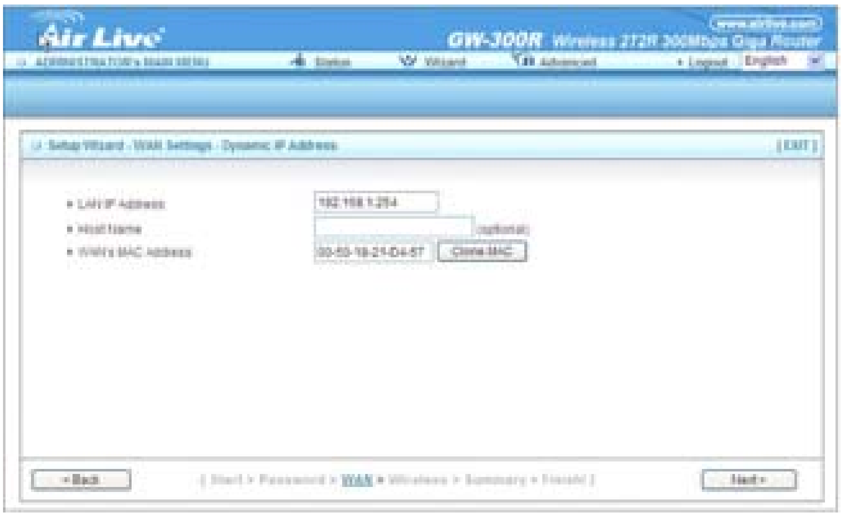
Step 3:
Setup the LAN IP and WAN Type.



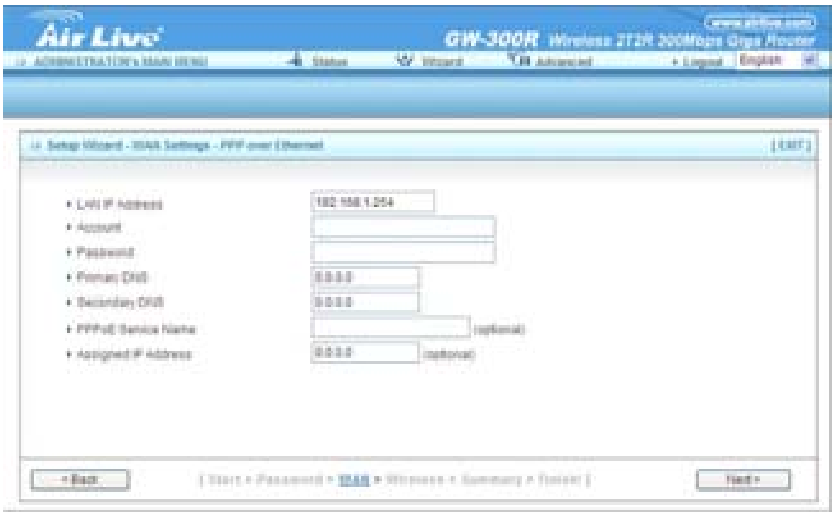
Setup Wizard - WAN Settings - Dynamic IP Address

- LAN IP Address: 192.168.1.254
- Host Name: (optional)
- WAN's MAC Address: 00-50-18-21-D4-57

[Start > Password > WAN > Wireless > Summary > Finish!]

Step 4:
Please fill in PPPoE service information which is provided by your ISP.

Example:

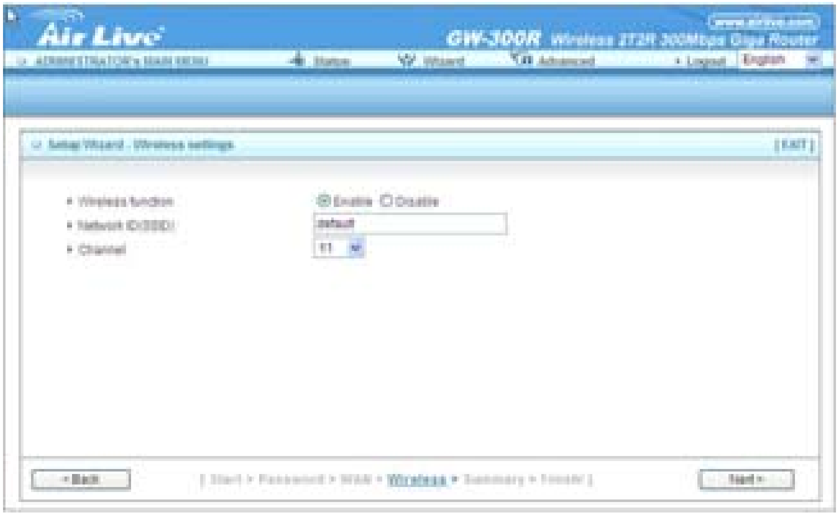


Setup Wizard - WAN Settings - PPP over Ethernet

- LAN IP Address: 192.168.1.254
- Account:
- Password:
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- PPPoE Service Name: (optional)
- Assigned IP Address: 0.0.0.0 (optional)

[Start > Password > WAN > Wireless > Summary > Finish!]

Step 5:
Set up your Wireless.

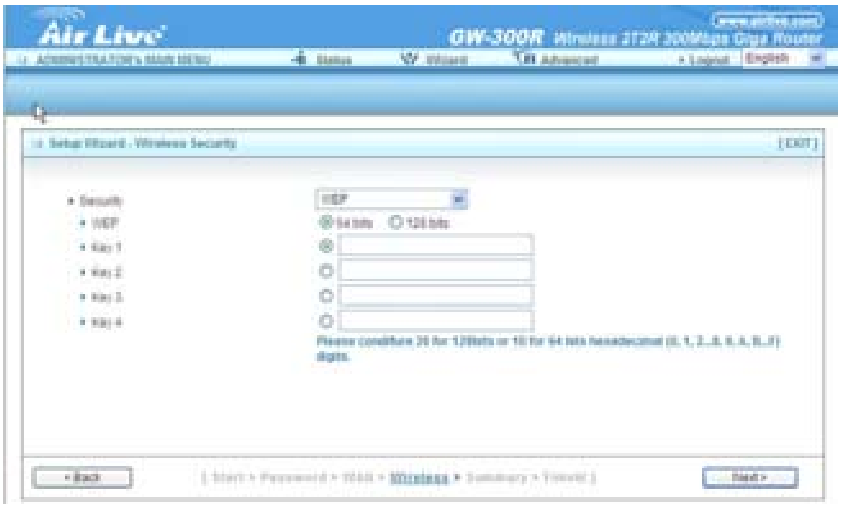


Setup Wizard - Wireless settings

- Wireless function: ● Enable ○ Disable
- Network ID(SSID): default
- Channel: 11

[Start > Password > WAN > Wireless > Summary > Finish!]

Set up your Authentication and Encryption.


Air Live
www.airlive.com
GW-300R Wireless 2T2R 300Mbps Giga Router
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
English

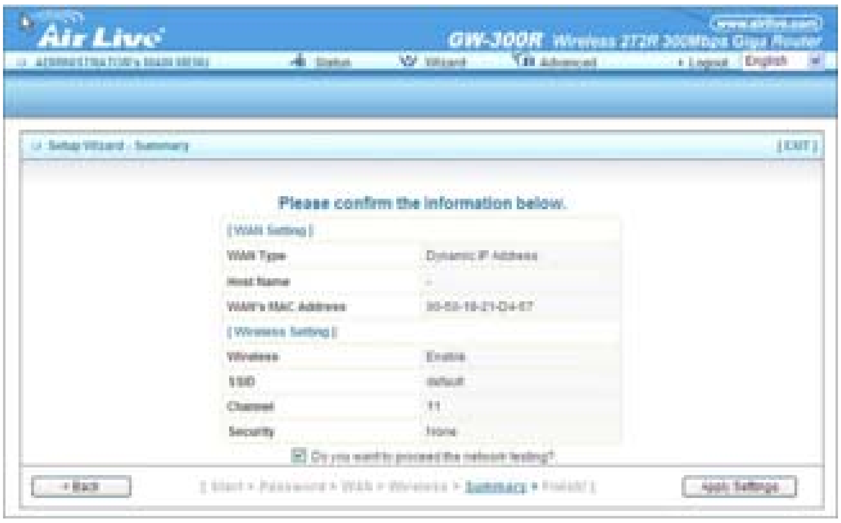
Setup Wizard - Wireless Security [EXIT]

- Security: WEP
  - WEP: ● 64 bits ○ 128 bits
  - Key 1: ●
  - Key 2: ○
  - Key 3: ○
  - Key 4: ○

Please constitute 26 for 128bits or 10 for 64 bits hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

< Back [Start > Password > WAN > Wireless > Summary > Finish!] Next >

Step 6:
Then click Apply Setting.
And then the device will reboot.


Air Live
www.airlive.com
GW-300R Wireless 2T2R 300Mbps Giga Router
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
English

Setup Wizard - Summary [EXIT]

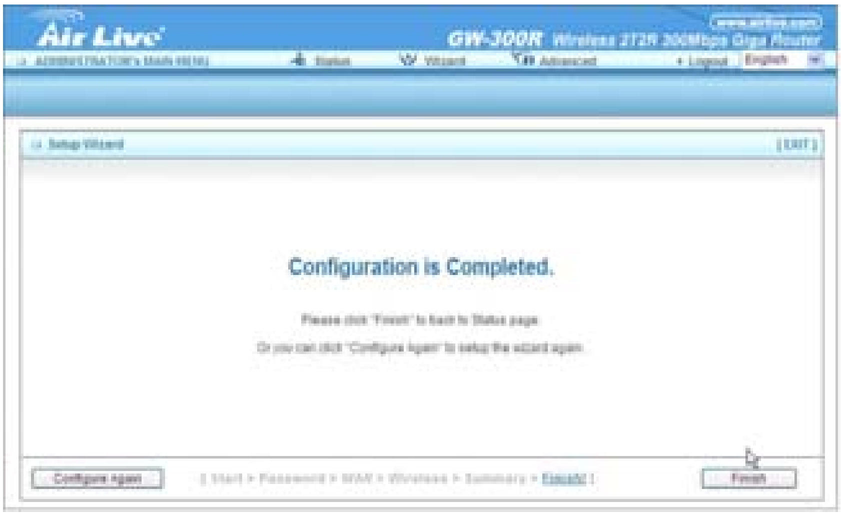
Please confirm the information below.

[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	-
WAN's MAC Address	00-50-18-21-D4-E7
[Wireless Setting]	
Wireless	Enable
SSID	default
Channel	11
Security	None

☑ Do you want to proceed the network testing?

< Back [Start > Password > WAN > Wireless > Summary > Finish!] Apply Settings

Step 7:
Click Finish to complete it.


Air Live
www.airlive.com
GW-300R Wireless 2T2R 300Mbps Giga Router
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
English

Setup Wizard [EXIT]

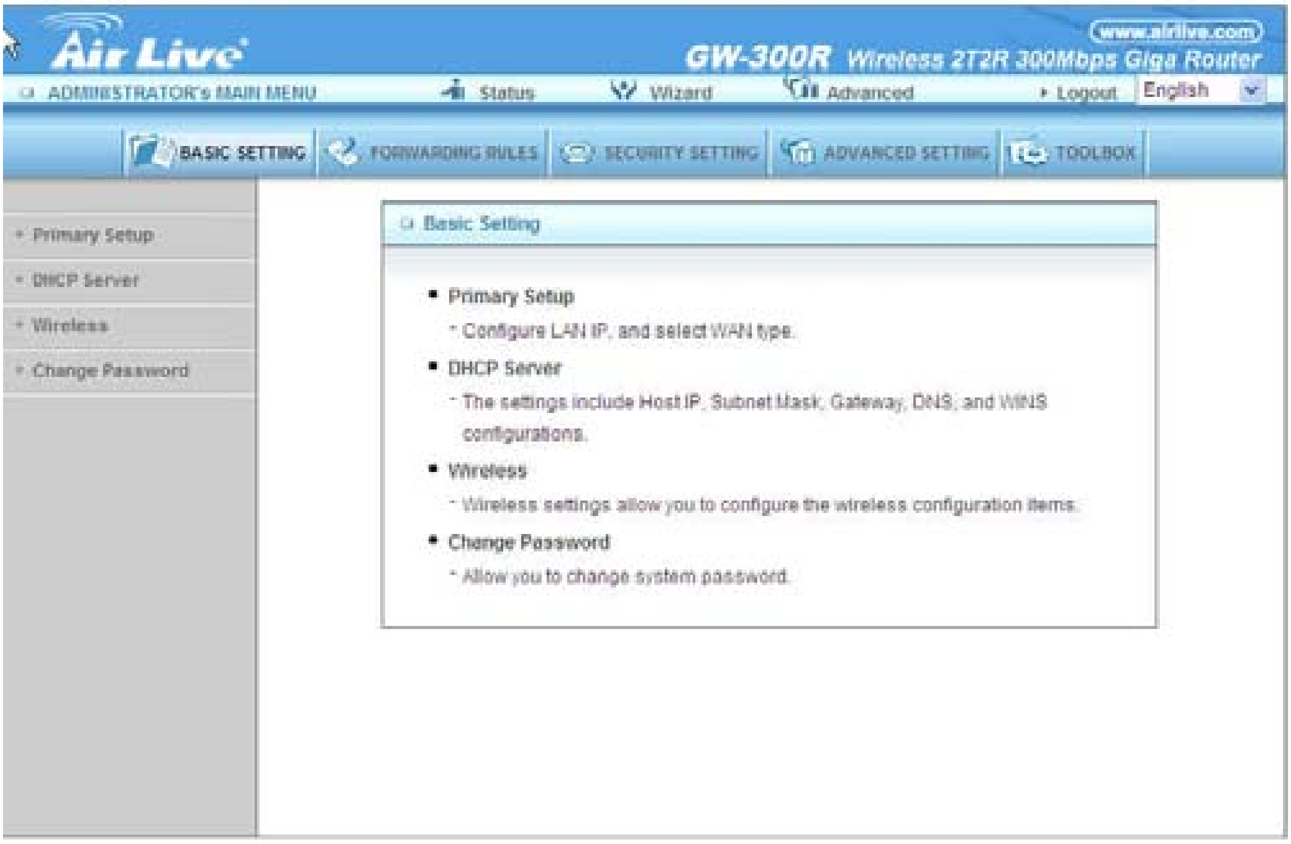
Configuration is Completed.

Please click "Finish" to back to Status page.

Or you can click "Configure Again" to setup the wizard again.

Configure Again [Start > Password > WAN > Wireless > Summary > Finish!] Finish

3.2 System Status



Basic Setting

- Primary Setup
  - Configure LAN IP, and select WAN type.
- DHCP Server
  - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless
  - Wireless settings allow you to configure the wireless configuration items.
- Change Password
  - Allow you to change system password.

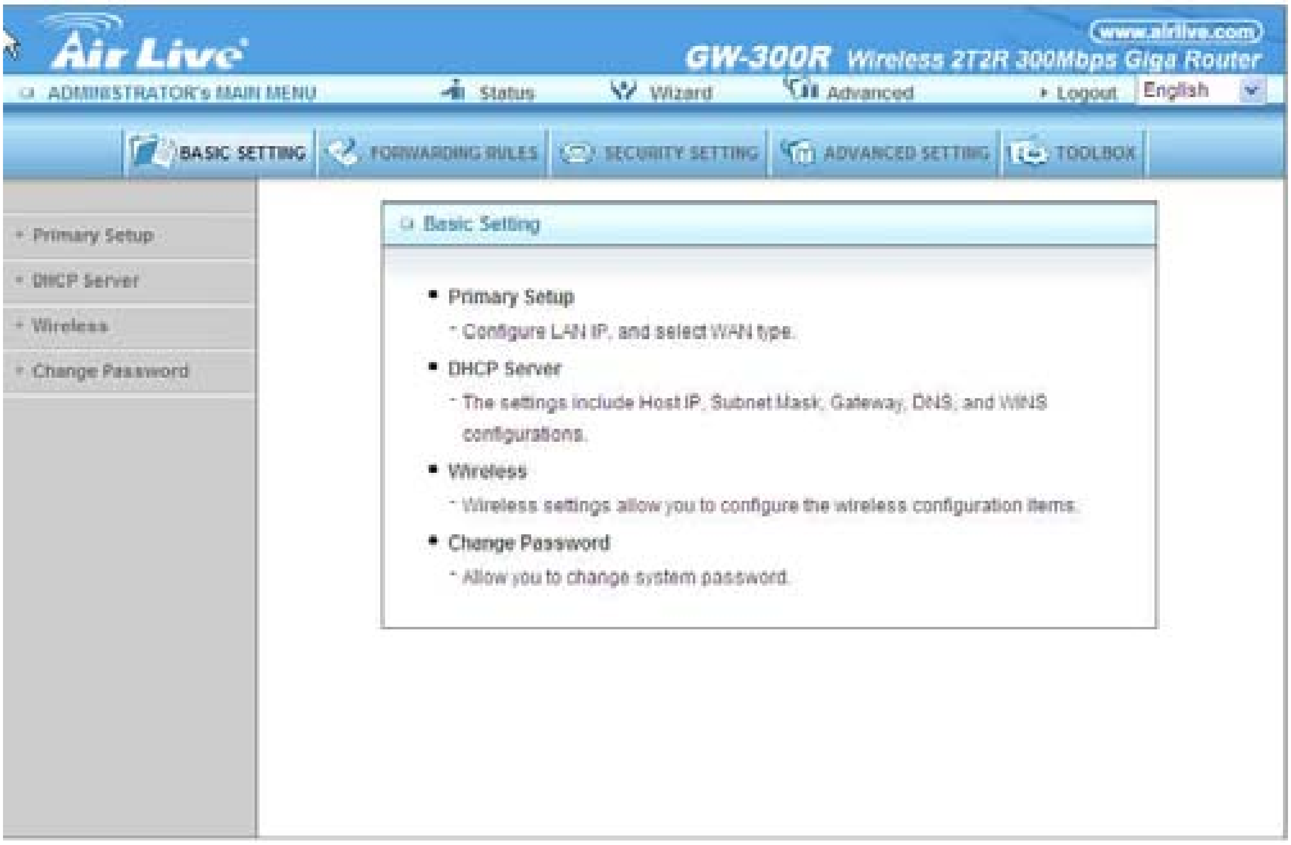
This option provides the function for observing this product's working status:
WAN Port Status.
If the WAN port is assigned a dynamic IP, there may appear a "Renew" or "Release" button on the Sidenote column. You can click this button to renew or release IP manually.

Statistics of WAN: enables you to monitor inbound and outbound packets

3.3 Advanced

3.3.1 Basic Setting

Please Select “Advanced Setup” to Setup

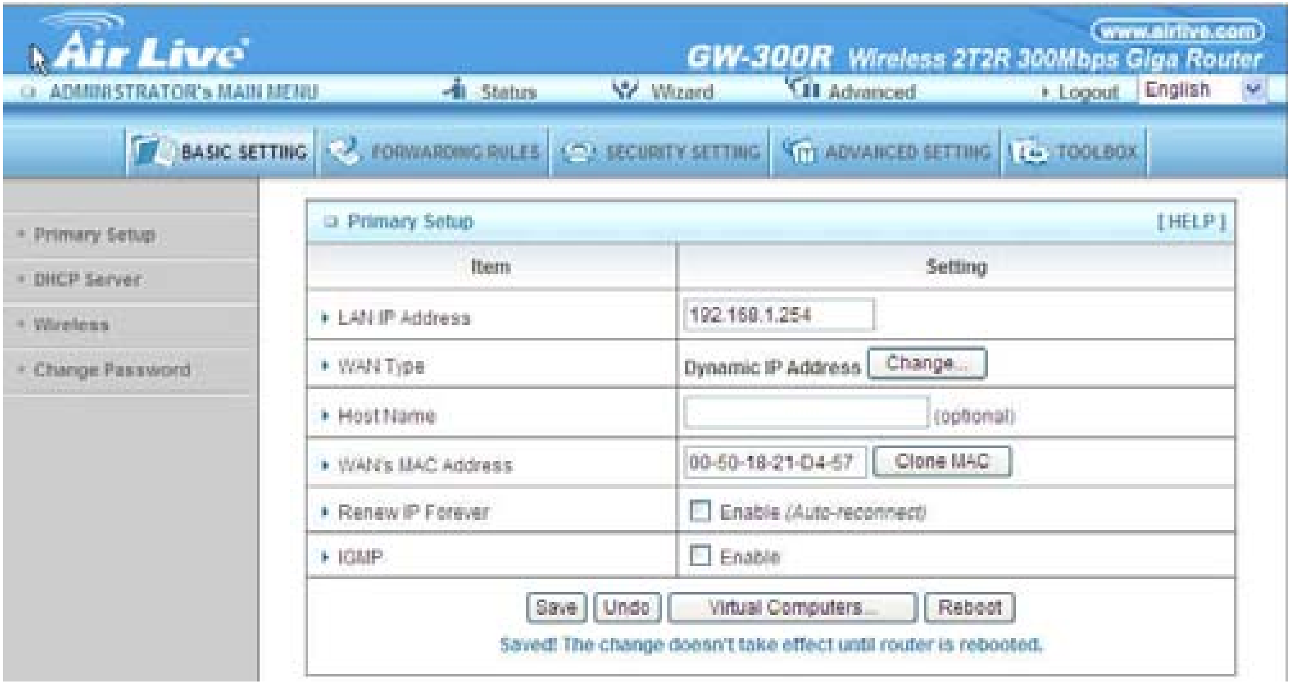


Basic Setting

- Primary Setup
  - Configure LAN IP, and select WAN type.
- DHCP Server
  - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless
  - Wireless settings allow you to configure the wireless configuration items.
- Change Password
  - Allow you to change system password.

3.3.1.1 Primary Setup – WAN Type, Virtual Computers

Press “Change”



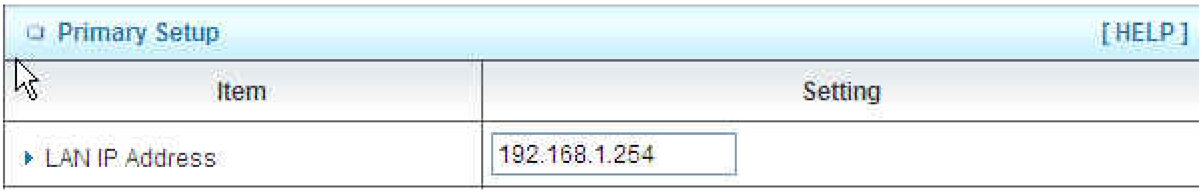
Primary Setup [HELP]

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	Dynamic IP Address Change...
Host Name	(optional)
WAN's MAC Address	00-50-18-21-D4-57 Clone MAC
Renew IP Forever	□ Enable *(Auto-reconnect)*
IGMP	□ Enable

Saved! The change doesn't take effect until router is rebooted.

This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

LAN IP Address: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.



Primary Setup [HELP]

Item	Setting
LAN IP Address	192.168.1.254

WAN Type: WAN connection type of your ISP. You can click Change button to choose a correct one from the following four options:

Static IP Address: ISP assigns you a static IP address.

Dynamic IP Address: Obtain an IP address from ISP automatically.

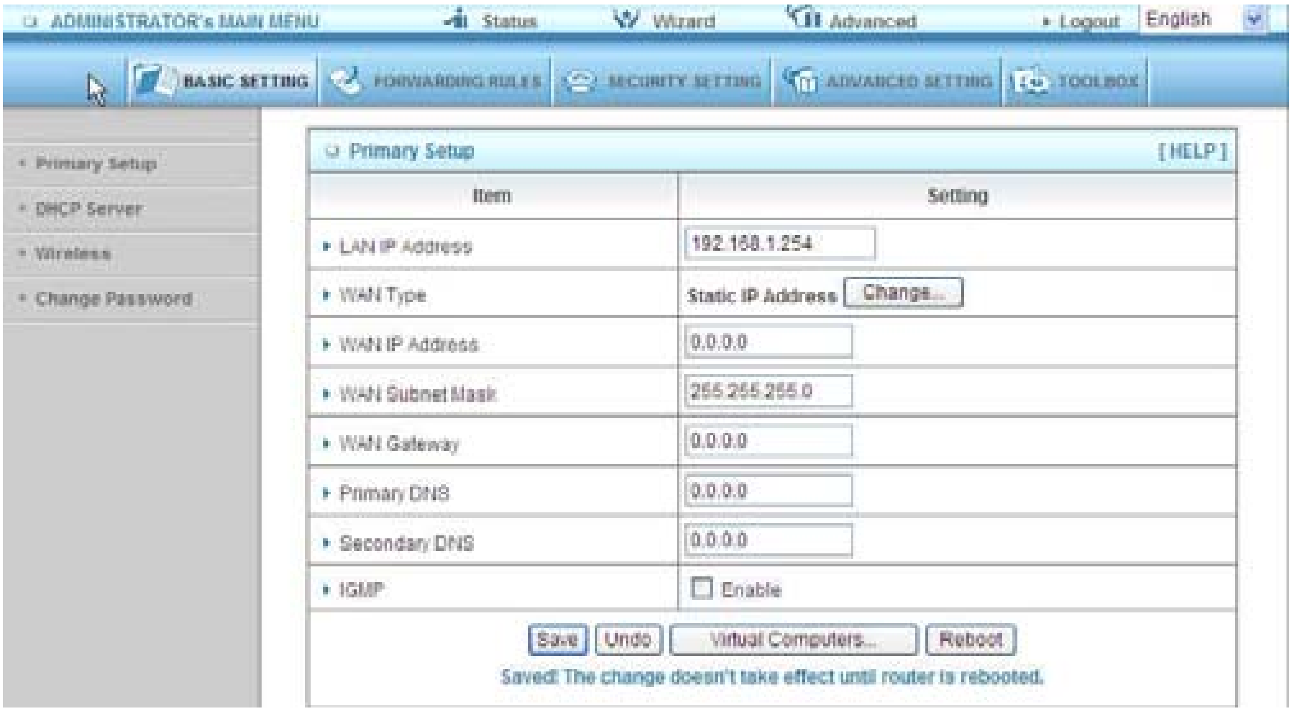
PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.

PPTP: Some ISPs require the use of PPTP to connect to their services.

F. L2TP: Some ISPs require the use of L2TP to connect to their services

Static IP Address: ISP assigns you a static IP address:

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.



Primary Setup

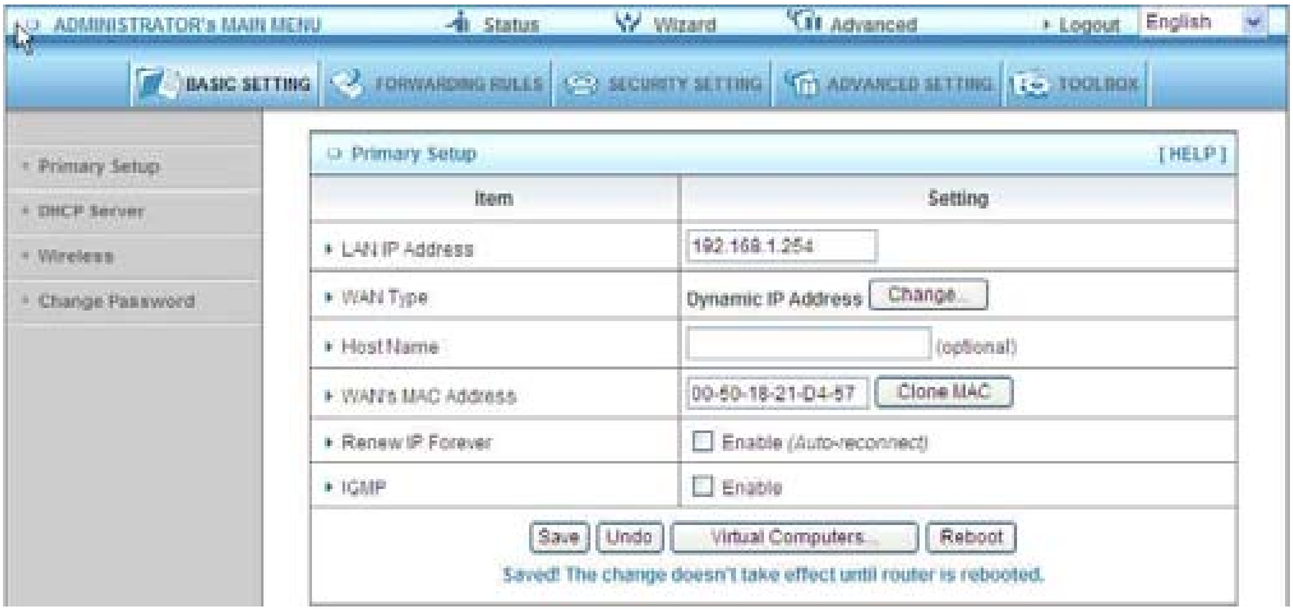
Item	Setting
LAN IP Address	192.168.1.254
WAN Type	Static IP Address
WAN IP Address	0.0.0.0
WAN Subnet Mask	255.255.255.0
WAN Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
IGMP	□ Enable

Saved! The change doesn't take effect until router is rebooted.

Dynamic IP Address: Obtain an IP address from ISP automatically.

Host Name: optional. Required by some ISPs, for example, @Home.

Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.



Primary Setup

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	Dynamic IP Address
Host Name	(optional)
WAN's MAC Address	00-50-18-21-D4-57
Renew IP Forever	□ Enable (Auto-reconnect)
IGMP	□ Enable

Saved! The change doesn't take effect until router is rebooted.

PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.

Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session.

Set it to zero or enable Auto-reconnect to disable this feature.

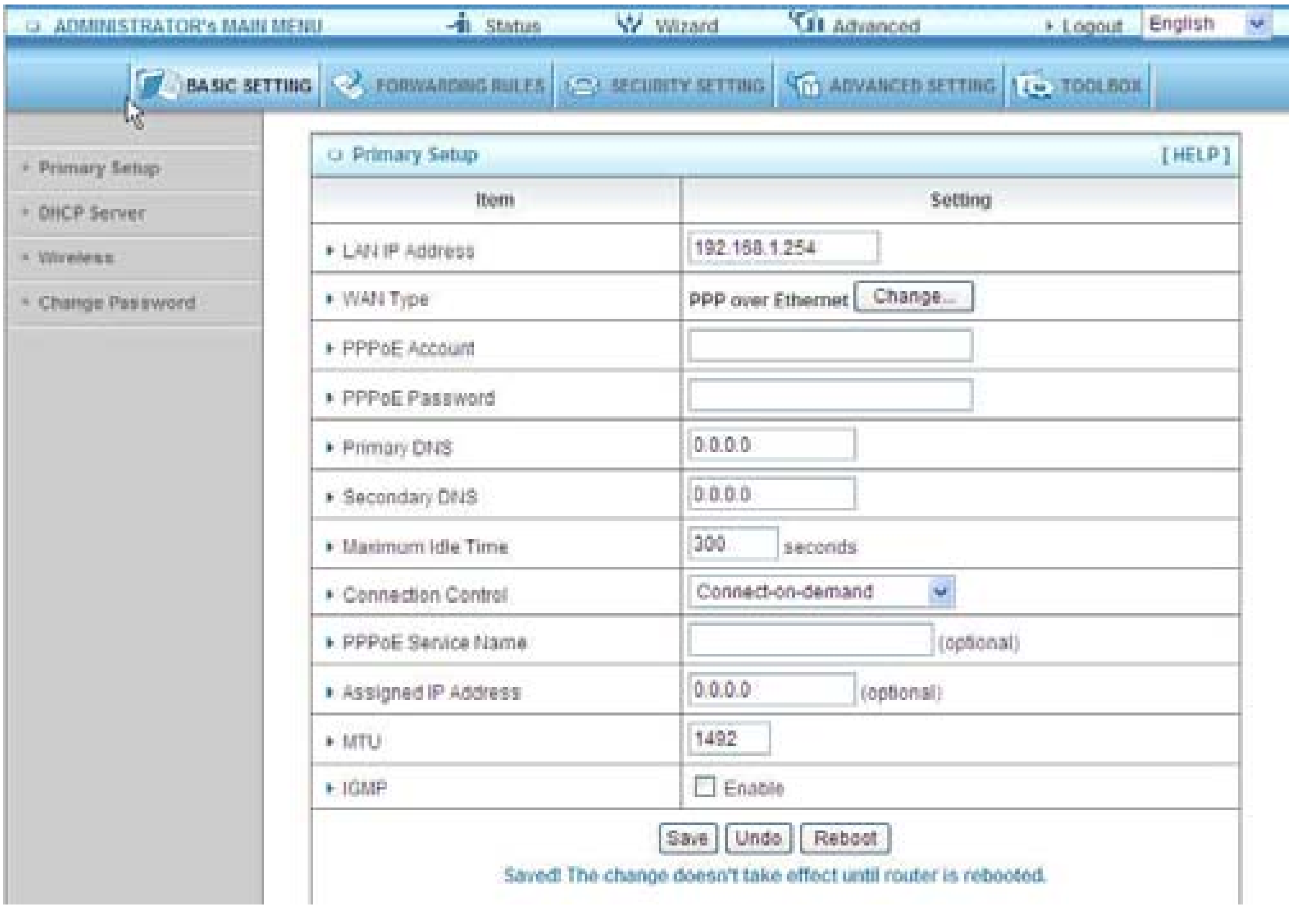
Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link with ISP until the connection is established.

Manually : The device will not make the link until someone clicks the connect-button in the Staus-page.



Primary Setup

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	PPP over Ethernet Change...
PPPoE Account	
PPPoE Password	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
PPPoE Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)
MTU	1492
IGMP	□ Enable

Saved! The change doesn't take effect until router is rebooted.

PPTP: Some ISPs require the use of PPTP to connect to their services

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

2. Server IP Address: the IP address of the PPTP server.

3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't
want to change the password, keep it empty.

4. Connection ID: optional. Input the connection ID if your ISP requires it.

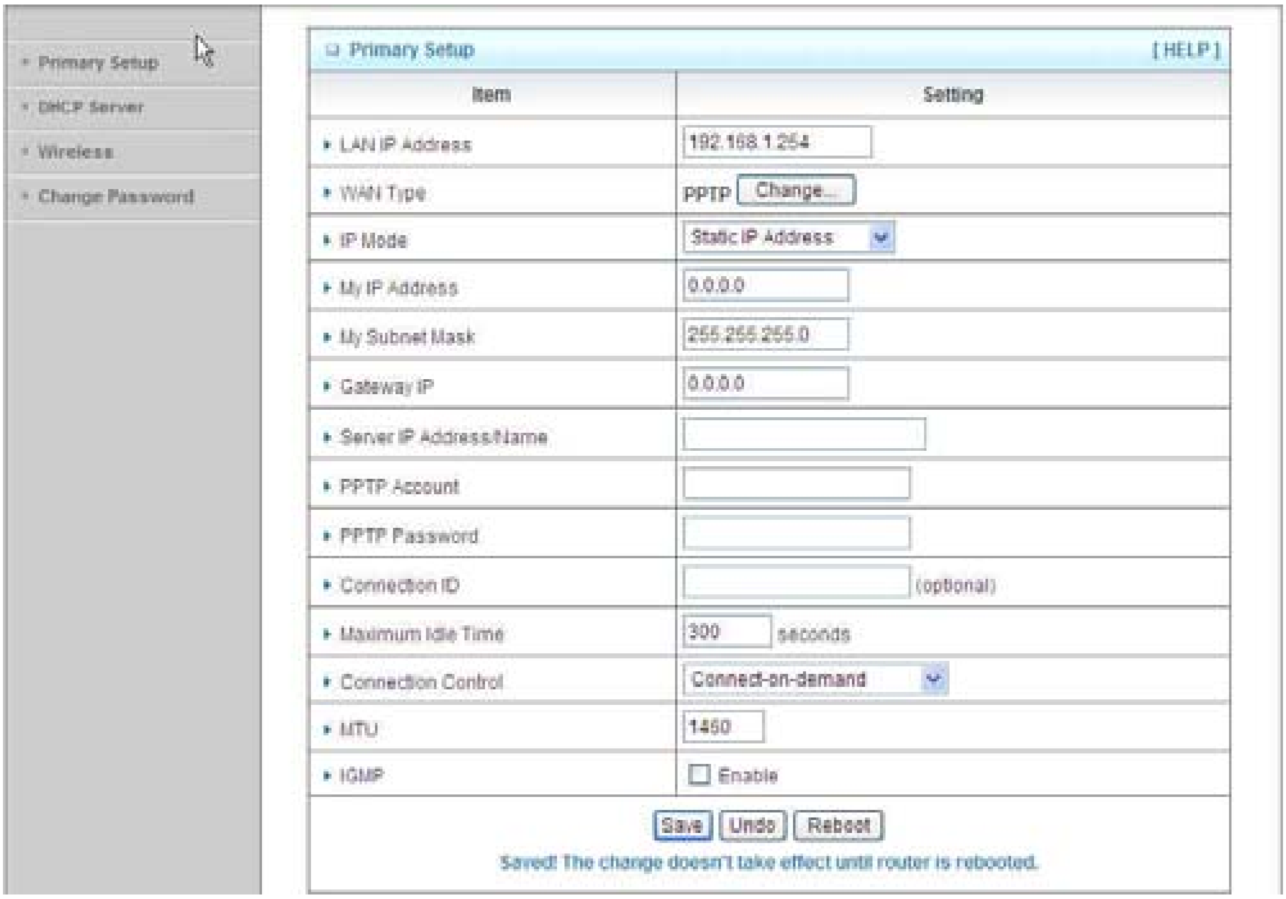
5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Staus-page.



Primary Setup [HELP]

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	PPTP Change...
IP Mode	Static IP Address
My IP Address	0.0.0.0
My Subnet Mask	255.255.255.0
Gateway IP	0.0.0.0
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
MTU	1460
IGMP	□ Enable

Save Undo Reboot

Saved! The change doesn't take effect until router is rebooted.

L2TP: Some ISPs require the use of L2TP to connect to their services

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned
to you.

2. Server IP Address: the IP address of the PPTP server.

3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't
want to change the password, keep it empty.

3. Connection ID: optional. Input the connection ID if your ISP requires it.

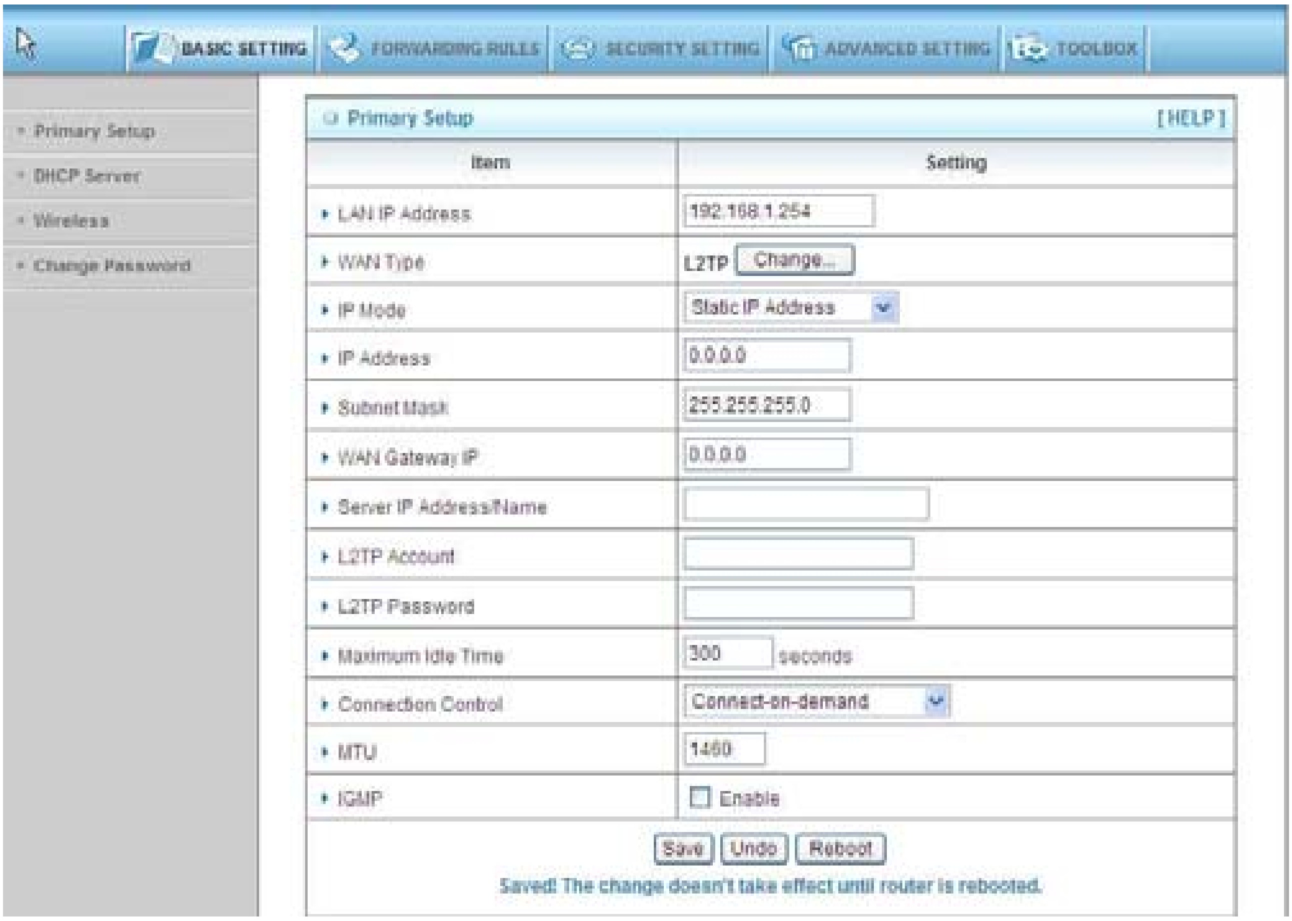
4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on):The device will link with ISP until the connection is established.

Manually :The device will not make the link until someone clicks the connect-button in the Staus-page.

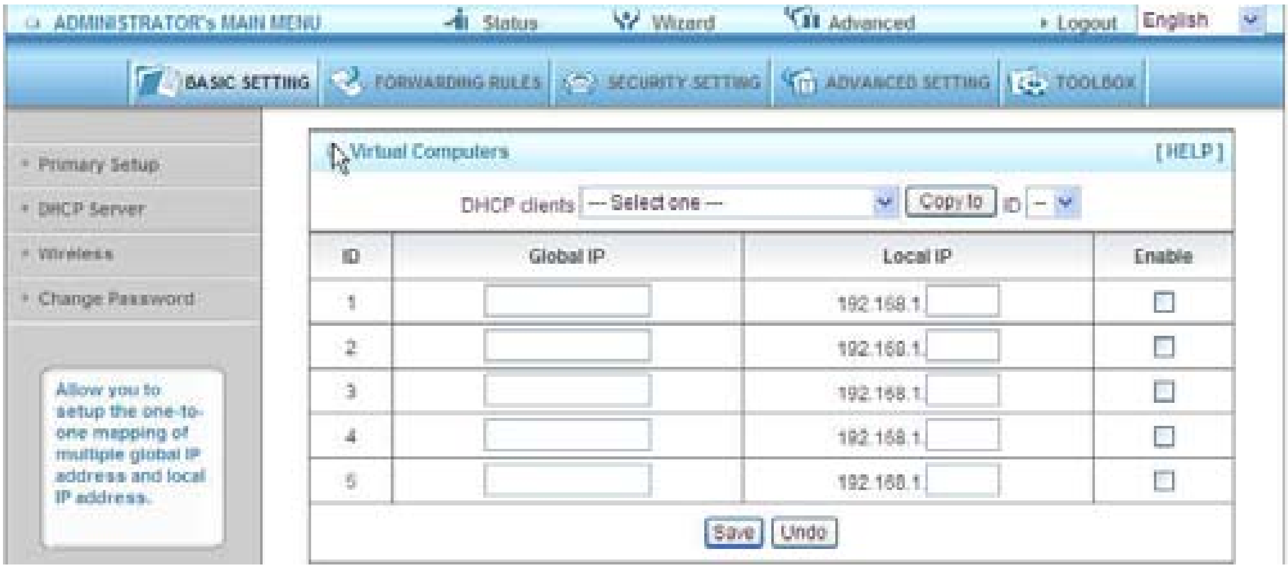


Primary Setup

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	L2TP Change...
IP Mode	Static IP Address
IP Address	0.0.0.0
Subnet Mask	255.255.255.0
WAN Gateway IP	0.0.0.0
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
MTU	1460
IGMP	□ Enable

Saved! The change doesn't take effect until router is rebooted.

Virtual Computers(Only for Static and dynamic IP address Wan type)



Allow you to setup the one-to-one mapping of multiple global IP address and local IP address.

Virtual Computers

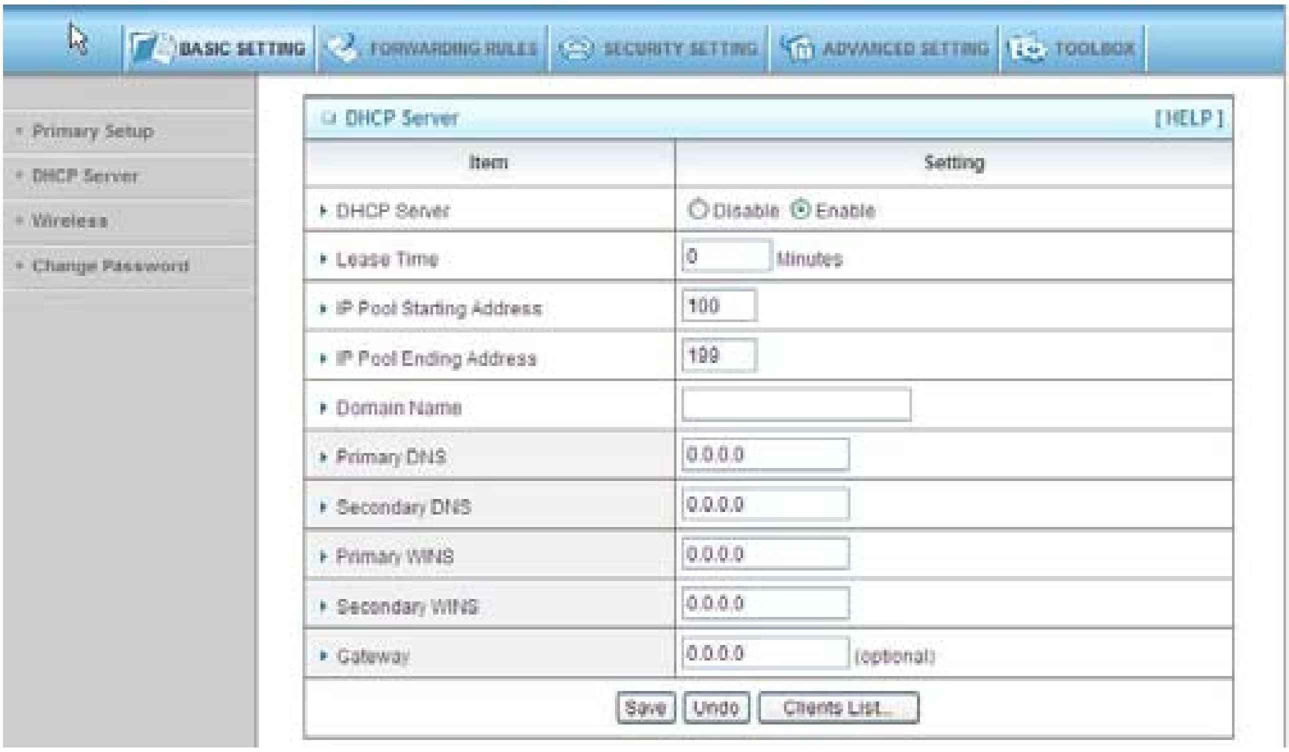
DHCP clients --- Select one --- ID --

ID	Global IP	Local IP	Enable
1		192.168.1.	□
2		192.168.1.	□
3		192.168.1.	□
4		192.168.1.	□
5		192.168.1.	□

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.
Global IP: Enter the global IP address assigned by your ISP.
Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.

Enable: Check this item to enable the Virtual Computer feature.

3.3.1.2 DHCP Server



DHCP Server [HELP]

Item	Setting
DHCP Server	○ Disable ● Enable
Lease Time	0 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Gateway	0.0.0.0 (optional)

Press “More>>”

DHCP Server: Choose “Disable” or “Enable.”

Lease time: This is the length of time that the client may use the IP address it has been Assigned by dhcp server.

IP pool starting Address/ IP pool starting Address: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

Domain Name: Optional, this information will be passed to the client.

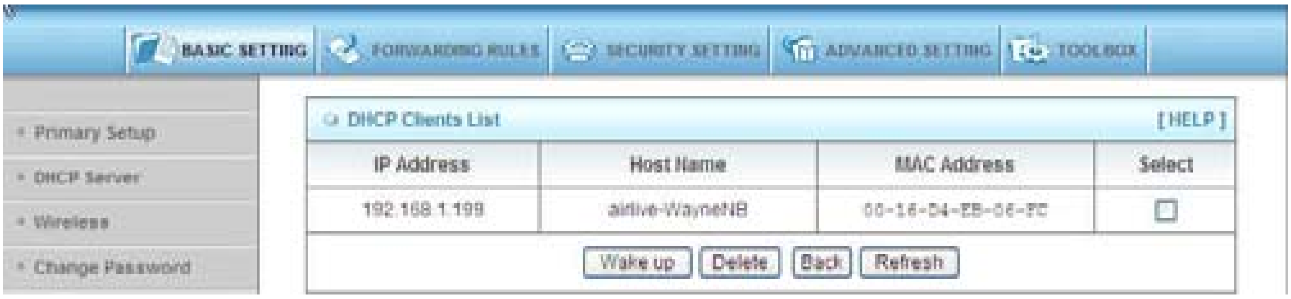
Primary DNS/Secondary DNS: This feature allows you to assign DNS Servers

Primary WINS/Secondary WINS: This feature allows you to assign WINS Servers

Gateway: The Gateway Address would be the IP address of an alternate Gateway.

This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

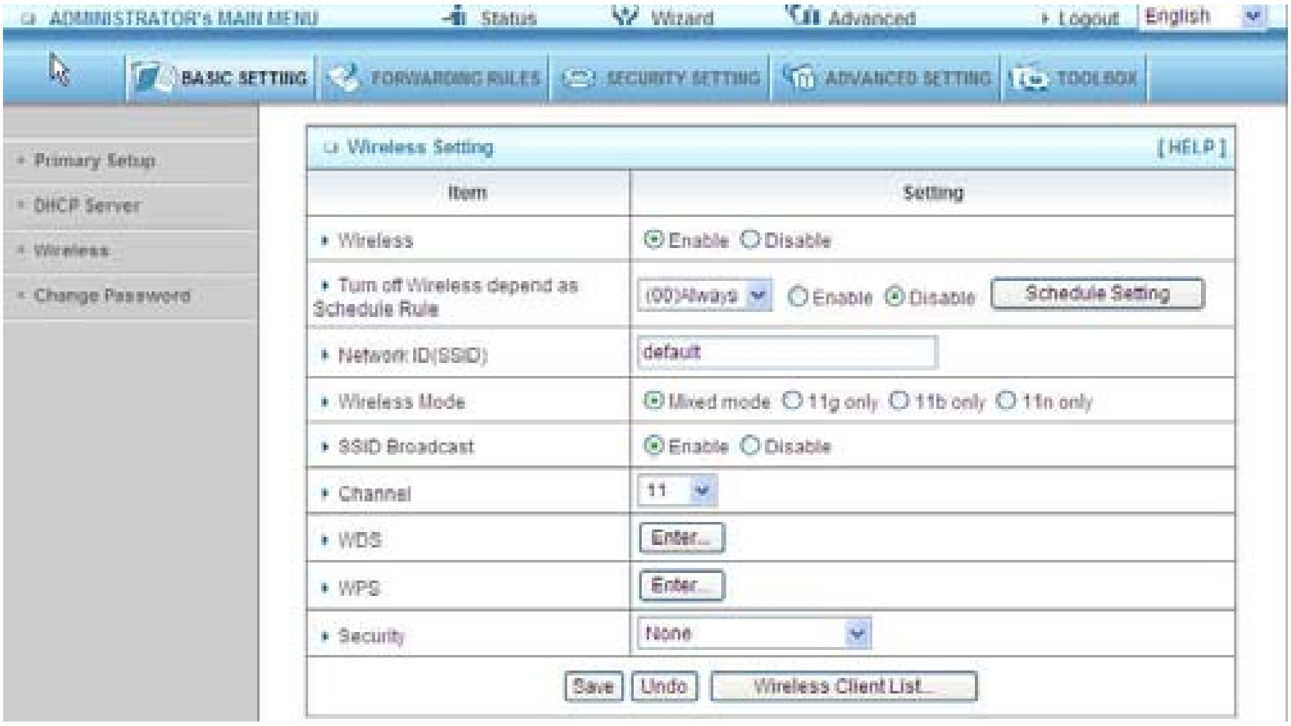
DHCP Client List:



DHCP Clients List

IP Address	Host Name	MAC Address	Select
192.168.1.199	airlive-WayneNB	00-16-D4-EB-06-FC	☐

3.3.1.3 Wireless



Wireless Setting

Item	Setting
Wireless	● Enable ○ Disable
Turn off Wireless depend as Schedule Rule	(00)Always ○ Enable ● Disable [Schedule Setting]
Network ID(SSID)	default
Wireless Mode	● Mixed mode ○ 11g only ○ 11b only ○ 11n only
SSID Broadcast	● Enable ○ Disable
Channel	11
WDS	[Enter...]
WPS	[Enter...]
Security	None

Wireless settings allow you to set the wireless configuration items.
Wireless : The user can enable or disalbe wireless function.

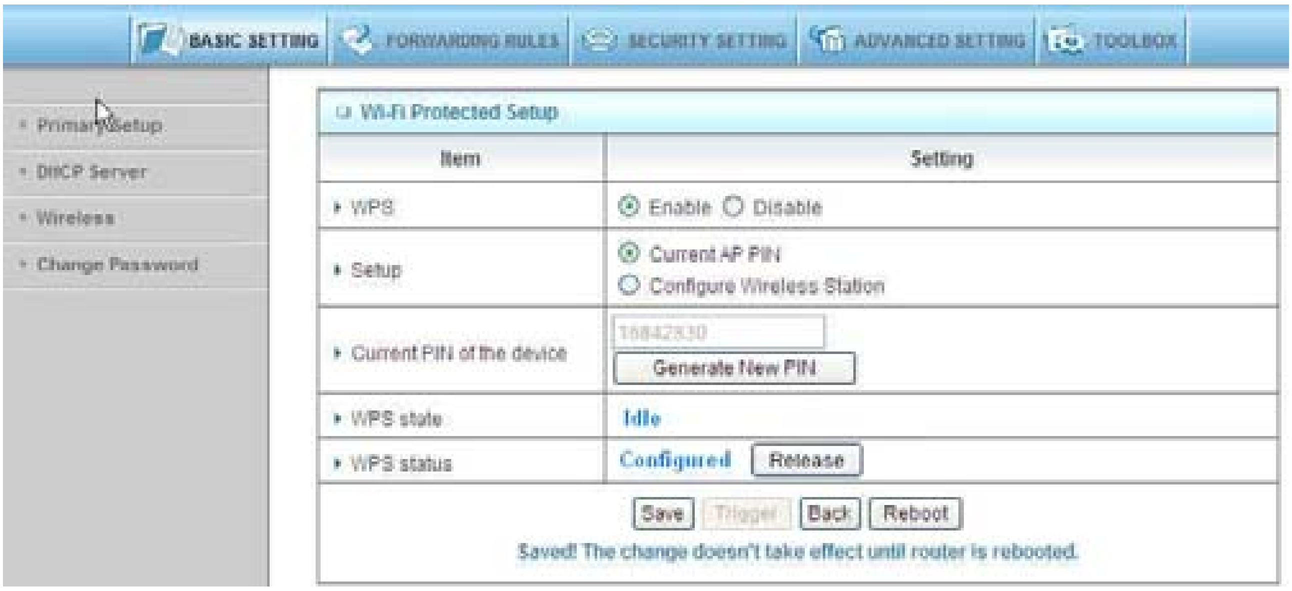
Wireless On/Off by time Schedule: The device can turn off Wireless depend as Schedule.

Network ID (SSID): Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “default”)

SSID Broadcast: The router will Broadcast beacons that have some information, including ssid so that the wireless clients can know how many ap devices by scanning function in the network. Therefore, this function is disabled, the wireless clients can not find the device from beacons.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain.

WPS (WiFi Protection Setup)
WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and
easy way in Wireless Connection.

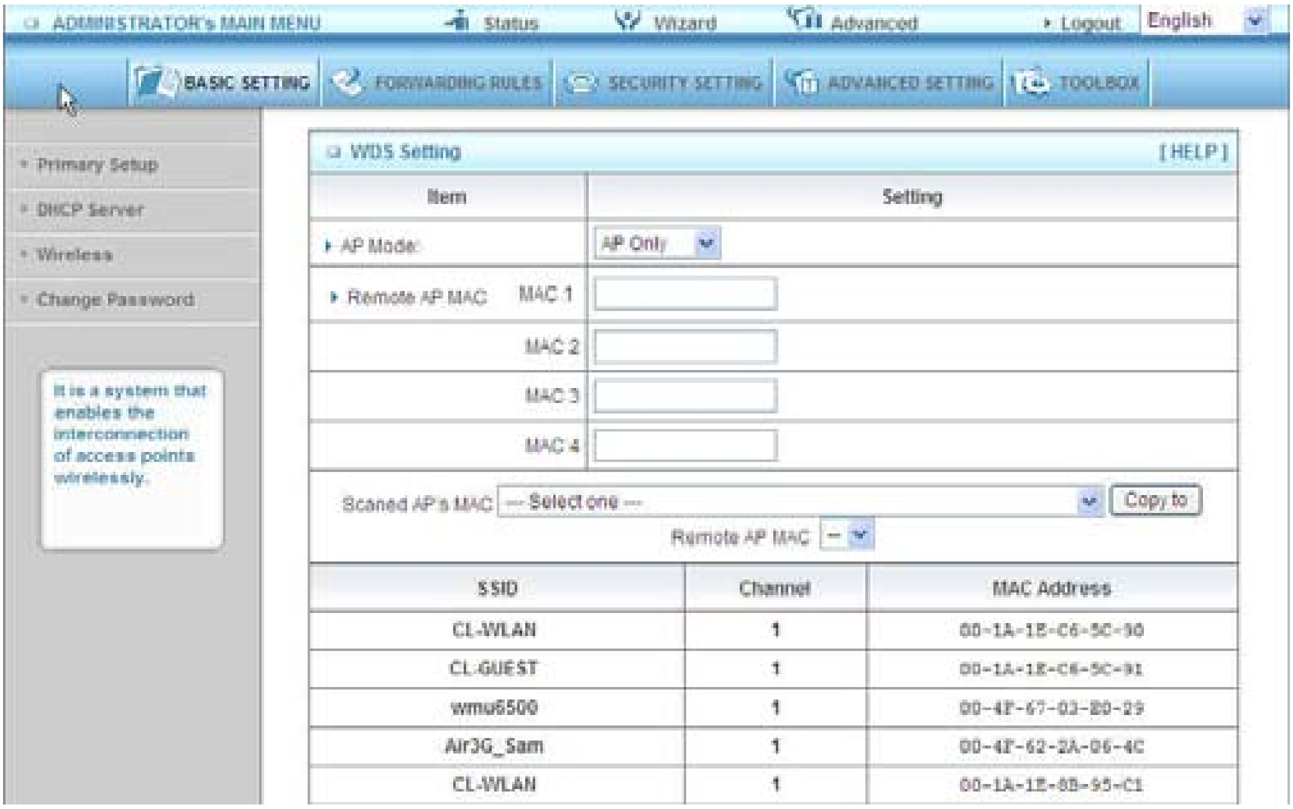


Wi-Fi Protected Setup

Item	Setting
WPS	● Enable ○ Disable
Setup	● Current AP PIN ○ Configure Wireless Station
Current PIN of the device	16842830 Generate New PIN
WPS state	Idle
WPS status	Configured Release

Saved! The change doesn't take effect until router is rebooted.

WDS(Wireless Distribution System)
WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.
Hybrid Mode
It means the device can support WDS and AP Mode simultaneously.



It is a system that enables the interconnection of access points wirelessly.

WDS Setting

Item	Setting
AP Mode:	AP Only
Remote AP MAC MAC 1	
MAC 2	
MAC 3	
MAC 4	

Scaned AP's MAC --- Select one ---

Remote AP MAC --

SSID	Channel	MAC Address
CL-WLAN	1	00-1A-1E-C6-5C-90
CL-GUEST	1	00-1A-1E-C6-5C-91
wmu6500	1	00-4F-67-03-B0-29
Air3G_Sam	1	00-4F-62-2A-06-4C
CL-WLAN	1	00-1A-1E-8B-95-C1

Security: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

There are several security types to use:

WEP :

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

802.1X

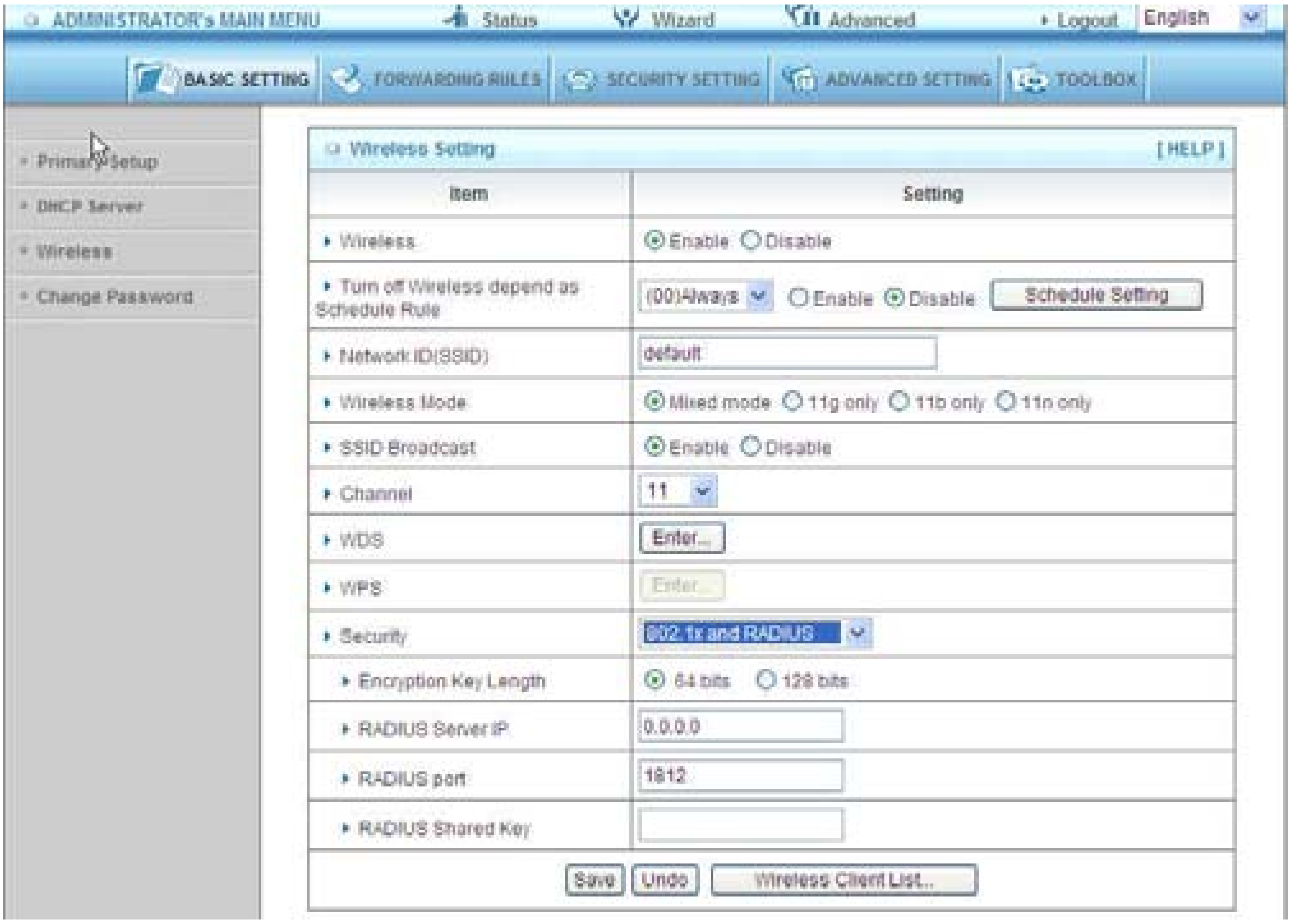
Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

RADIUS Server

IP address or the 802.1X server's domain-name.

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.



Wireless Setting

Item	Setting
Wireless	● Enable ○ Disable
Turn off Wireless depend as Schedule Rule	(00)Always ○ Enable ● Disable Schedule Setting
Network ID(SSID)	default
Wireless Mode	● Mixed mode ○ 11g only ○ 11b only ○ 11n only
SSID Broadcast	● Enable ○ Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	802.1x and RADIUS
Encryption Key Length	● 64 bits ○ 128 bits
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

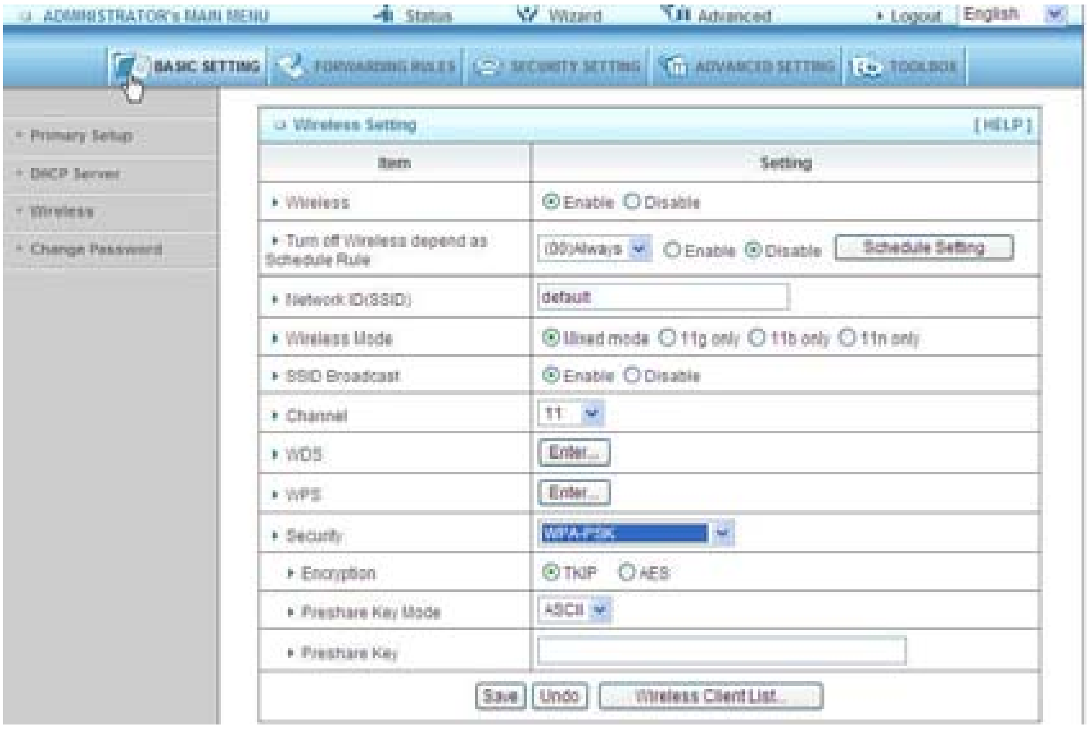
WPA-PSK

1. Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678



Wireless Setting [HELP]

Item	Setting
Wireless	● Enable ○ Disable
Turn off Wireless depend as Schedule Rule	(00)Always ○ Enable ● Disable [Schedule Setting]
Network ID(SSID)	default
Wireless Mode	● Mixed mode ○ 11g only ○ 11b only ○ 11n only
SSID Broadcast	● Enable ○ Disable
Channel	11
WDS	[Enter...]
WPS	[Enter...]
Security	WPA-PSK
Encryption	● TKIP ○ AES
Preshare Key Mode	ASCII
Preshare Key	

[Save] [Undo] [Wireless Client List...]

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA2-PSK(AES)

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

WPA2(AES)

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server

IP address or the 802.1X server's domain-name.

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK /WPA2-PSK

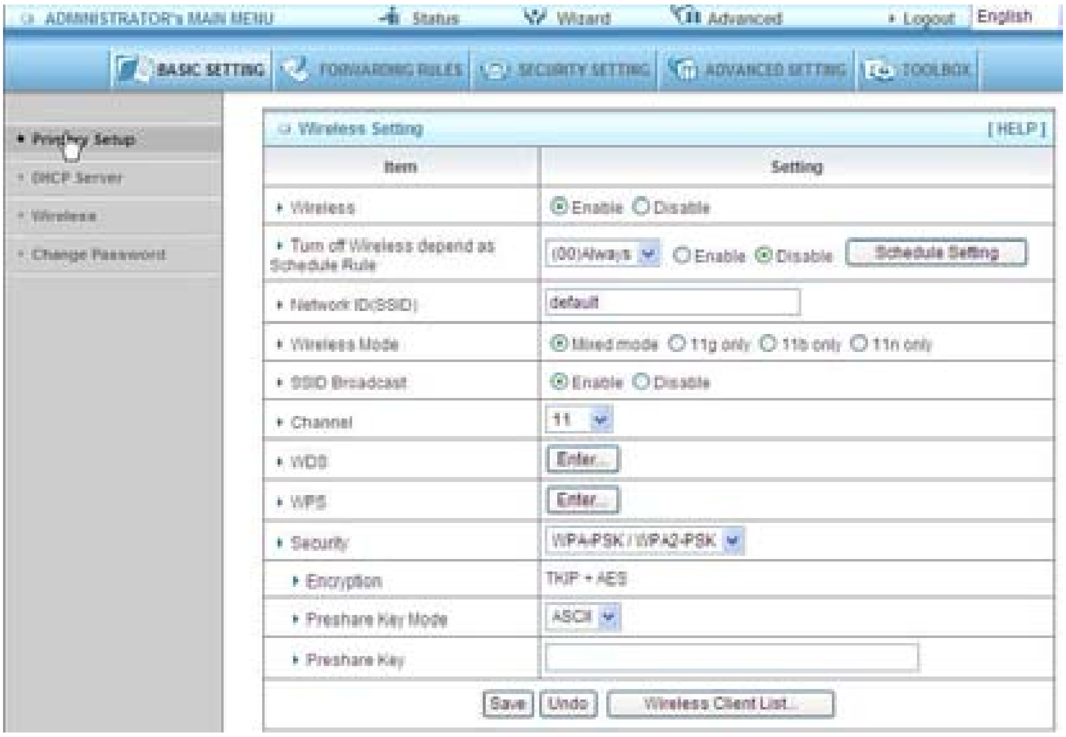
The router will detect automatically which Security type the client uses to encrypt.

1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678



Wireless Setting

Item	Setting
Wireless	● Enable ○ Disable
Turn off Wireless depend as Schedule Rule	(00)Always ○ Enable ● Disable Schedule Setting
Network ID(SSID)	default
Wireless Mode	● Mixed mode ○ 11g only ○ 11b only ○ 11n only
SSID Broadcast	● Enable ○ Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WPA-PSK / WPA2-PSK
Encryption	TKIP + AES
Preshare Key Mode	ASCII
Preshare Key	

WPA/WPA2

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service. RADIUS Server

The router will detect automatically which Security type(Wpa-psk version 1 or 2) the client uses to encrypt.

IP address or the 802.1X server's domain-name.

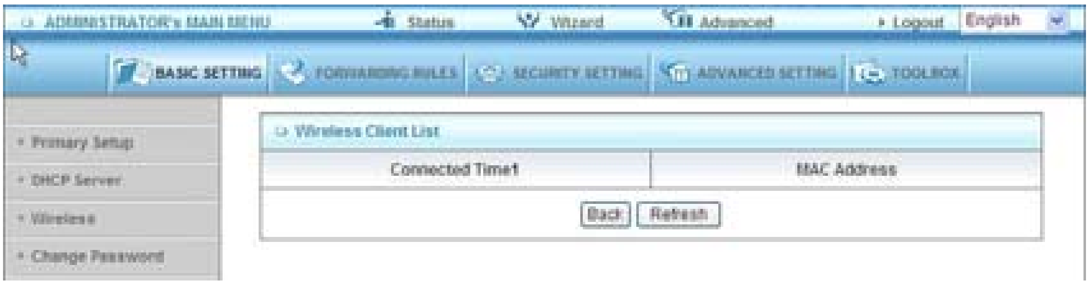
Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

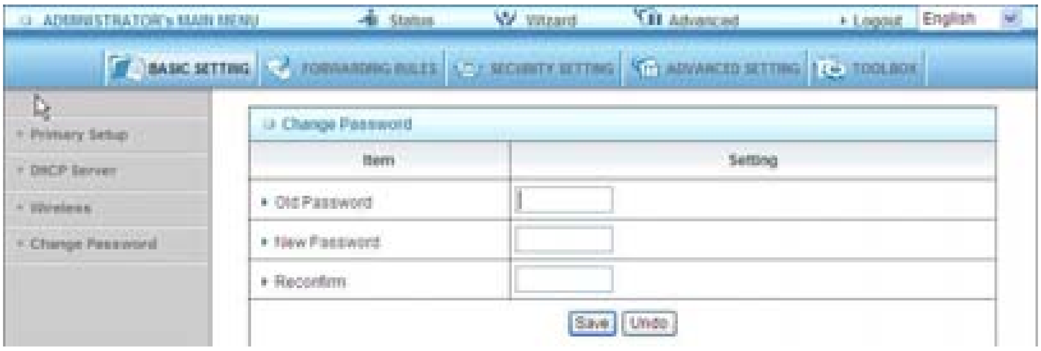
Wireless Client List



Wireless Client List

Connected Time1	MAC Address

3.3.1.4 Change Password

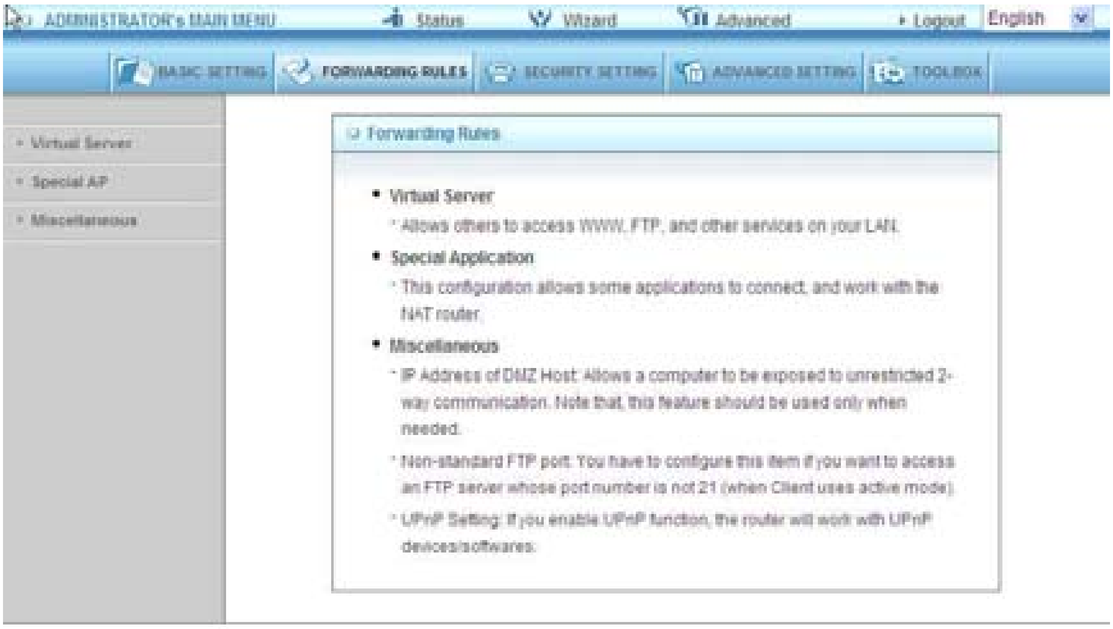


Change Password

Item	Setting
Old Password	
New Password	
Reconfirm	

You can change Password here. We strongly recommend you to change the system password for security reason.

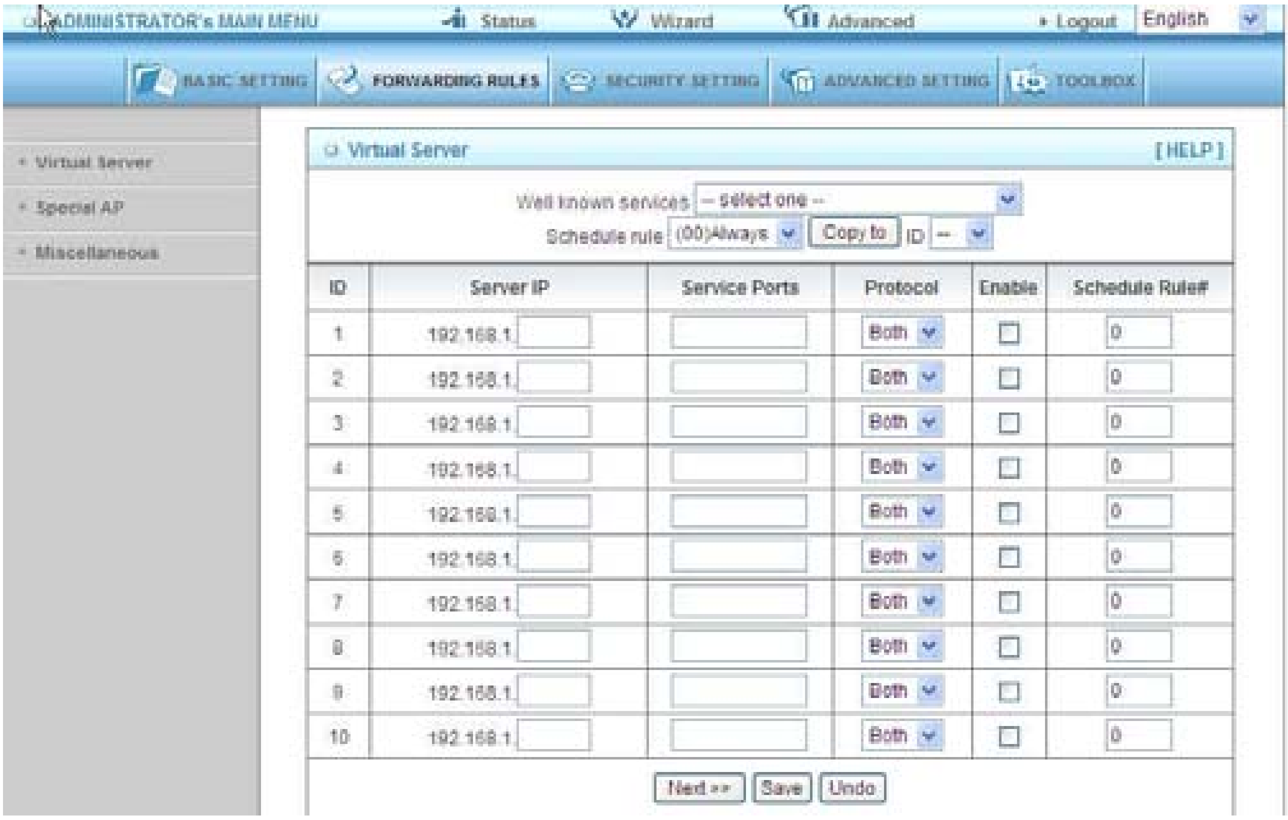
3.3.2 Forwarding Rules



Forwarding Rules

- Virtual Server
  - Allows others to access WWW, FTP, and other services on your LAN.
- Special Application
  - This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous
  - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
  - Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).
  - UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

3.3.2.1 Virtual Server



Virtual Server

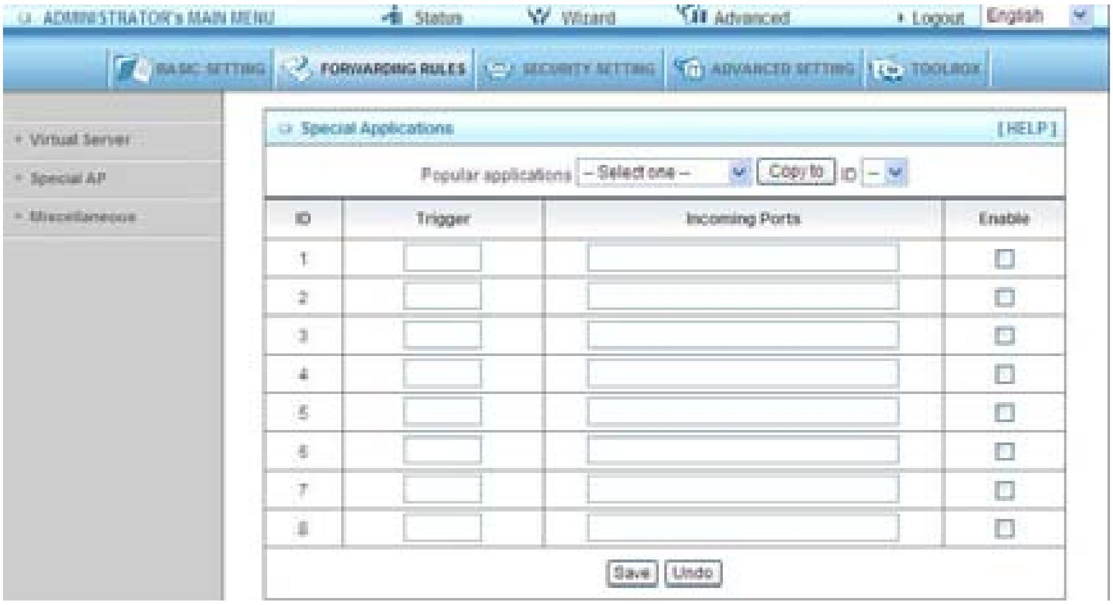
Well known services: -- select one --

Schedule rule: (00)Always ID --

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.1.		Both	□	0
2	192.168.1.		Both	□	0
3	192.168.1.		Both	□	0
4	192.168.1.		Both	□	0
5	192.168.1.		Both	□	0
6	192.168.1.		Both	□	0
7	192.168.1.		Both	□	0
8	192.168.1.		Both	□	0
9	192.168.1.		Both	□	0
10	192.168.1.		Both	□	0

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.
A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

3.3.2.2 Special AP



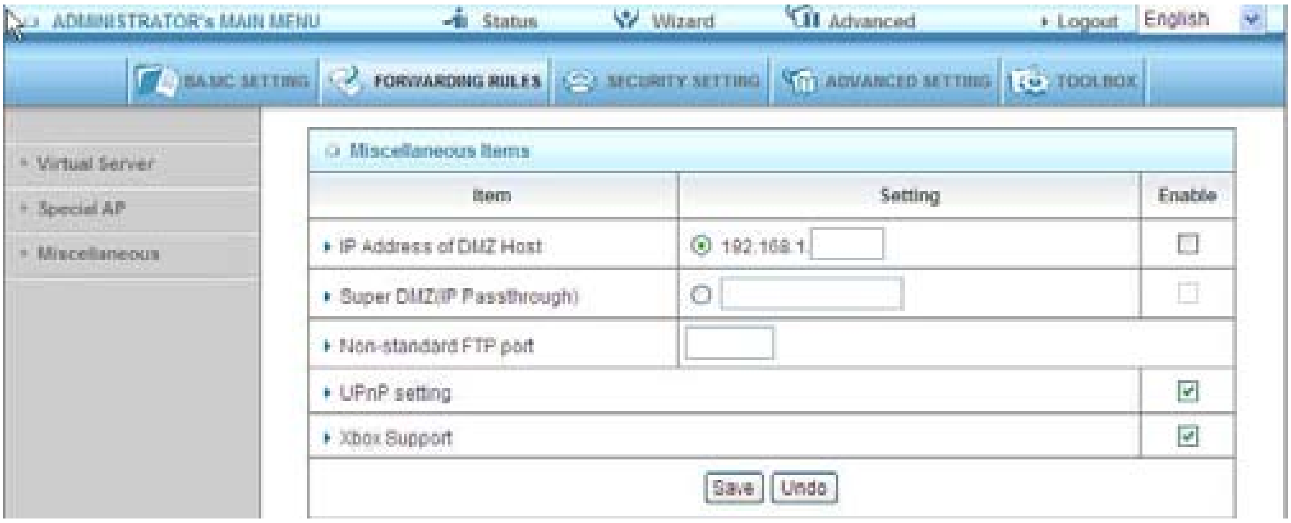
Special Applications

Popular applications -- Select one -- ID --

ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The Special Applications feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.
Trigger: the outbound port number issued by the application..
Incoming Ports: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
This product provides some predefined settings Select your application and click Copy to to add the predefined setting to your list.
Note! At any given time, only one PC can use each Special Application tunnel.

3.3.2.3 Miscellaneous Items



Miscellaneous Items

Item	Setting	Enable
▸ IP Address of DMZ Host	● 192.168.1.	□
▸ Super DMZ(IP Passthrough)	○	□
▸ Non-standard FTP port		
▸ UPnP setting		☑
▸ Xbox Support		☑

IP Address of DMZ Host

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

Super DMZ (IP Passthrough)

Super DMZ (IP Passthrough) is a useful feature if a host computer or server on the Local Area Network needs to have access into it from the internet with a real public IP address. With IP Passthrough configured, all IP traffic, not just TCP/UDP, is forwarded back to the host computer. This can be necessary with certain types of software that do not function reliably through Network Address Translation.

Non-standard FTP port

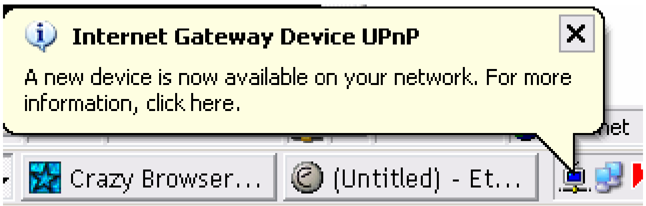
You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

Xbox Support

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

UpnP Setting

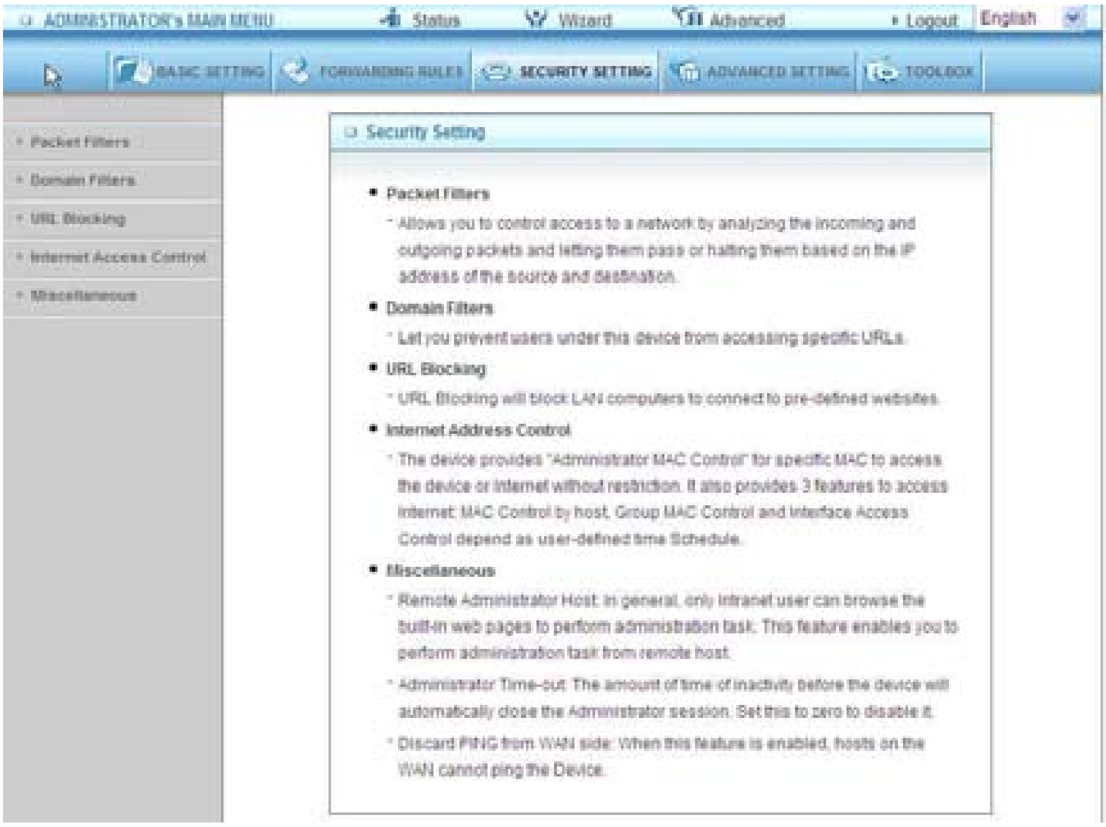
The device also supports this function.If the OS supports this function enable it,like Windows Xp.When the user get ip from Device and will see icon as below:



Internet Gateway Device UPnP

A new device is now available on your network. For more information, click here.

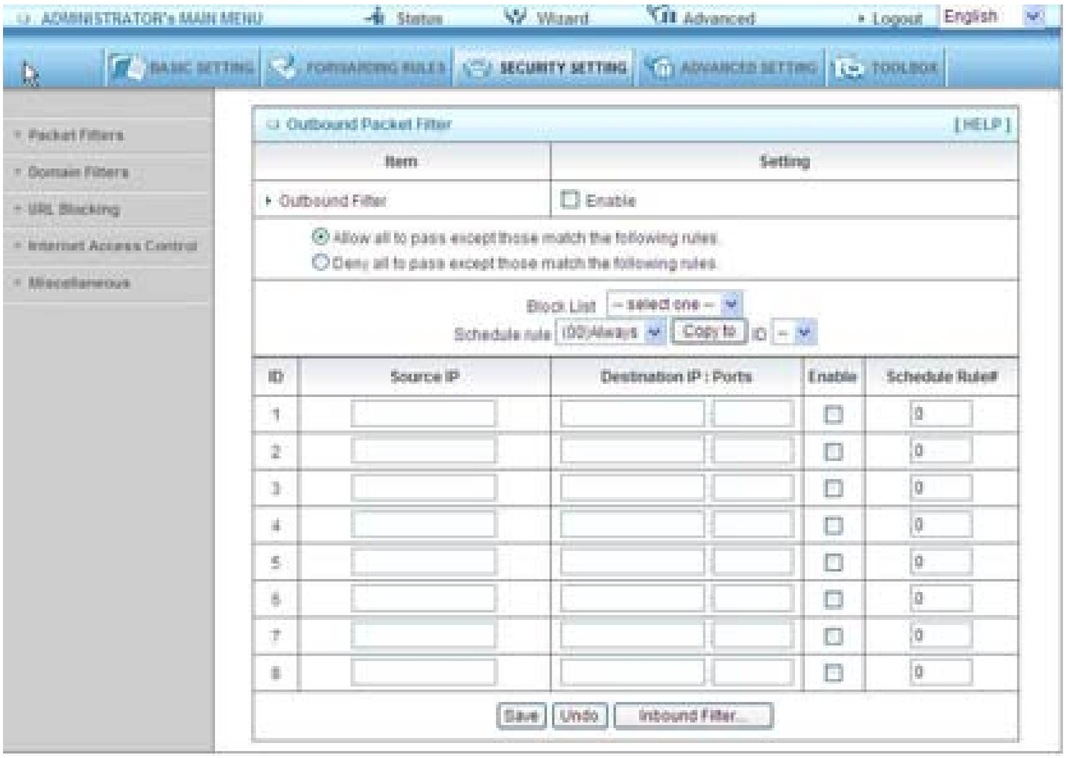
3.3.3 Security Settings



Security Setting

- Packet Filters
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters
  - Let you prevent users under this device from accessing specific URLs.
- URL Blocking
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- Internet Address Control
  - The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.
- Miscellaneous
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.3.3.1 Packet Filters



Outbound Packet Filter

Item	Setting
Outbound Filter	□ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

Block List: -- select one --
Schedule rule: (00)Always · Copy to · ID: --

ID	Source IP	Destination IP : Ports		Enable	Schedule Rule#
1				□	0
2				□	0
3				□	0
4				□	0
5				□	0
6				□	0
7				□	0
8				□	0

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

Allow all to pass except those match the specified rules

Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

Source IP address

Source port address

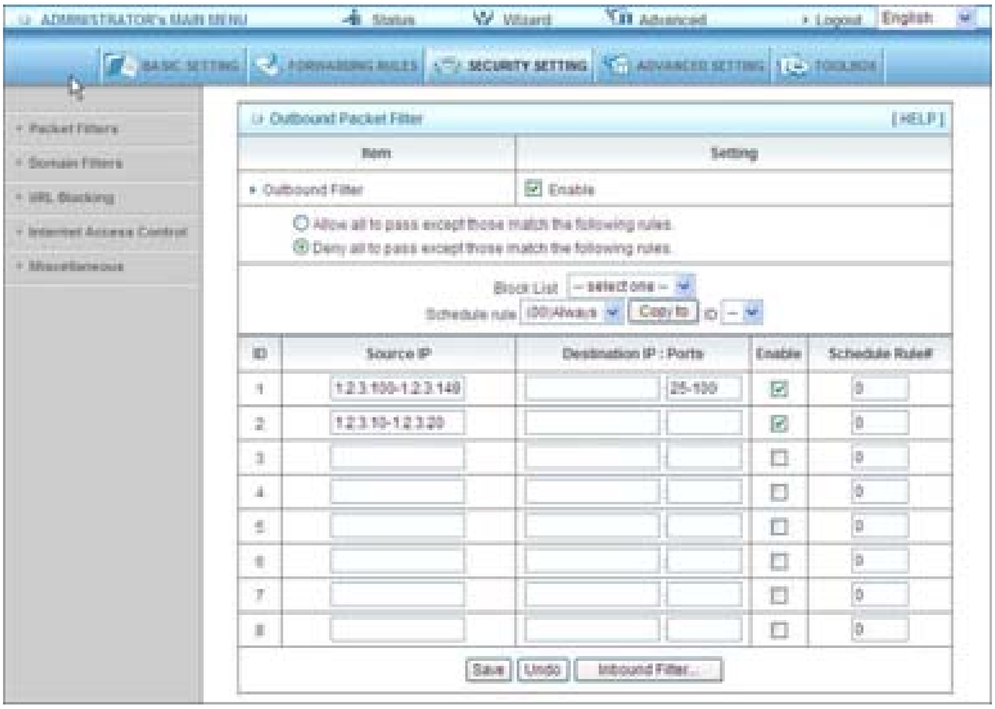
Destination IP address

Destination port address

Protocol: TCP or UDP or both.

Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.
Each rule can be enabled or disabled individually.
Inbound Filter:
To enable Inbound Packet Filter click the check box next to Enable in the Inbound Packet Filter field.
Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.
Example 1:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

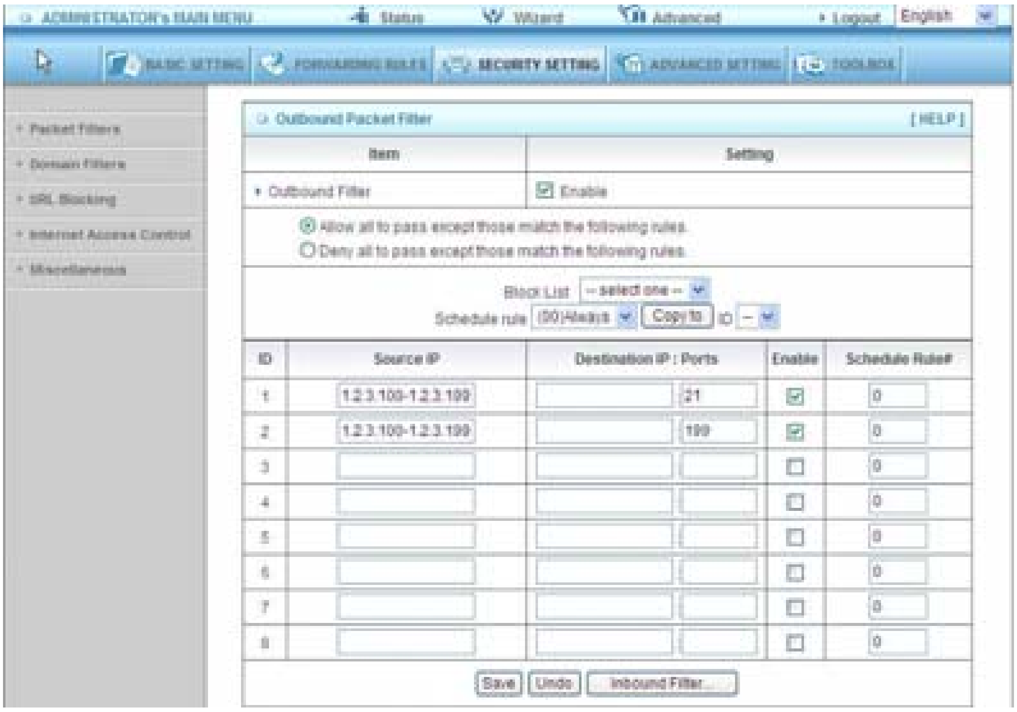
○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

Block List -- select one --
Schedule rule (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports		Enable	Schedule Rule#
1	1.2.3.100-1.2.3.149		25-100	☑	0
2	1.2.3.10-1.2.3.20			☑	0
3				□	0
4				□	0
5				□	0
6				□	0
7				□	0
8				□	0

(1.2.3.100-1.2.3.149) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)
(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing)
Others are all blocked.

Example 2:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

Block List: -- select one --
Schedule rule: (00)Always ID: --

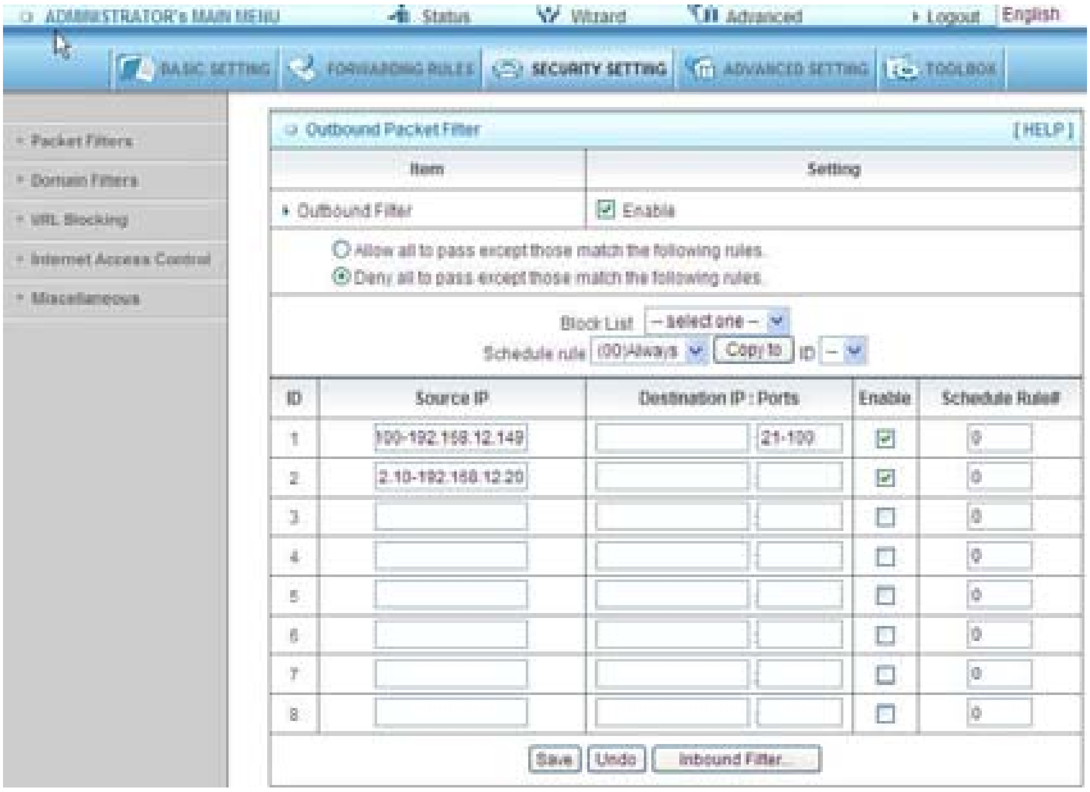
ID	Source IP	Destination IP : Ports		Enable	Schedule Rule#
1	1.2.3.100-1.2.3.199		21	☑	0
2	1.2.3.100-1.2.3.199		199	☑	0
3				□	0
4				□	0
5				□	0
6				□	0
7				□	0
8				□	0

(1.2.3.100-1.2.3.119) Remote hosts can do everything except read net news (port 119) and transfer files via FTP (port 21) behind Router Server.
Others are all allowed.

After Inbound Packet Filter setting is configured, click the save button.

Outbound Filter:
To enable Outbound Packet Filter click the check box next to Enable in the Outbound Packet Filter field.

Example 1:
Router LAN IP is 192.168.12.254



Outbound Packet Filter [HELP]

Item	Setting
Outbound Filter	☑ Enable

○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

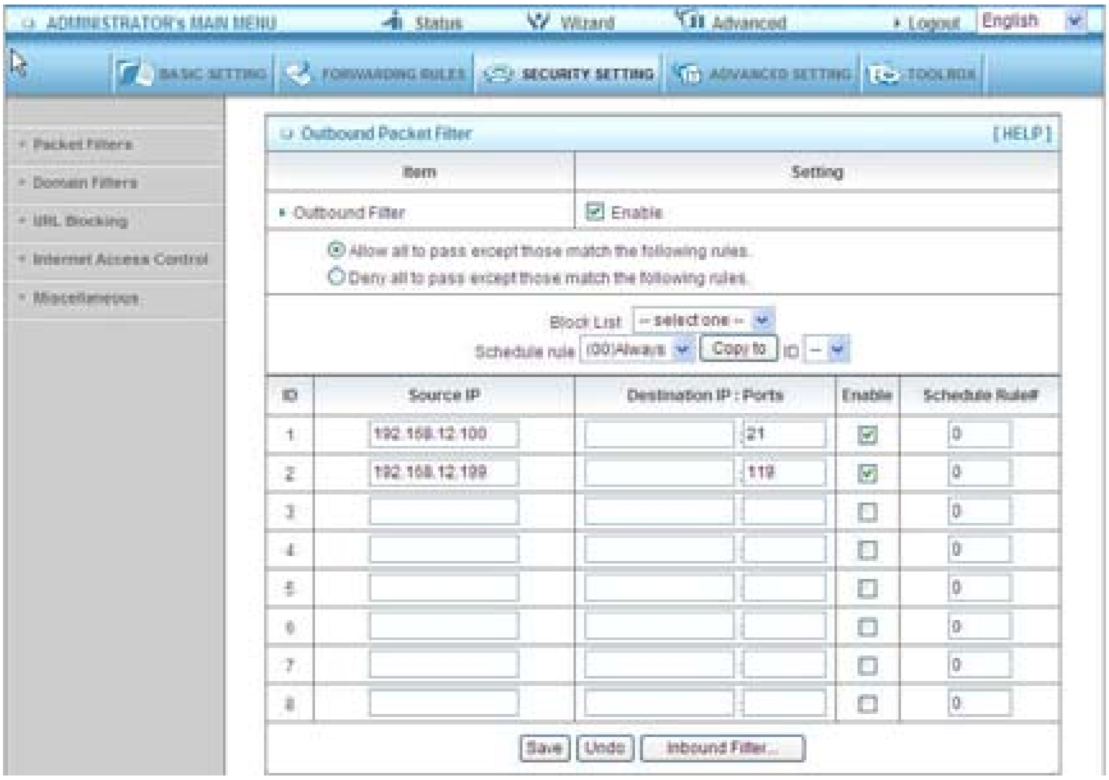
Block List -- select one --
Schedule rule (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports		Enable	Schedule Rule#
1	100-192.168.12.149		21-100	☑	0
2	2.10-192.168.12.20			☑	0
3				□	0
4				□	0
5				□	0
6				□	0
7				□	0
8				□	0

(192.168.12.100-192.168.12.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing)
Others are all blocked.

Example 2:
Router LAN IP is 192.168.12.254



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

Block List -- select one --
Schedule rule (00)Always Copy to ID --

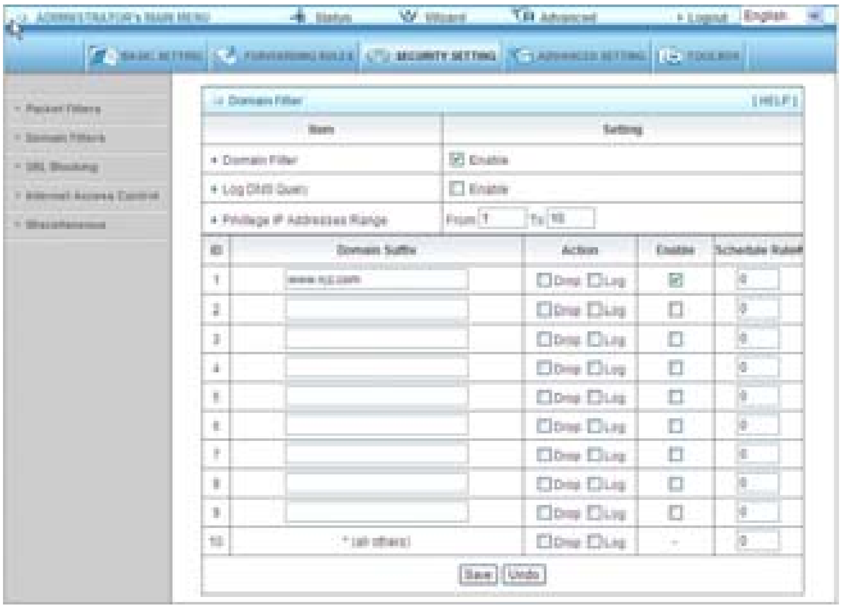
ID	Source IP	Destination IP : Ports		Enable	Schedule Rule#
1	192.168.12.100		21	☑	0
2	192.168.12.199		119	☑	0
3				□	0
4				□	0
5				□	0
6				□	0
7				□	0
8				□	0

(192.168.12.100 and 192.168.12.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After Outbound Packet Filter setting is configured, click the save button.

3.3.3.2 Domain filters



Domain Filter [HELP]

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	□ Enable
Privilege IP Addresses Range	From 1 To 10

ID	Domain Suffix	Action	Enable	Schedule Rule#
1	www.xyz.com	□ Drop □ Log	☑	0
2		□ Drop □ Log	□	0
3		□ Drop □ Log	□	0
4		□ Drop □ Log	□	0
5		□ Drop □ Log	□	0
6		□ Drop □ Log	□	0
7		□ Drop □ Log	□	0
8		□ Drop □ Log	□	0
9		□ Drop □ Log	□	0
10	* (all others)	□ Drop □ Log	-	0

Save Undo

Domain Filter

Let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

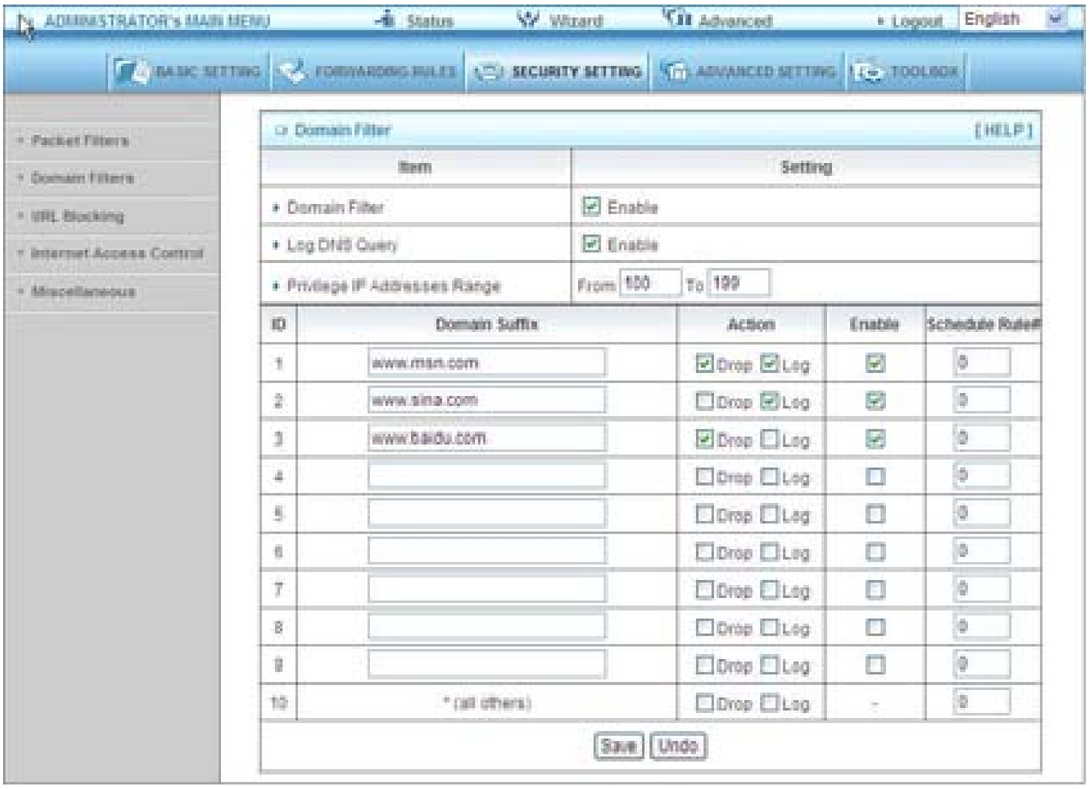
Action

When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check log to log these access.

Enable

Check to enable each rule.

Example:



Domain Filter

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	☑ Enable
Privilege IP Addresses Range	From 100 To 199

ID	Domain Suffix	Action	Enable	Schedule Rule#
1	www.msn.com	☑ Drop ☑ Log	☑	0
2	www.sina.com	□ Drop ☑ Log	☑	0
3	www.baidu.com	☑ Drop □ Log	☑	0
4		□ Drop □ Log	□	0
5		□ Drop □ Log	□	0
6		□ Drop □ Log	□	0
7		□ Drop □ Log	□	0
8		□ Drop □ Log	□	0
9		□ Drop □ Log	□	0
10	* (all others)	□ Drop □ Log	-	0

In this example:

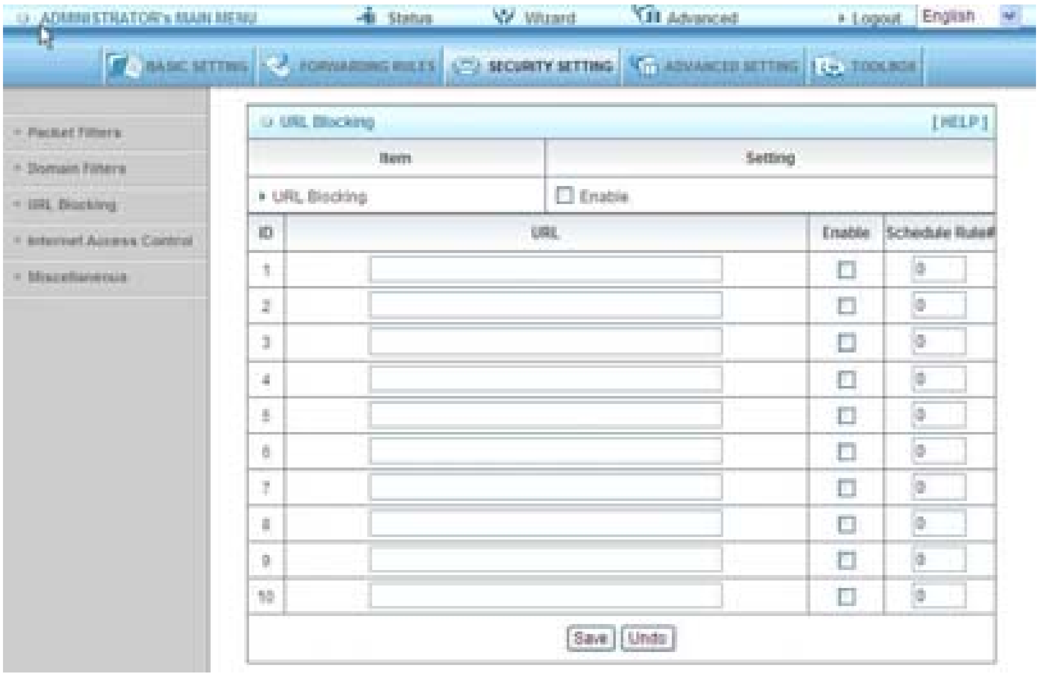
URL include “www.msn.com” will be blocked, and the action will be record in log-file.

URL include “www.sina.com” will not be blocked, but the action will be record in log-file.

URL include “www.baidu.com” will be blocked, but the action will not be record in log-file.

IP address x.x.x.1~x.x.x.99 can access Internet without restriction.

3.3.3.3 URL Blocking



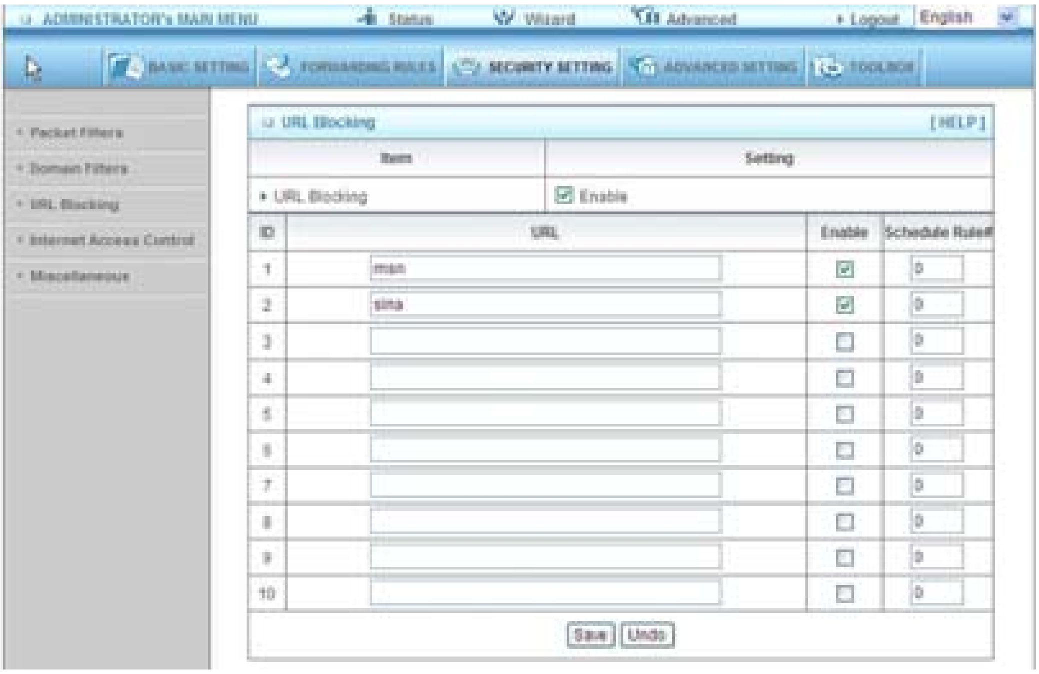
URL Blocking [HELP]

Item	Setting
URL Blocking	□ Enable

ID	URL	Enable	Schedule Rule#
1		□	0
2		□	0
3		□	0
4		□	0
5		□	0
6		□	0
7		□	0
8		□	0
9		□	0
10		□	0

URL Blocking will block LAN computers to connect to pre-defined Websites.
The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

URL Blocking Enable
Checked if you want to enable URL Blocking.
URL
If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
Enable
Checked to enable each rule.



URL Blocking

Item	Setting
URL Blocking	☑ Enable

ID	URL	Enable	Schedule Rule#
1	msn	☑	0
2	sina	☑	0
3		□	0
4		□	0
5		□	0
6		□	0
7		□	0
8		□	0
9		□	0
10		□	0

In this example:

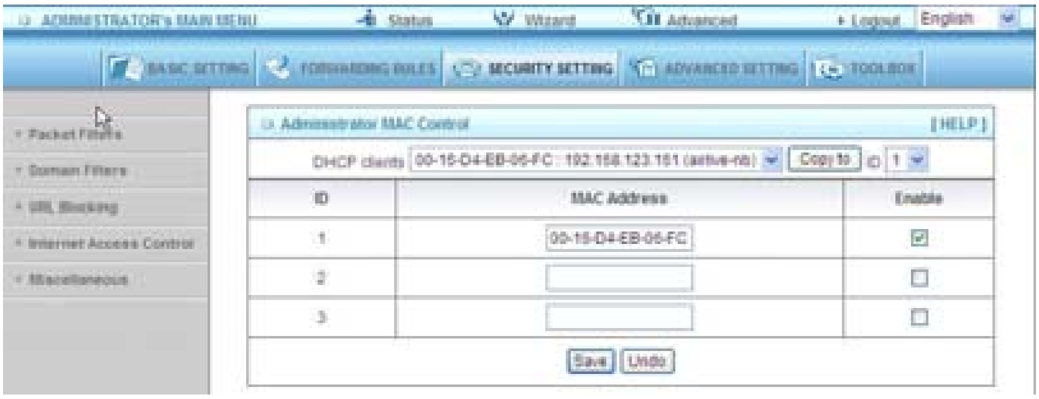
1. URL include “msn” will be blocked, and the action will be record in log-file.
2. URL include “sina” will be blocked, but the action will be record in log-file

3.3.3.4 Internet Access Control

The device provides "Administrator MAC Control" for specific MAC to access the device or Internet without restriction. It also provides 3 features to access Internet: MAC Control by host, Group MAC Control and Interface Access Control depend as user-defined time Schedule.

Administrator MAC Control

Regardless the MAC access configuration of administrator, specific MAC can access the device.

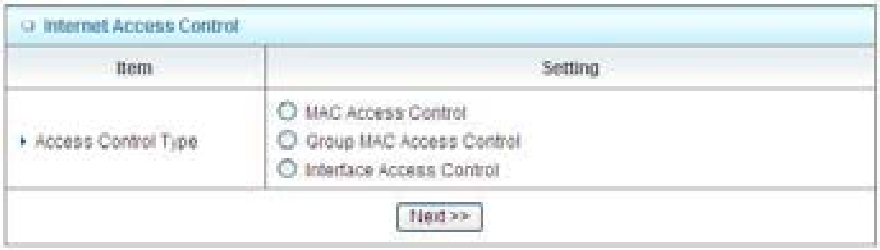


Administrator MAC Control

DHCP clients 00-15-D4-EB-06-FC : 192.168.123.151 (active-nb) ID 1

ID	MAC Address	Enable
1	00-15-D4-EB-06-FC	☑
2		□
3		□

This device can record 3 sets. When the host(should be admin) logins Web management, the device will record MAC address of this host. Before this host configures Internet Access Control , Suggest end-user to enable this feature, first.

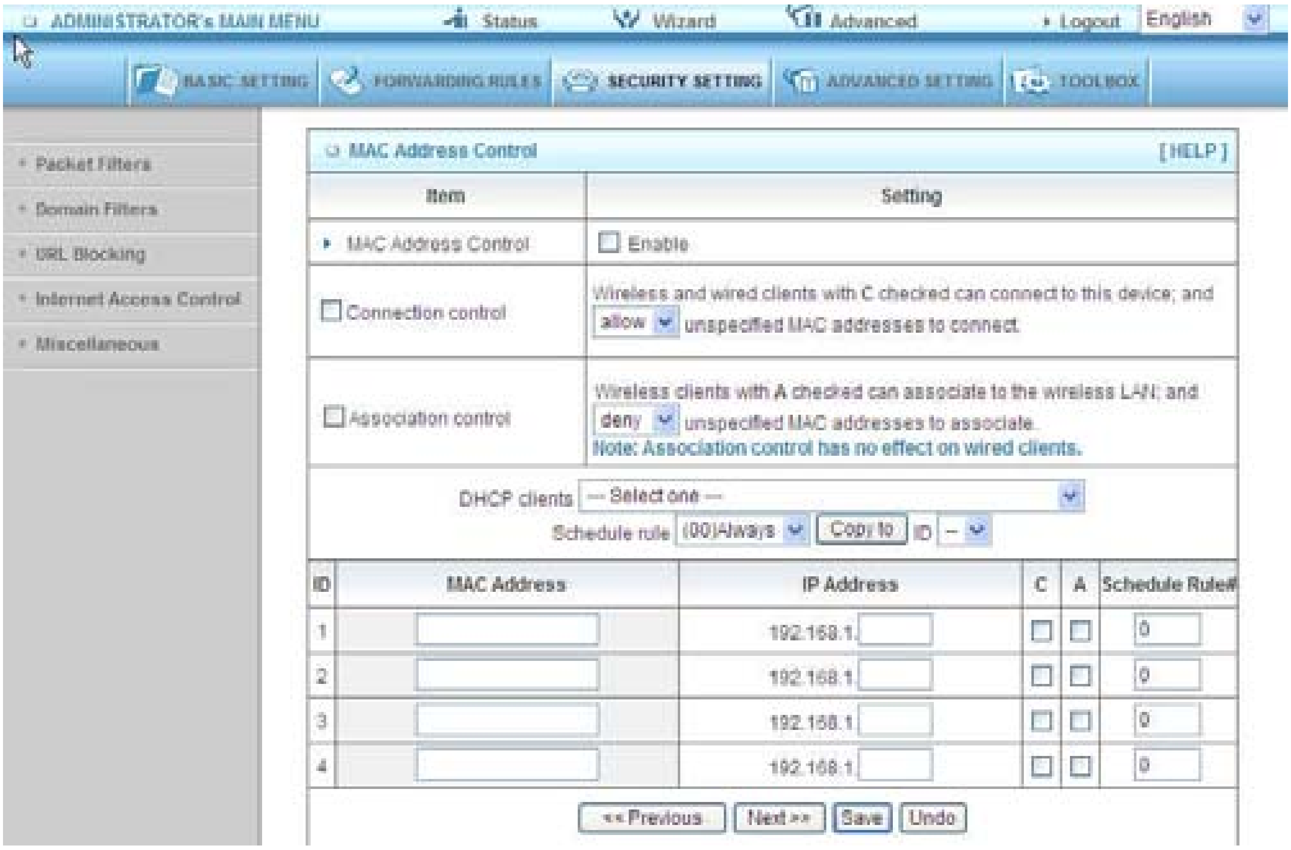


Internet Access Control

Item	Setting
▸ Access Control Type	○ MAC Access Control ○ Group MAC Access Control ○ Interface Access Control

Next >>

MAC control



MAC Address Control [HELP]

Item	Setting
▸ MAC Address Control	□ Enable
□ Connection control	Wireless and wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.
□ Association control	Wireless clients with A checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate. Note: Association control has no effect on wired clients.

DHCP clients -- Select one --

Schedule rule (00)Always Copy to ID --

ID	MAC Address	IP Address	C	A	Schedule Rule#
1		192.168.1.	□	□	0
2		192.168.1.	□	□	0
3		192.168.1.	□	□	0
4		192.168.1.	□	□	0

<< Previous Next >> Save Undo

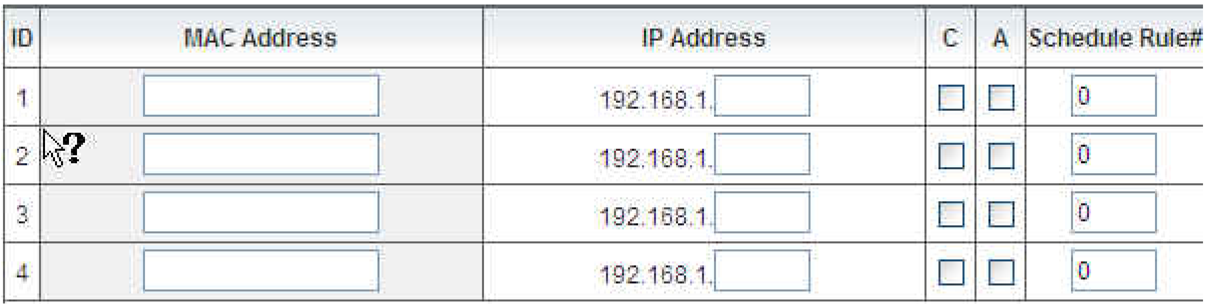
MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

Connection control Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

Association control   Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Control table

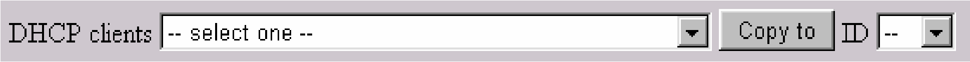


ID	MAC Address	IP Address	C	A	Schedule Rule#
1		192.168.1.	□	□	0
2		192.168.1.	□	□	0
3		192.168.1.	□	□	0
4		192.168.1.	□	□	0

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When "Connection control" is checked, check "C" will allow the corresponding client to connect to this device.
A	When "Association control" is checked, check "A" will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combobox and button to help you to input the MAC address.

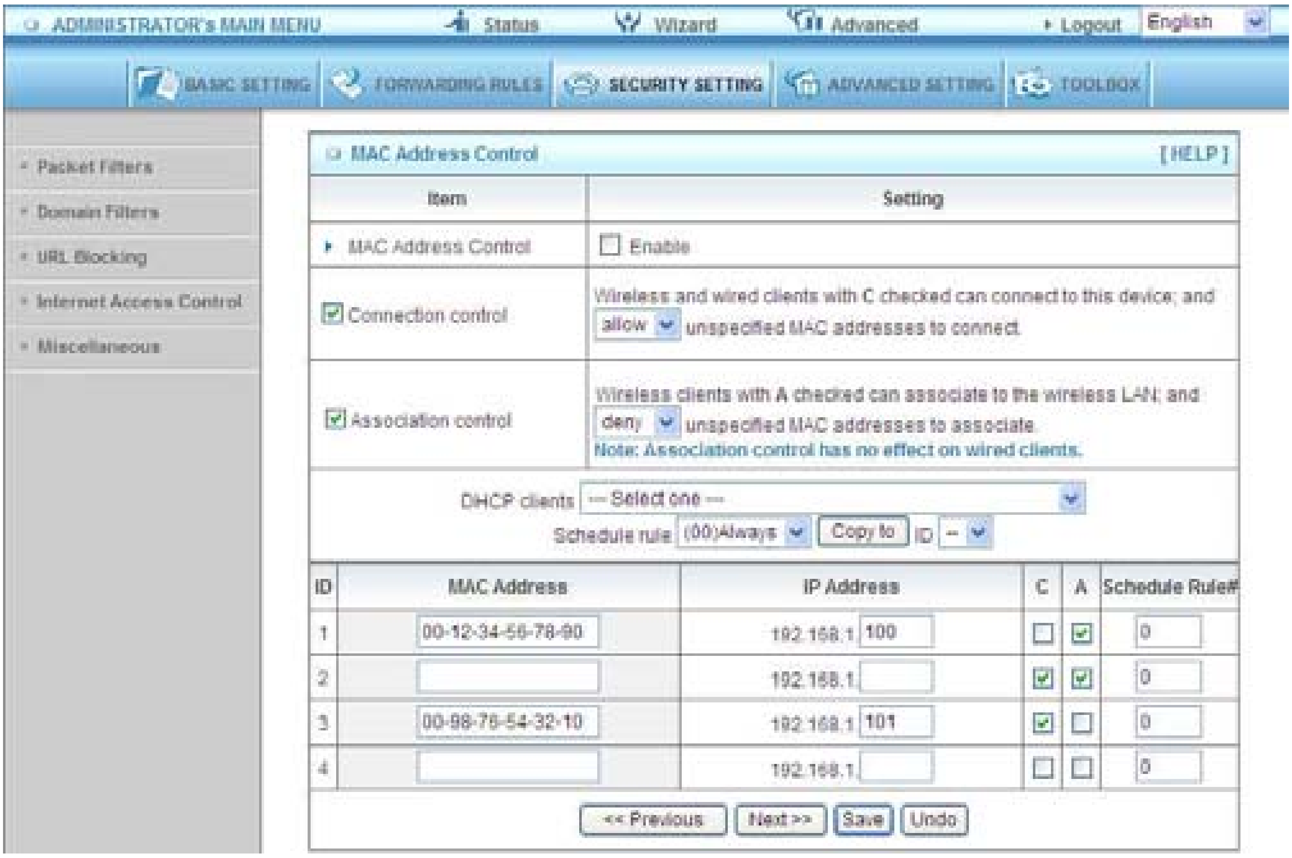


DHCP clients -- select one -- Copy to ID --

You can select a specific client in the “DHCP clients” Combobox, and then click on the “Copy to” button to copy the MAC address of the client you select to the ID selected in the “ID” Combobox.

Previous page and Next Page To make this setup page simple and clear, we have divided the “Control table” into several pages. You can use these buttons to navigate to different pages.

Example:



MAC Address Control

Item	Setting
MAC Address Control	□ Enable
☑ Connection control	Wireless and wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.
☑ Association control	Wireless clients with A checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate. Note: Association control has no effect on wired clients.

DHCP clients --- Select one ---
Schedule rule (00)Always Copy to ID --

ID	MAC Address	IP Address	C	A	Schedule Rule#
1	00-12-34-56-78-90	192.168.1. 100	□	☑	0
2		192.168.1.	☑	☑	0
3	00-98-76-54-32-10	192.168.1. 101	☑	□	0
4		192.168.1.	□	□	0

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

1.The "MAC Address Control" function is enabled.

2."Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.

3."Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.

4.Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:

ID 1 - "00-12-34-56-78-90" --> 192.168.1.100
ID 3 - "00-98-76-54-32-10" --> 192.168.1.101

Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.
If, for example, client 3 tries to use an IP address different from the address listed in the Control
table (192.168.12.101), it will be denied to connect to this device.

5.Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.

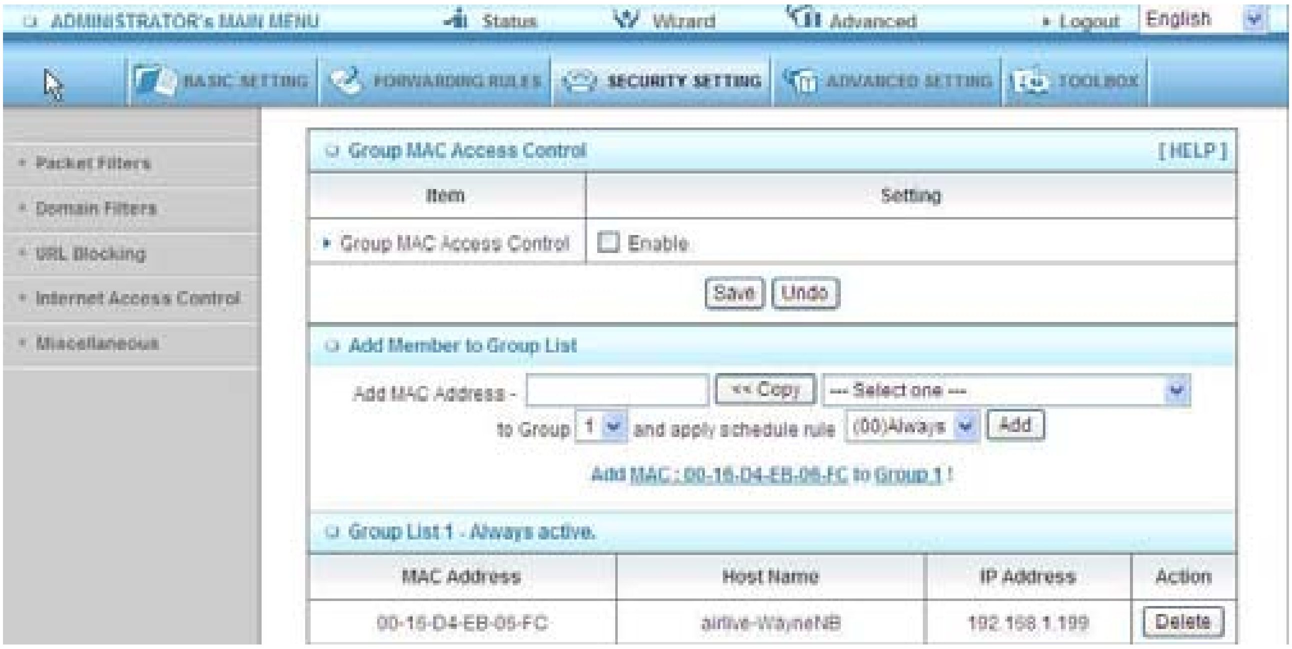
6.Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

Group MAC Access Control

Administrator can define hosts in which Group to allow Internet. For example, Father and Mother are in Group1 without limitation and hosts Brother and Sister are in Group2 to access according as Schedule Rule2.

For example,

Schedule Rule 1 sets “always” everyday with limitation.



Group MAC Access Control [HELP]

Item	Setting
Group MAC Access Control	☐ Enable

Save Undo

Add Member to Group List

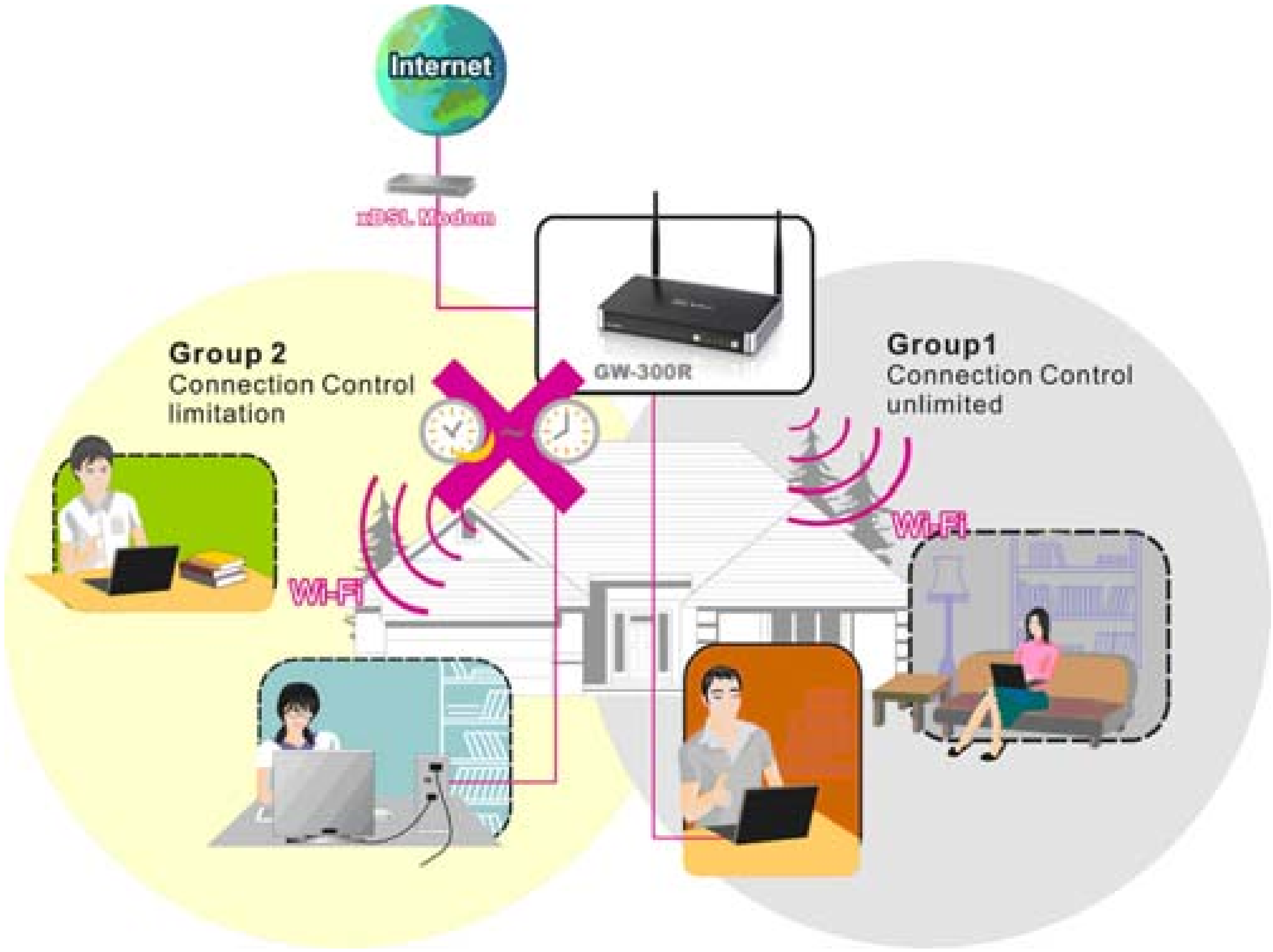
Add MAC Address - << Copy --- Select one ---

to Group 1 and apply schedule rule (00)Always Add

Add MAC : 00-16-D4-EB-06-FC to Group 1 !

Group List 1 - Always active.

MAC Address	Host Name	IP Address	Action
00-16-D4-EB-06-FC	airlive-WayneNB	192.168.1.199	Delete



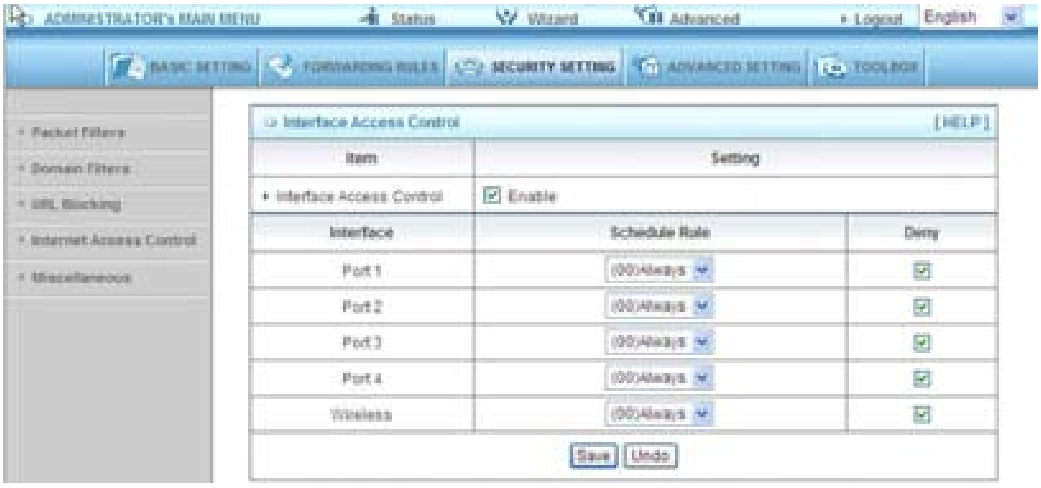
Interface Access Control

The device defines 5 Interfaces as Lan1,Lan2, Lan3,Lan4 and WiFi. The device allows different interface to access Internet by time schedule

For example, Schedule Rule 1 sets “always” everyday with limitation.
Schedule Rule 2 sets 08:00~23:00 Monday ~ Friday.

Administrator can set guests in Lan3 and Lan4 to access Internet according as Schedule Rule

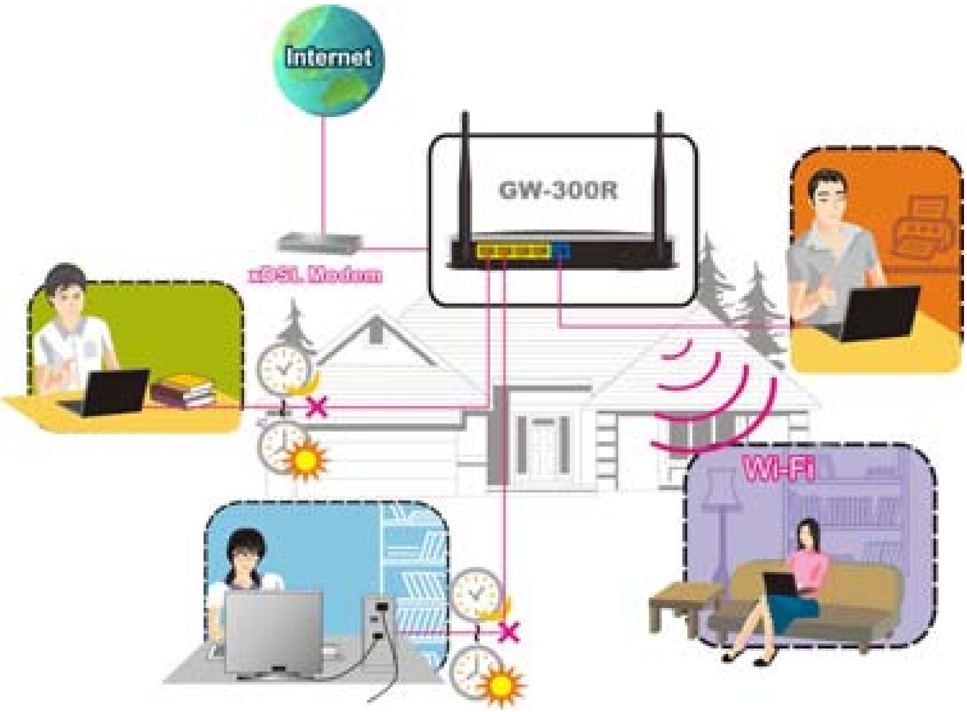
2. Set Friends in Lan1 ,Lan2 and WiFi according as Schedule Rule 1.



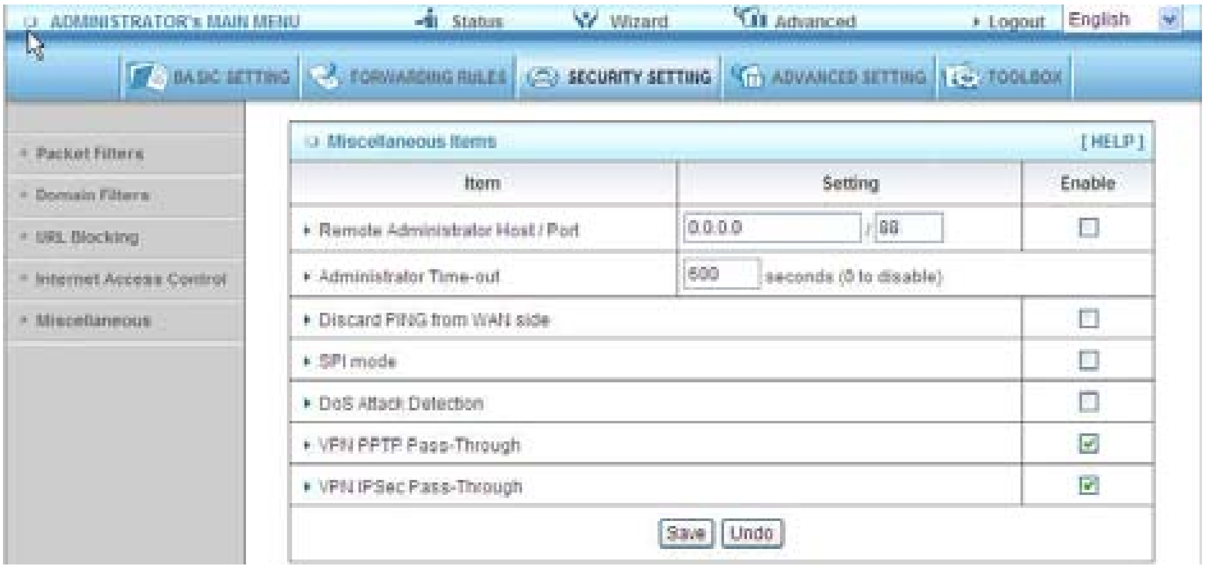
Interface Access Control

Item	Setting
Interface Access Control	☑ Enable

Interface	Schedule Rule	Deny
Port 1	(00)Always	☑
Port 2	(00)Always	☑
Port 3	(00)Always	☑
Port 4	(00)Always	☑
Wireless	(00)Always	☑



3.3.3.5 Miscellaneous Items



Miscellaneous Items [HELP]

Item	Setting	Enable
Remote Administrator Host / Port	0.0.0.0 / 88	□
Administrator Time-out	600 seconds (0 to disable)	
Discard PING from WAN side		□
SPI mode		□
DoS Attack Detection		□
VPN PPTP Pass-Through		☑
VPN IPSec Pass-Through		☑

Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

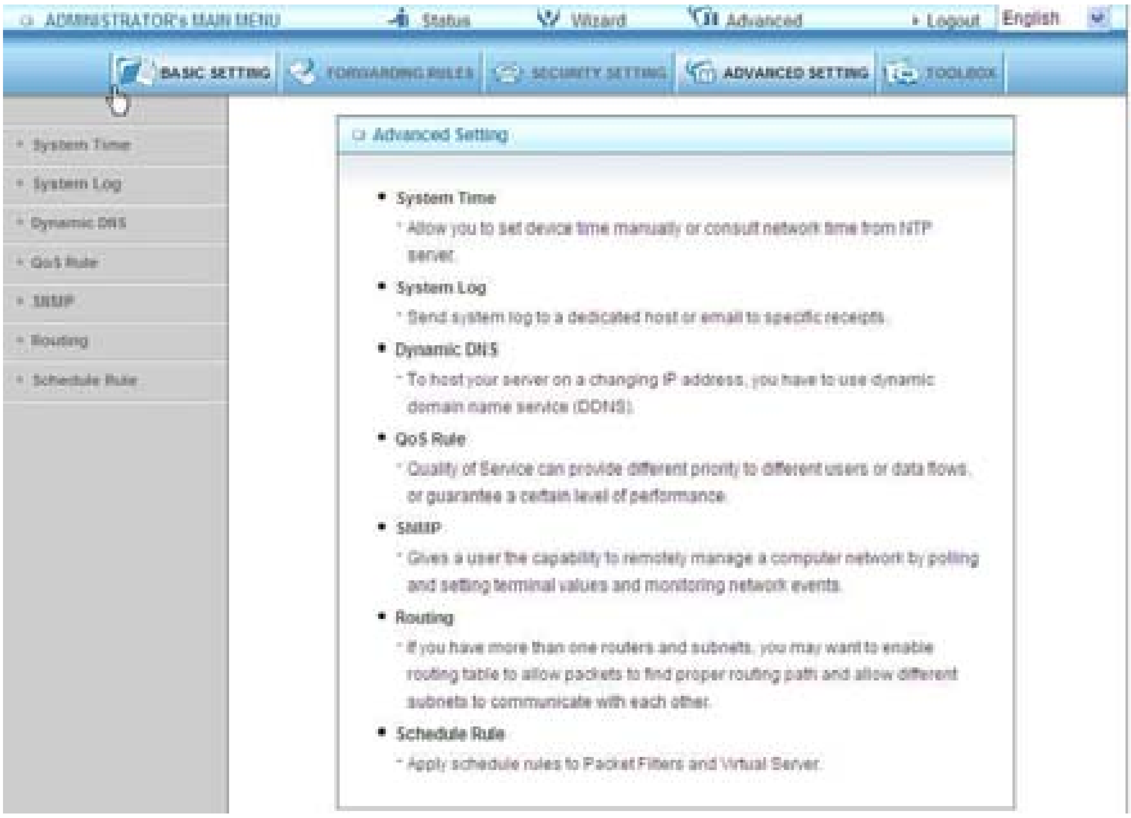
DoS Attack Detection

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

VPN IPSec Pass-Through

It is a setting/feature on routers which is required to implement secure exchange of packets at
the IP layer and allow IPSec tunnels to pass through the router.
VPN PPTP Pass-Through
It is a setting/feature on routers which is required in order to connect to a Remote PPTP VPN account.

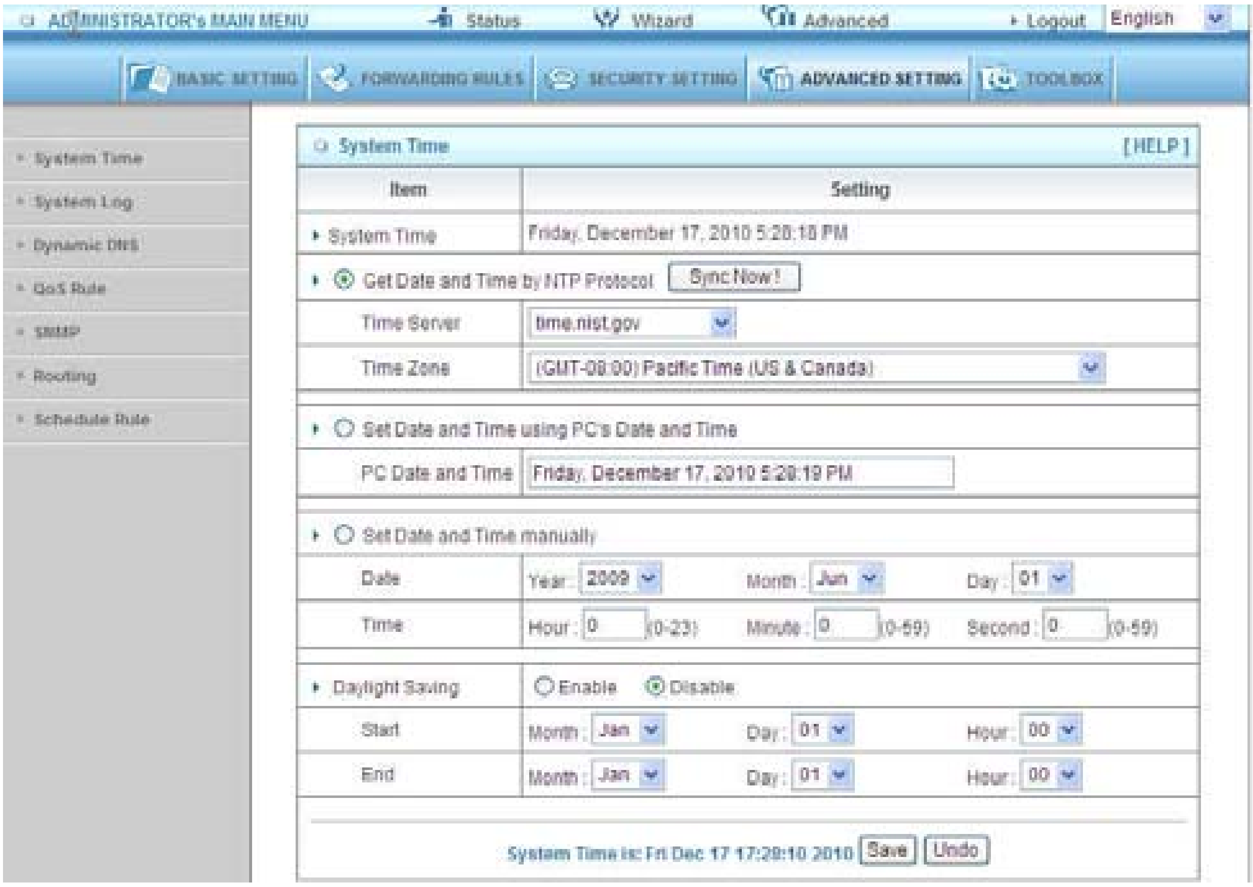
3.3.4 Advanced Settings



Advanced Setting

- System Time
  - Allow you to set device time manually or consult network time from NTP server.
- System Log
  - Send system log to a dedicated host or email to specific receipts.
- Dynamic DNS
  - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- QoS Rule
  - Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- SNMP
  - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing
  - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- Schedule Rule
  - Apply schedule rules to Packet Filters and Virtual Server.

3.3.4.1 System Time



System Time

Item	Setting
System Time	Friday, December 17, 2010 5:28:18 PM
● Get Date and Time by NTP Protocol	Sync Now!
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
○ Set Date and Time using PC's Date and Time	
PC Date and Time	Friday, December 17, 2010 5:28:19 PM
○ Set Date and Time manually	
Date	Year : 2009 Month : Jun Day : 01
Time	Hour : 0 (0-23) Minute : 0 (0-59) Second : 0 (0-59)
Daylight Saving	○ Enable ● Disable
Start	Month : Jan Day : 01 Hour : 00
End	Month : Jan Day : 01 Hour : 00

System Time is: Fri Dec 17 17:28:10 2010

Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

Set Date and Time manually

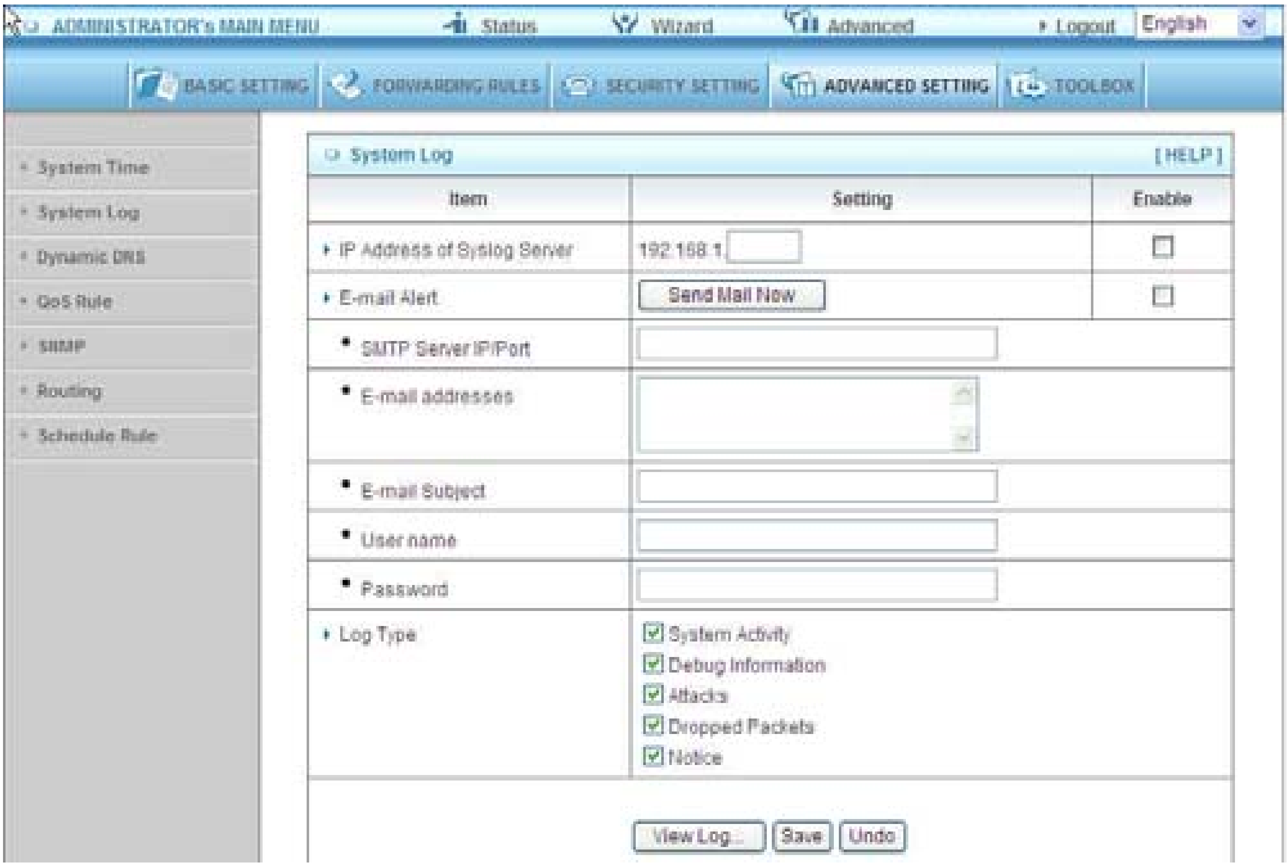
Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

Daylight Saving:Set up where the location is.

3.3.4.2 System Log



System Log [HELP]

Item	Setting	Enable
IP Address of Syslog Server	192.168.1.	□
E-mail Alert	Send Mail Now	□
• SMTP Server IP/Port		
• E-mail addresses		
• E-mail Subject		
• User name		
• Password		
Log Type	☑ System Activity ☑ Debug Information ☑ Attacks ☑ Dropped Packets ☑ Notice	

This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check Enable to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

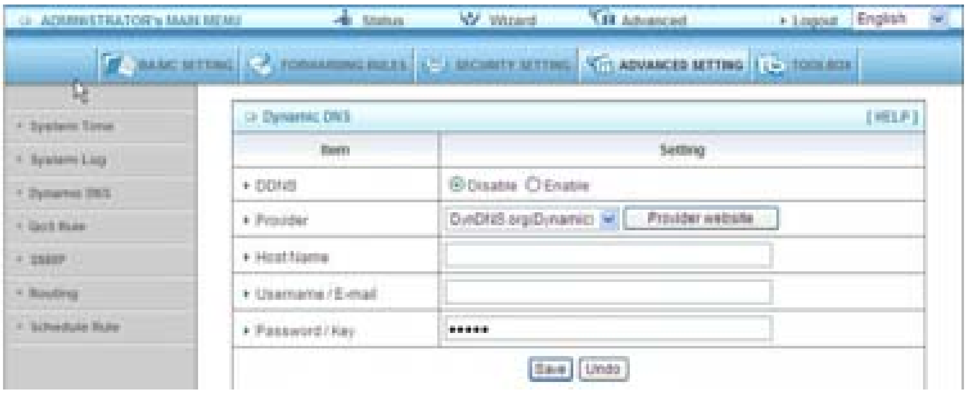
Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

Send E-mail alert to

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

3.3.4.3 DDNS Service



Dynamic DNS [HELP]

Item	Setting
DDNS	● Disable ○ Enable
Provider	DynDNS.org(Dynamic) Provider website
Host Name	
Username / E-mail	
Password / Key	●●●●●

Save Undo

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in provider field.

To enable Dynamic DNS click the check box next to Enable in the DDNS field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

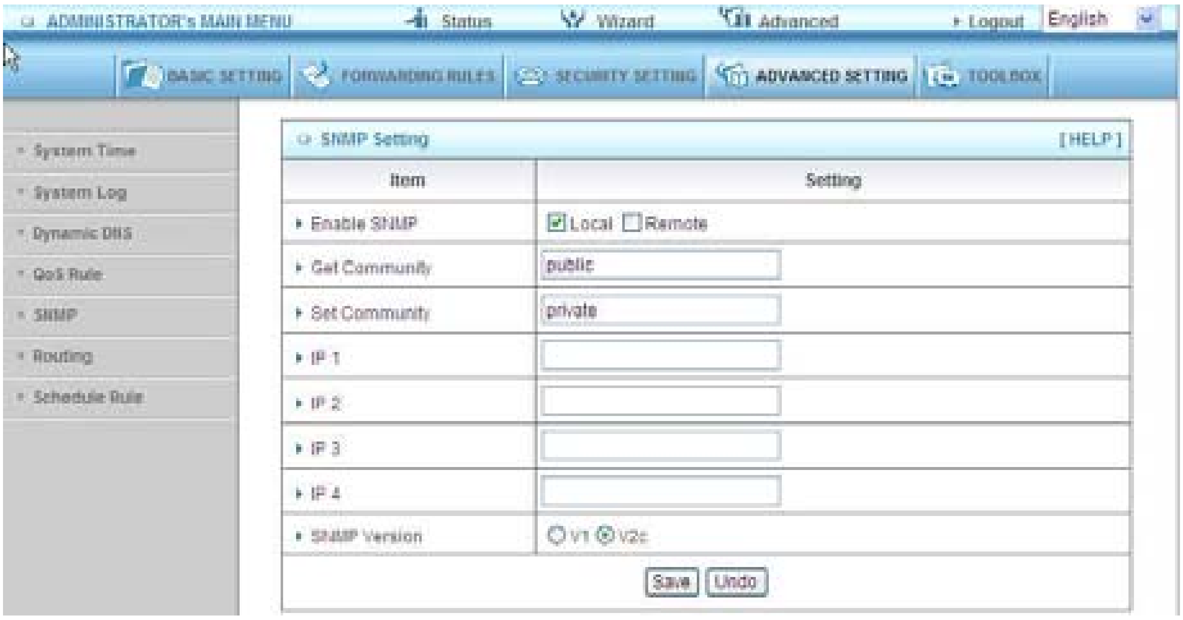
Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

3.3.4.4 SNMP



SNMP Setting

Item	Setting
Enable SNMP	☑ Local □ Remote
Get Community	public
Set Community	private
IP 1	
IP 2	
IP 3	
IP 4	
SNMP Version	○ V1 ● V2c

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

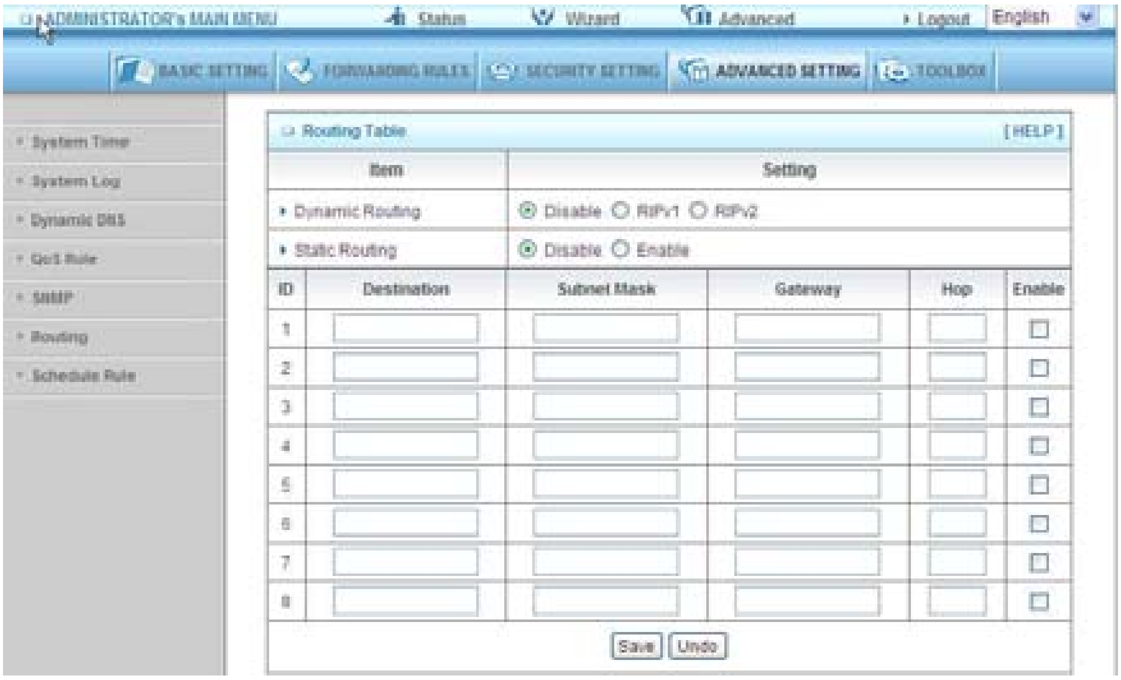
IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports.

3.3.4.5 Routing



Routing Table

Item	Setting
Dynamic Routing	● Disable ○ RIPv1 ○ RIPv2
Static Routing	● Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static.

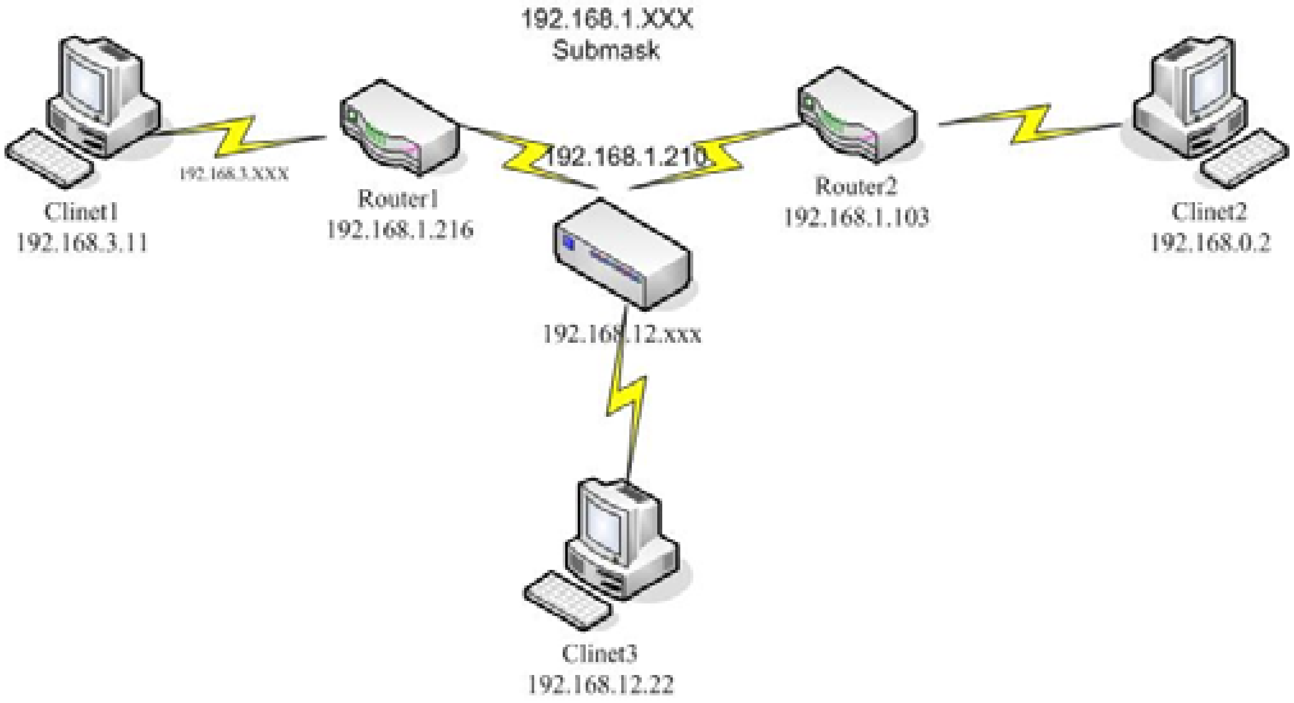
Dynamic Routing

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network.

Otherwise, please select RIPv1 if you need this protocol.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

Example:

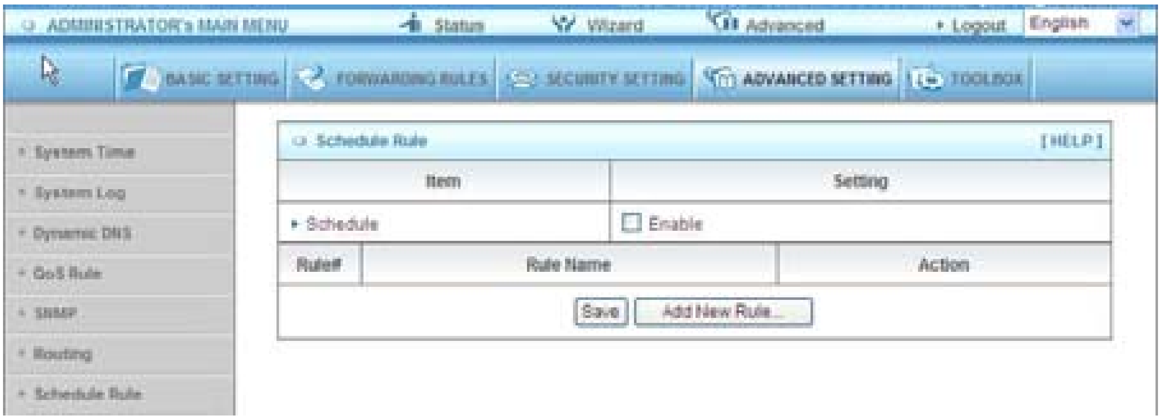


Configuration on NAT Router

Destination	SubnetMask	Gateway	Hop	Enabled
192.168.3.0	255.255.255.0	192.168.1.216	1	ˇ
192.168.0.0	255.255.255.0	192.168.1.103	1	ˇ

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.1.103 (a gateway),
And if it sends Packets to 192.168.3.11 will go via 192.168.1.216
Each rule can be enabled or disabled individually.
After routing table setting is configured, click the save button.

3.3.4.6 Schedule Rule



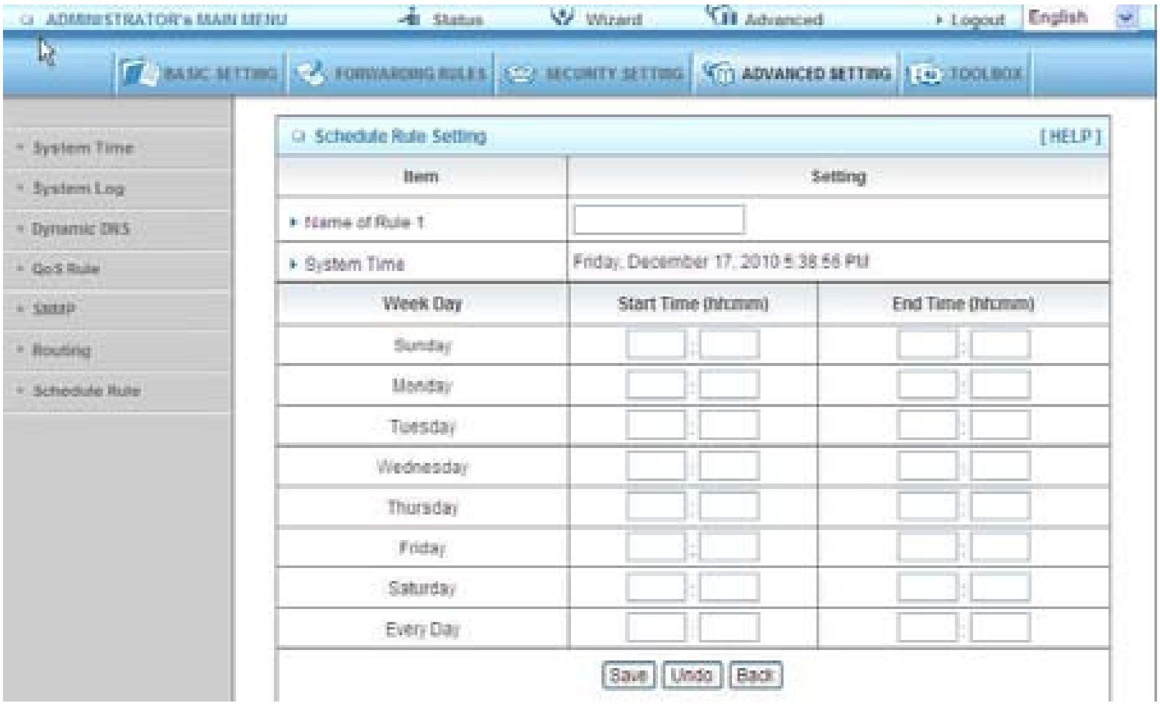
Schedule Rule [HELP]

Item	Setting
Schedule	□ Enable

Rule#	Rule Name	Action

You can set the schedule time to decide which service will be turned on or off. Select the "enable" item.
Press "Add New Rule"

You can write a rule name and set which day and what time to schedule from "Start Time" to "End Time". The following example configure "ftp time" as everyday 14:10 to 16:20



Schedule Rule Setting [HELP]

Item	Setting
Name of Rule 1	
System Time	Friday, December 17, 2010 5:38:56 PM

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:
Every Day	:	:

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

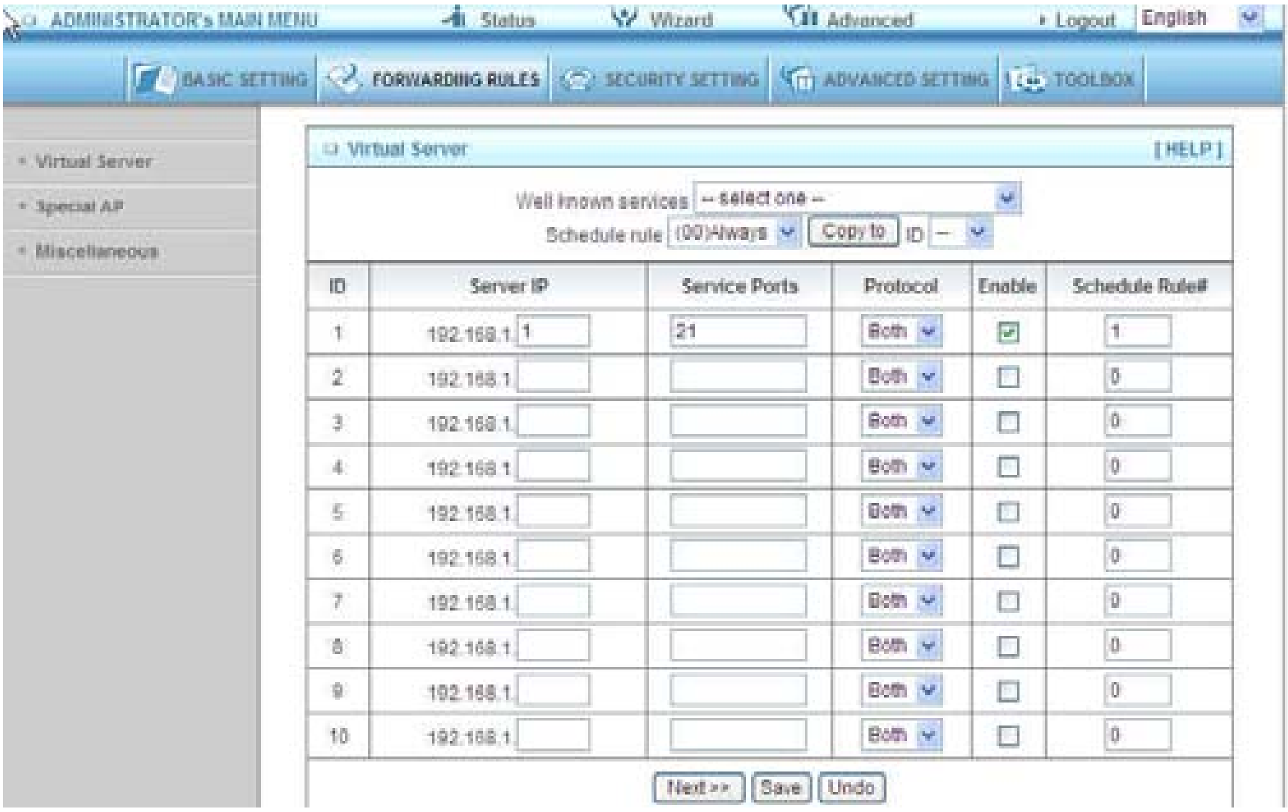
To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Exanple1: Virtual Server – Apply Rule#1 (ftp time: everyday 14:20 to 16:30)

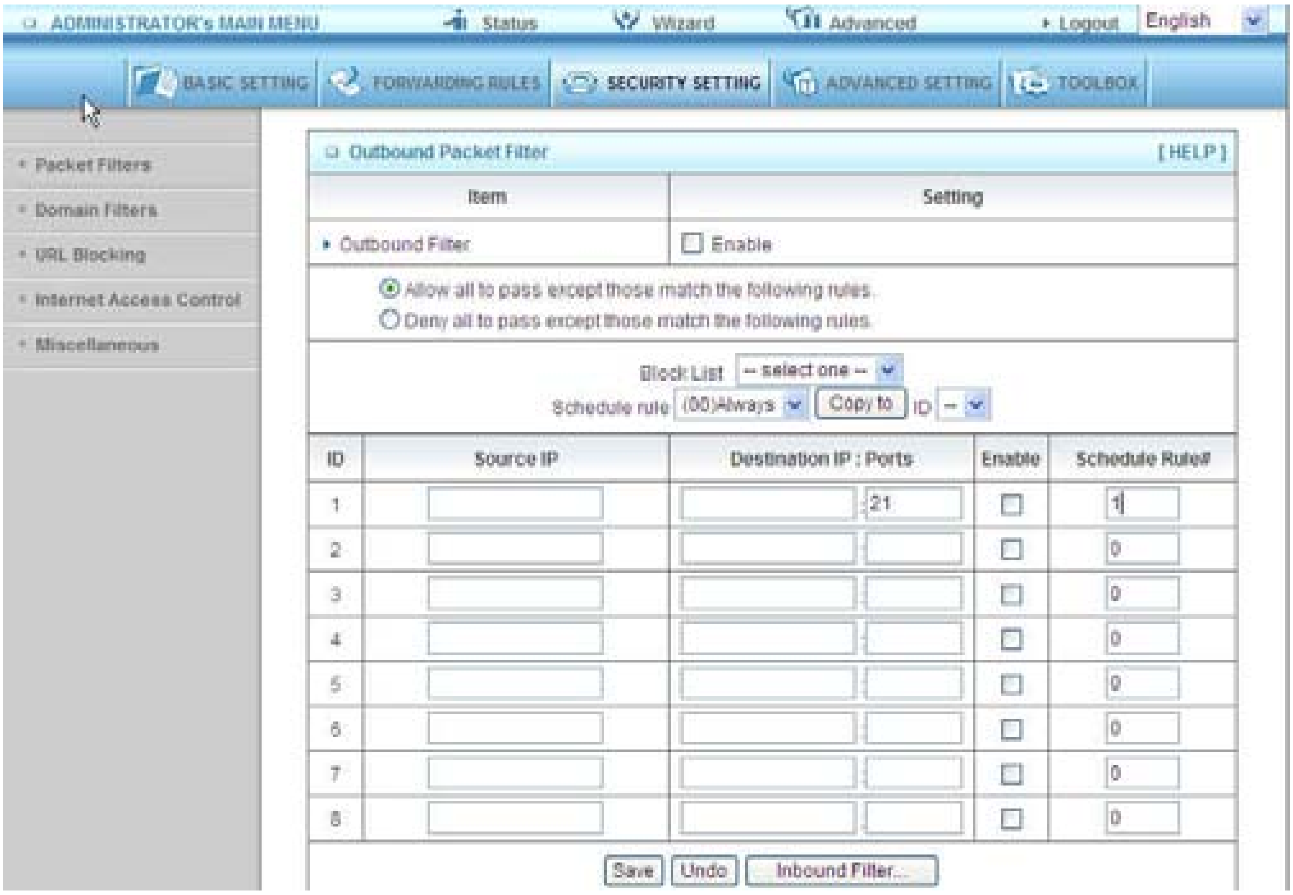


Well known services: -- select one --

Schedule rule: (00)Always ID: --

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.1. 1	21	Both	☑	1
2	192.168.1.		Both	□	0
3	192.168.1.		Both	□	0
4	192.168.1.		Both	□	0
5	192.168.1.		Both	□	0
6	192.168.1.		Both	□	0
7	192.168.1.		Both	□	0
8	192.168.1.		Both	□	0
9	192.168.1.		Both	□	0
10	192.168.1.		Both	□	0

Exanple2: Packet Filter – Apply Rule#1 (ftp time: everyday 14:20 to 16:30).



Outbound Packet Filter [HELP]

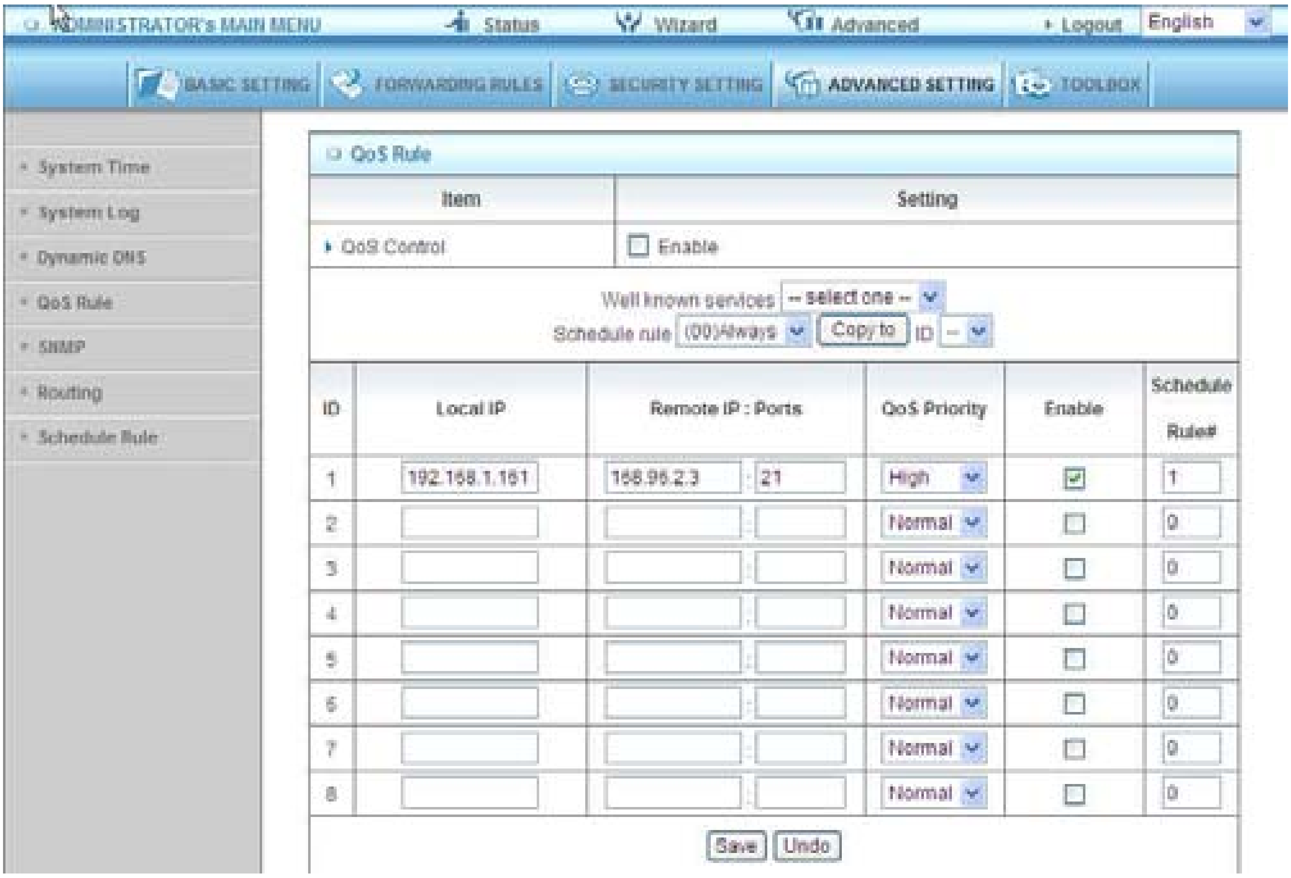
Item	Setting
Outbound Filter	□ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

Block List -- select one --
Schedule rule (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1		: 21	□	1
2		:	□	0
3		:	□	0
4		:	□	0
5		:	□	0
6		:	□	0
7		:	□	0
8		:	□	0

3.3.4.7 QoS Rule



QoS Rule

Item	Setting
QoS Control	☐ Enable

Well known services: -- select one --
Schedule rule: (00)Always   Copy to   ID --

ID	Local IP	Remote IP : Ports		QoS Priority	Enable	Schedule Rule#
1	192.168.1.161	168.96.2.3	21	High	☑	1
2				Normal	☐	0
3				Normal	☐	0
4				Normal	☐	0
5				Normal	☐	0
6				Normal	☐	0
7				Normal	☐	0
8				Normal	☐	0

Local IP:
Please input Client IP,ex192.168.1.161.

Remote Priority:
Please input Global IP and port,ex:168.96.2.3 and port 21