish connection.

Remote Group Setup



Remote Security client Type: This setting offers three operation modes, which are:

Domain Name (FQDN)

E-mail Address (USER FQDN)

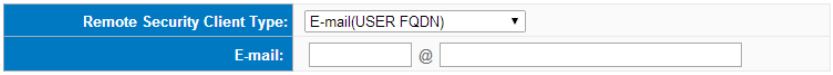
Microsoft XP/2000 VPN Client

(1) Domain Name(FQDN)

If users select Domain Name type, please enter the domain name to be authenticated. FQDN refers to the combination of host name and domain name that are available on the Internet (i.e. vpn.Server.com).The domain name must be identical to the status setting of the client end to establish successful connection.

(2) E-mail Addr. (USER FQDN)

If users select this option, only filling in the E-mail address allows access to this tunnel.



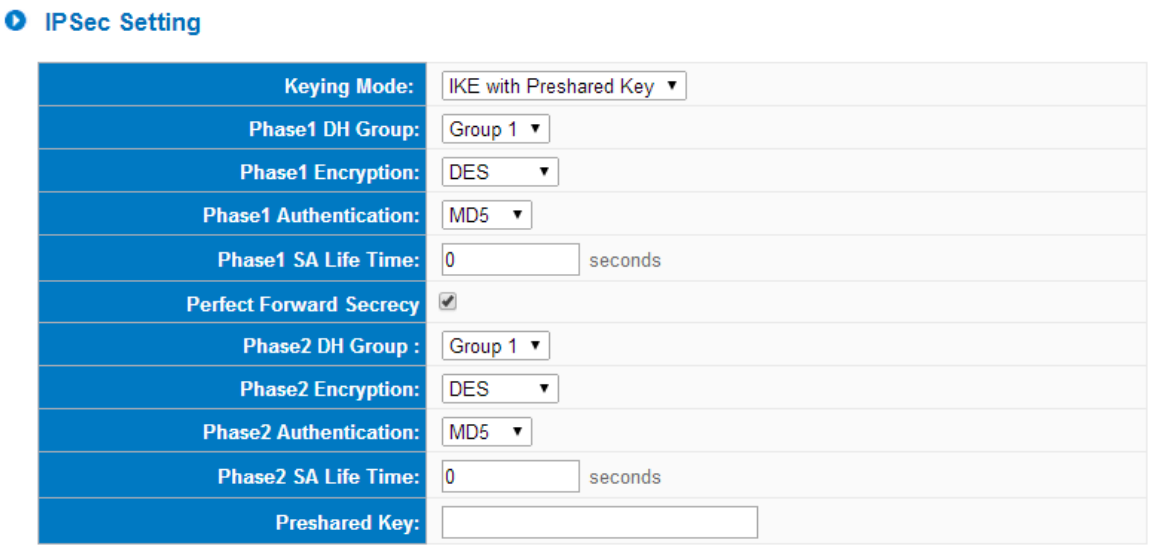
(3) Microsoft XP/2000 VPN Client

If users select XP/2000 VPN Client end status, users don't need to do extra settings.

IPSec Setup

If there is any encryption mechanism, the encryption mechanism of these two VPN channel settings must be identical in order to establish connection. And the transmission data must be encrypted with IPSec key, which is also known as the encryption "key". The device provides the following two types of encryption management modes: Manual and IKE automatic encryption mode- IKE with Preshared Key (automatic). If the Group VPN is selected or the dynamic IP address of the Remote Security Gateway Type is applied, Aggressive Mode will be enabled automatically without the option of Manual mode.

Encryption Management Protocol:

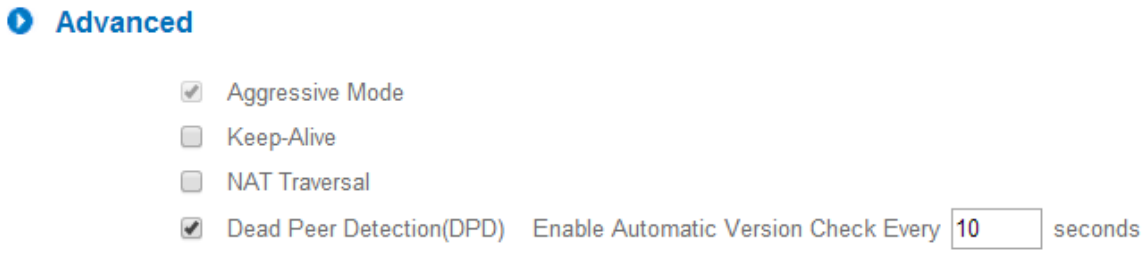


- **Perfect Forward Secrecy:** When users check the PFS option, make sure to activate the PFS feature of the VPN device and that VPN Client as well.
- **Phase 1/Phase 2 DH Group:** This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
- **Phase1/Phase2 Encryption:** This option allows users to set this VPN channel 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”.

- **Phase1 SA Life Time:** The life time for this exchange code is 28800 seconds (or 8 hours) by default. This allows the automatic generation of other exchange passwords 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 3600 seconds (or 1 hour) by default. This allows the automatic generation of other exchange passwords 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 character 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 Preshared Key Only



The advanced settings include Main Mode and Aggressive mode. In Main mode, the default setting is VPN operation mode. The connection is the same as most of the VPN device.

- 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.
- Keep Alive: If this option is selected, VPN channel 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.
- 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

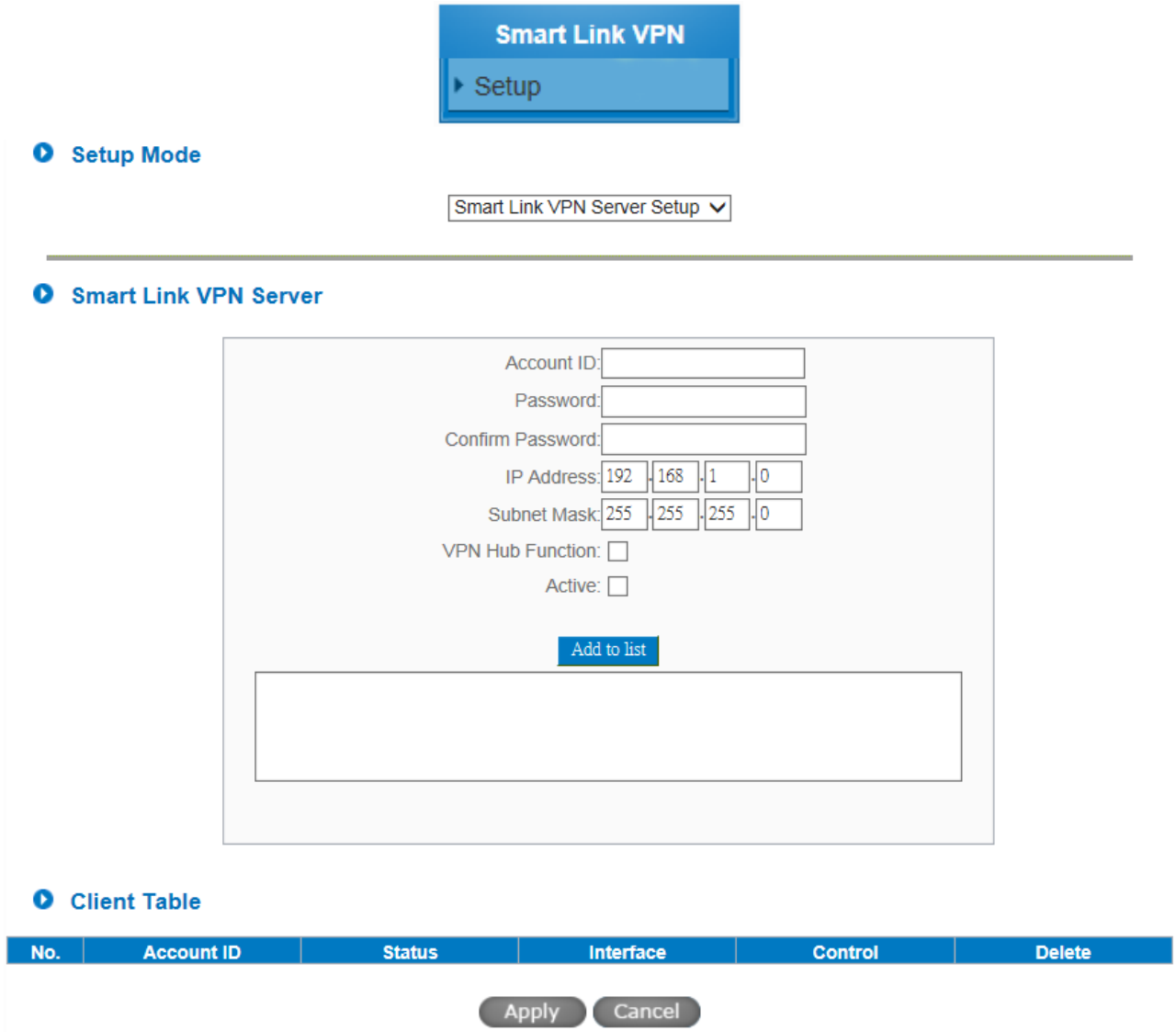
11.2. SmartLink VPN Function Setup

SmartLink VPN devices provide three major convenient functions:

1. **SmartLink 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.

11.3.1. SmartLink Server Settings

Select SmartLink Feature as Server mode：



Account ID： Must be identical to that of the remote client end. Please enter the remote client user name in either English or Chinese.

Password： Must be identical to that of the remote client end.

Confirm Password： Please enter the password and confirm again.

IP Address： Refers to the specific network IP address and subnet mask,

Subnet Mask： which has to build connection with the remote client end.

VPN Hub Function：	After branch and headquarter are connected, branches can access each other easily without having other tunnels.
Enabled：	Enable this account.
Add to list：	Add a new account and password.
Delete selected item：	Delete the selected user.

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

11.3.2. SmartLink Status

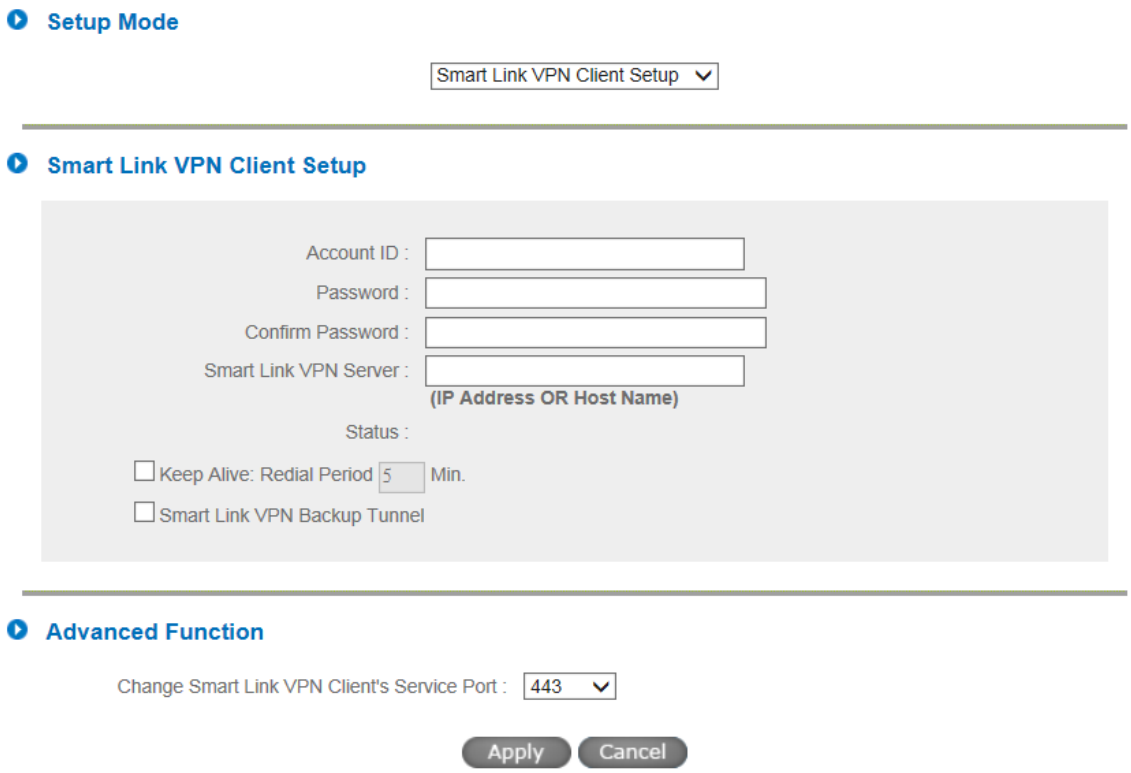
Client Table

No.	Account ID	Status	Interface	Control	Delete

Account：	Displays the remote client user. Green means connection, blue waiting for connection and red for SmartLink disconnection.
Status：	Displays the SmartLink VPN connection status. Red means disconnection and green means connection.
Interface：	Shows which WAN port is applied to connect to this remote SmartLink.
Start Time：	Shows the starting time of SmartLink.
End Time：	Shows the ending time of SmartLink.
Duration：	Shows the total time used from the Start to the End of this SmartLink.
Control：	Shows the status of this SmartLink: waiting for connection (**Waiting**), stop the connection (**Disconnect**), and **Disable** this feature/ **Enable** this SmartLink to enter the status of waiting for connection.
Config.：	Click Edit to enter the setting items to be changed.

11.3.3. SmartLink Client Settings

Select SmartLink feature as Client mode：



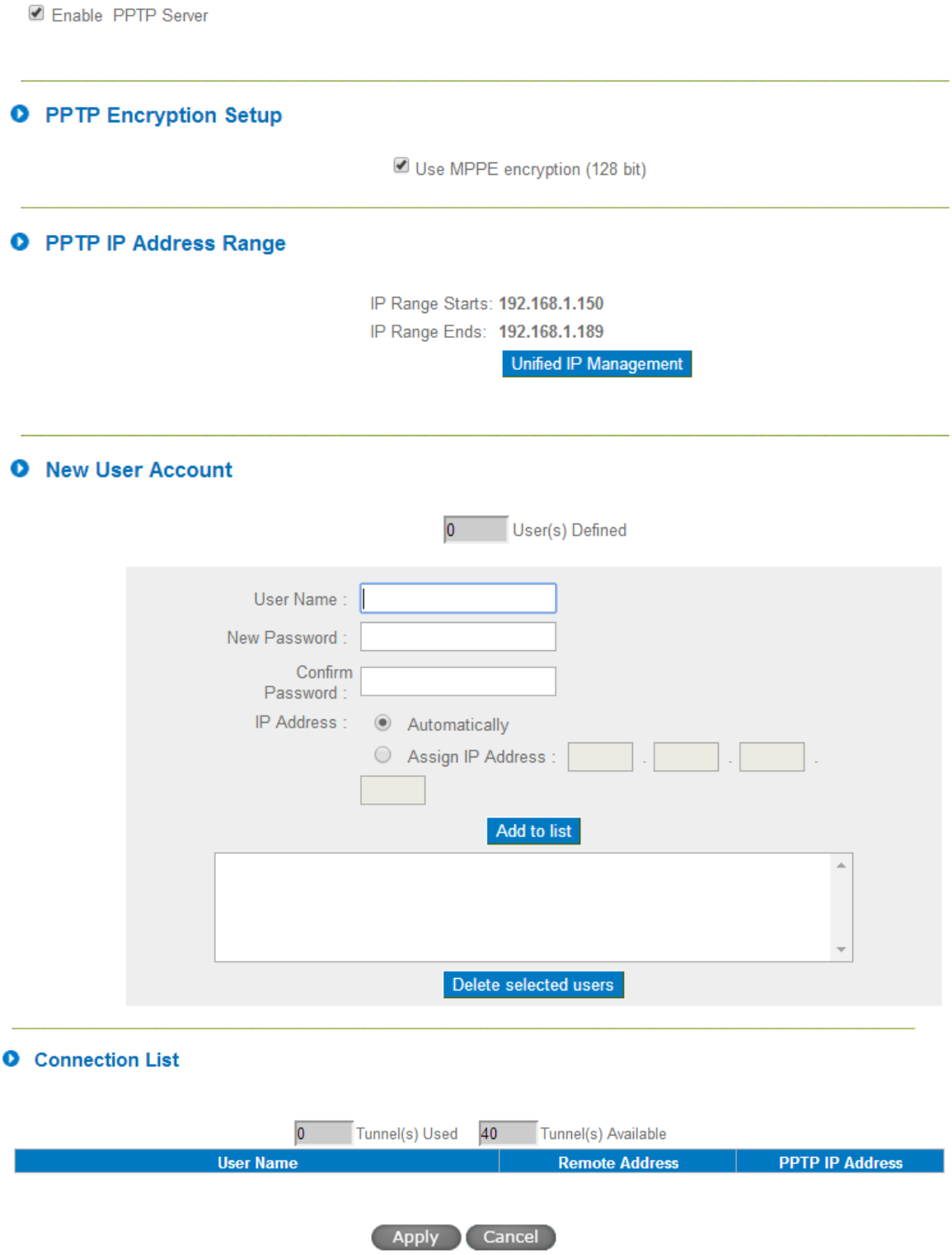
Account ID：	Must be identical to that of the server account ID.
Password：	Must be identical to that of the server password.
Confirm Password：	Please enter the password and confirm again.
SmartLink VPN（IP Address or Dynamic Domain Name）：	Input SmartLink VPN Server IP address or domain name.
Status：	Displays QVN connection status.
Keep Alive: Redial Period 5 Mins：	This function is to set re- connect duration if SmartLink contention drops. The range is 1~60 mins.
SmartLink 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 SmartLink Client's Service Port：	In some environment, port 443 has been used, for example, E-Mail Forwarding. To avoid the conflict with SmartLink, SmartLink 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.

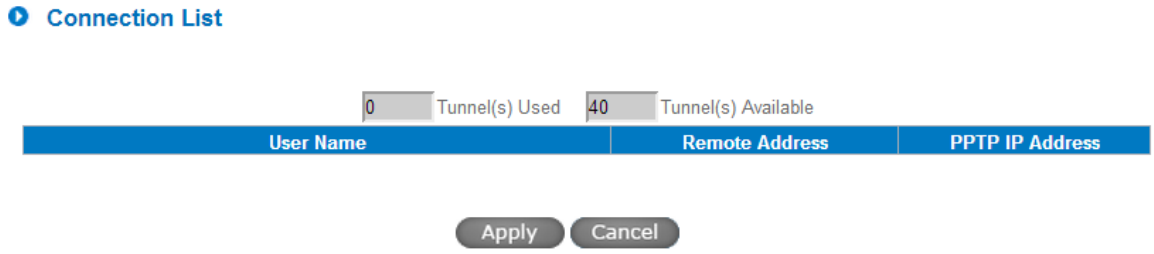
11.3. PPTP Setting

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



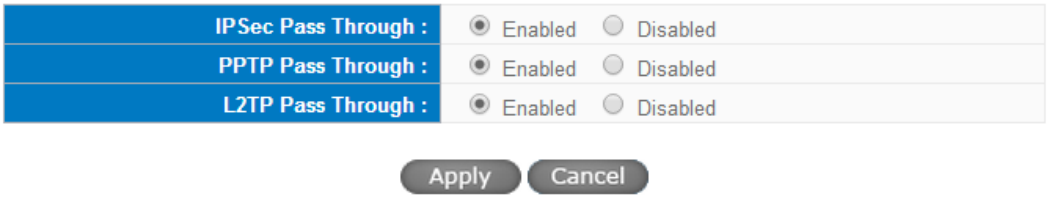
Enabled PPTP Server:	When this option is selected, the point-to-point tunnel protocol PPTP server can be enabled.
PPTP Client IP Range:	Please enter PPTP IP address range so as to provide the remote users with an entrance IP into the local network. Enter Range Start: Enter the value into the last field. Enter Range End: Enter the value into the last field.
Username:	Please enter the name of the remote user.
Password:	Enter the password and confirm again by entering the new password.
Confirm Password:	
Add to list:	Add a new account and password.
Delete selected item:	Delete Selected Item.

All PPTP Status:Displays all successfully connected users, including username, remote IP address, and PPTP address.



11.4. VPN Pass Through

VPN Pass Through



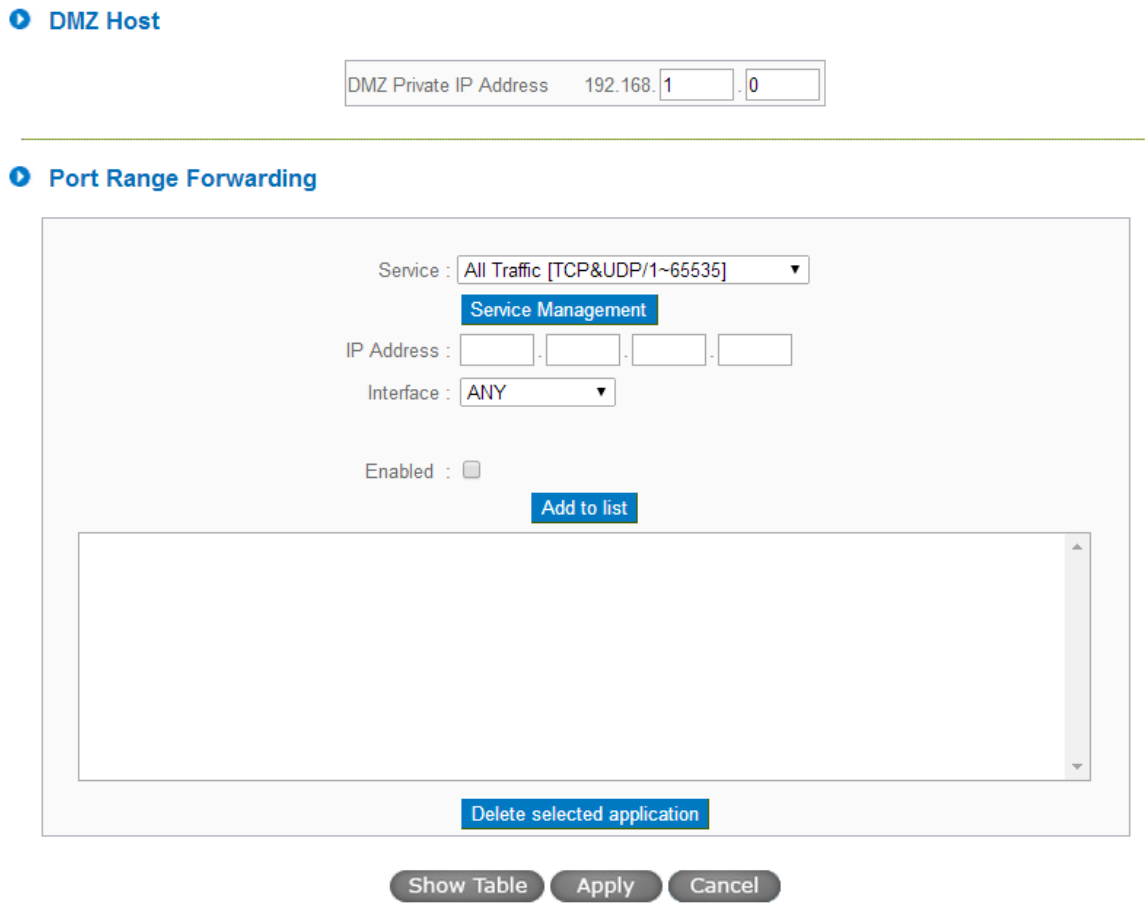
IPSec Pass Through: If this option is **enabled**, the PC is allowed to use VPN-IPSec packet to pass in order to connect to external VPN device.

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.

XII. Advanced Function

12.1 DMZ Host/ Port Range Forwarding



12.1.1 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.

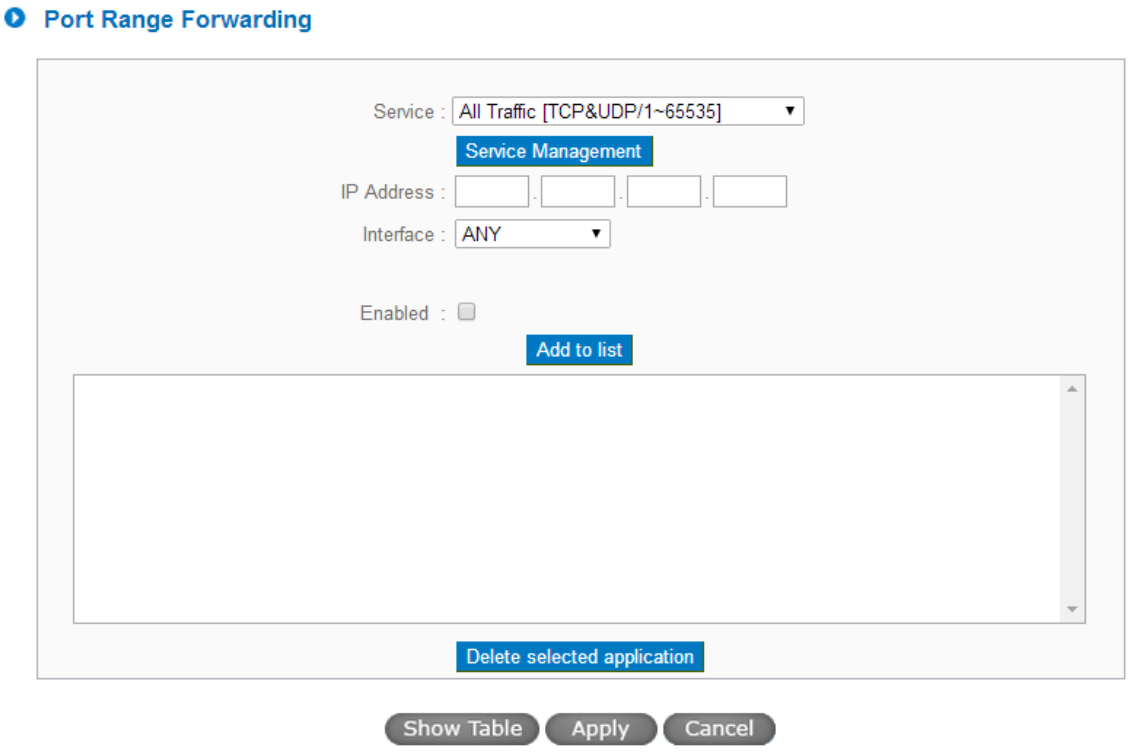
After the changes are completed, click “Apply” to save the network configuration modification, or click “Cancel" to leave without making any changes.

12.1.2 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.

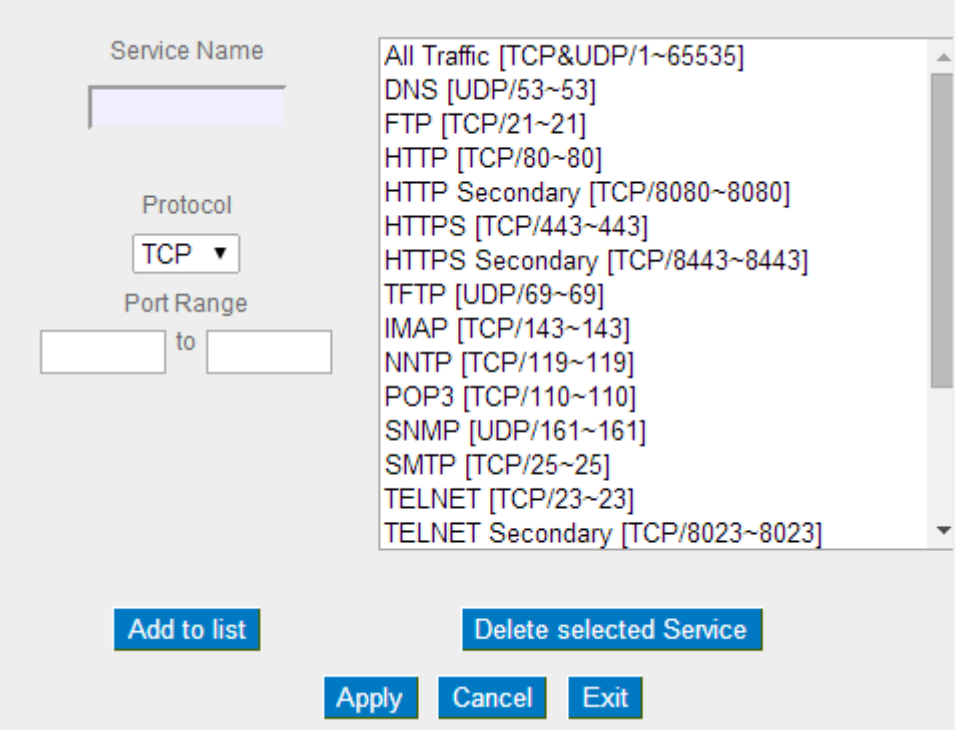


Service: To select from this option the default list of service ports of the virtual host that users want to activate.
Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and 21~21 for FTP. Please refer to the list of default service ports.

Internal IP Address:	Input the virtual host IP address.
Interface:	Select the WAN port.
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:

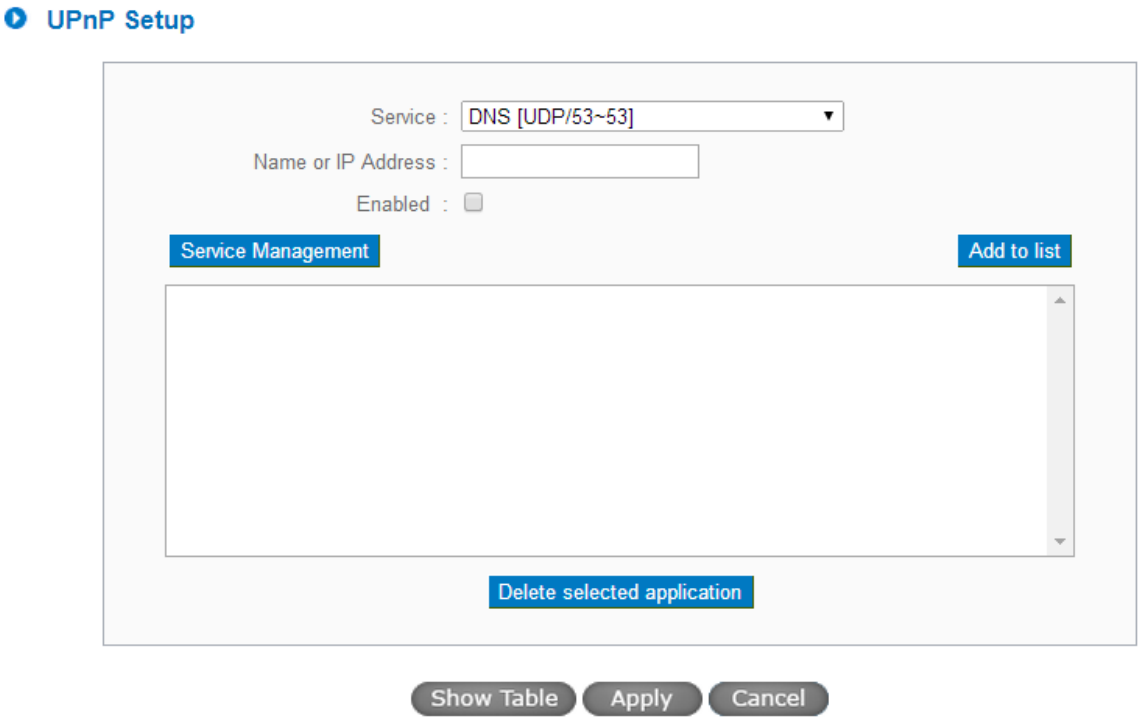


Service Name:	Input the name of the service port users want to activate on the list, such as E-donkey, etc.
Protocol:	To select whether a service port is TCP or UDP.
Port Range:	To activate this function, input the range of the service port locations users want to activate.

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

12.2 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.



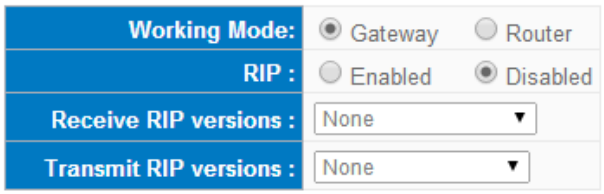
Service Port:	Select the UPnP service number default list here; for example, WWW is 80~80, FTP is 21~21. Please refer to the default service number list.
Host Name or IP Address:	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.
Enabled:	Activate this function.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

12.3 Routing

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

Dynamic Routing

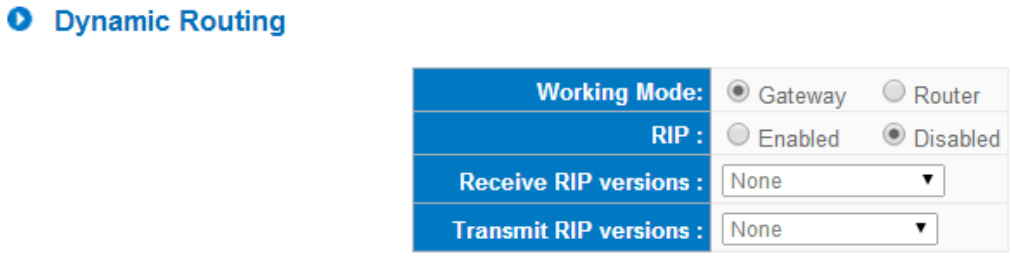


Static Routing

11.3.1 Dynamic Routing

The abbreviation of Routing Information Protocol is RIP. There are two kinds of RIP in the IP environment – RIP I and RIP II. Since there is usually only one router in a network, ordinarily just Static Routing will be used. RIP is used when there is more than one router in a network, and if an administrator doesn't want to assign a path list one by one to all of the routers, RIP can help refresh the paths.

RIP is a very simple routing protocol, in which Distance Vector is used. Distance Vector determines transmission distance in accordance with the number of routers, rather than based on actual session speed. Therefore, sometimes it will select a path through the least number of routers, rather than through the fastest routers.



Working Mode: Select the working mode of the device: NAT mode or Router mode.

RIP: Click "Enabled" to open the RIP function.

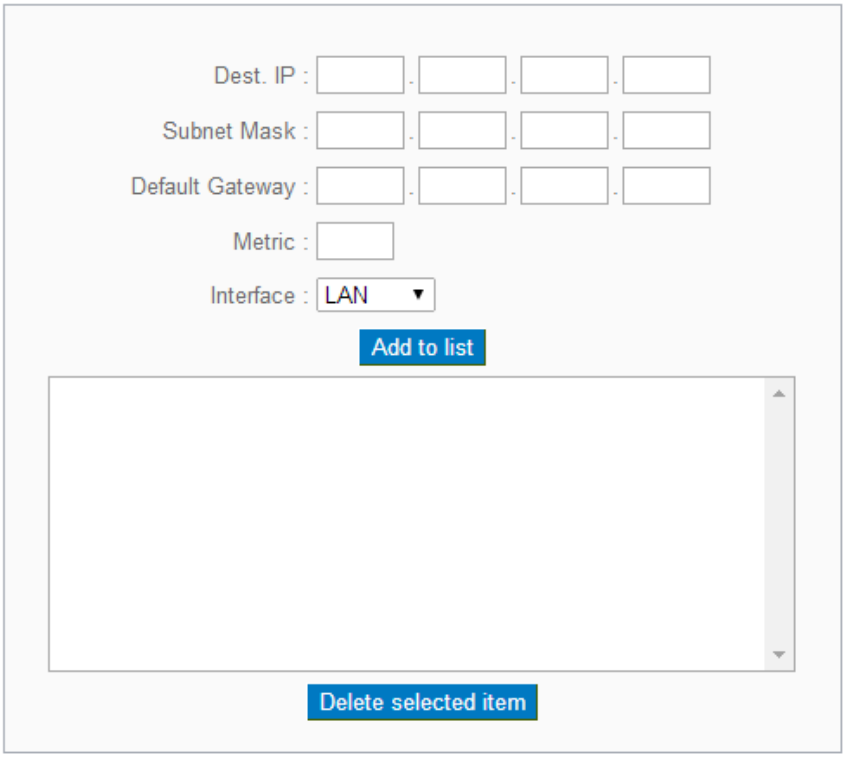
Receive RIP versions: Use Up/Down button to select one of "**None**， **RIPv1**，**RIPv2**，**Both RIPv1 and v2**" as the "**TX**" function for transmitting dynamic RIP.

Transmit RIP versions: Use Up/Down button to select one of "**None**，**RIPv1**，**RIPv2-Broadcast**，**RIPv2-Multicast**" as the "**RX**" function for receiving dynamic RIP.

11.3.2 Static Routing

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

Static Routing



Dest. IP:	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.

12.4 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

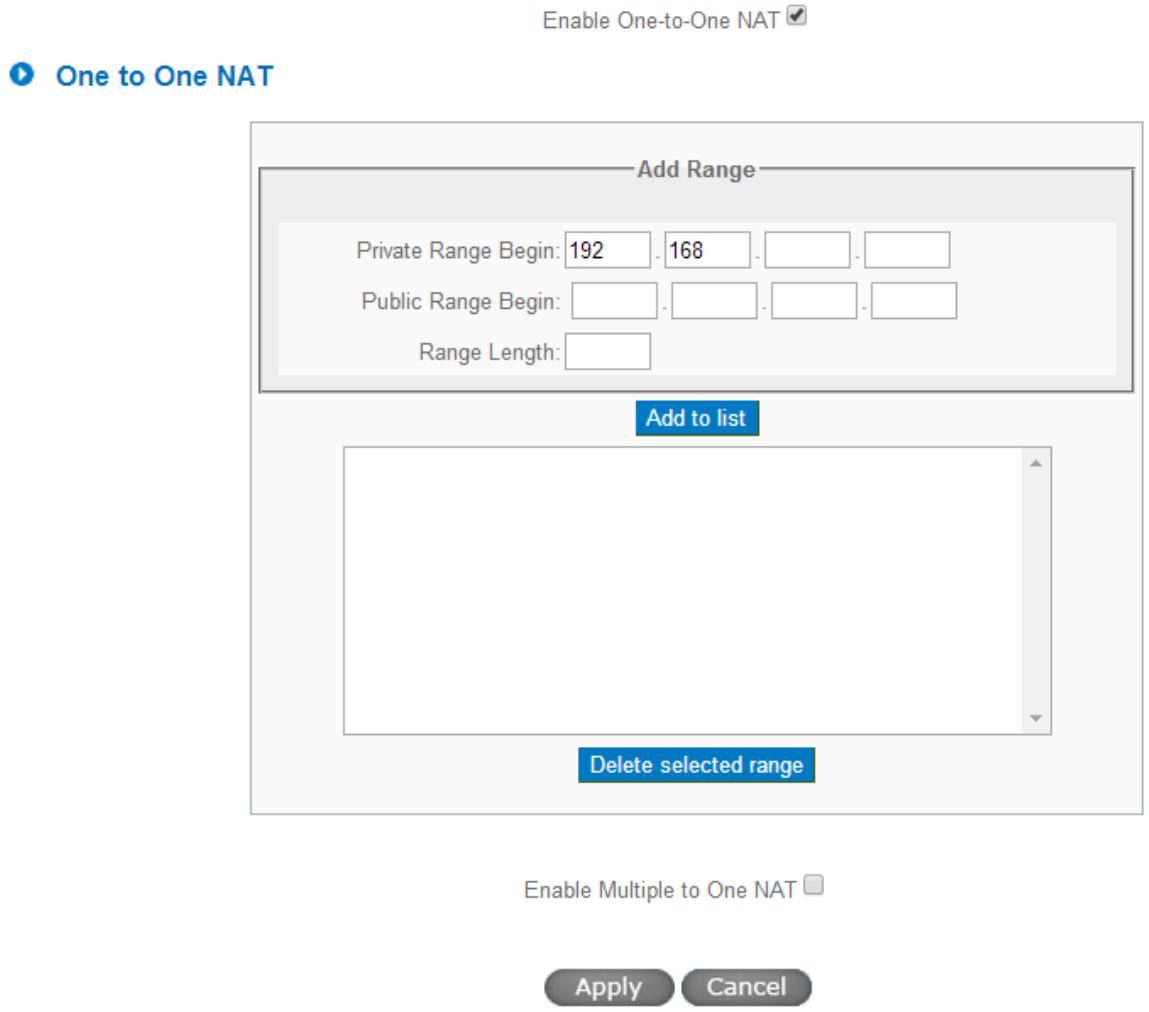
210.11.1.3→ 192.168.1.4

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.



Enabled One to One NAT: To activate or close the One-to-One NAT function. (Check to activate the function).

Private IP Range Begin: Input the Private IP address for the Intranet One-to-One NAT function.

Public IP Range Begin: Input the Public IP address for the Internet One-to-One NAT function.

Range Length: The numbers of final IP addresses of actual Internet IP addresses. (Please do not include IP addresses in use by WANs.)

Add to List: Add this configuration to the One-to-One NAT list.

Delete Selected Item: Remove a selected One-to-One NAT list.

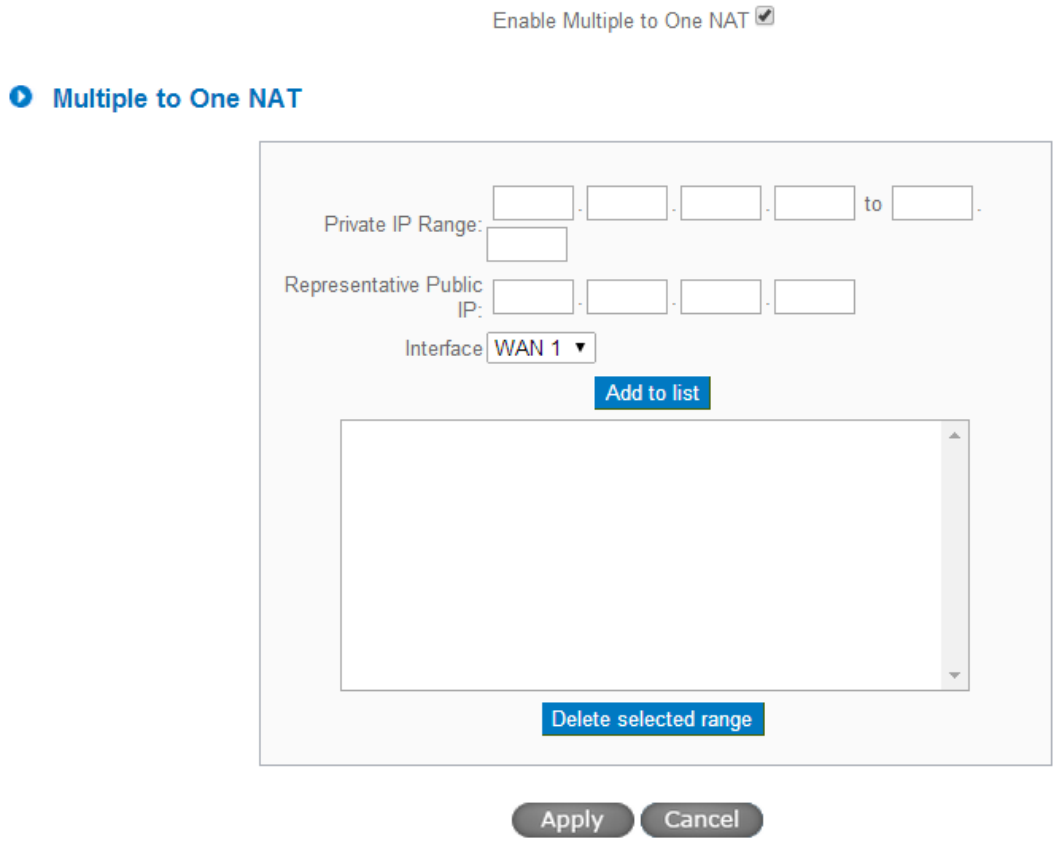
Apply: Click **"Apply"** to save the network configuration modification.

Cancel: Click **"Cancel"** to leave without making any changes.

Attention !

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.

Multiple to One NAT

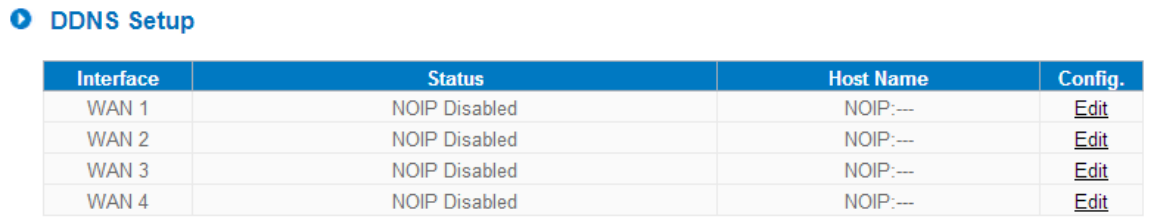


Enable Multiple to One NAT	Click to enable multiple to one NAT function.
Private IP Range	Input intranet IPs for NAT mapping.
Respective Public IP	Input the respective public IP addresses. This should go along with the following interface selection. If the IP address is not within the interface ranges,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

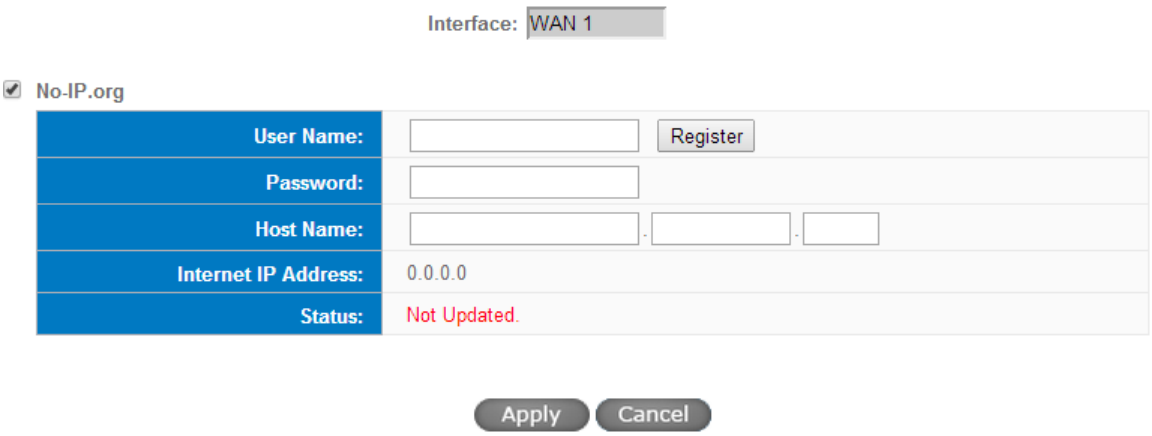
Add to List	Add this configuration to the One-to-One NAT list.
Delete selected range	Remove a selected One-to-One NAT list.
Apply	Click **"Apply"** to save the network configuration modification.
Cancel	Click **"Cancel"** to leave without making any changes.

12.5 DDNS- Dynamic Domain Name Service

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 NOIP DDNS.



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.



Username	The name which is set up for DDNS.
Password	The password which is set up for DDNS.
Host Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.
Internet IP Address	Input the actual dynamic IP address issued by the ISP.
Status	An indication of the status of the current IP function refreshed by DDNS.

12.6 MAC Clone

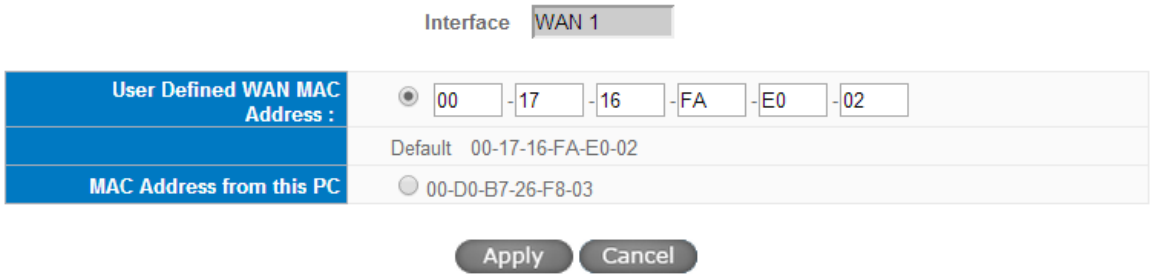
Some ISP will request for a fixed MAC address (network card physical address) for distributing IP address, which is mostly suitable for cable mode users. Users can input the network card physical address (MAC address: 00-xx-xx-xx-xx-xx) here. The device will adopt this MAC address when requesting IP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

MAC Clone

Interface	MAC Address	Config.
WAN 1	00-11-22-FA-E0-02	Edit
WAN 2	00-11-22-FA-E0-03	Edit
WAN 3	00-11-22-FA-E0-04	Edit
WAN 4	00-11-22-FA-E0-05	Edit

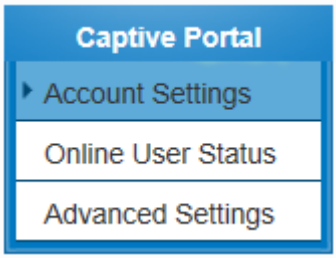
Select the WAN port to which the configuration is to be edited; click the hyperlink to enter and edit its configuration. Users can input the MAC address manually. Press “Apply” to save the setting, and press “Cancel” to remove the setting.

Default MAC address is the WAN MAC address.



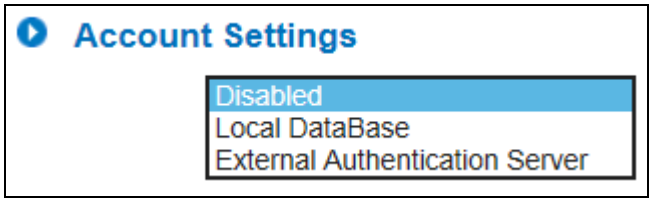
12.7 Captive Portal

Captive Portal forces all internal LAN PCs to enter an account and password before having access to the internet. Effectively enables administrators the control of who has internet access and who does not.



12.7.1 Enable Captive Portal:

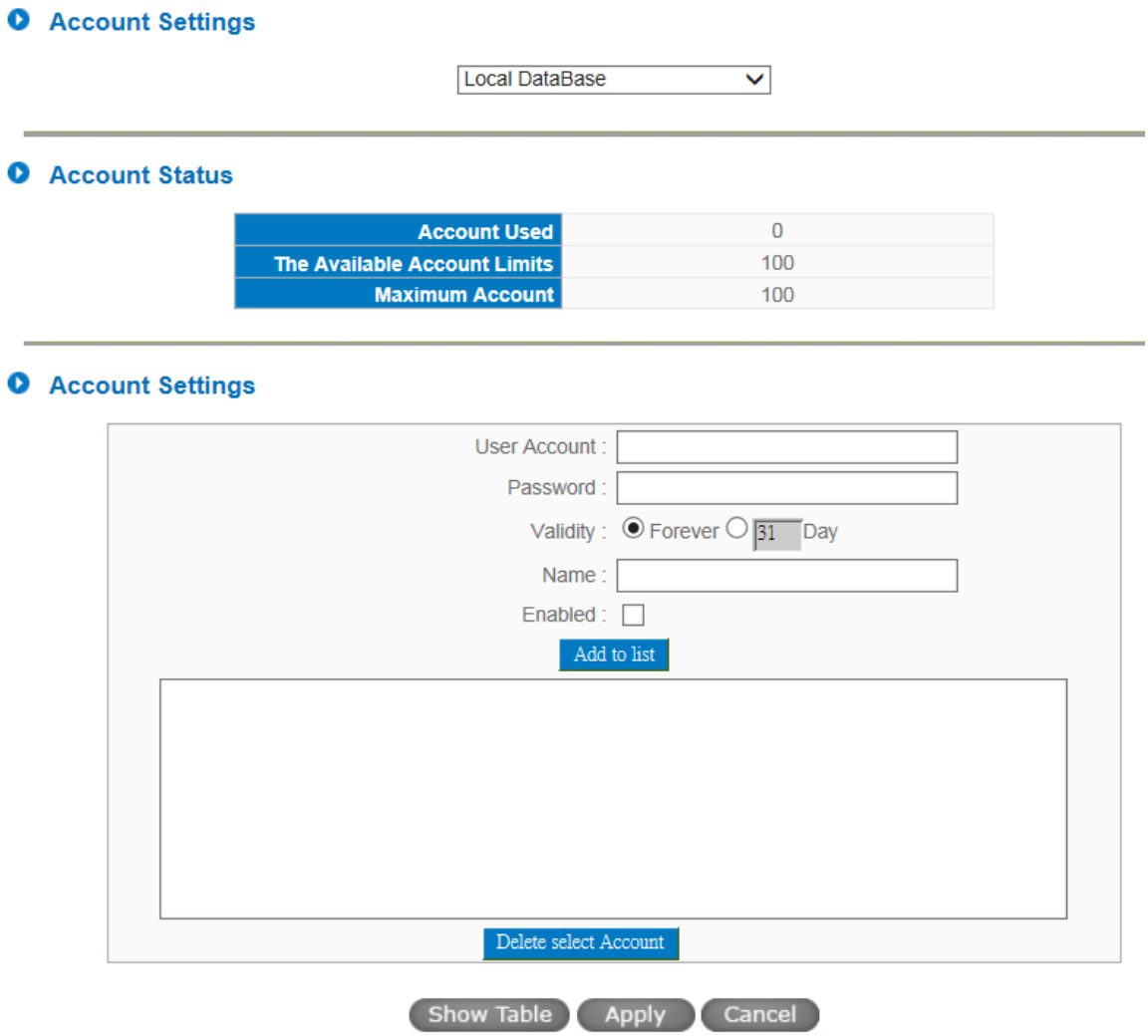
Under Account Settings → Select Database



Disabled	Disables the function.
Local Database	Builds the database locally in the router.
External Authentication Server	Choose this option if there is an existing external authentication server, such as a Radius Server.

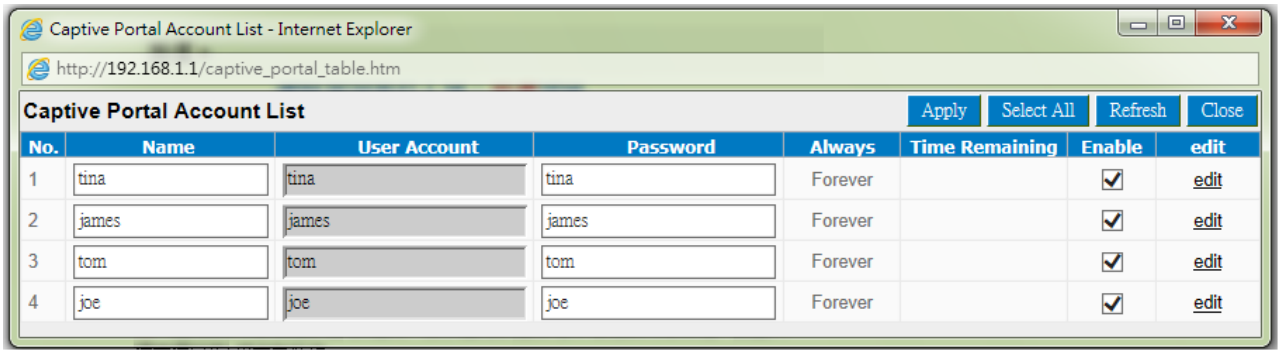
12.7.2 Local Database

2-1 Local Database



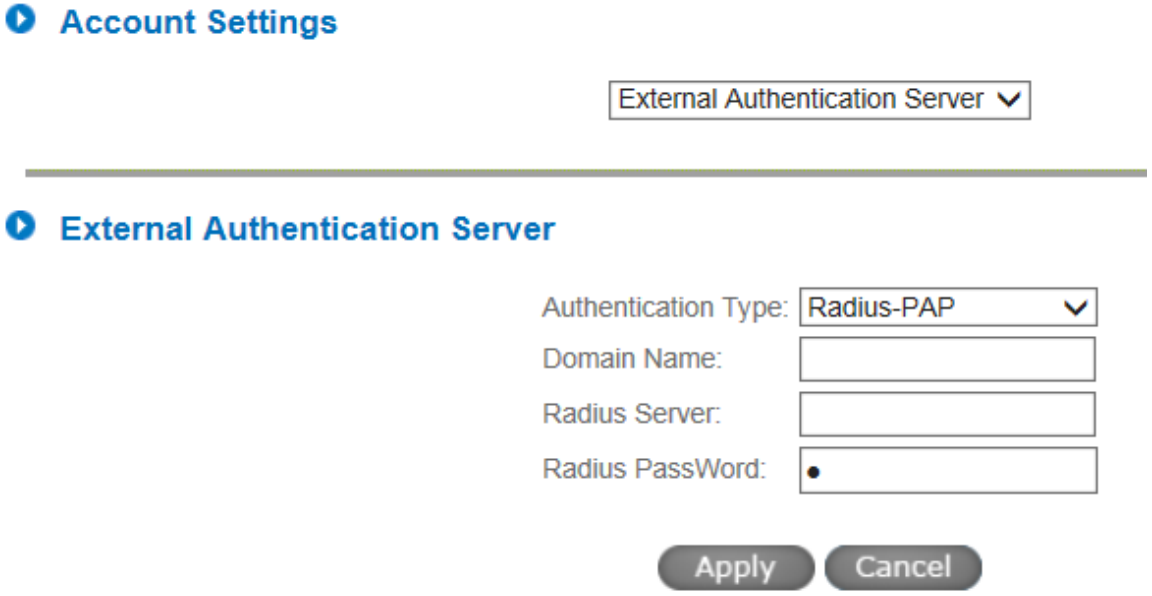
User Account	Name of the account the user needs to enter during login.
Password	The password associated with the User Account.
Validity	Length of time the account will remain in effect. Forever: the account does not expire. Day: number of days after the account is created will expire.
Name	A name can be given to the account for easy identification.
Enabled	Check to enable, or leave unchecked to disable, the account.

Click  to configure multiple accounts.



12.7.3 External Authentication Server

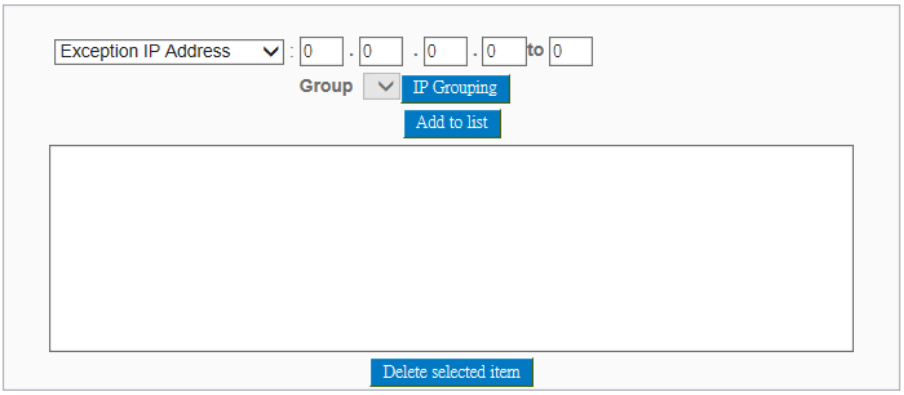
Other than Local Database authentication method, ALLNET GmbH routers support various other methods of authentication, such as, Radius-PAP/CHAP/MSCHAP/MSCHAPV2, NT-Domain, Active Directory and LDAP.



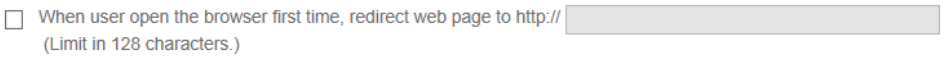
12.7.4 Advanced Settings

Exception Service Port

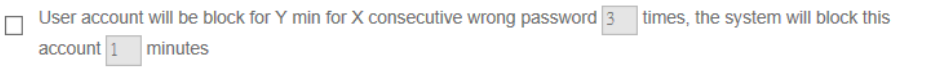
Exception IP or MAC



Web Page Redirection

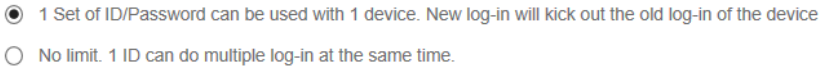


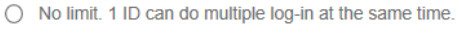
Password Protection



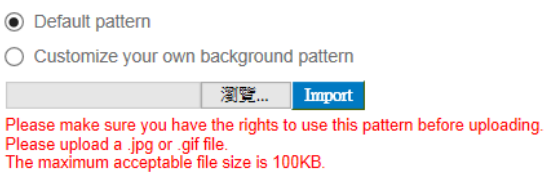
Portal Message

Device Count Limit



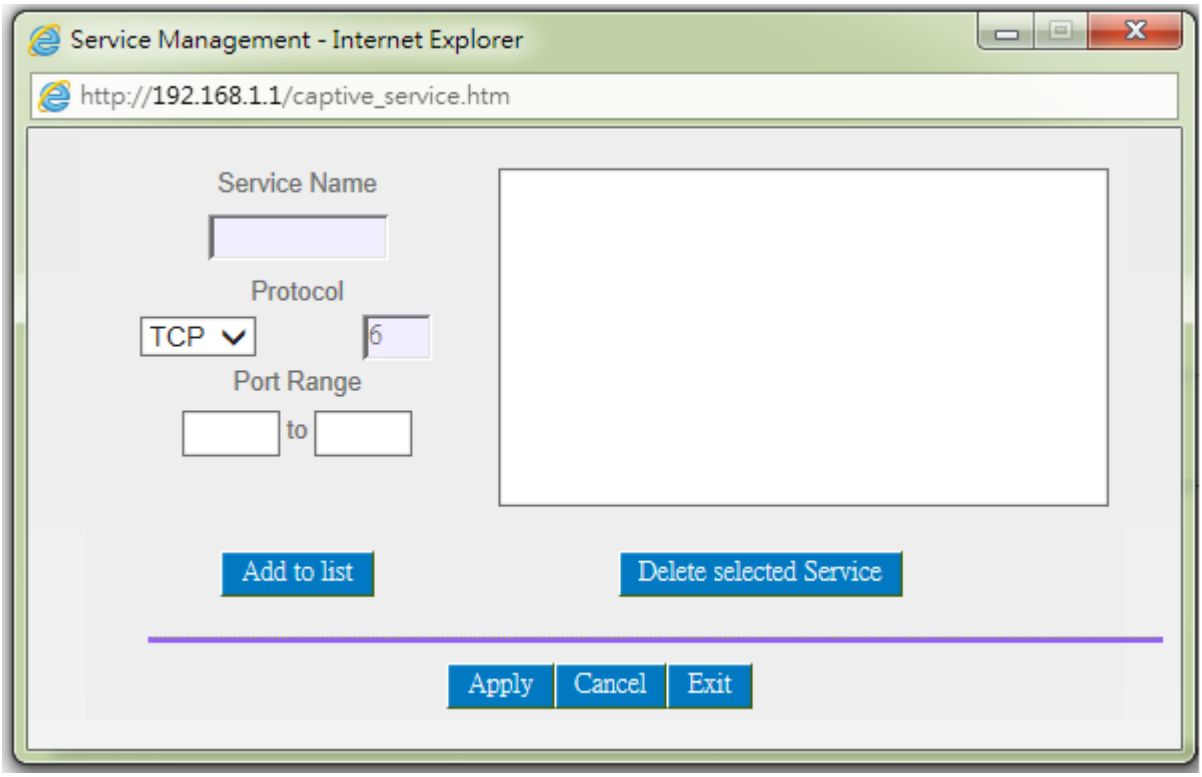


Background pattern of the login page



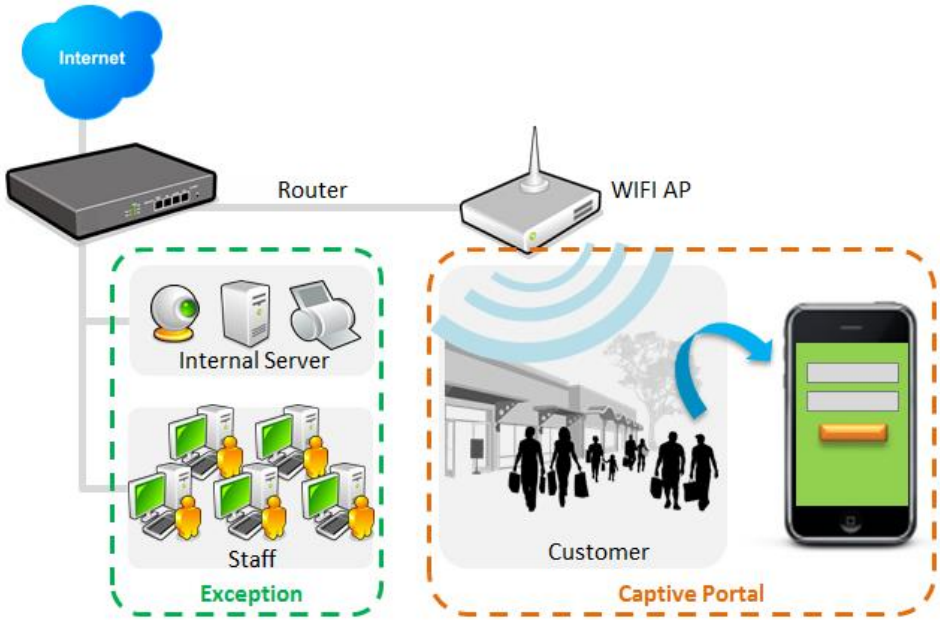
(1) Exception Service Port

If configured, the traffic with these specified ports will not be authenticated. Some examples can be POP3 or IMAP for email services. ***Note: if Captive Portal is used in conjunction with the APC feature, CAPWAP's UDP ports of 5246 & 5247 must be entered and added here to prevent disconnection of AP(s).***

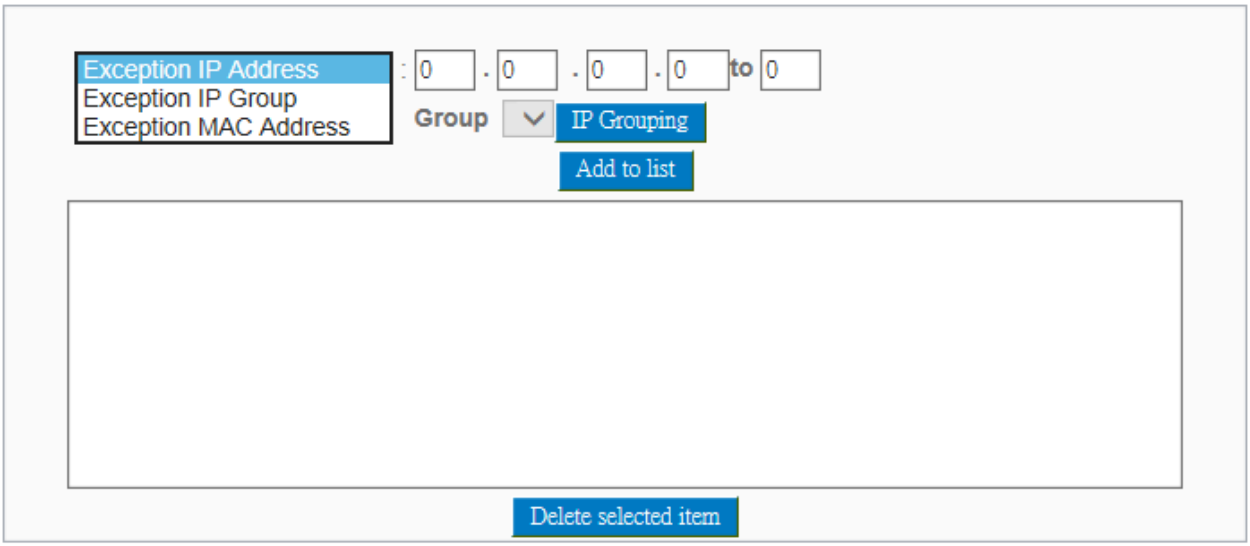


(2) Exception IP or MAC

If configured, devices with specified IP or MAC addresses will not be authenticated. Such devices can be business' employees or internal servers.



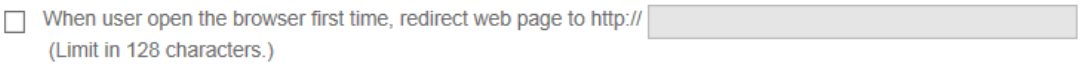
Exception IP or MAC



(3) Web Page Redirection

If enabled, users will see the redirected web page, when starting a web browser for the first time, after a successful login. Some examples may be a corporate web page, image or identity sites.

Web Page Redirection

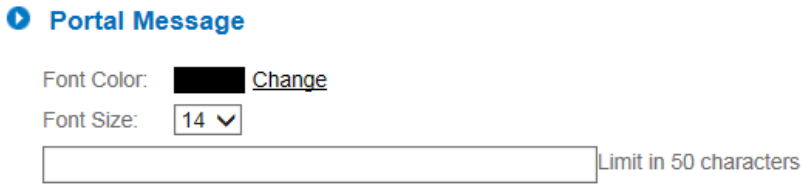


(4) Password Protection

In preventing malicious brute-force password attacks, if this feature is enabled, when a password is entered for X amount of times, the system will block the account for Y number of minutes.

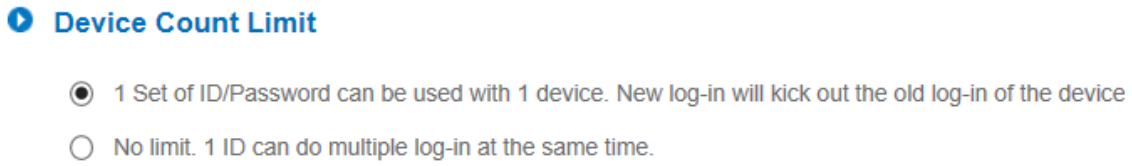
(5) Portal Message

A simple message the user will see on the user login screen. Color and size of the font used can be changed.



(6) Device Count Limit

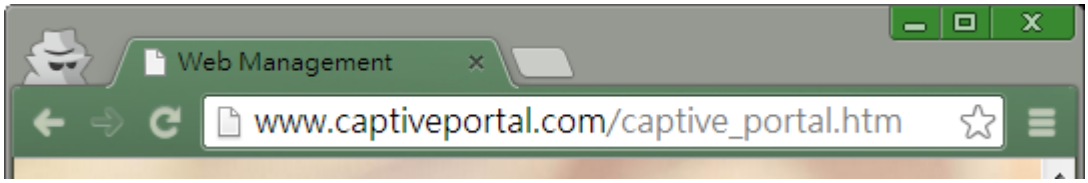
Choose whether to permit only one login per account, or allow multiple logins for an account. Please note, however, that although multiple users are using the same account to login, the number of available logins will still be reduced by the number of multiple logins. For instance, let's say the number of Maximum Account is 20 (this is also the number of available logins), and there are five connected devices using the same login. The number of available logins is reduced by five, not one.



(7) Advanced Settings

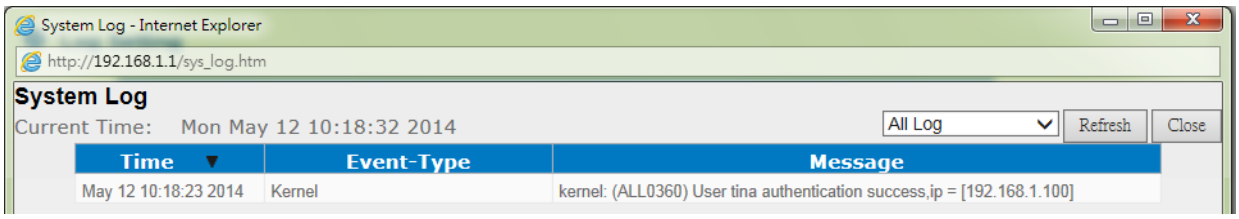
Captive Portal URL show the LAN IP address of router

If enabled, the URL in the address bar will show the LAN IP address of the router. Disabling this feature, the address bar will display the URL as pictured below.



Write user's MAC address in log message

If enabled, users' MAC addresses will be recorded in Log entries.

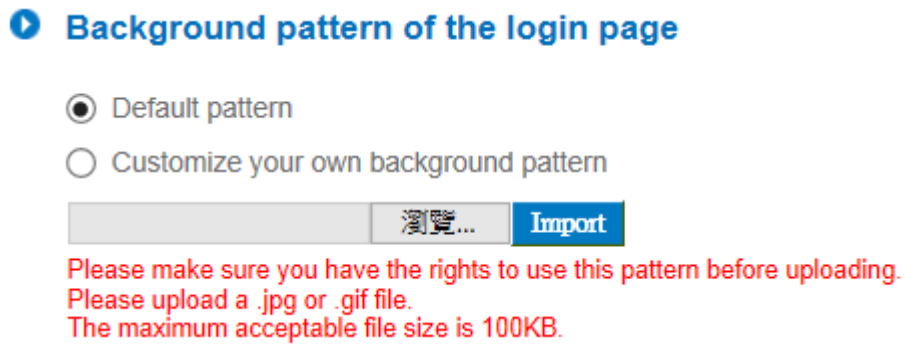


Connection time kick the customers out when he uses the internet for X minutes after he successfully logs-in

System will automatically kick users after certain amount of time (in minutes) of usage.

(8) Background pattern of the login page

Background image of the login page can be customized. Accepted image formats are either jpg or gif, and not bigger than 100KB in file size.



Using a restaurant as an example↓

12.7.5. Online User Status

Statuses of logged in users can be monitored in this page. Here, it shows a list of logged in users, as well as, the ability to disconnect particular users.

Online Users Status

Online Users	1
The Available Online User Limits	59
Maximum Online Users	60

Captive Portal Account List

*Clicking the IP address directly can show you the user's traffic usage and status

No.	Name	User Account ▲	IP Address ▲	Login Time ▲	Disconnect
1	tina	tina	192.168.1.100	2014/5/12-10:18	Disconnect

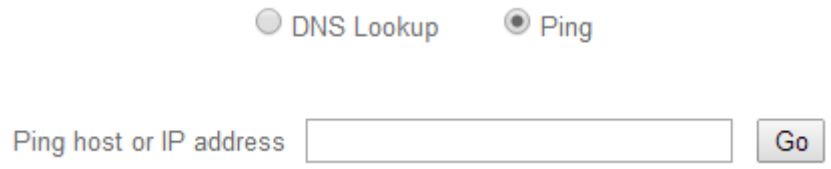
XIII. System Tool

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.

13.1 Diagnostic

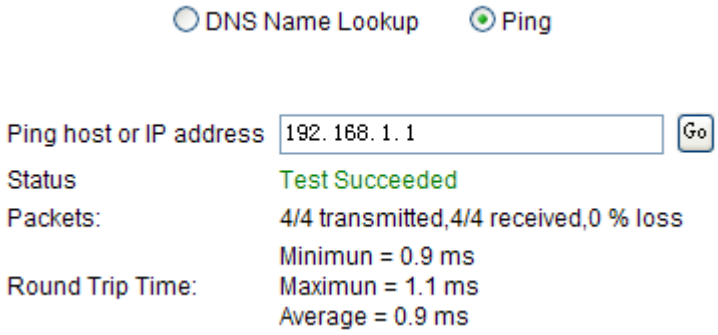
The device provides a simple online network diagnostic tool to help users troubleshoot network-related problems. This tool includes **DNS Name Lookup** (Domain Name Inquiry Test) and **Ping** (Packet Delivery/Reception Test).



DNS Name 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.

Ping



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.

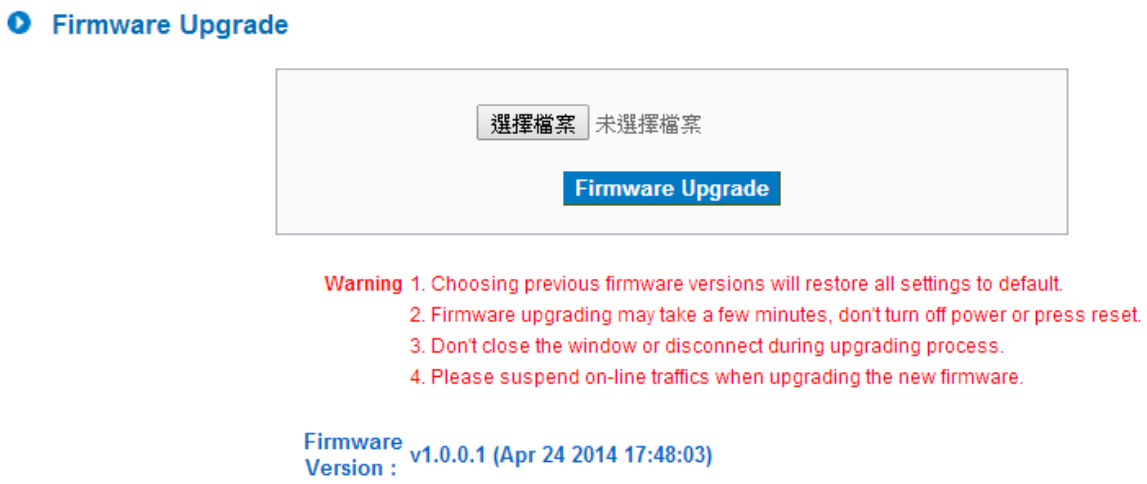
12.2 Firmware Upgrade

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.



12.3 Setting Backup

Import Configuration File:

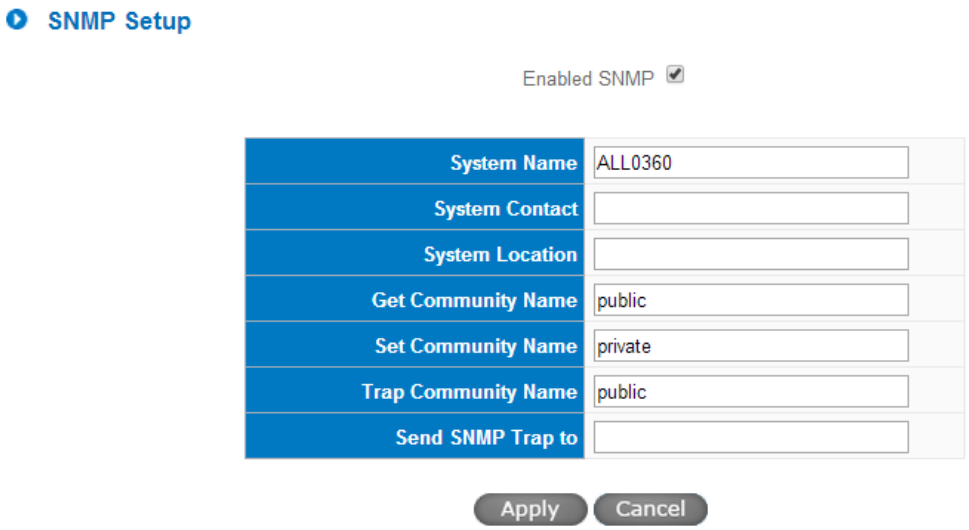
This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to import the file.

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.



Enabled: Activate SNMP feature. The default is activated.

System Name: Set the name of the device such as Allnet.

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.

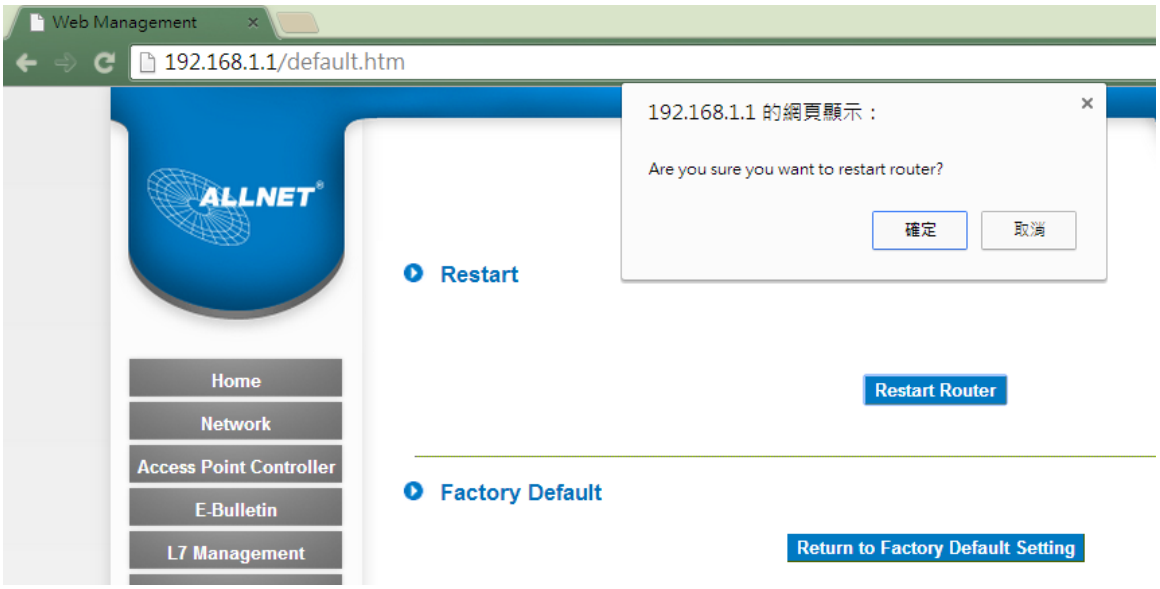
Cancel: Press **"Cancel"** to keep the settings unchanged.

13.5 System Recover

Users can restart the device with System Recover button.

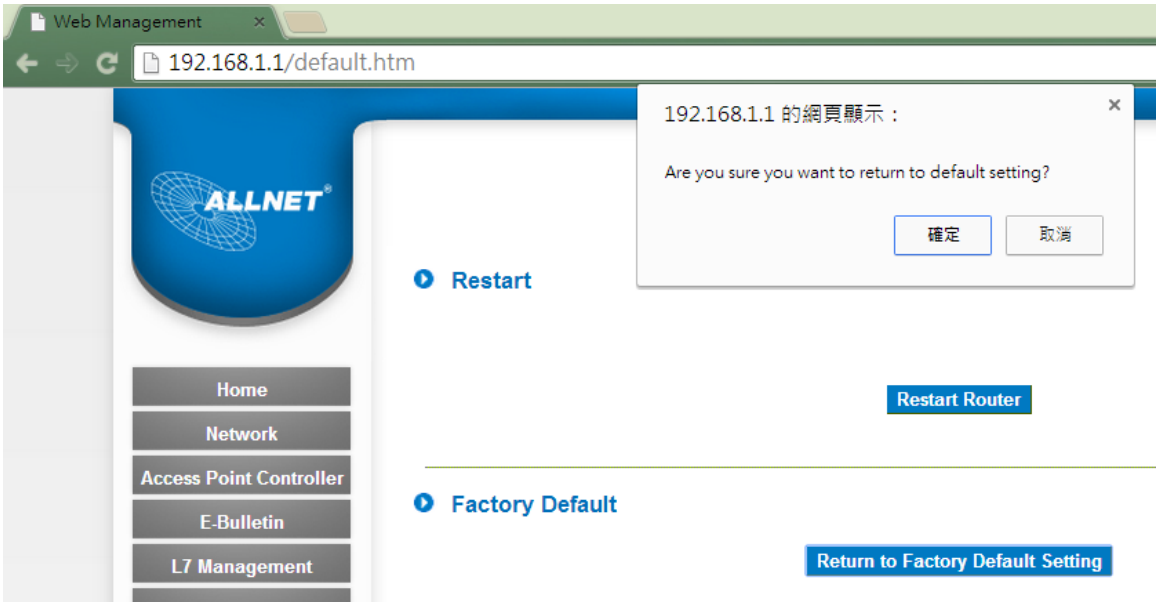
Restart

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



Return to Factory Default Setting

If clicking “Return to Factory Default Setting, the dialog block will pop out, if the device will return to factory default.



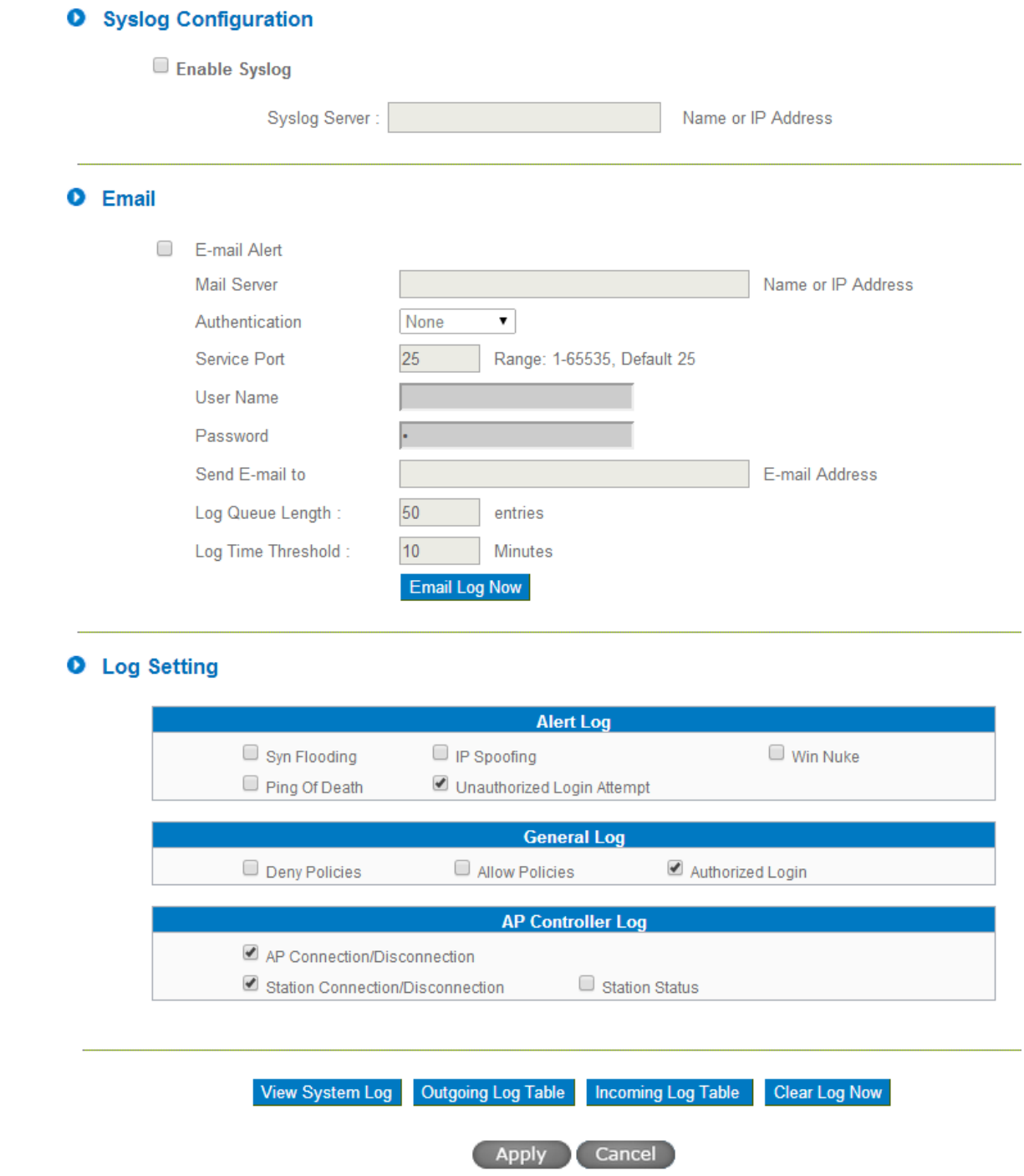
It's recommended to save the current configuration before upgrading firmware. After firmware upgraded, import the configuration file after returning to factory default to ensure system stable. (Please refer to 12.3)

XIII. 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.

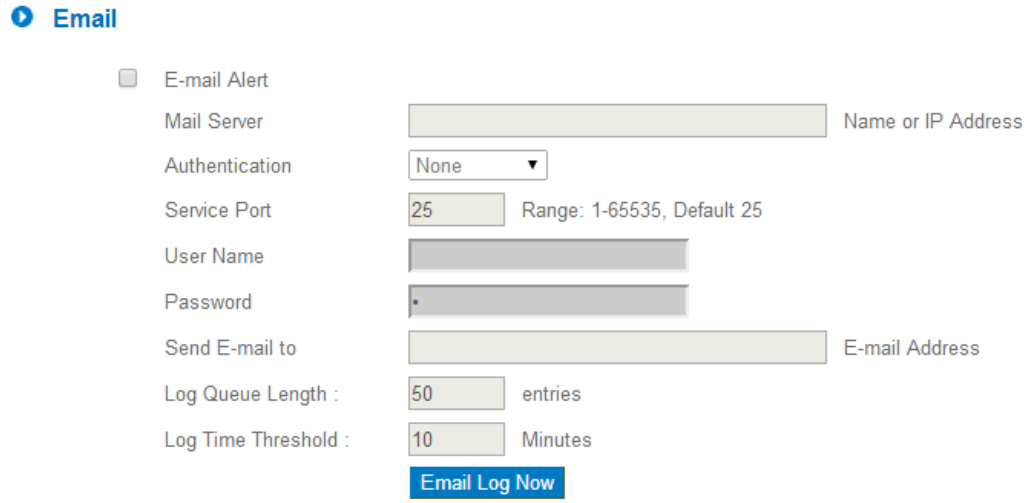


System Log

Enabled: If this option is selected, the System Log feature will be enabled.

Host Name: 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.

E-mail Alert



Enabled: If this option is selected, E-mail Warning will be enabled.

Mail Server: If users wish to send out all the logs, please enter the E-mail server name or the IP address; for instance, mail.abc.com .

E- mail: This is set as system log recipient email address such as abc@mail.abc.com.

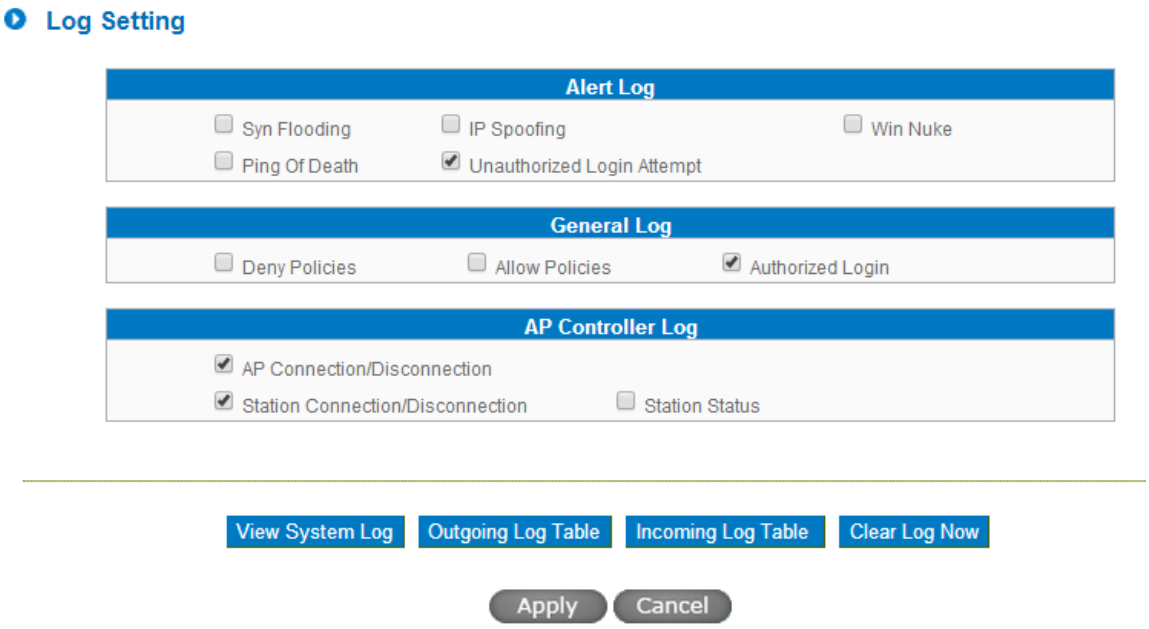
Log Queue Length: Set the number of Log entries, and the default entry number is 50. When this defined number is reached, it will automatically send out the log mail.

Log Time Threshold: Set the interval of sending the log, and the default is set to 10 minutes. Reaching this defined number, it will automatically send out the Mail log.

The device will detect which parameter (either entries or intervals) reaches the threshold first and send the log message of that parameter to the user.

Send Log to E- mail: Users may send out the log right away by pressing this button.

Log Setting



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

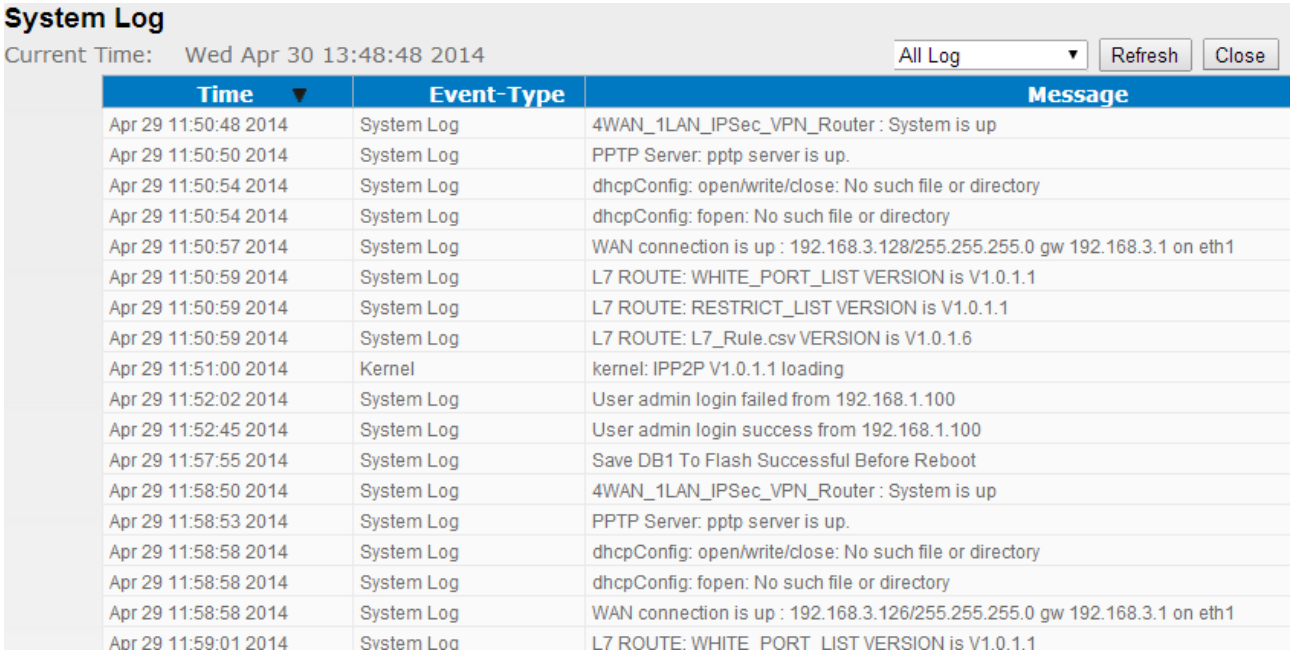
The device provides the following warning message. Click to activate the feature. System error message, blocked regulations, regulation of passage permission, system configuration change and registration verification.

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, Firewall Log,** and **VPN log**, which is illustrated as below.

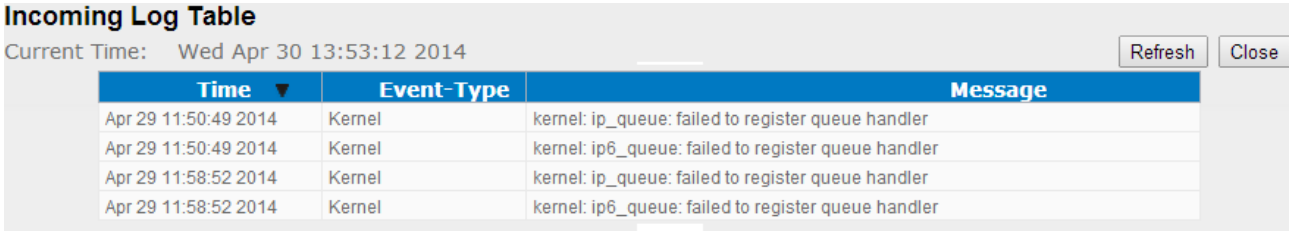


Outgoing Packet Log:

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

Incoming Packet Log:

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

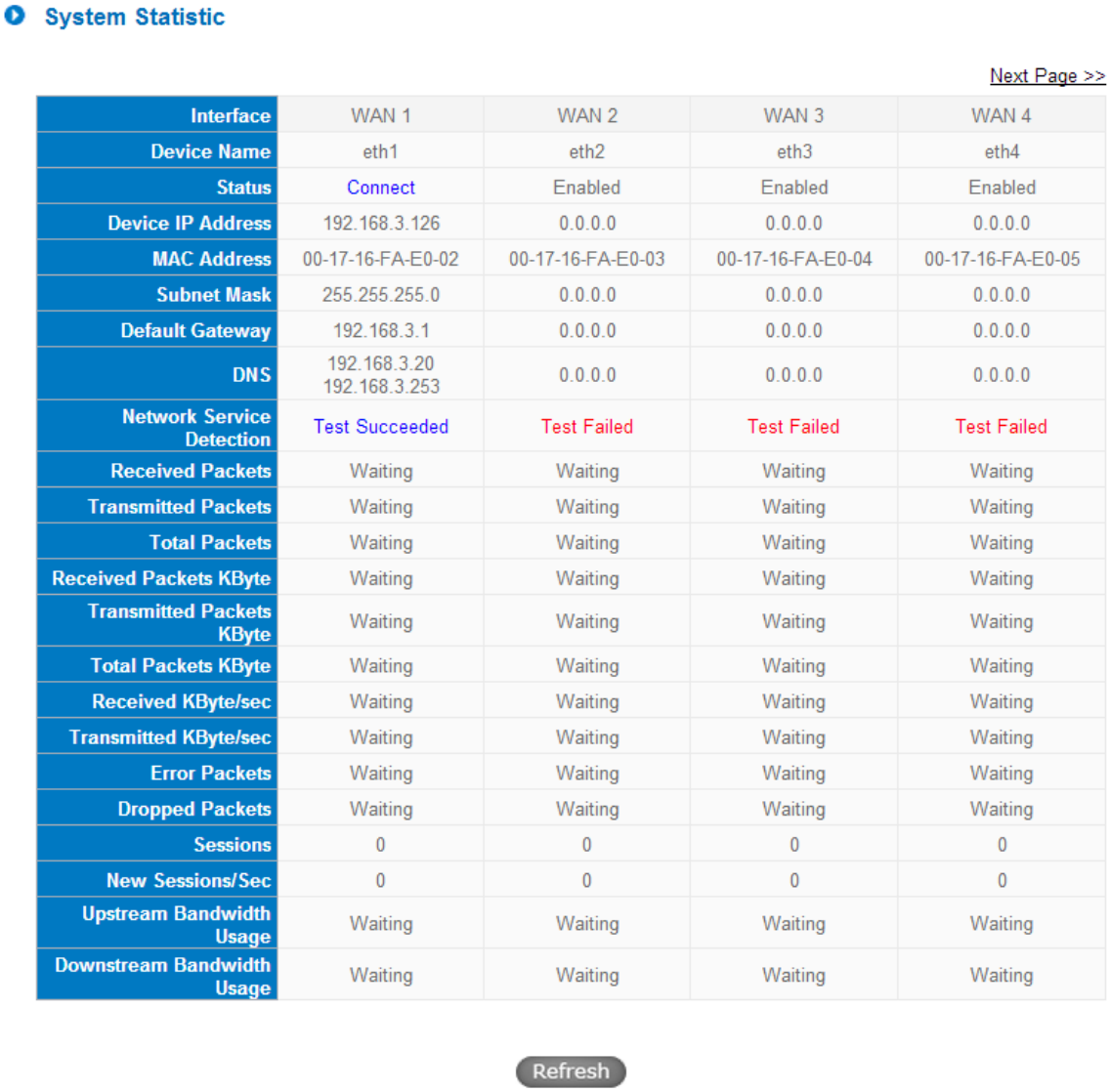


Clear Log Now:

This feature clears all the current information on the log.

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

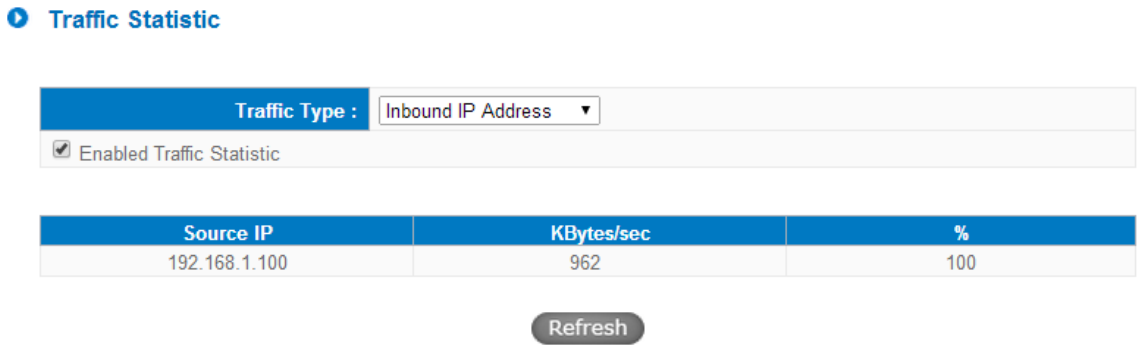
Next Page >>

Interface	WAN 1	WAN 2	WAN 3	WAN 4
Device Name	eth1	eth2	eth3	eth4
Status	Connect	Enabled	Enabled	Enabled
Device IP Address	192.168.3.126	0.0.0.0	0.0.0.0	0.0.0.0
MAC Address	00-17-16-FA-E0-02	00-17-16-FA-E0-03	00-17-16-FA-E0-04	00-17-16-FA-E0-05
Subnet Mask	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	192.168.3.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS	192.168.3.20 192.168.3.253	0.0.0.0	0.0.0.0	0.0.0.0
Network Service Detection	Test Succeeded	Test Failed	Test Failed	Test Failed
Received Packets	Waiting	Waiting	Waiting	Waiting
Transmitted Packets	Waiting	Waiting	Waiting	Waiting
Total Packets	Waiting	Waiting	Waiting	Waiting
Received Packets KByte	Waiting	Waiting	Waiting	Waiting
Transmitted Packets KByte	Waiting	Waiting	Waiting	Waiting
Total Packets KByte	Waiting	Waiting	Waiting	Waiting
Received KByte/sec	Waiting	Waiting	Waiting	Waiting
Transmitted KByte/sec	Waiting	Waiting	Waiting	Waiting
Error Packets	Waiting	Waiting	Waiting	Waiting
Dropped Packets	Waiting	Waiting	Waiting	Waiting
Sessions	0	0	0	0
New Sessions/Sec	0	0	0	0
Upstream Bandwidth Usage	Waiting	Waiting	Waiting	Waiting
Downstream Bandwidth Usage	Waiting	Waiting	Waiting	Waiting

Refresh

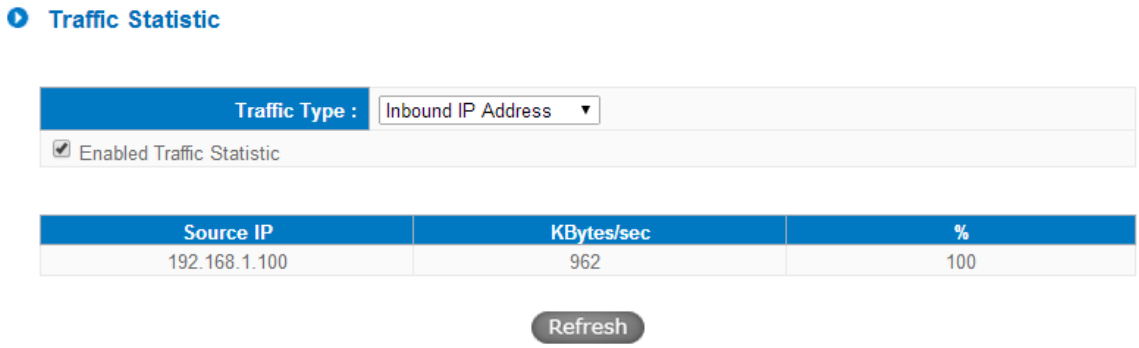
13.3 Traffic Statistic

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



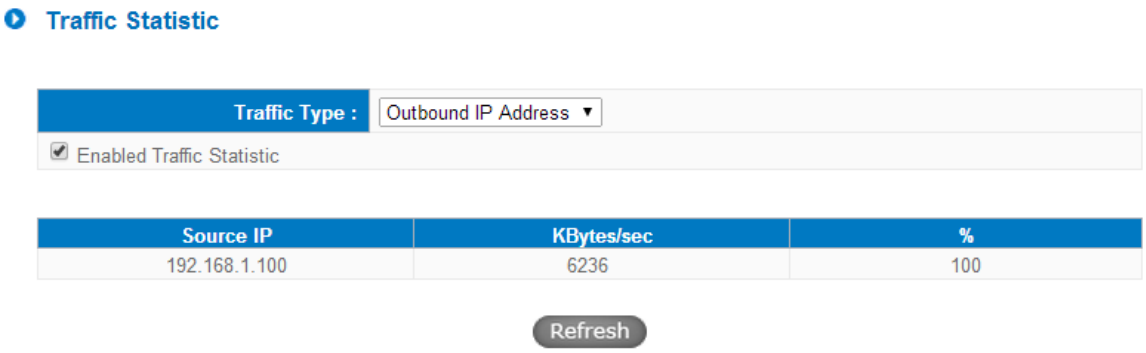
By Inbound IP Address:

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



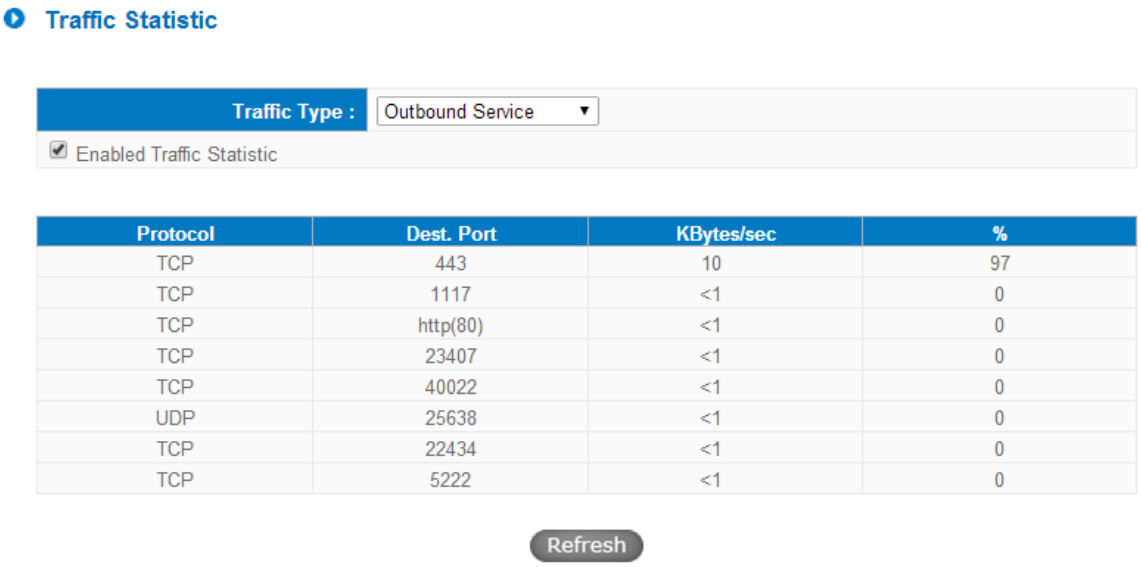
By outbound IP Address:

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



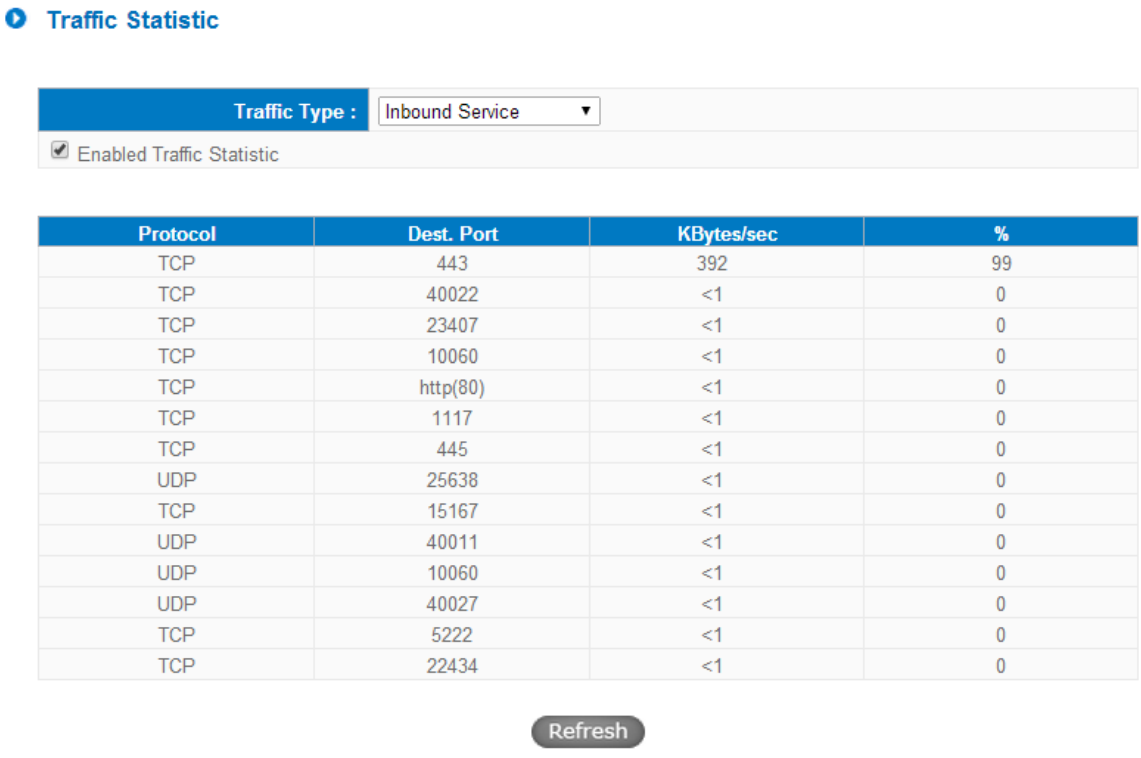
By Outbound Port:

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



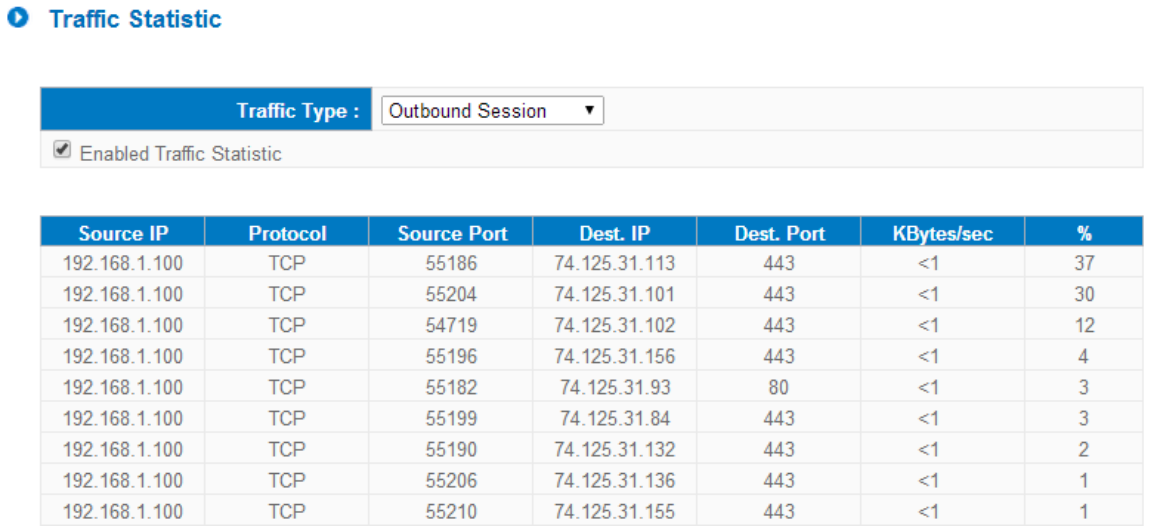
By Inbound Port:

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



By Outbound Session:

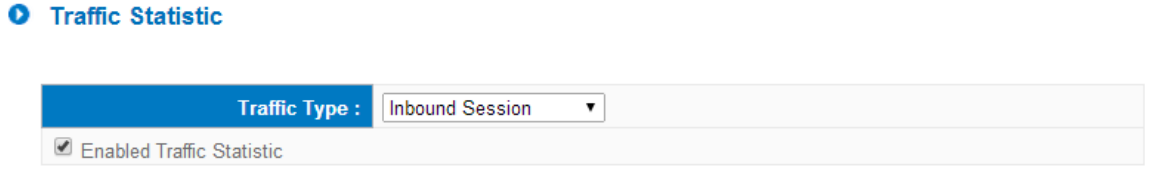
The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.



Source IP	Protocol	Source Port	Dest. IP	Dest. Port	KBytes/sec	%
192.168.1.100	TCP	55186	74.125.31.113	443	<1	37
192.168.1.100	TCP	55204	74.125.31.101	443	<1	30
192.168.1.100	TCP	54719	74.125.31.102	443	<1	12
192.168.1.100	TCP	55196	74.125.31.156	443	<1	4
192.168.1.100	TCP	55182	74.125.31.93	80	<1	3
192.168.1.100	TCP	55199	74.125.31.84	443	<1	3
192.168.1.100	TCP	55190	74.125.31.132	443	<1	2
192.168.1.100	TCP	55206	74.125.31.136	443	<1	1
192.168.1.100	TCP	55210	74.125.31.155	443	<1	1

By Inbound Session:

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



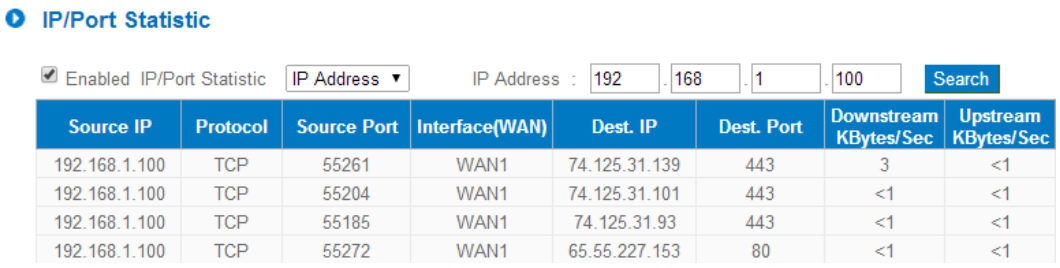
Source IP	Protocol	Source Port	Dest. IP	Dest. Port	KBytes/sec	%
192.168.1.100	TCP	55186	74.125.31.113	443	16	95
192.168.1.100	TCP	55204	74.125.31.101	443	<1	1
192.168.1.100	TCP	54719	74.125.31.102	443	<1	1
192.168.1.100	TCP	55190	74.125.31.132	443	<1	0
192.168.1.100	TCP	55235	23.53.66.101	443	<1	0
192.168.1.100	TCP	49570	111.221.74.24	40022	<1	0
192.168.1.100	TCP	49616	64.4.61.49	443	<1	0
192.168.1.100	TCP	55199	74.125.31.84	443	<1	0
192.168.1.100	UDP	22190	61.231.115.116	25638	<1	0

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.

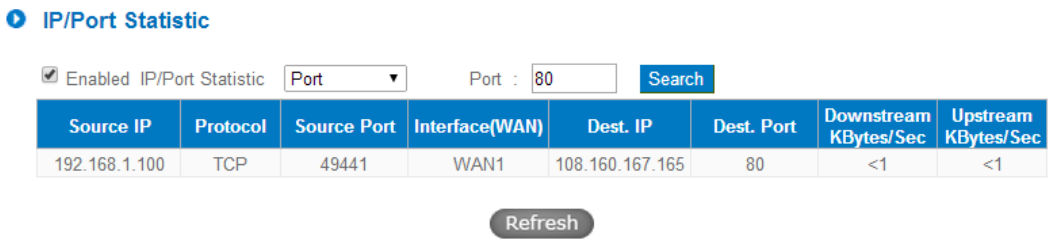
Specific IP Status：

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.



Specific Port Status：

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



13.5 QRTG (Allnet Router Traffic Grapher)

QRTG utilizes dynamic GUI and simple statistic to display system status of Allnet Firewall/ Router presently, including CPU Utilization(%), Memory Utilization(%), Session and WAN Traffic.

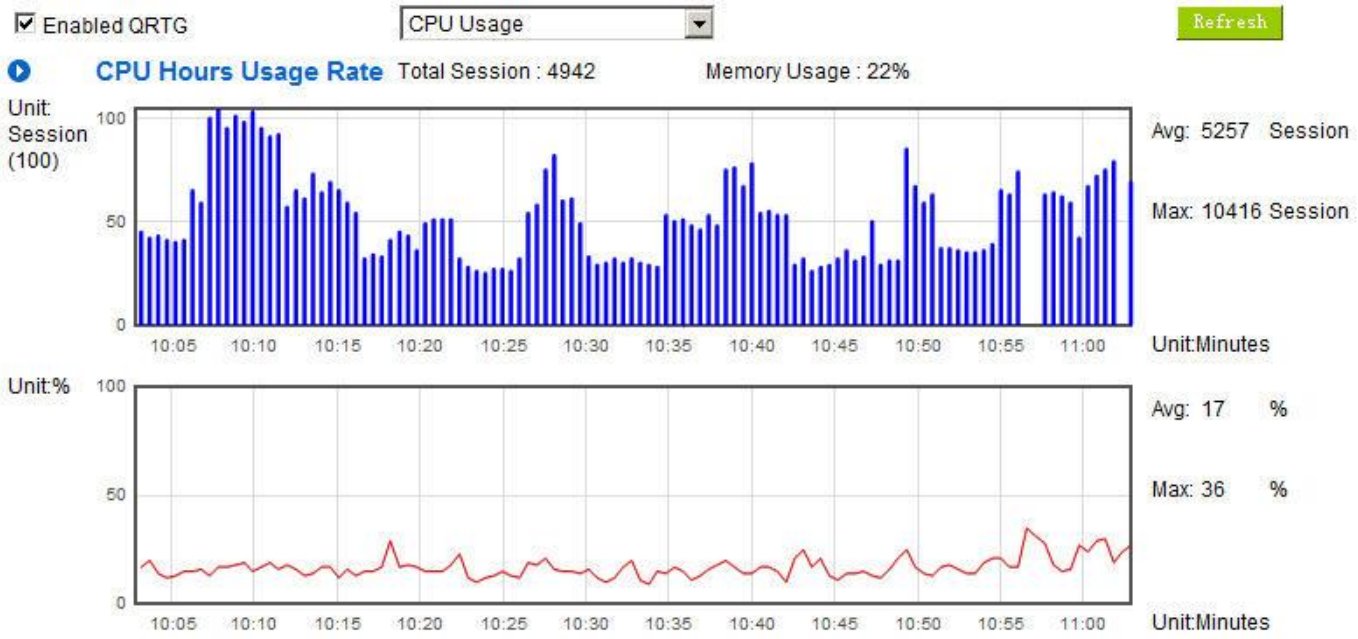
Enable QRTG: The funcation is disabled by default. When you are going to enable the QRTG function, system will pop-up a warning massage to remind you this function will be enabled, which may influence router efficiency. You can use drop down menu to select current status that including statistic and graphics of the following items when this function is enabled. System will refresh the statistic and graphics to latest data timing when you click “Refresh” button.

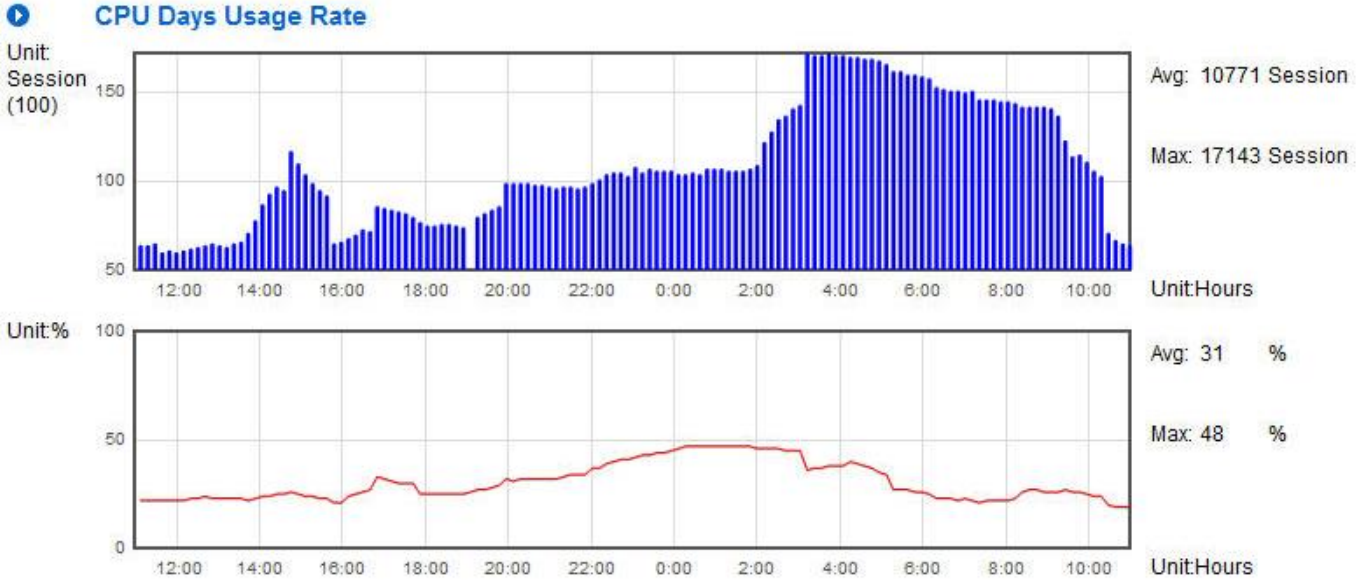
I. CPU Usage (As in the the following figure)

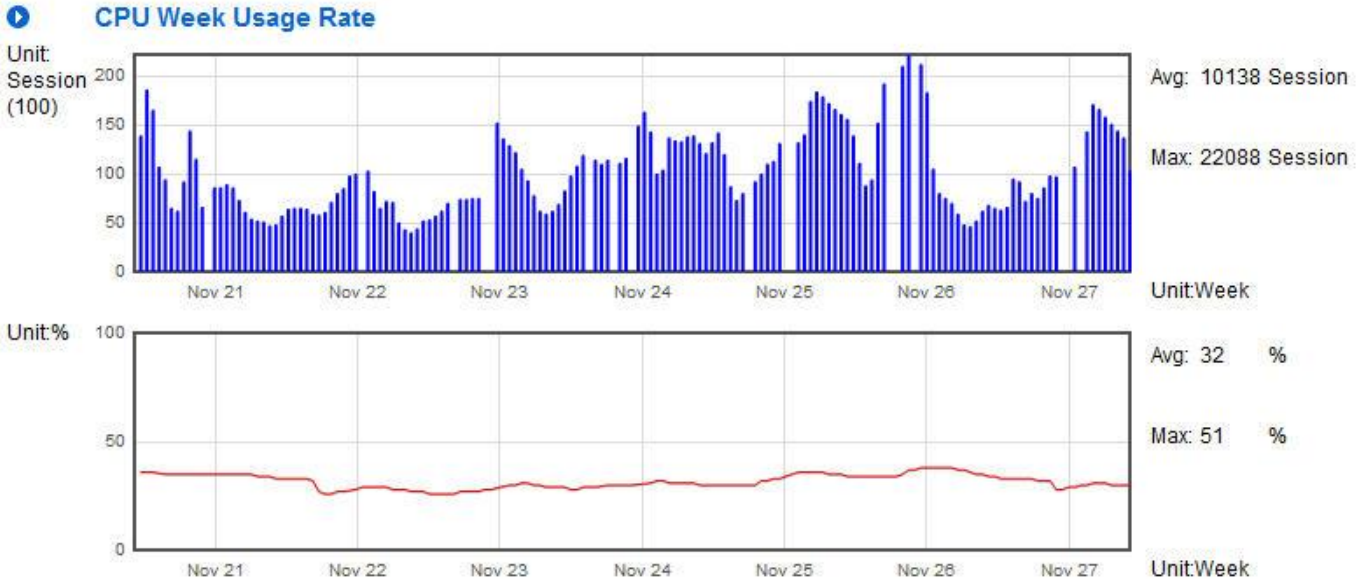
(1) CPU Hours Usage Rate graphic / average/ maximum

(2) CPU Days Usage Rate graphic / average/ maximum

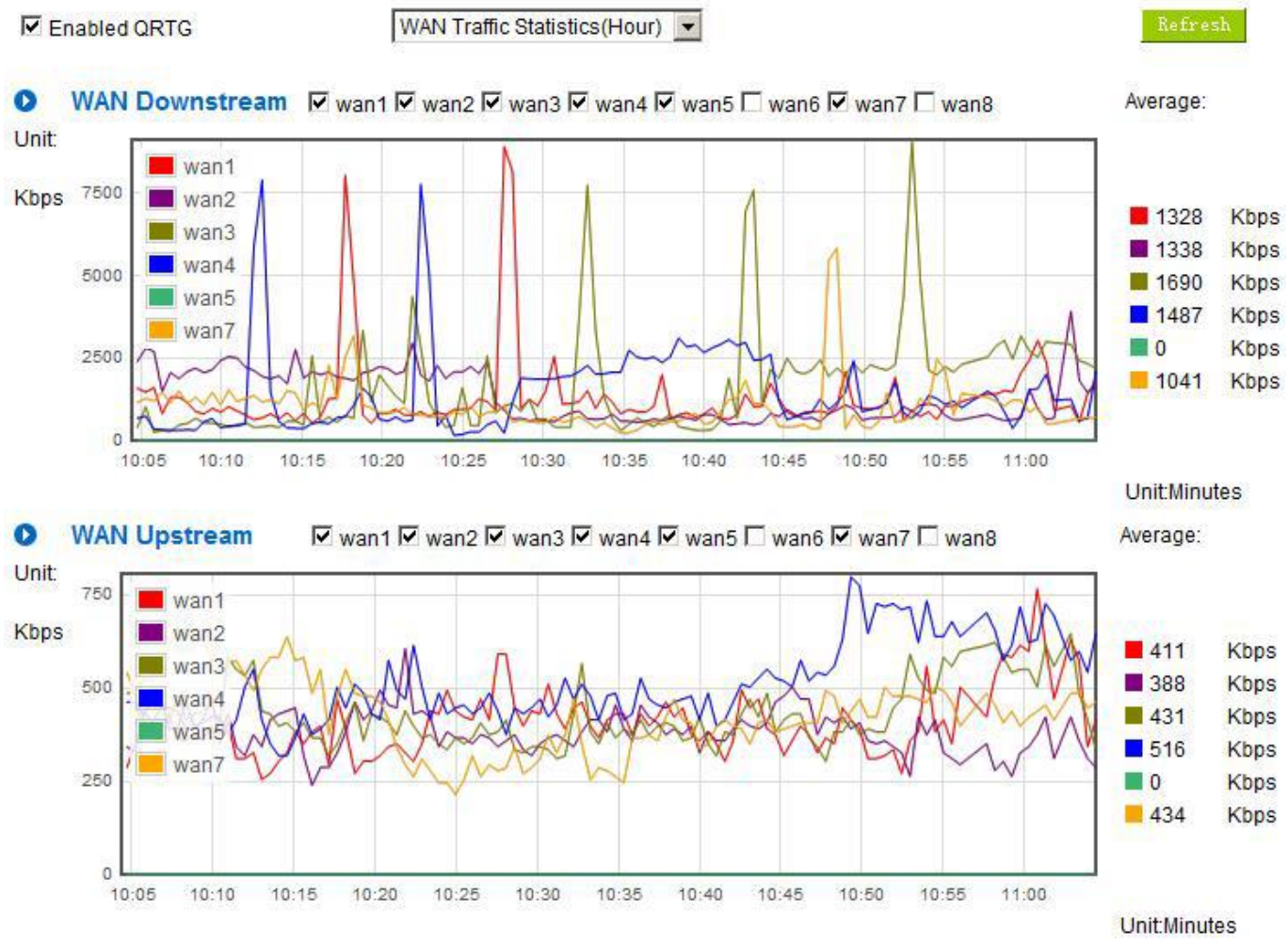
(3) CPU, Week Usage Rate graphic / average/ maximum





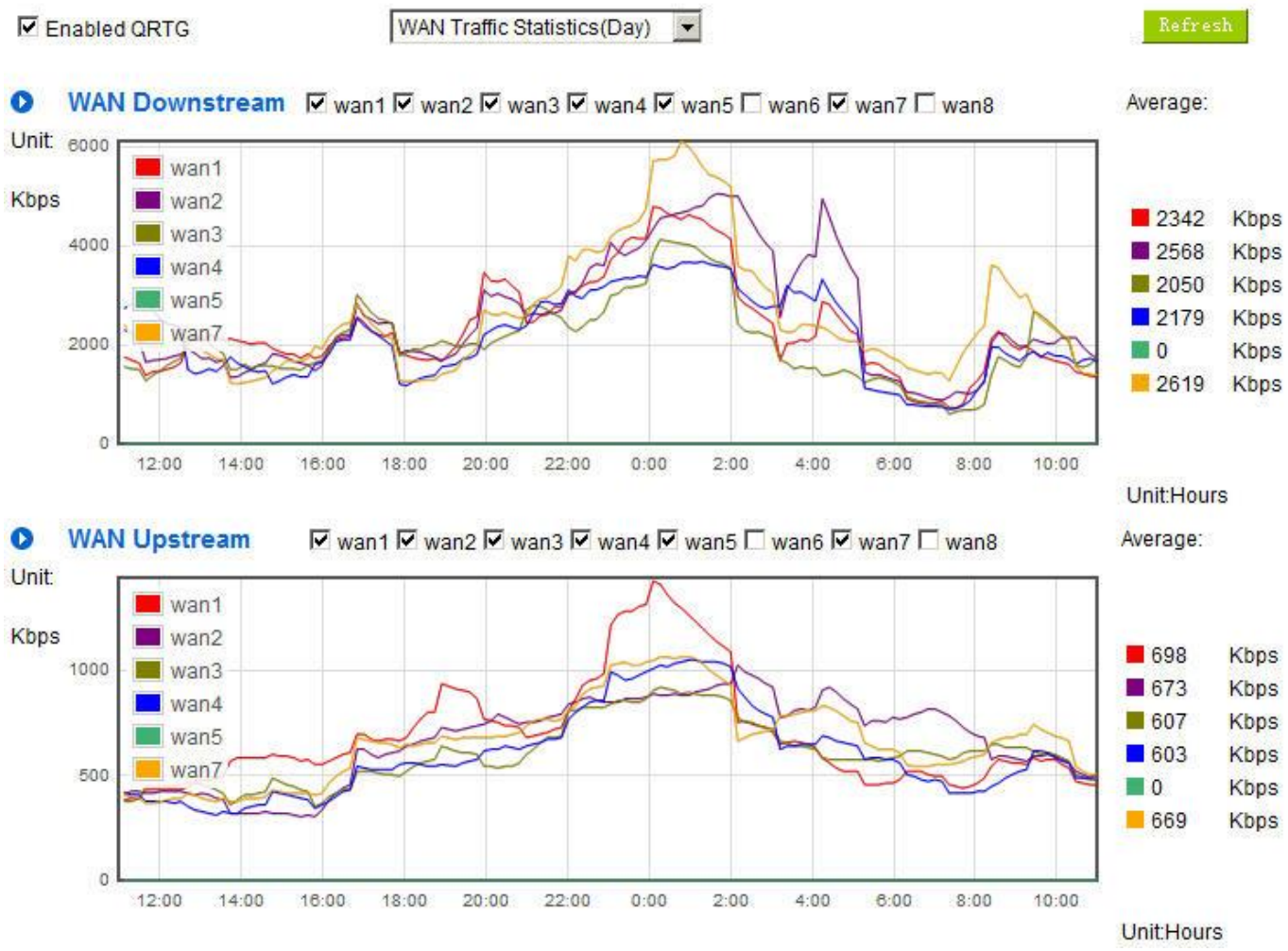


II. WAN Traffic Statistic (hourly) graphic and average (up/down stream) (As in the following figures)



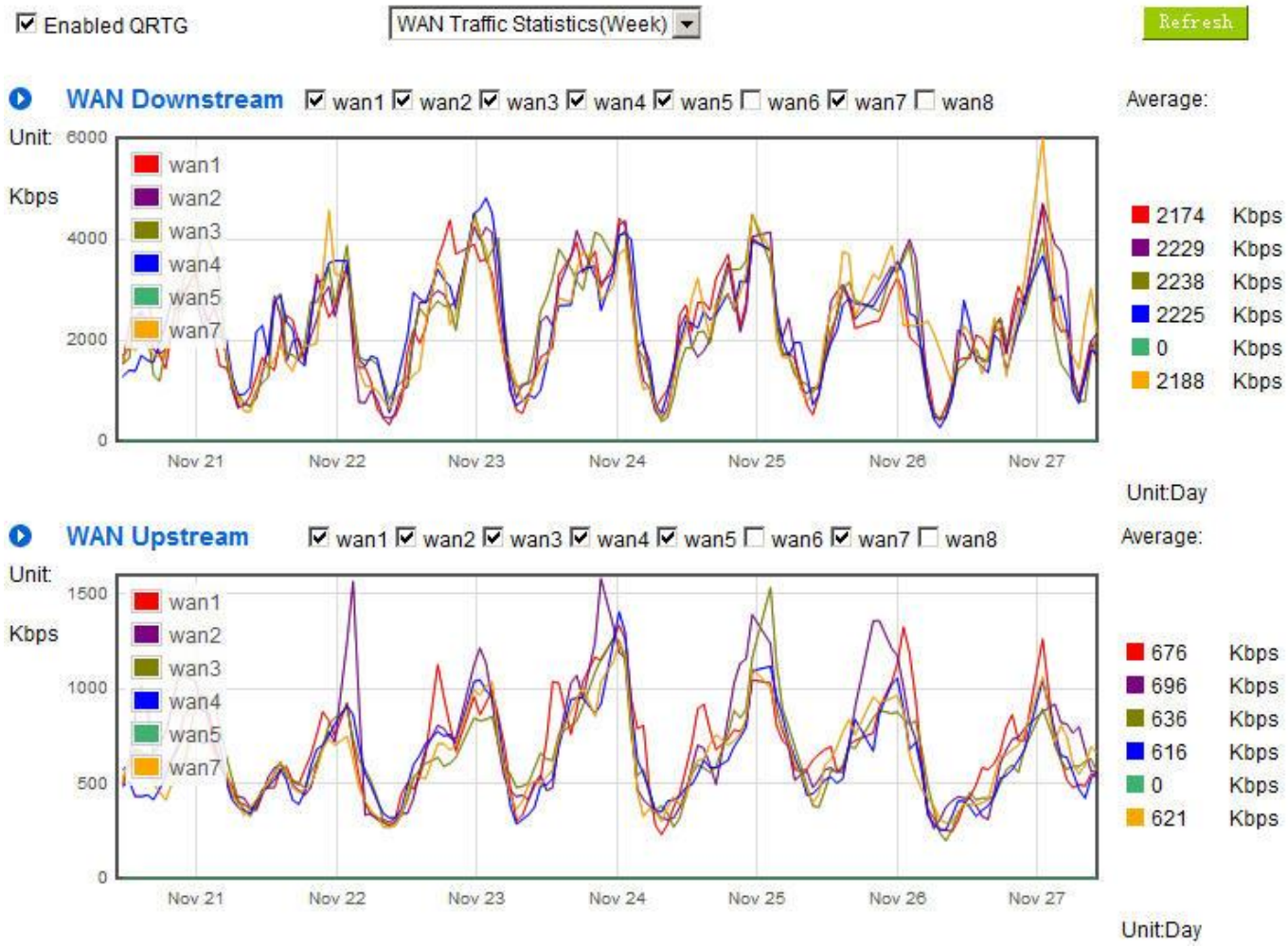
* The UI might vary from model to model, depending on different product lines.

III. WAN Traffic Statistic (Day) graphic and average (up/down stream)(As in the following figures)



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

IV. WAN Traffic Statistic (Week) graphic and average (up/down stream)(As in the following figures)



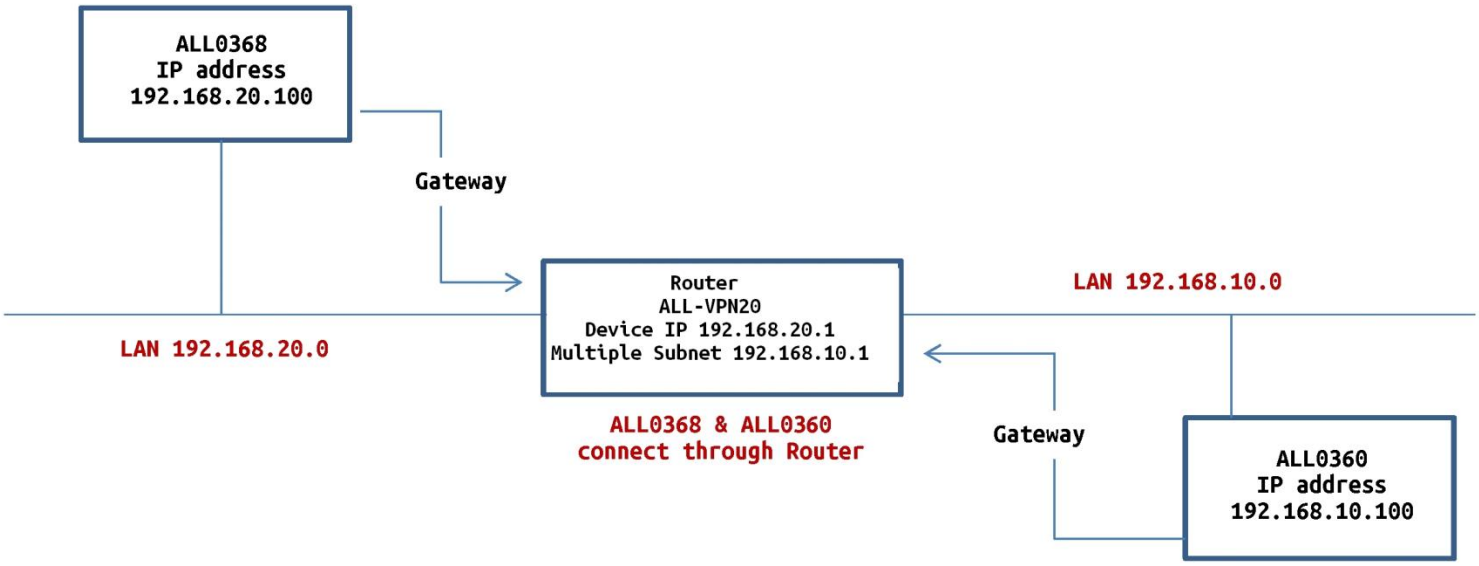
* The UI might vary from model to model, depending on different product lines.

XIV. 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.

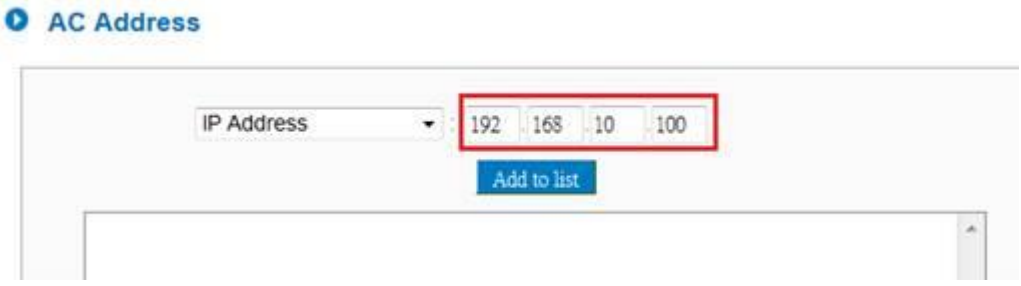
XV. Layer 3 Management

Example Configuration:



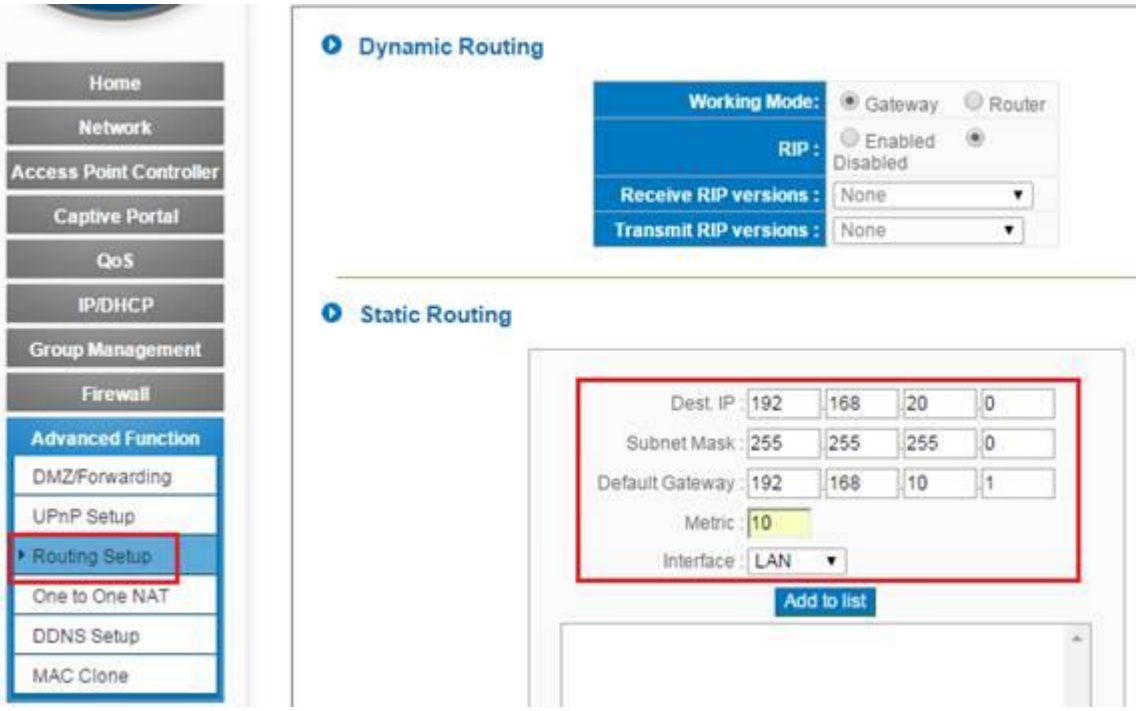
A) Configuration ALL0368:

IP Address	192.168.20.100
Add AC Address	192.168.10.100



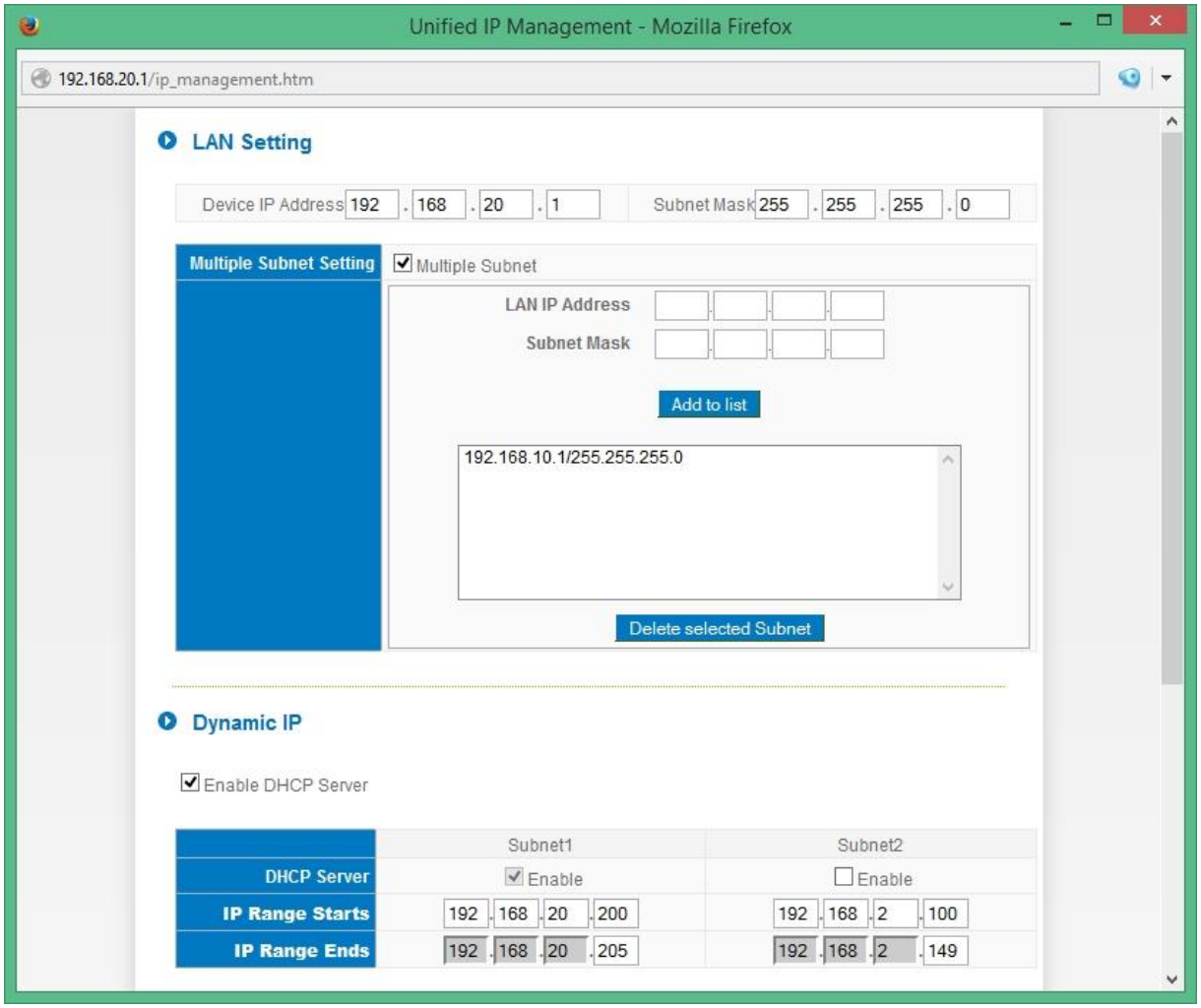
B) Configuration ALL0360

IP Address 192.168.10.100
Add Static Routing:
Destination IP 192.168.20.0
Subnet Mask 255.255.255.0
Default Gateway: 192.168.10.1
Metric: 10



C) Configuration ALL-VPN20:

IP Address	192.168.20.1
Add Multiple Subnet	192.168.10.1



CE-Declaration of Conformity

For the following equipment:

Germering, 30th of October, 2014

Wireless Controller

ALL0360

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 ALL0360 conforms to the Council Directives of 2004/108/EC.

This equipment meets the following conformance standards:

EN 55022:2010+AC:2011, Class B
AS/NZS CISPR 22: 2009+A1 2010, Class B
CISPR 22:2008, Class B
EN 61000-3-2:2006+A1:2009+A2:2009, Class A
EN 61000-3-3:2013
EN 55024:2010

IEC 61000-4-2:2008 ED.2.0
IEC 61000-4-3:2010 ED. 3.2
IEC 61000-4-4:2012 ED. 3.0
IEC 61000-4-5:2005 ED. 2.0
IEC 61000-4-6:2013 ED. 4.0
IEC 61000-4-8:2009 ED. 2.0
IEC 61000-4-11:2004 ED. 2.0

This equipment is intended to be operated in all countries.

This declaration is made by
ALLNET Computersysteme GmbH
Maistraße 2
82110 Germering
Germany

Germering, 30.10.2014

Wolfgang Marcus Bauer
CEO

DISCLAIMER_OF_WARRANTY

This Program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This Program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The full text of the GNU General Public License version 2 is included with the software distribution in the file LICENSE.GPLv2

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Written Offer for Source Code

For binaries that you receive from ALLNET GmbH Computersysteme on physical media or within the download of the offered firmware that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

ALLNET GmbH Computersysteme
Maistrasse 2
82110 Germering

Your request should include: (i) the name of the covered binary, (ii) the version number of the ALLNET product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available). We may charge you a nominal fee to cover the cost of the media and distribution. Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code. For your convenience, some or all of the source code may

also be found at:

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

LICENSE.GPLv2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License,

whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections and 2 above on a medium customarily used for software interchange; or,
   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail. If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.
You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LICENSE.LGPLv2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.
When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed

to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people

to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is

intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER

SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!