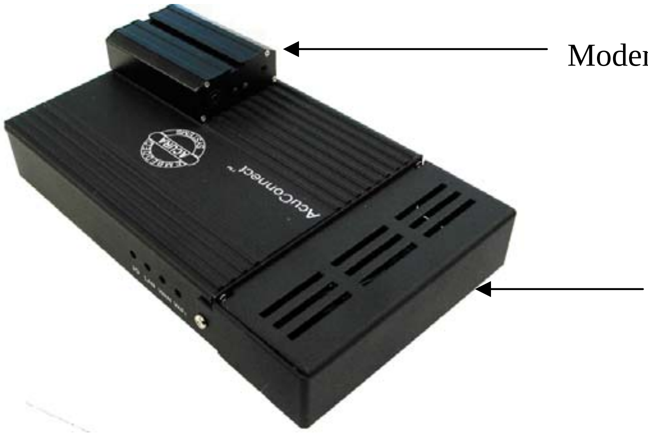
AcuConnect™2.0
3G Wireless WAN Mobile Broadband Modem + Router User Manual

1.1. Establish WiFi Connection

If you selected either **WEP** or **WPA-PSK** encryption, ensure these settings match your WiFi adapter settings.

WiFi and encryption settings must match for access to the Wireless WAN Mobile Broadband modem and Router Configuration Menu, and the Internet. Please refer to your WiFi adapter documentation for additional information.

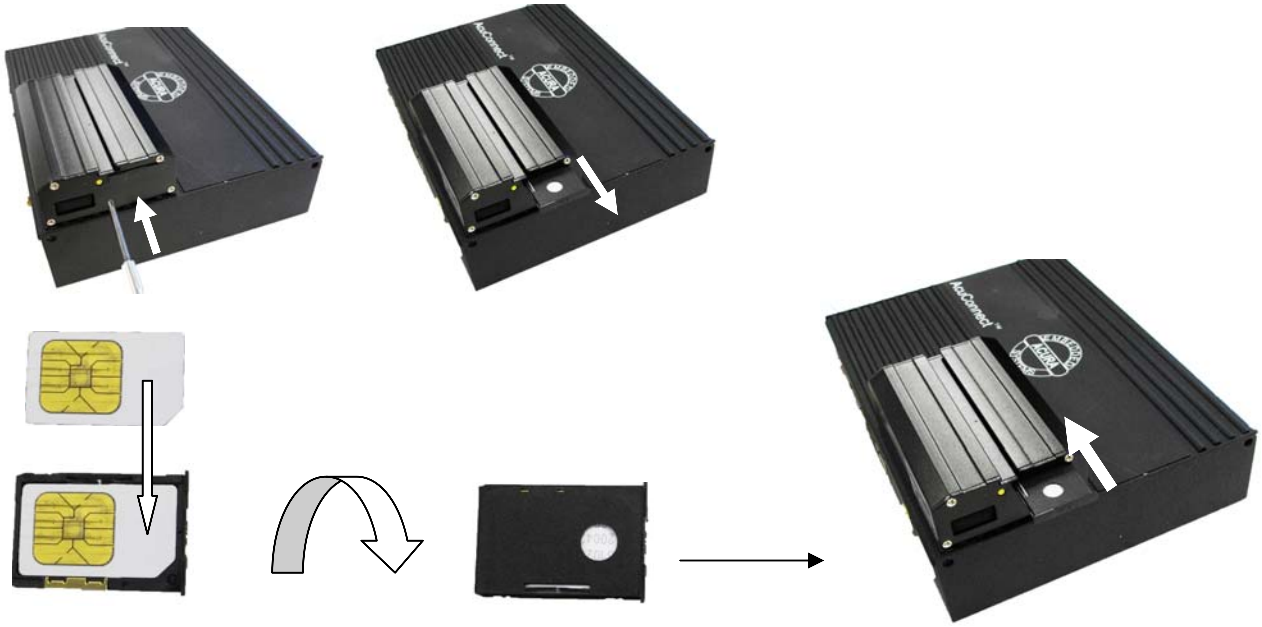


Modem

Open Protect cover.
PCMCIA modem slot will be found.

In general, for connecting with internet, pulg **SIM card** in the modem slot as follow.

press yellow button on the modem and **Sim** Card holder will pop out.



Plug **Sim** card holder with **SIM** card in the modem slot .

1.2. Using the Configuration Menu

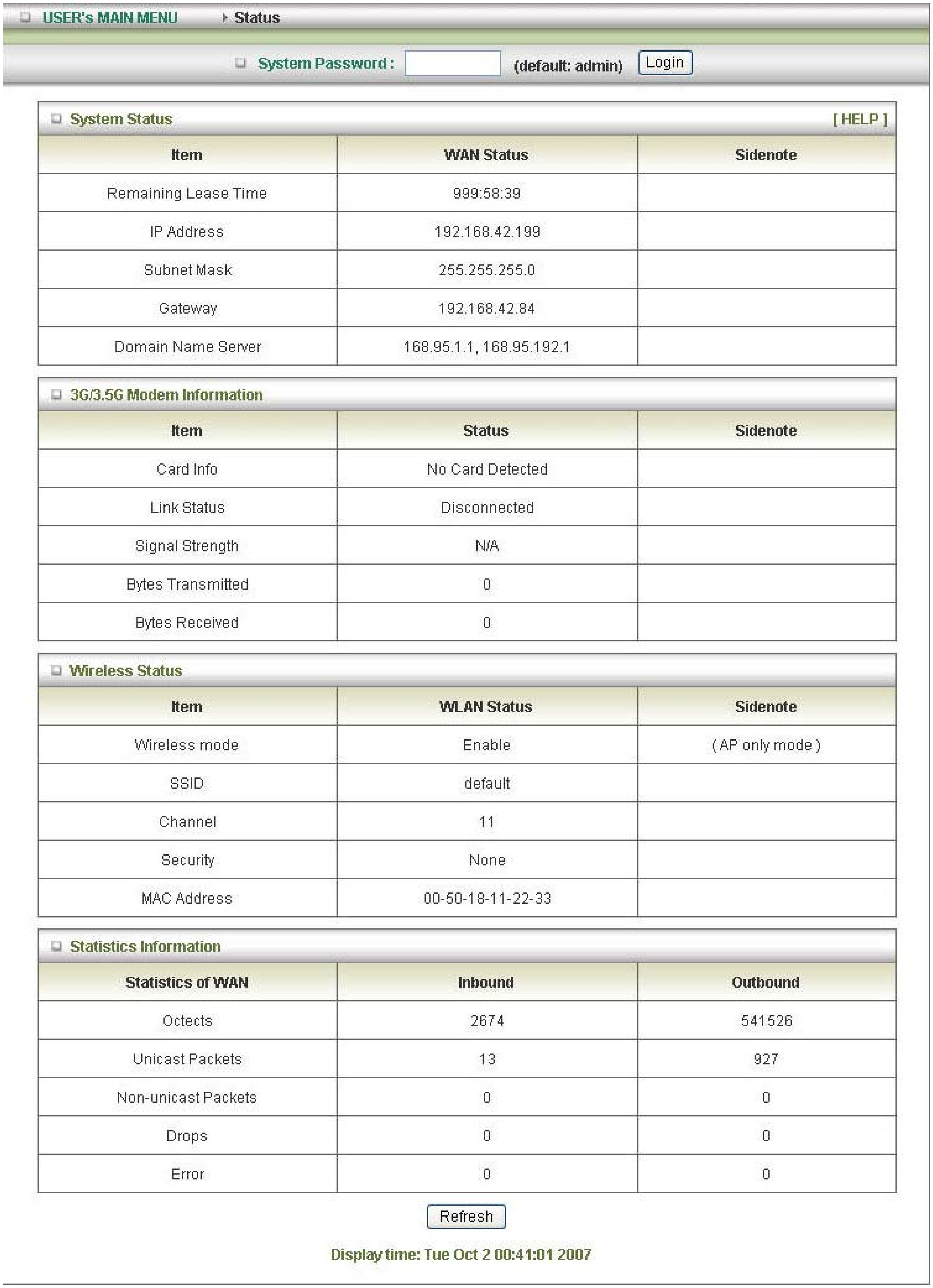
Once properly configured, the Wireless WAN Mobile Broadband Router will obtain and assign IP address information automatically. Configuration settings can be established through the Wireless WAN Mobile Broadband Router Configuration Menu. You can access this interface by performing the steps listed below:

1. Open a web-browser.

2. Type in the **IP Address** (**http://192.168.123.254**) of the Wireless WAN Mobile Broadband Router

3. Type “admin” in the Password field.

Note: If you have changed the **default** IP Address assigned to the Wireless WAN Mobile Broadband Router, ensure you enter the correct IP Address now.



System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	999:58:39	
IP Address	192.168.42.199	
Subnet Mask	255.255.255.0	
Gateway	192.168.42.84	
Domain Name Server	168.95.1.1, 168.95.192.1	

3G/3.5G Modem Information

Item	Status	Sidenote
Card Info	No Card Detected	
Link Status	Disconnected	
Signal Strength	N/A	
Bytes Transmitted	0	
Bytes Received	0	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(AP only mode)
SSID	default	
Channel	11	
Security	None	
MAC Address	00-50-18-11-22-33	

Statistics Information

Statistics of WAN	Inbound	Outbound
Octects	2674	541526
Unicast Packets	13	927
Non-unicast Packets	0	0
Drops	0	0
Error	0	0

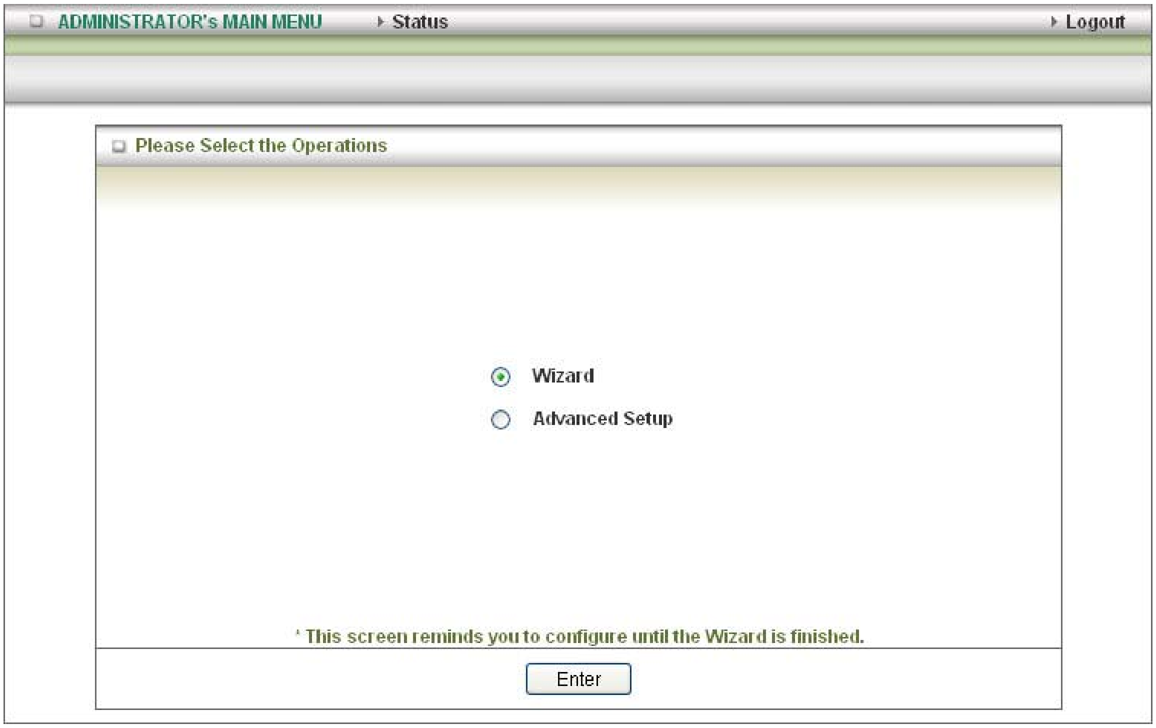
Display time: Tue Oct 2 00:41:01 2007

Type “admin” in the Password field.Then, Click “**logon”** button**.**

1.2.1. Wizard setting

- Press “**Wizard**” button **-**□ for basic settings with simpler way. (Please check section 2.2.1)

- Or you may click on “**Advanced Setup**” **-**□ for advanced settings. (Please check each item from section 2.2.2



◉ Wizard
○ Advanced Setup

* This screen reminds you to configure until the Wizard is finished.

- **Click on “Enter” button to get start.**

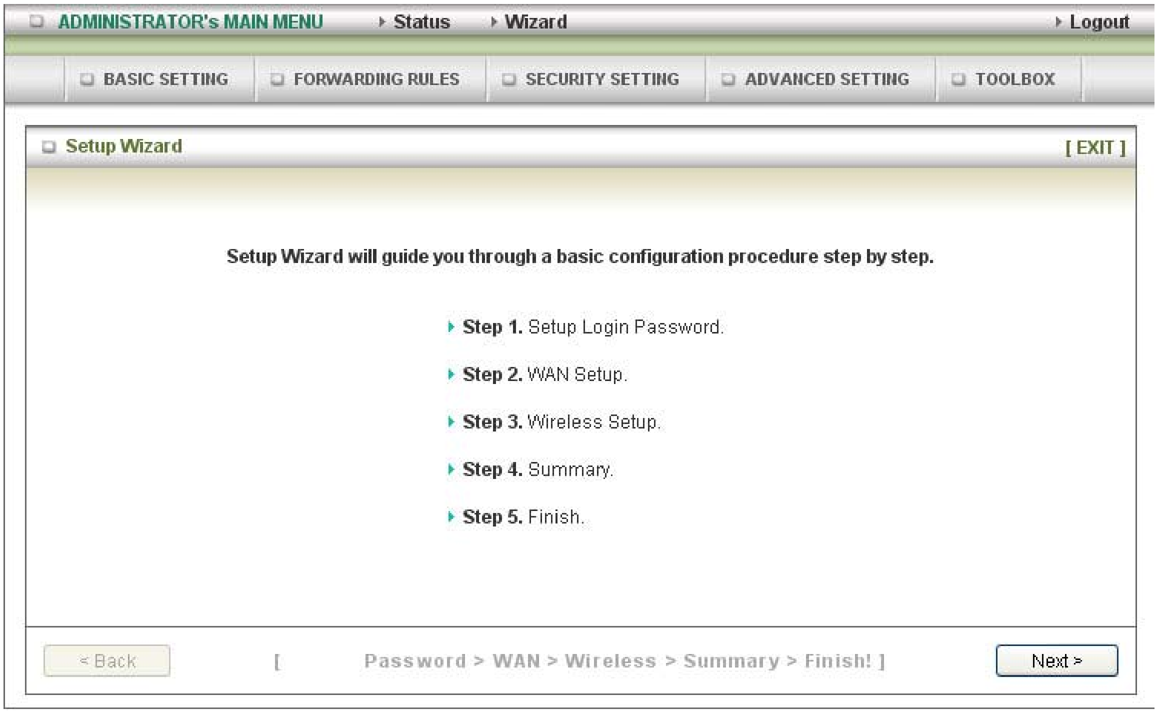
With wizard setting steps, you could configure the router in a very simple way. This configuration wizard includes settings of

a. **Login Password**,

b. **WAN Setup**

c. **Wireless Setup**,

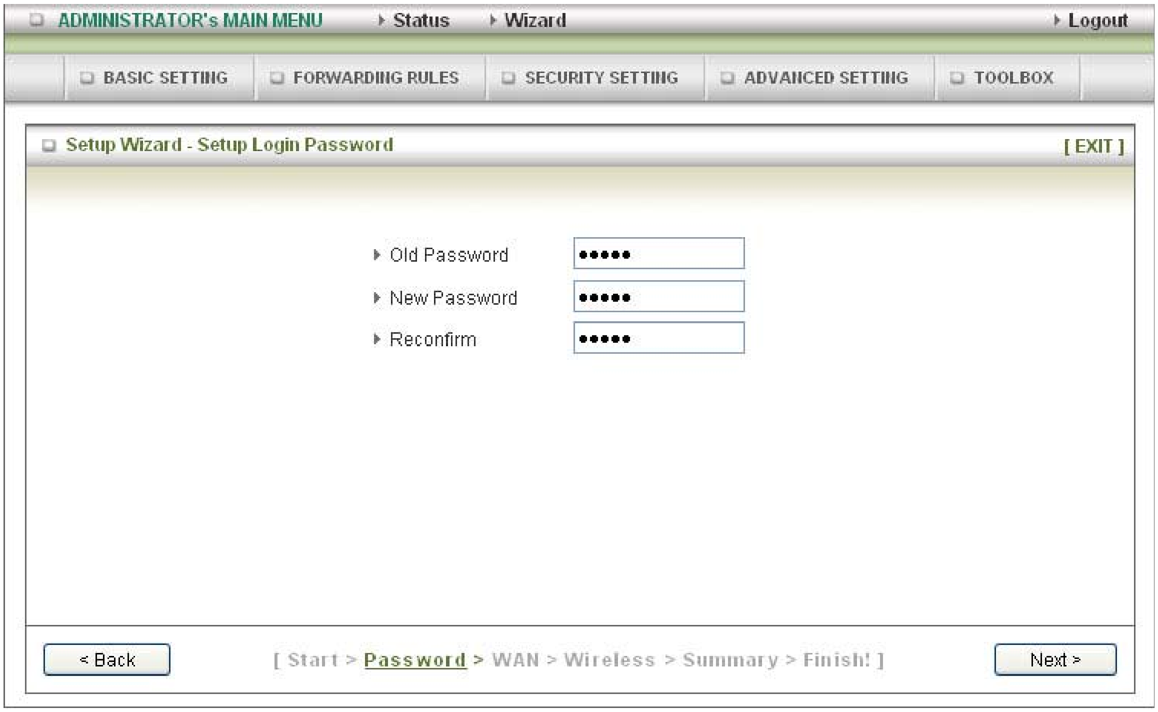
Press **“Next”** button to start configuration.



Setup Wizard will guide you through a basic configuration procedure step by step.

- **Step 1.** Setup Login Password.
- **Step 2.** WAN Setup.
- **Step 3.** Wireless Setup.
- **Step 4.** Summary.
- **Step 5.** Finish.

Step 1: Allow you to change the system password.


ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Setup Wizard - Setup Login Password
[EXIT]
< Back
[Start > Password > WAN > Wireless > Summary > Finish!]
Next >

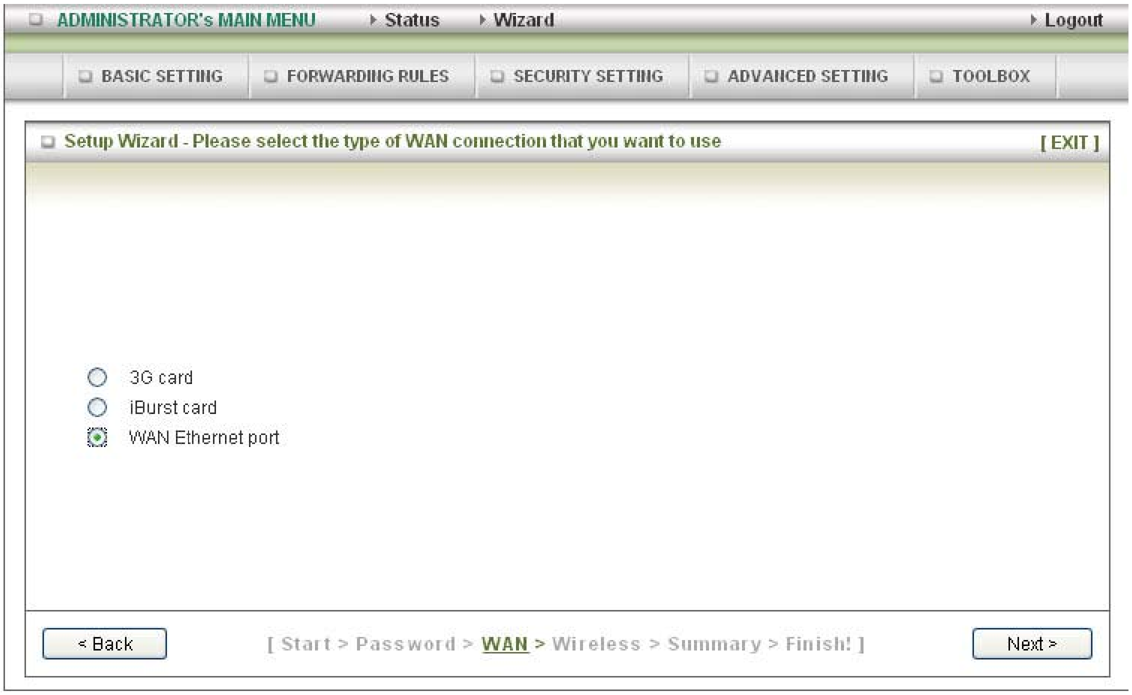
Old Password	●●●●●
New Password	●●●●●
Reconfirm	●●●●●

You can change Password here.

It is recommended that you change the system the basis of security

1. Key in your Old Password (if it is the first initiation, the “ admin” will be the defaulted one.
2: Enter your New Password
3: Enter your Password again for confirmation; it must be the same as the New Password.
4. Then click on “Next” to get into next installation.

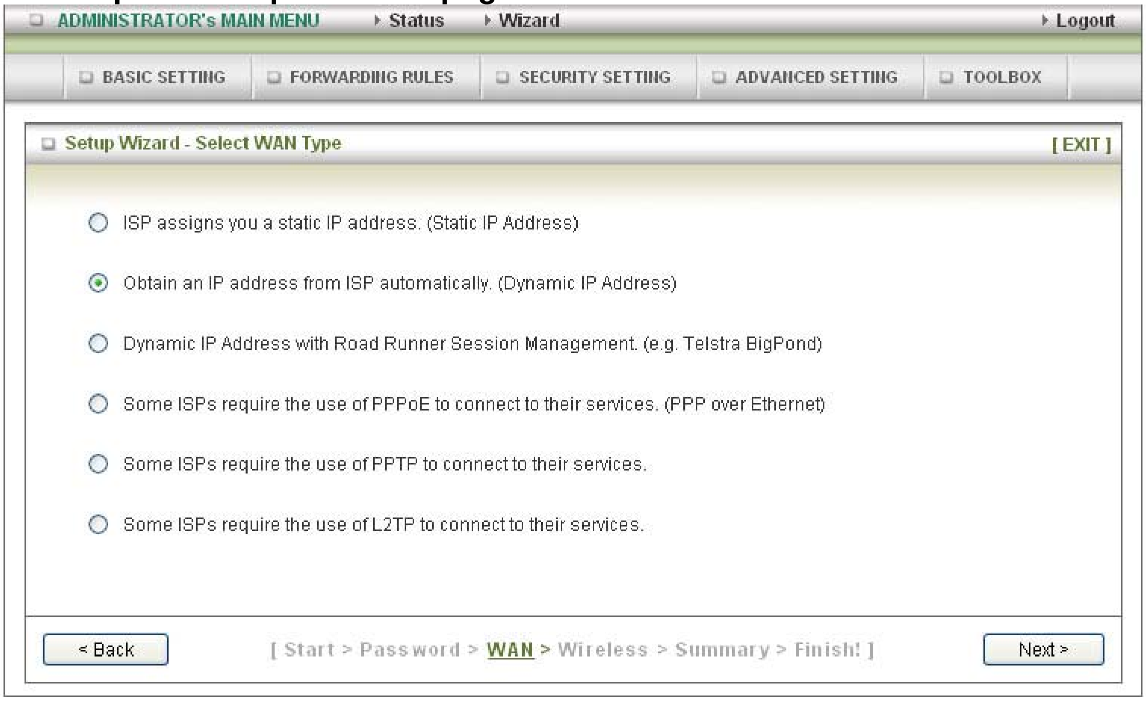
Step 2：Select WAN Types will be used for Internet connection



Setup Wizard - Please select the type of WAN connection that you want to use

○ 3G card
○ iBurst card
● WAN Ethernet port

To setup 3G card please see page 36



Setup Wizard - Select WAN Type

○ ISP assigns you a static IP address. (Static IP Address)

● Obtain an IP address from ISP automatically. (Dynamic IP Address)

○ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

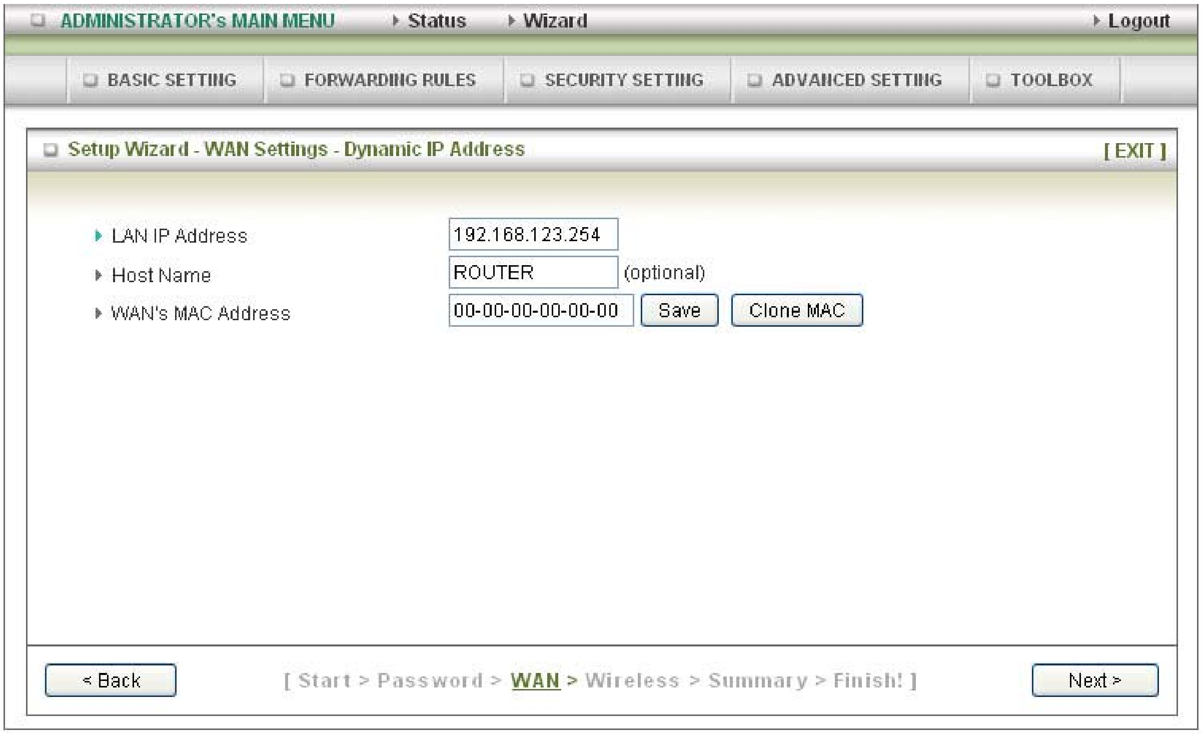
○ Some ISPs require the use of PPTP to connect to their services.

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

Pick up one of type you preferred to.

Click on “Next” button

Step 3: Configure the LAN IP Address, Host Name and Wan MAC Address



Setup Wizard - WAN Settings - Dynamic IP Address

LAN IP Address	192.168.123.254
Host Name	ROUTER (optional)
WAN's MAC Address	00-00-00-00-00-00

LAN is short for Local Area Network, and is considered your internal network. These are the IP settings of the LAN interface for the Wireless WAN Mobile Broadband Router, and they may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

Note: There are 254 addresses available on the Wireless WAN Mobile Broadband Router when using a 255.255.255.0 (Class C) subnet. Example: The router's IP address is 192.168.123.1. The available client IP range is 192.168.123.2 through 192.168.123.254.

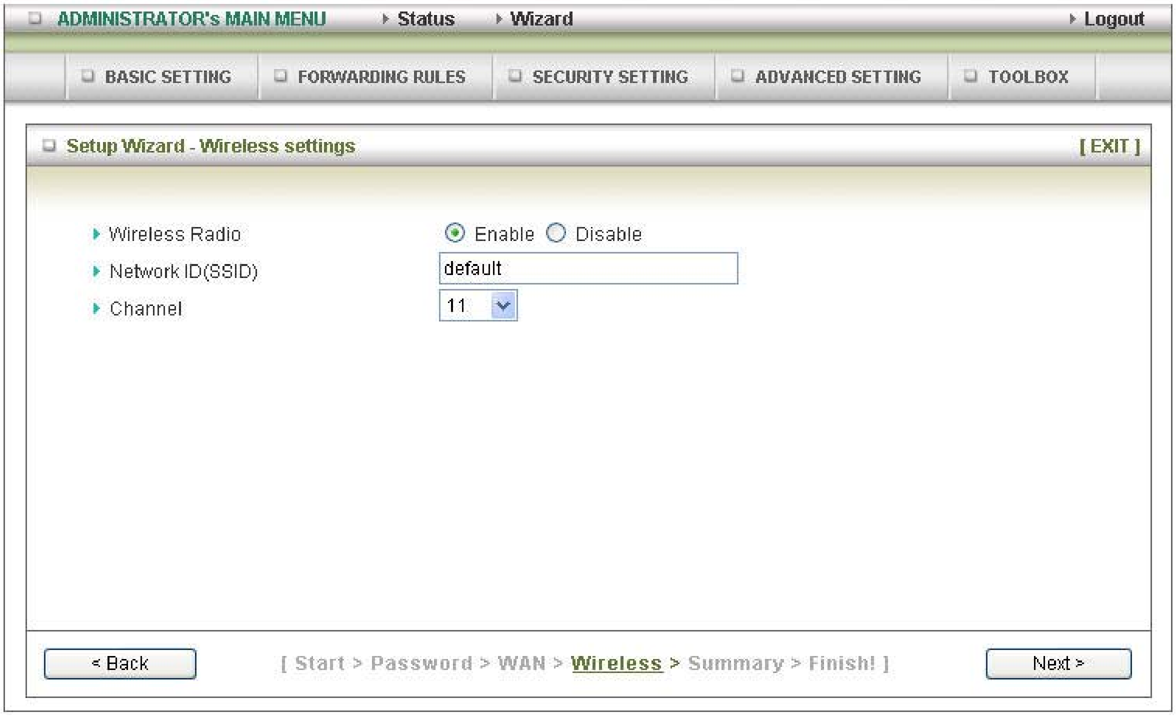
1. LAN IP Address- The IP address of the LAN interface. The **default** IP address is: **192.168.123.254**

2. Host Name is optional

3. WAN’s MAC Address
If you click the Clone MAC button, you will find the MAC address of your NIC shown in WAN's MAC Address

4. Click on ” **Next**” to continue.

Step 4: Configure the wireless settings.



Setup Wizard - Wireless settings

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

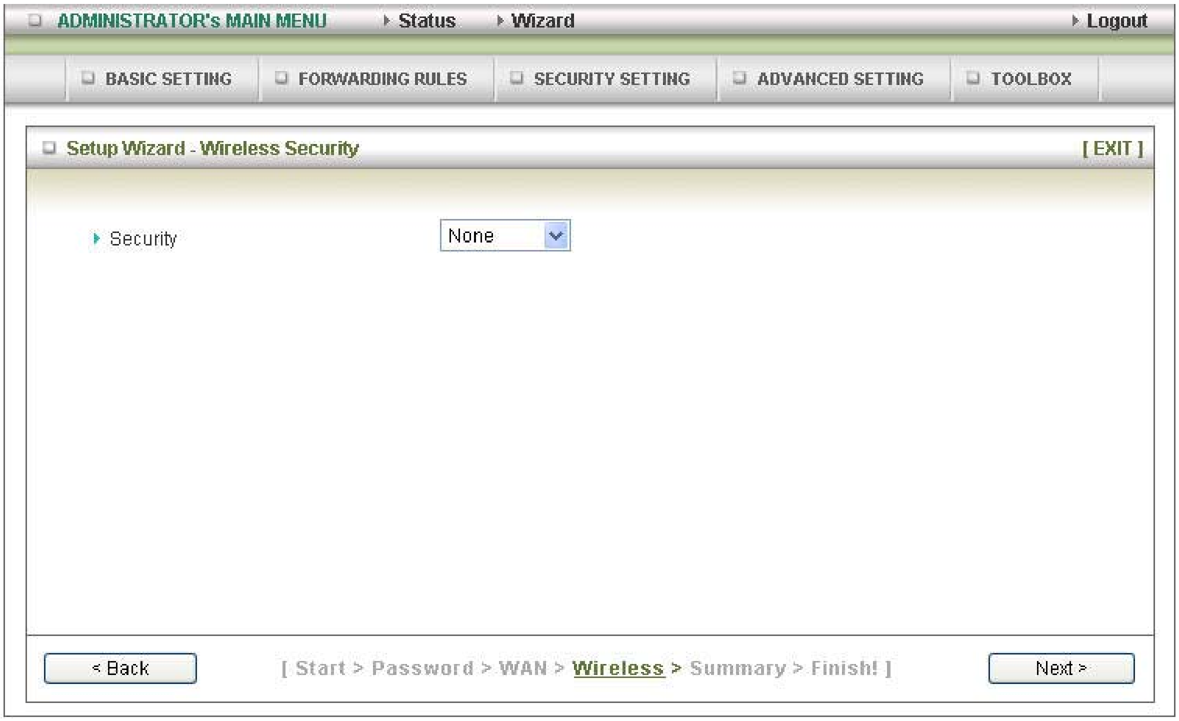
1. Select **Enabled** or **Disabled**. The **default** setting is **Enabled**.

2. Network ID(SSID) will be defaulted

3: Channel-□ Select Wireless Channel matching to your local area for Wireless connection

4: Click on ” **Next**” to continue.

Step 5: Select the Wireless security method of your wireless configuration.

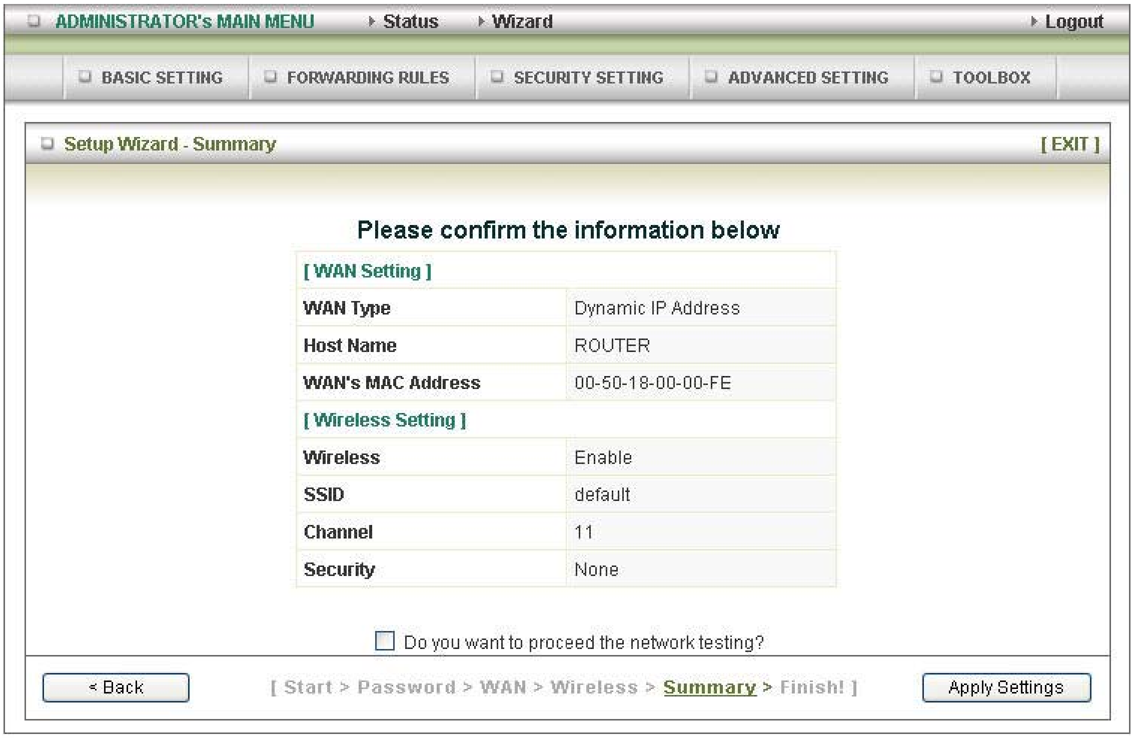


Setup Wizard - Wireless Security

Security None

Click on ” **Next**” to continue.

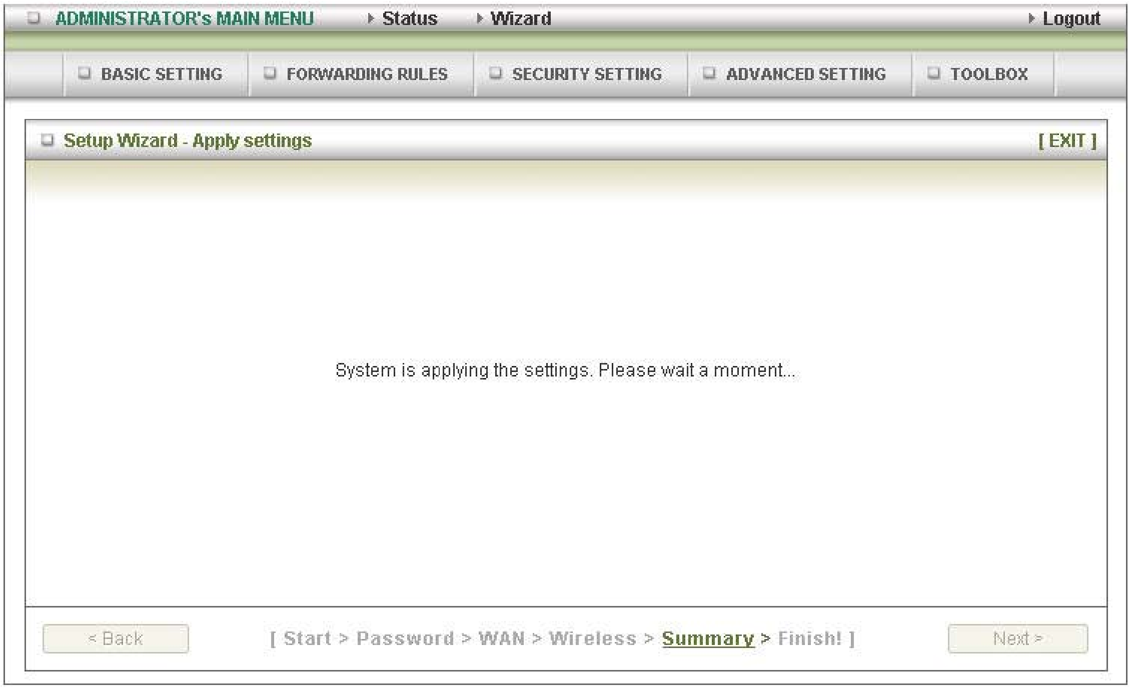
Step 6: Summary



Please confirm the information below

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

□ Do you want to proceed the network testing?


ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Setup Wizard - Apply settings
[EXIT]
< Back
[Start > Password > WAN > Wireless > Summary > Finish!]
Next >

System is applying the settings. Please wait a moment...

Clicking “Finish” button to back to Status Page

1.2.2. Advanced Setup > Basic Setting

1. **LAP 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.

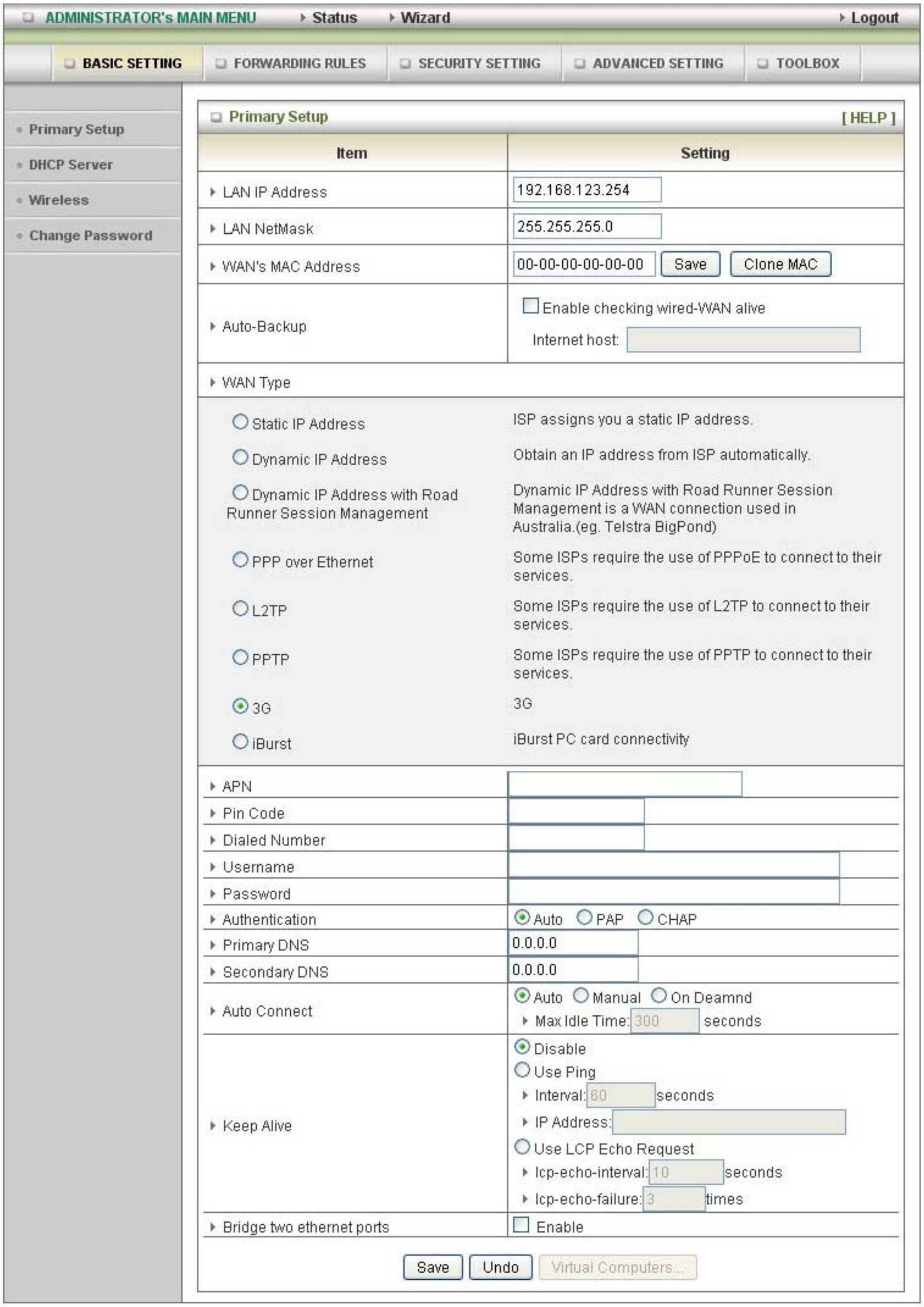
2. **LAN Netmask:** the Netmask of the local IP address

3. **WAN's MAC Address:** The WAN's MAC of this device. If you want to clone the MAC address from your NIC, just click the Clone MAC and save

4. **WAN Type**: WAN connection type of your ISP. You can select a correct one from the following options

Advanced Setup > Basic Setting > Primary Setup

Select the WAN types you prefer to get on the internet connection



Primary Setup

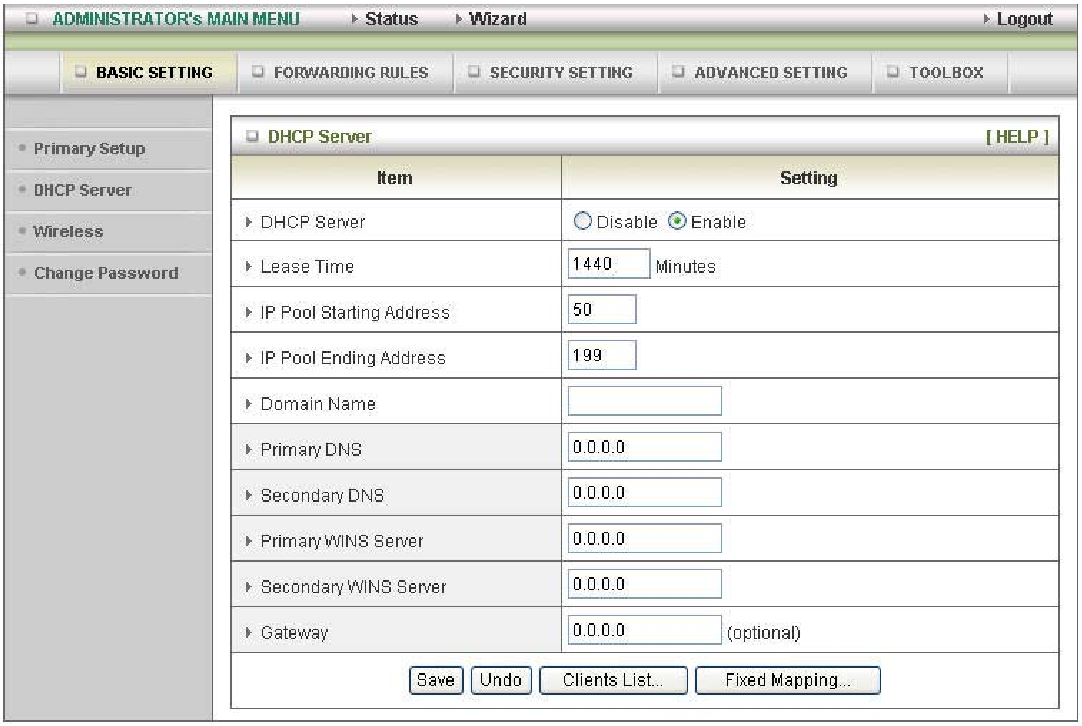
Item	Setting
LAN IP Address	192.168.123.254
LAN NetMask	255.255.255.0
WAN's MAC Address	00-00-00-00-00-00 Save Clone MAC
Auto-Backup	□ Enable checking wired-WAN alive Internet host:
WAN Type	
○ Static IP Address	ISP assigns you a static IP address.
○ Dynamic IP Address	Obtain an IP address from ISP automatically.
○ Dynamic IP Address with Road Runner Session Management	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. Telstra BigPond)
○ PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
○ L2TP	Some ISPs require the use of L2TP to connect to their services.
○ PPTP	Some ISPs require the use of PPTP to connect to their services.
● 3G	3G
○ iBurst	iBurst PC card connectivity
APN	
Pin Code	
Dialed Number	
Username	
Password	
Authentication	● Auto ○ PAP ○ CHAP
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Auto Connect	● Auto ○ Manual ○ On Deamnd Max Idle Time: 300 seconds
Keep Alive	● Disable ○ Use Ping Interval: 60 seconds IP Address: ○ Use LCP Echo Request lcp-echo-interval: 10 seconds lcp-echo-failure: 3 times
Bridge two ethernet ports	□ Enable

Caution: For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a **User Name** and **Password** to connect to the 3G network. Please refer to your documentation or service provider for additional

information.

□ **APN-** Enter the APN for your PC card here.
□ **Pin Code-**Enter the Pin Code for your PC card
□ **Dial-Number-** This field should not be altered except when required by your service provider.
□ **User Name-** Enter the new **User Name** for your PC card here.
□ **Password-** Enter the new **Password** for your PC card here.
□ **Primary DNS-** This feature allows you to assign a Primary DNS Server (Optional）
□ **Secondary DNS-** This feature allows you to assign a Secondary DNS Server Optional）
□ **Maximum Idle Time-**The Connection will be broken when the idle time arrives.
1: Pick up one of the types you preferred to.
2: Click on “ **Next**” button

Advanced Setup > Basic Setting > DHCP Server



DHCP Server

Item	Setting
DHCP Server	○ Disable ● Enable
Lease Time	1440 Minutes
IP Pool Starting Address	50
IP Pool Ending Address	199
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Gateway	0.0.0.0 (optional)

1. DHCP Server: Choose either **Disable** or **Enable**

2. Lease Time: DHCP lease time to the DHCP client

3. IP Pool Starting/Ending 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 / ending address of the IP address pool

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

5. Primayr DNS/Secondary DNS: This feature allows you to assign a DNS Servers

6. Primary WINS/Secondary WINS: This feature allows you to assign a **WINS** Servers

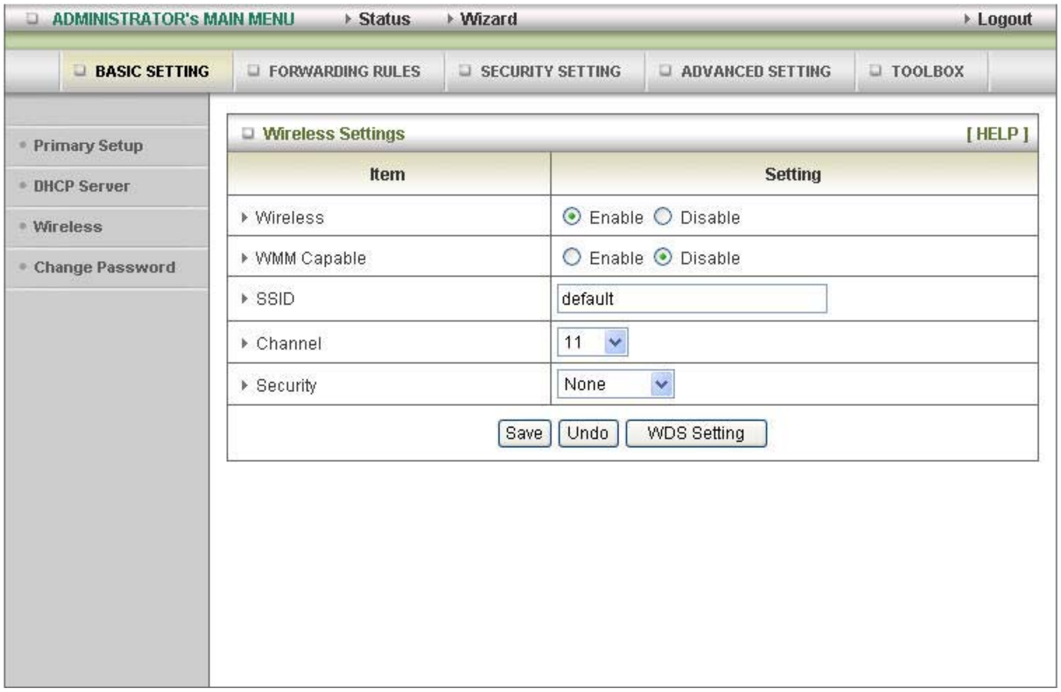
7. Gateway: The Gateway Address would be the IP address of an alternate Gateway.

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

After you finish your selection then

Either Click on **"Save"** to store what you just pick or click "**Undo"** to give up

Advanced Setup > Basic Setting > Wireless



Wireless Settings [HELP]

Item	Setting
Wireless	● Enable ○ Disable
WMM Capable	○ Enable ● Disable
SSID	default
Channel	11
Security	None

□ **Wireless - Enabled** is the **default.** Selecting this option will allow you to set your Wireless Access Point (WAP) settings.
□ **WMM Capable-** Choose Enable or Disable WMM function
□ **SSID-** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory **default** setting is **default**. The SSID can be easily changed to establish a new wireless network.(Note: SSID names may contain up to 32 ASCII characters).
□ **Channel- Channel 11** is the **default**. Devices on the network must share the same channel. (Note: Wireless adapters automatically scan and match the wireless settings. You may also select the channel you wish to use).
□ **Security-** You may select from three levels of encryption to secure your wireless network:
□ **No Encryption, WEP.802.1x, WPA-PSK, WPA, WPA2-PSK, or WPA2.**
□ **Security- No Encryption** is the **default** (as shown in the screen above)**.**

1. **WEP Security**: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. The standardized IEEE 802.11 WEP (128 or 64-bit) is used here.

2. **WEP Key 1, 2, 3 & 4**: 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.

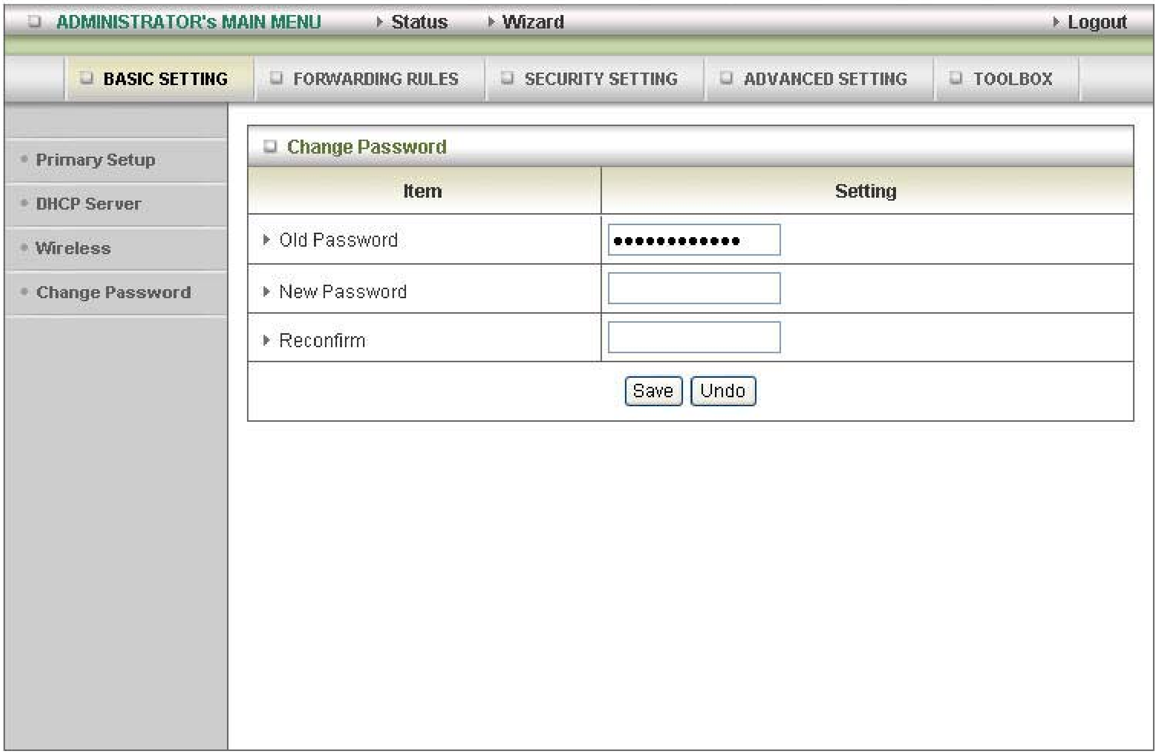
3. **802.1X:** Check Box was used to switch the function of the 802.1X. When the 802.1X function is enable

4. ***WPA-PSK/WPA-PSK2*** : Another encryption options for WPA-PSK-TKIP and WPA-PSK2-ADE . Enter a password in the WPA-PSK /WPA-PSK2 field between 8 and 63 characters long for ASCII.64 characters(0~9,a~f) for HEX.

WPA/WPA2 :The uses have to get a access form RADIUS server by performing user authentication. Enter the IP address of Radius server and RADIUS Shared Key.

5: Click on “**Save**” to store you just select

Advanced Setup > Basic Setting > Change Password



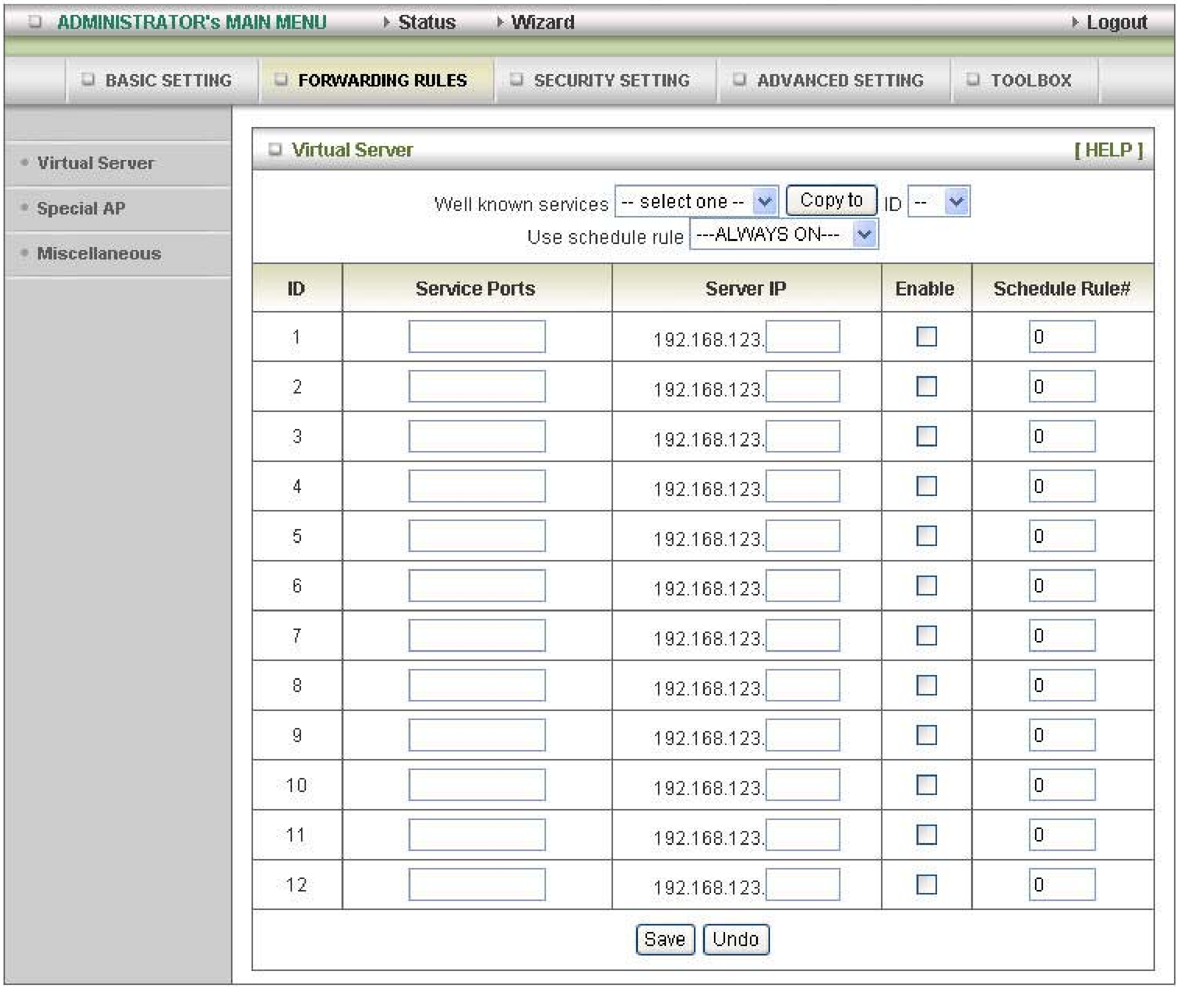
Change Password

Item	Setting
Old Password	●●●●●●●●●●●●
New Password	
Reconfirm	

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

Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Forwarding Rules > Virtual Server



Well known services: -- select one -- ID: --
Use schedule rule: ---ALWAYS ON---

ID	Service Ports	Server IP	Enable	Schedule Rule#
1		192.168.123.	☐	0
2		192.168.123.	☐	0
3		192.168.123.	☐	0
4		192.168.123.	☐	0
5		192.168.123.	☐	0
6		192.168.123.	☐	0
7		192.168.123.	☐	0
8		192.168.123.	☐	0
9		192.168.123.	☐	0
10		192.168.123.	☐	0
11		192.168.123.	☐	0
12		192.168.123.	☐	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**.

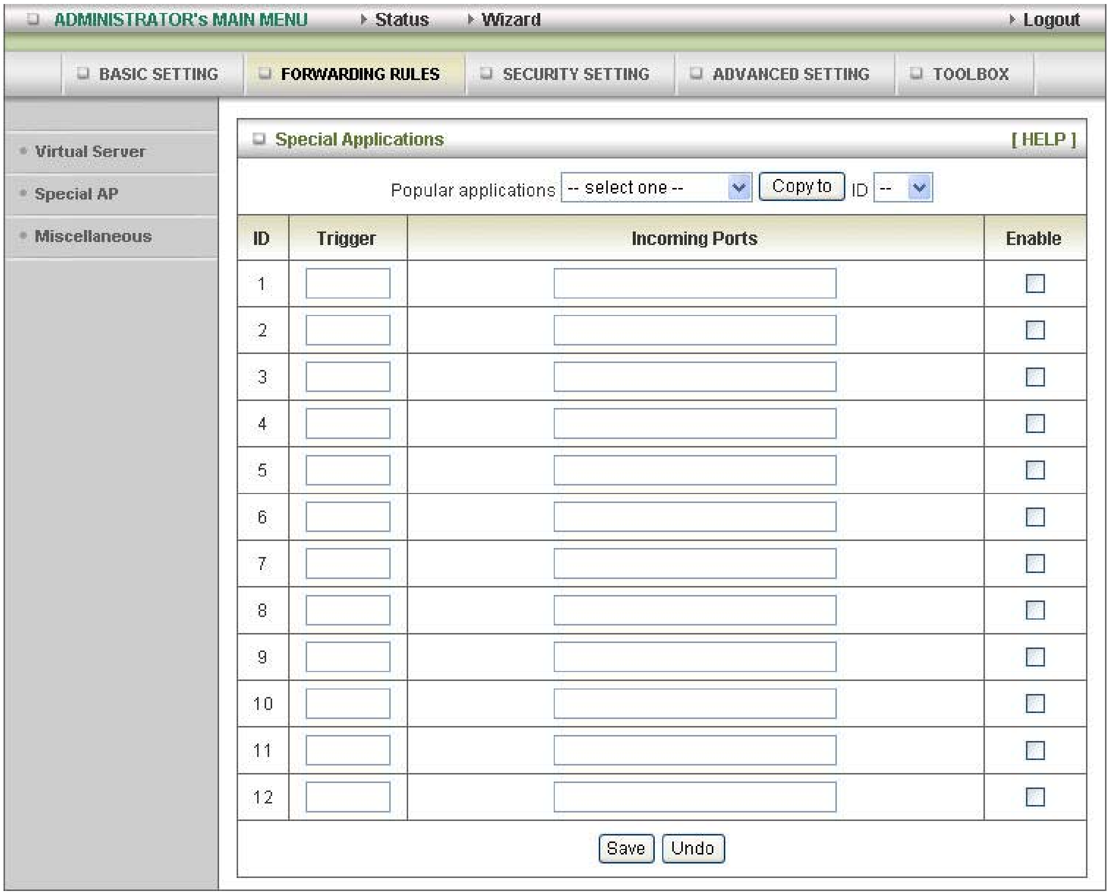
For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable

21 19	2.168.123.1	V
80 19	2.168.123.2	V
1723 19	2.168.123.6	V

Click on **"Save"** to store what you just select or **"Undo"** to give up

Advanced Setup > Forwarding Rules > Special AP



Popular applications -- select one -- ID --

ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□
11			□
12			□

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.

1. **Trigger**: the outbound port number issued by the application.
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

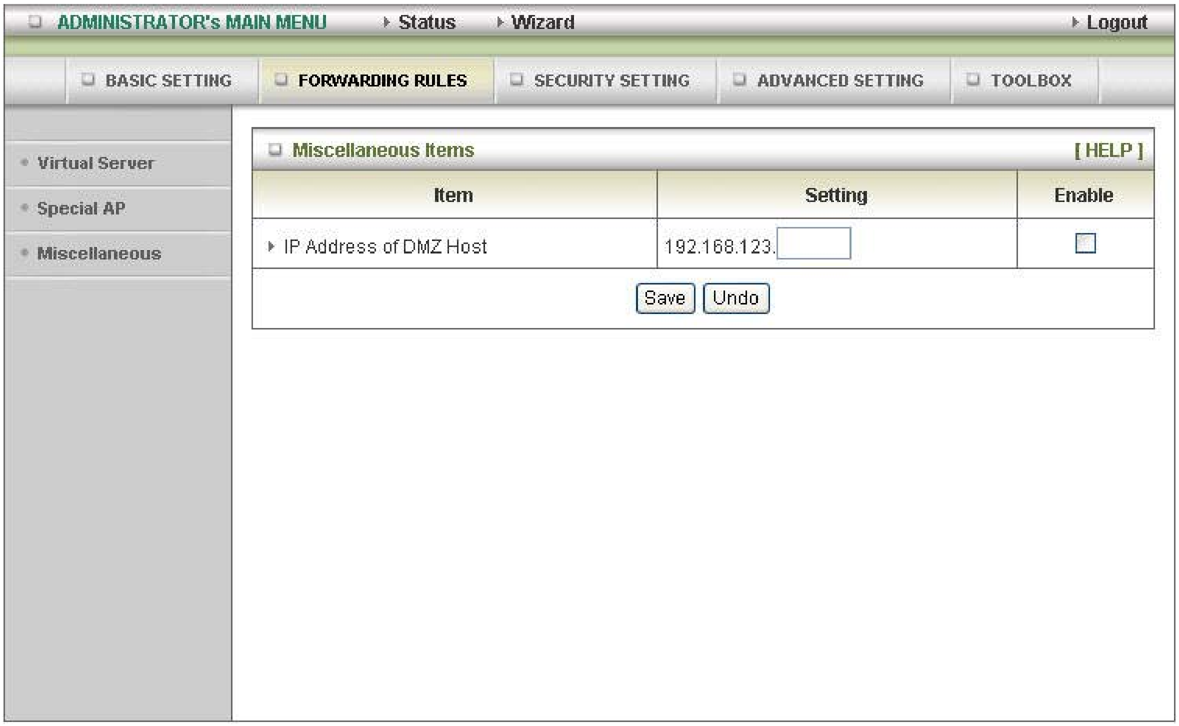
This product provides some predefined settings.

1. Select your application and
2. 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.

Click on **“Save”** to store what you just select or**” Undo”** to give up

Advanced Setup > Forwarding Rules > Miscellaneous



Miscellaneous Items [HELP]

Item	Setting	Enable
IP Address of DMZ Host	192.168.123.	□

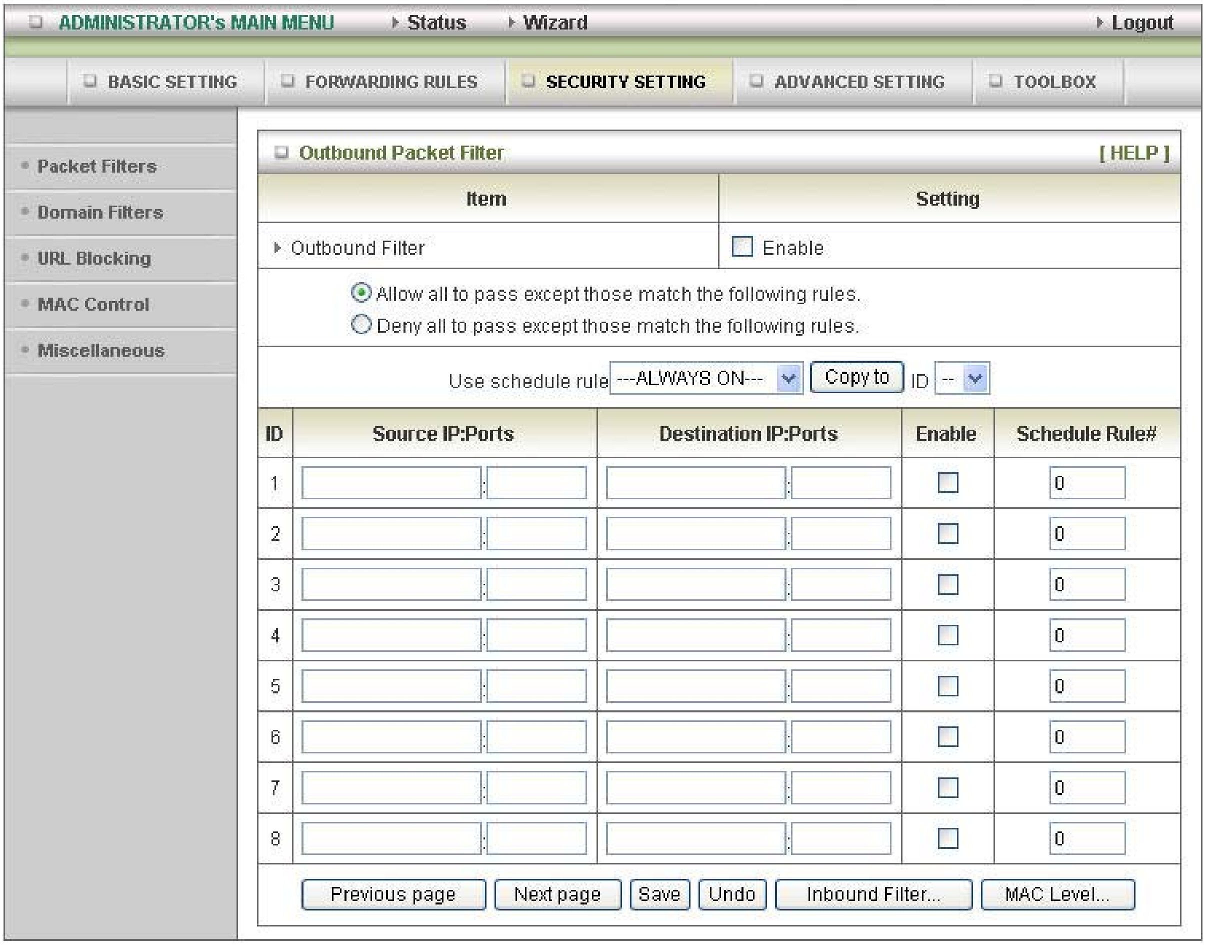
IP Address of DMZ Host

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.

Click on **“Save”** to store what you just select or **“Undo”** to give up

NOTE: This feature should be used only when needed.

Advanced Setup > Security Setting > Packet Filters



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.

Use schedule rule ---ALWAYS ON--- Copy to ID --

ID	Source IP:Ports	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:

1. Allow all to pass except those match the specified rules
2. 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
- Destination IP address
- Destination port
- 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.

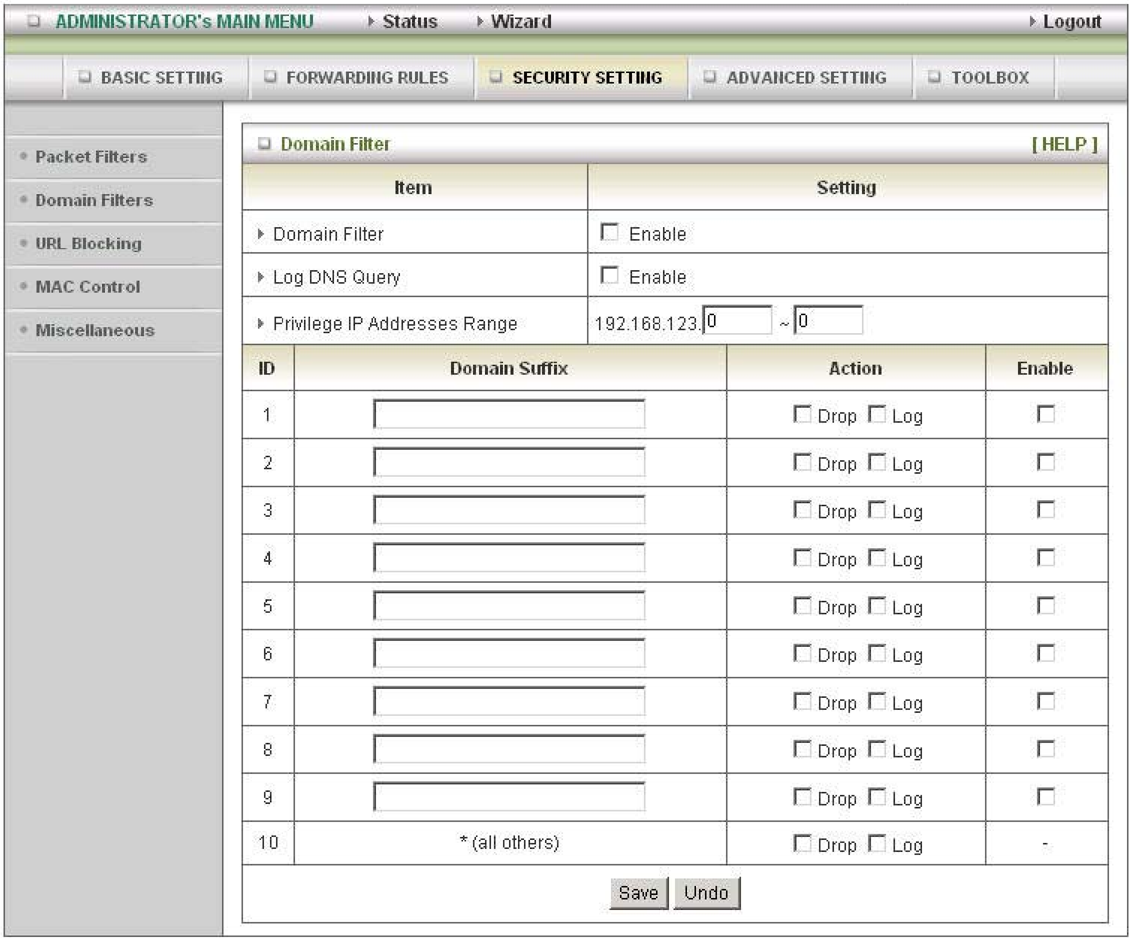
Click on **“Save”** to store what you just select or **“Undo”** to give up

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field

Click on “Save” to store what you just select or “Undo” to give up

Advanced Setup > Security Setting > Domain Filters



Domain Filter

Item	Setting
Domain Filter	□ Enable
Log DNS Query	□ Enable
Privilege IP Addresses Range	192.168.123. 0 ~ 0

ID	Domain Suffix	Action	Enable
1		□ Drop □ Log	□
2		□ Drop □ Log	□
3		□ Drop □ Log	□
4		□ Drop □ Log	□
5		□ Drop □ Log	□
6		□ Drop □ Log	□
7		□ Drop □ Log	□
8		□ Drop □ Log	□
9		□ Drop □ Log	□
10	* (all others)	□ Drop □ Log	-

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.

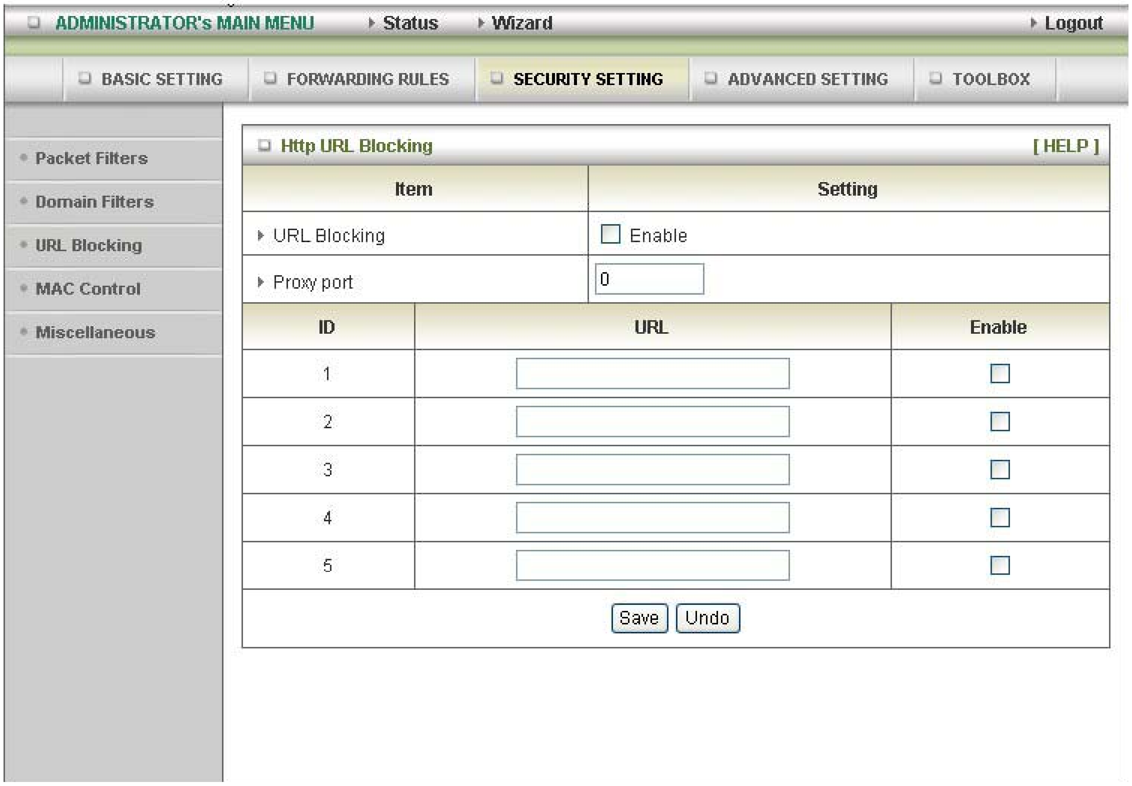
Privilege IP Address Range
Setting a group of hosts and privilege these hosts to access network without restriction.

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.
Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Security Setting > URL Blocking



Http URL Blocking [HELP]

Item	Setting
URL Blocking	□ Enable
Proxy port	0

ID	URL	Enable
1		□
2		□
3		□
4		□
5		□

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**.

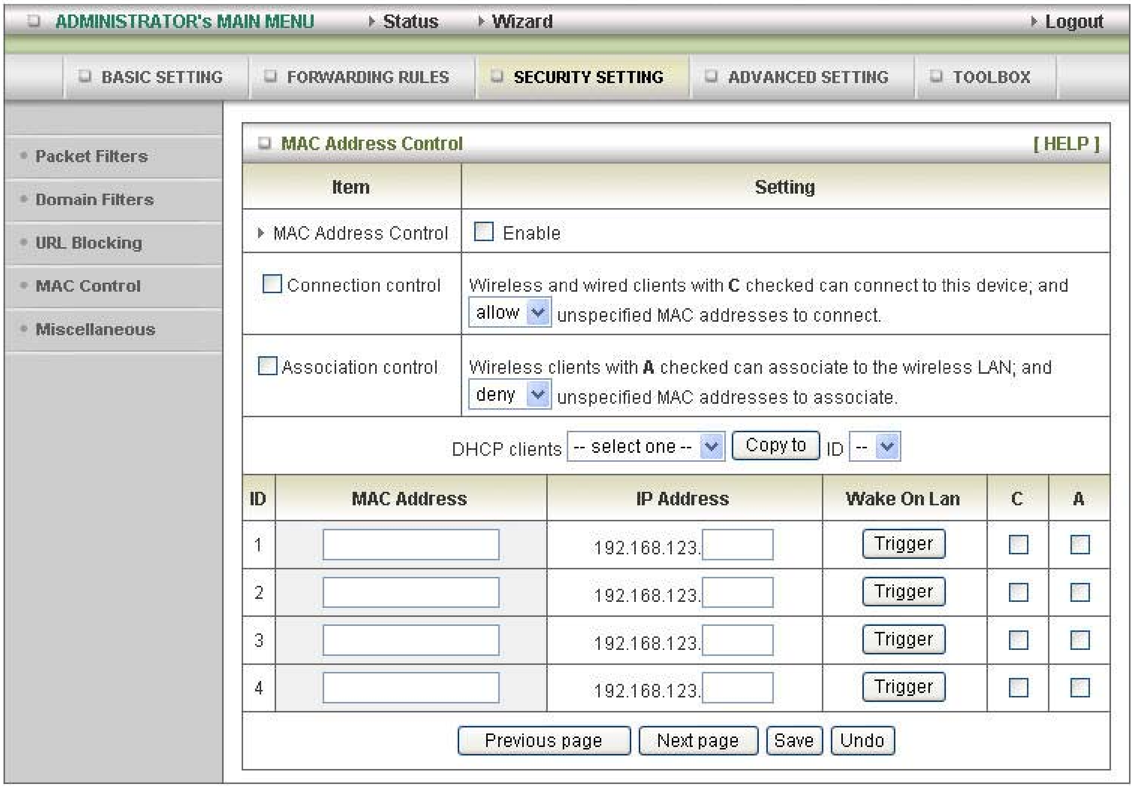
URL Blocking Enable
Check if you want to enable URL Blocking.

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
Check to enable each rule.
Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Security Setting > MAC Control



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.

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

ID	MAC Address	IP Address	Wake On Lan	C	A
1		192.168.123.	Trigger	□	□
2		192.168.123.	Trigger	□	□
3		192.168.123.	Trigger	□	□
4		192.168.123.	Trigger	□	□

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.

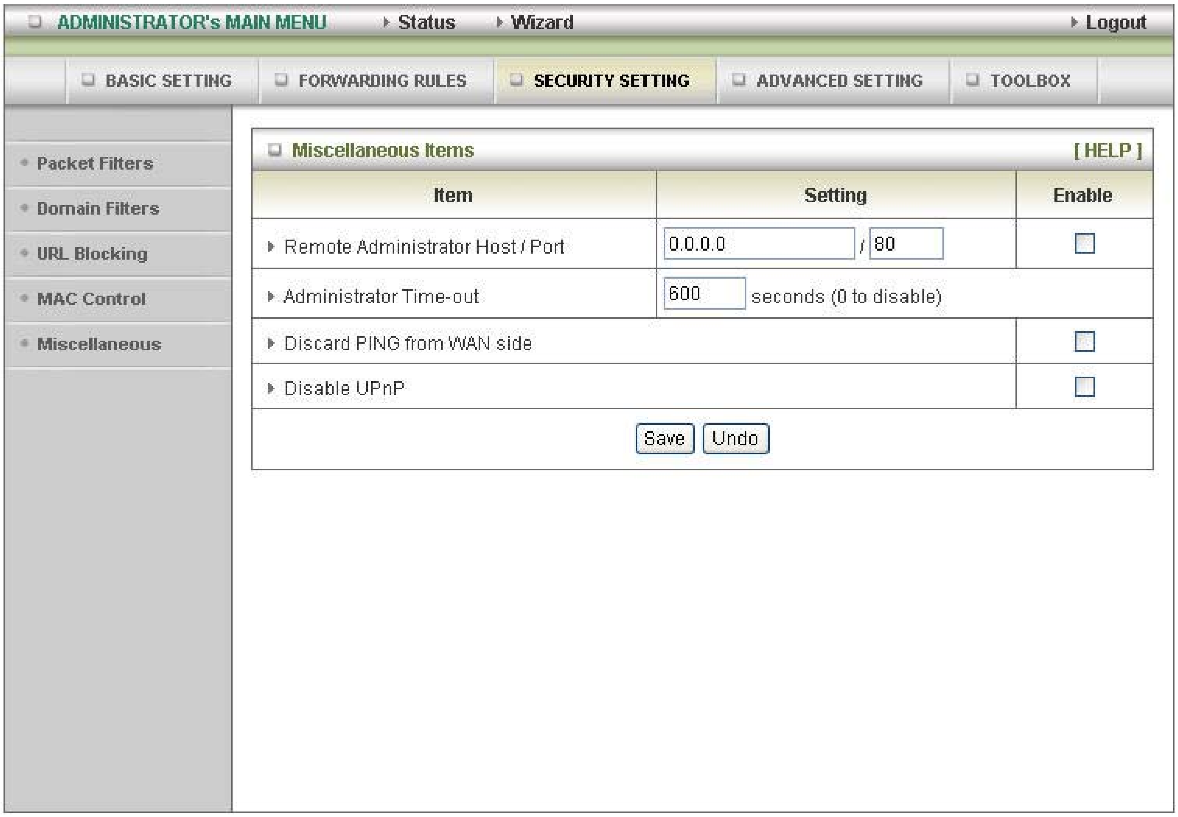
MAC Address Control Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

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

1: Click on **“Save”** to store what you just select or **“Undo”** to give up
2: Click on **“Next Page”** to go down or **“Previous page”** back to last page

Advanced Setup > Security Setting > Miscellaneous



Item	Setting	Enable
Remote Administrator Host / Port	0.0.0.0 / 80	□
Administrator Time-out	600 seconds (0 to disable)	
Discard PING from WAN side		□
Disable UPnP		□

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 80. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically, you may set it to zero to disable this feature.

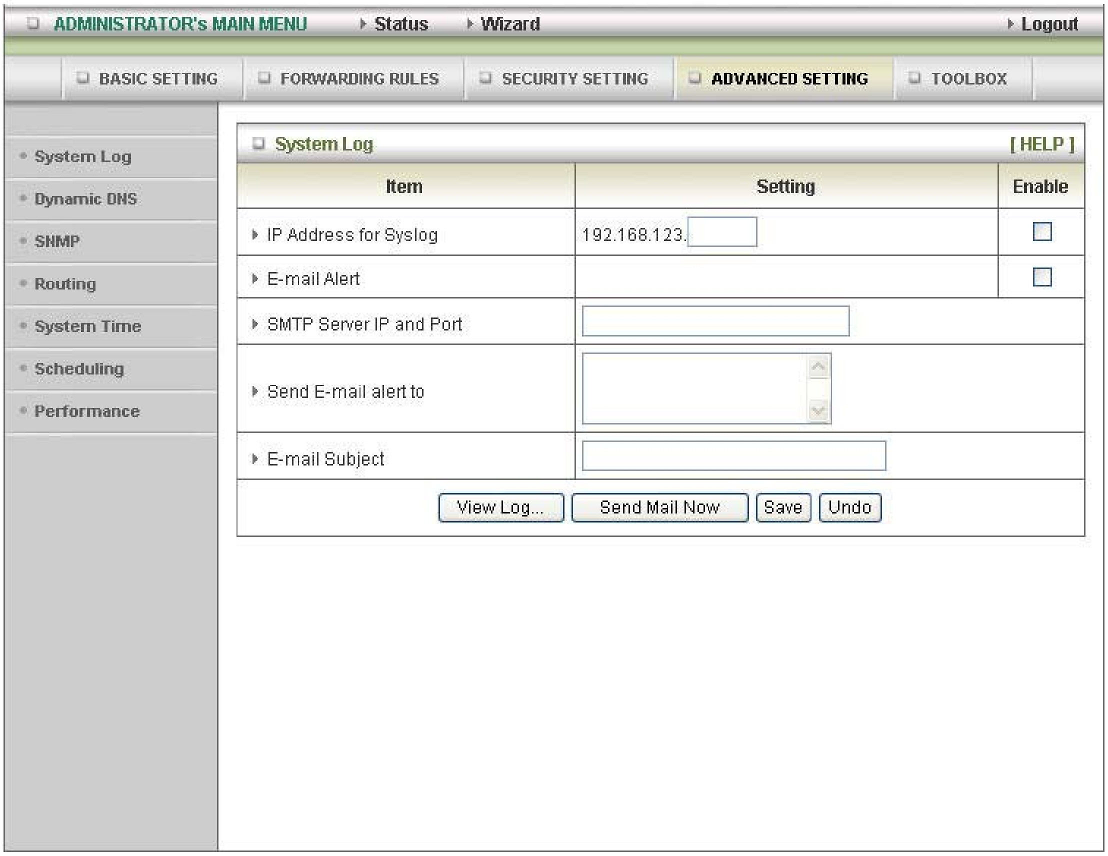
Discard PING from WAN side

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

Disable UPNP: Choose enable or disable the UPNP feature

Click on **“Save”** to store what you just select or**” Undo”** to give up

Advanced Setup > Advanced Setting > System Log



System Log

Item	Setting	Enable
IP Address for Syslog	192.168.123.	□
E-mail Alert		□
SMTP Server IP and Port		
Send E-mail alert to		
E-mail Subject		

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 syslog 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".

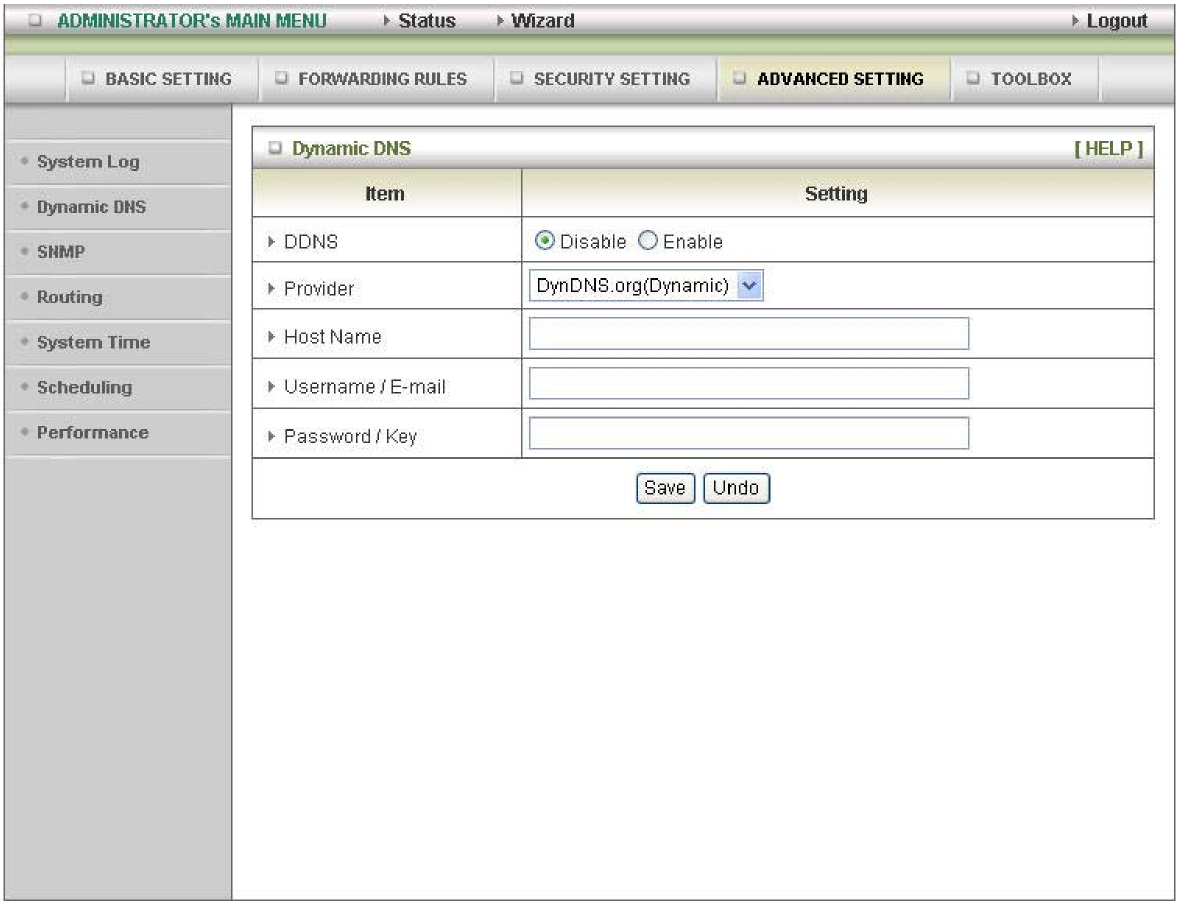
Send E-mail alert to

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

E-mail Subject

The subject of email alert, this setting is optional.
Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Advanced Setting > Dynamic DNS



Dynamic DNS

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

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

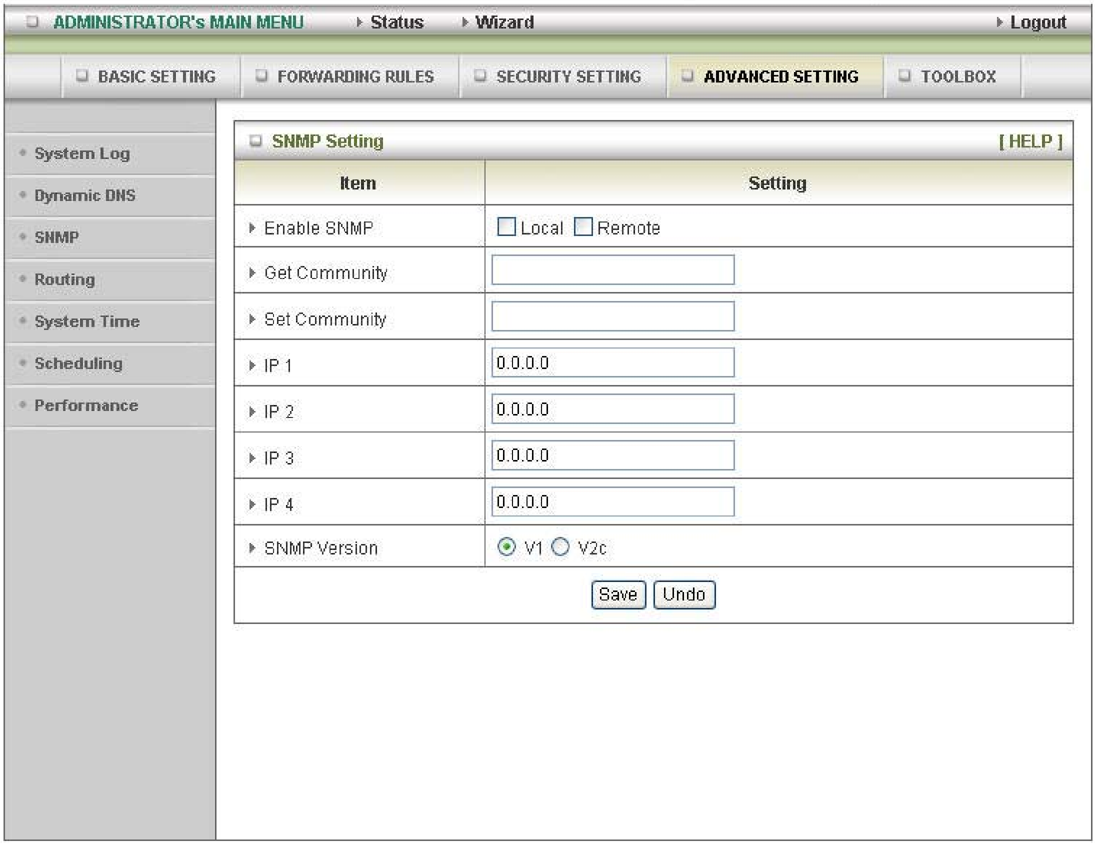
Username/E-mail

Password/Key

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

Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Advanced Setting > SNMP



SNMP Setting

Item	Setting
Enable SNMP	□ Local □ Remote
Get Community	
Set Community	
IP 1	0.0.0.0
IP 2	0.0.0.0
IP 3	0.0.0.0
IP 4	0.0.0.0
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 either Local or 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

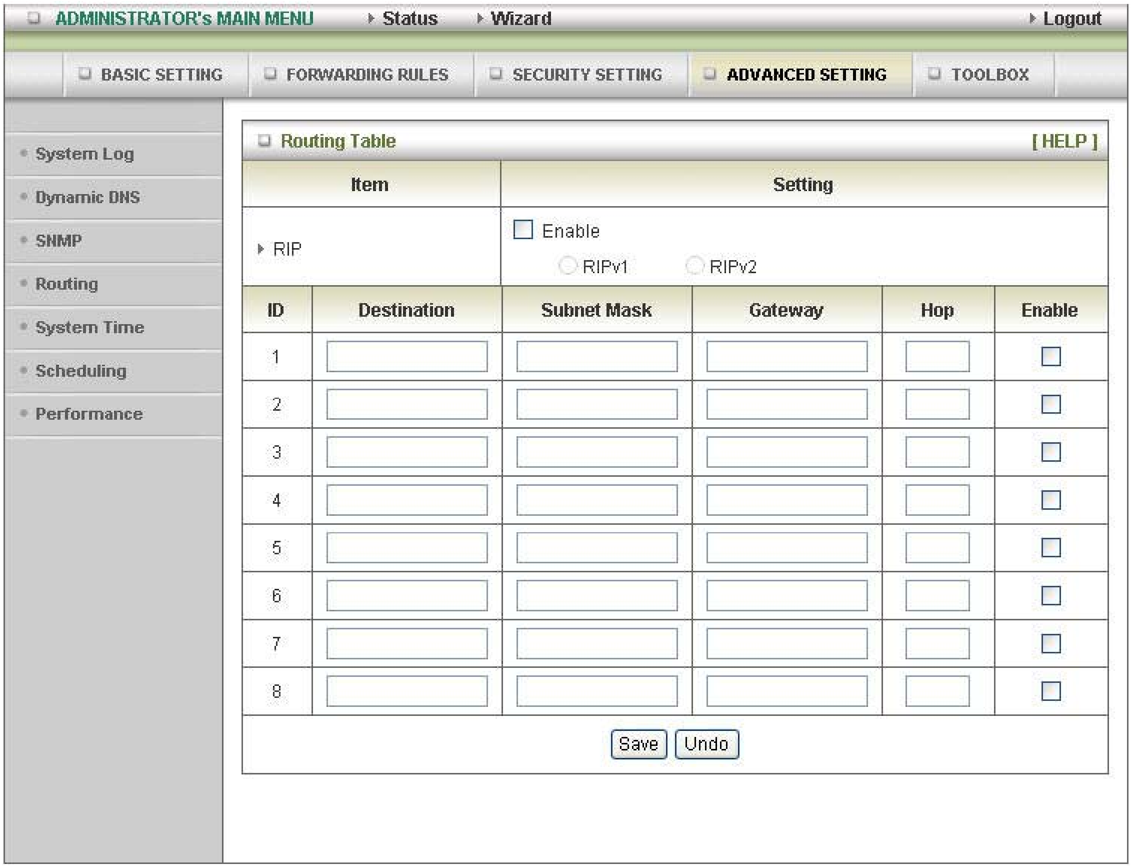
Setting the community of SetRequest your device will accept.
IP 1,IP 2,IP 3,IP 4
Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

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

Click on **"Save"** to store what you just select or **"Undo"** to give up.

Advanced Setup > Advanced Setting > Routing



Routing Table

Item	Setting
RIP	□ Enable ○ RIPv1 ○ RIPv2

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 and dynamic routing.

Dynamic Routing

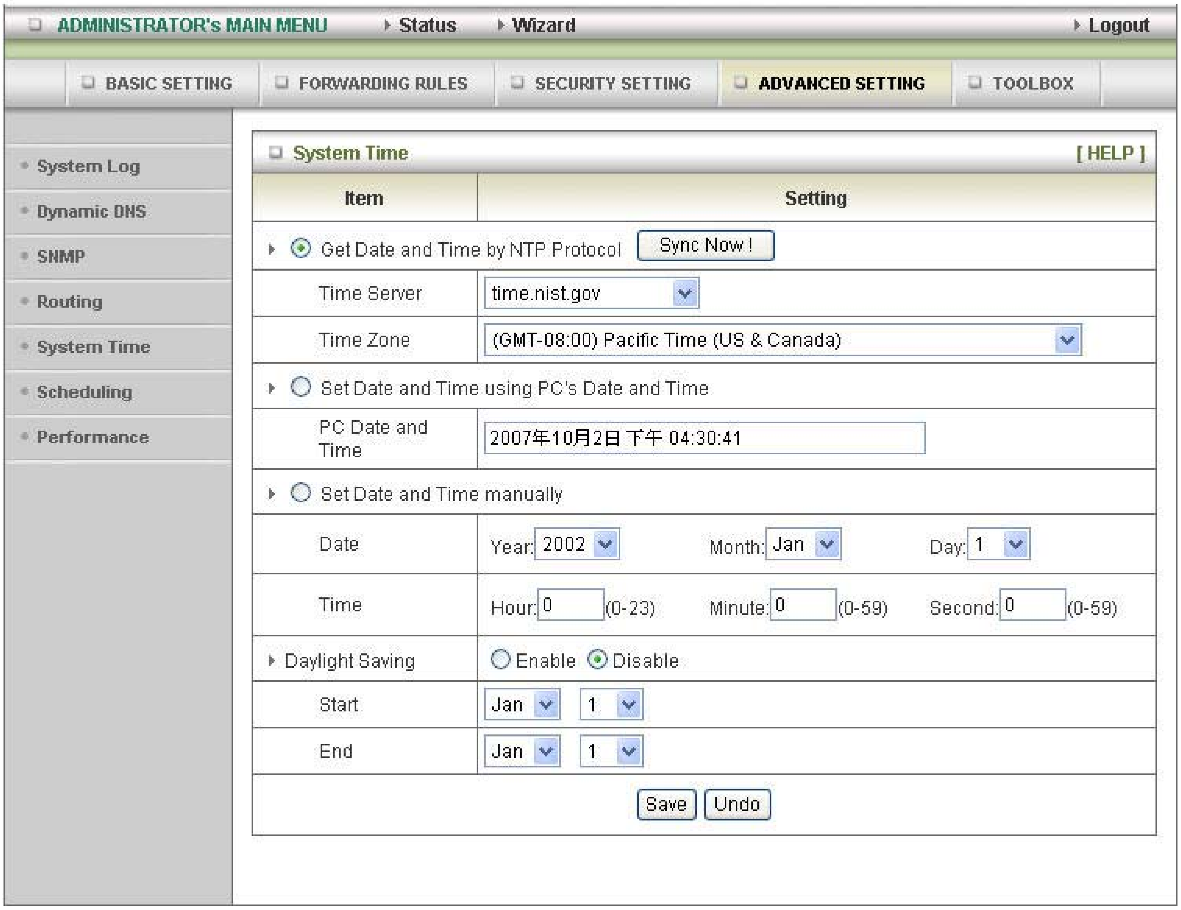
Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

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 un-checking the Enable checkbox.

Click on **“Save”** to store what you just select or **“Undo”** to give up**.**

Advanced Setup > Advanced Setting > System Time



Item	Setting
● 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	2007年10月2日 下午 04:30:41
○ Set Date and Time manually	
Date	Year: 2002 Month: Jan Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)
Daylight Saving	○ Enable ● Disable
Start	Jan 1
End	Jan 1

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 using PC's Date and Time

Set the Date and Time from your PC

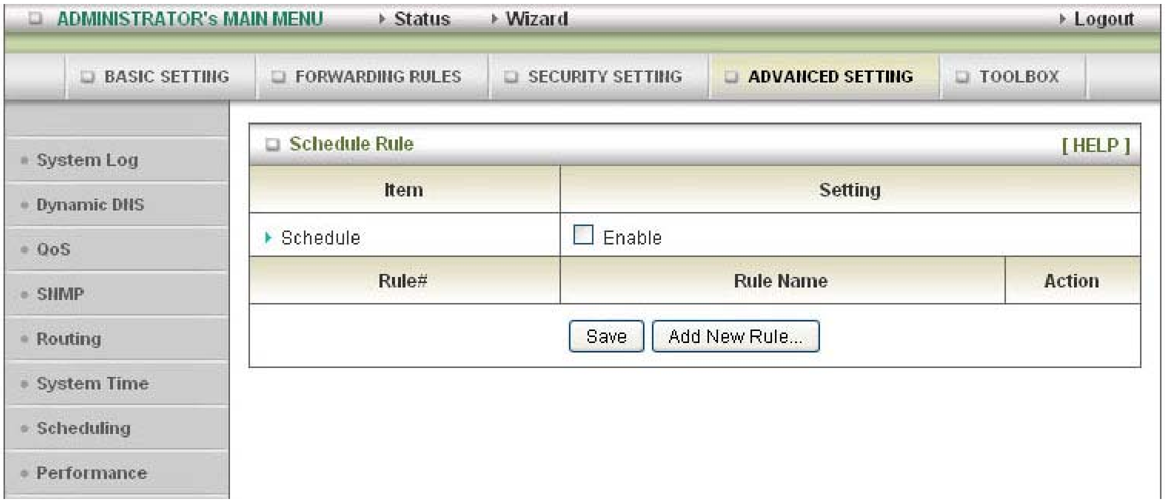
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Daylight Saving

Click on **"Save"** to store what you just select or **"Undo"** to give up.

Advanced Setup > Advanced Setting > Scheduling



Schedule Rule

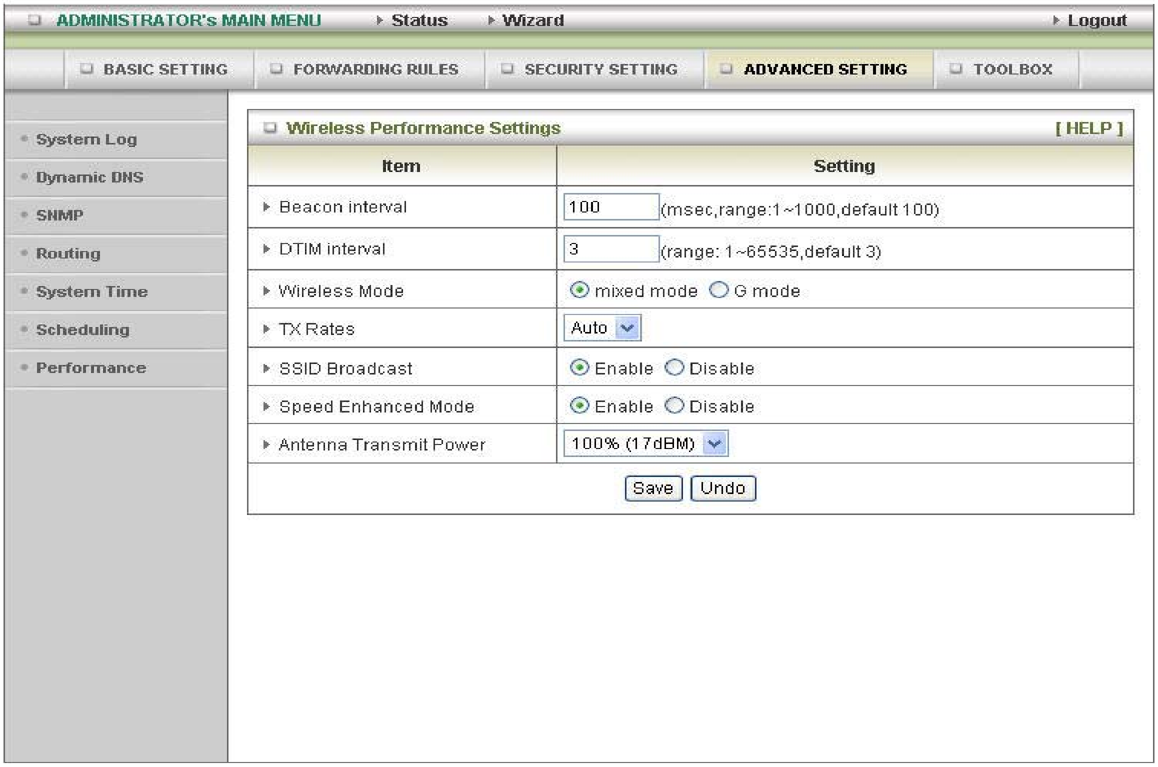
Item	Setting
Schedule	□ Enable

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
Click on "**Save"** to store what you just select.

Advanced Setup > Advanced Setting > Performance



Wireless Performance Settings

Item	Setting
Beacon interval	100 (msec,range:1~1000,default 100)
DTIM interval	3 (range: 1~65535,default 3)
Wireless Mode	● mixed mode ○ G mode
TX Rates	Auto
SSID Broadcast	● Enable ○ Disable
Speed Enhanced Mode	● Enable ○ Disable
Antenna Transmit Power	100% (17dBM)

Beacon Interval

Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a Beacon interval value between 1 and 1000. The default value is set to 100 milliseconds.

DTIM interval：

Enter a value between 1 and 65535 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages.The default value for DTIM interval is set to 3

Wireless mode

Select wireless connection mode for wireless connection

TX Rates

Slect the basic transfer rates based on the speed of wireless adapters on the WLAN (wireless local area network).

SSID Broadcast

Choose enable or disable the wireless SSID broadcast. By turning off the broadcast of the SSID ,it is possible to make your wireless network nearly invisible.

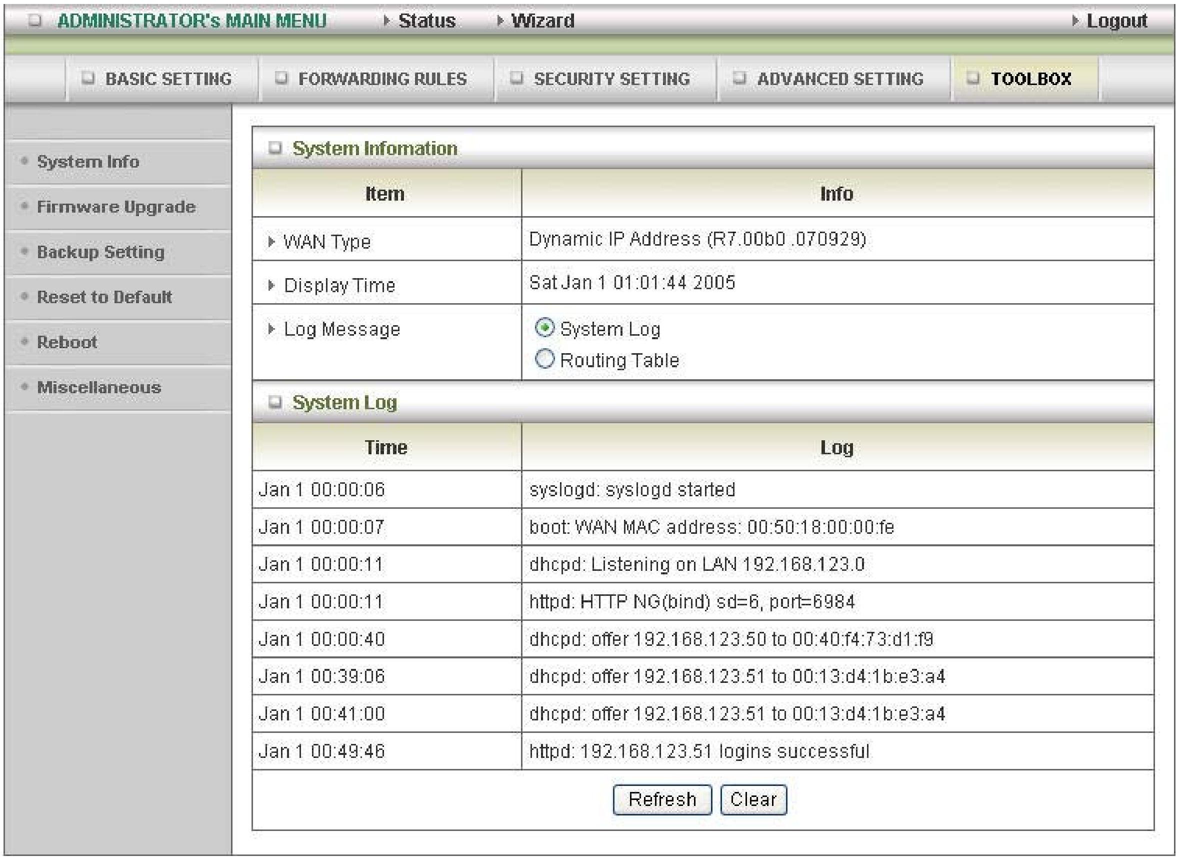
Speed Enhanced Mode
This is Tx Brust function for Ralink wireless solution

Antenna Transmit Power:

Select the Transmit Power of the Antenna

Click on **“Save”** to store what you just select or **“Undo”** to give up

Advanced Setup > Tool Box > System Info



System Infomation

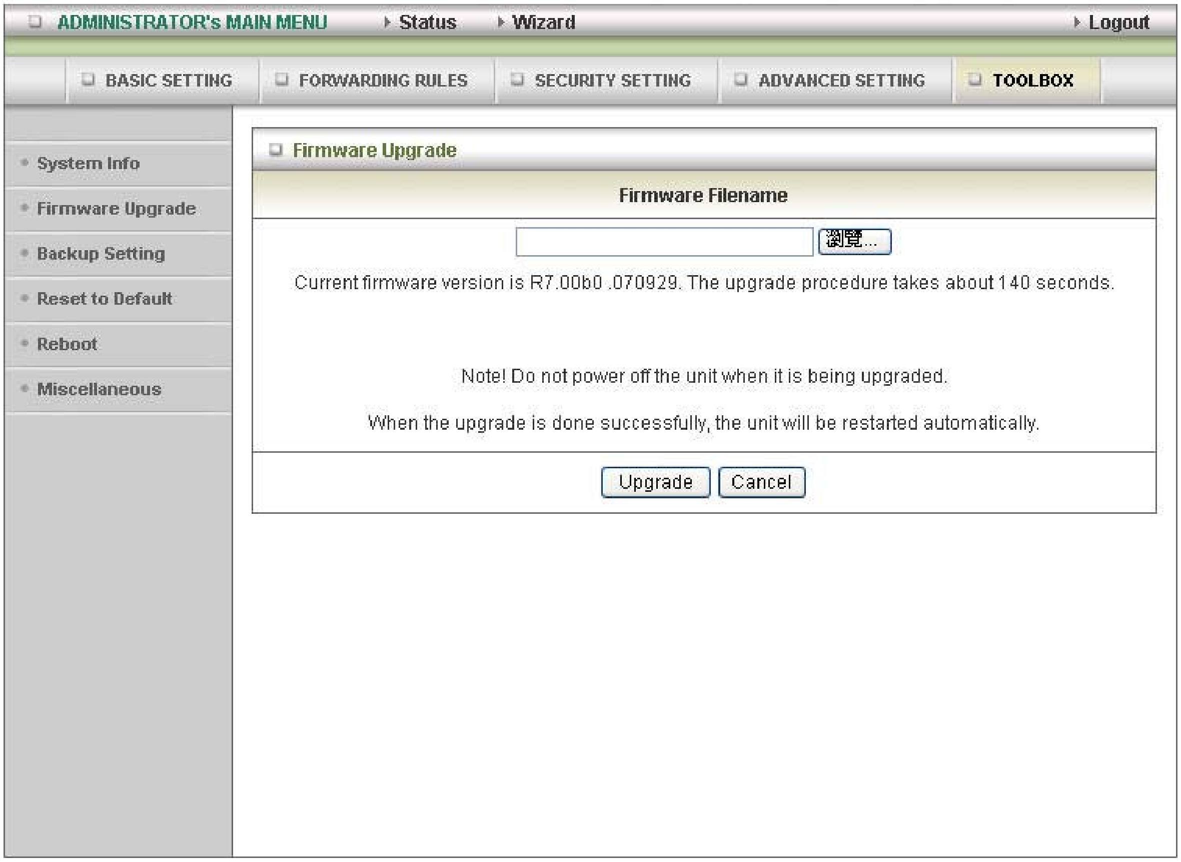
Item	Info
WAN Type	Dynamic IP Address (R7.00b0 .070929)
Display Time	Sat Jan 1 01:01:44 2005
Log Message	● System Log ○ Routing Table

System Log

Time	Log
Jan 1 00:00:06	syslogd: syslogd started
Jan 1 00:00:07	boot: WAN MAC address: 00:50:18:00:00:fe
Jan 1 00:00:11	dhcpd: Listening on LAN 192.168.123.0
Jan 1 00:00:11	httpd: HTTP NG(bind) sd=6, port=6984
Jan 1 00:00:40	dhcpd: offer 192.168.123.50 to 00:40:f4:73:d1:f9
Jan 1 00:39:06	dhcpd: offer 192.168.123.51 to 00:13:d4:1b:e3:a4
Jan 1 00:41:00	dhcpd: offer 192.168.123.51 to 00:13:d4:1b:e3:a4
Jan 1 00:49:46	httpd: 192.168.123.51 logins successful

You can view the System log, Routing Table information in this page

Advanced Setup > Tool Box > Firmware Upgrade



Current firmware version is R7.00b0 .070929. The upgrade procedure takes about 140 seconds.

Note! Do not power off the unit when it is being upgraded.

When the upgrade is done successfully, the unit will be restarted automatically.

You can upgrade firmware by clicking **Firmware "Upgrade"** button

Advanced Setup > Tool Box > Backup Setting

You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved

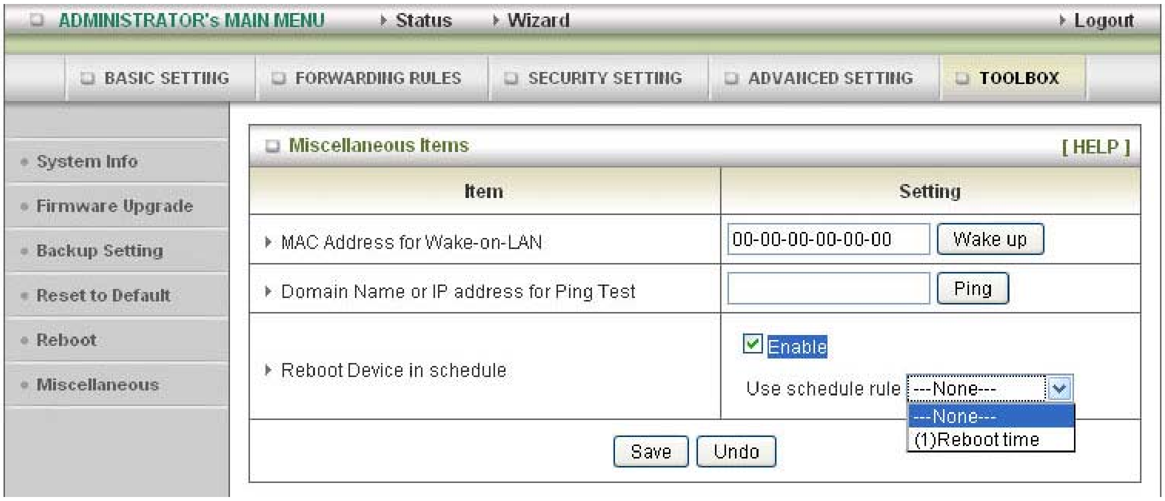
Advanced Setup > Tool Box > Reset to Default

You can also reset this product to factory default by clicking the **Reset to default** button

Advanced Setup > Tool Box > Reboot

You can also reboot this product by clicking the **Reboot** button

Advanced Setup > Tool Box > Miscellaneous



Miscellaneous Items

Item	Setting
MAC Address for Wake-on-LAN	00-00-00-00-00-00
Domain Name or IP address for Ping Test	
Reboot Device in schedule	☑ Enable Use schedule rule ---None---

MAC Address for **Wake-on-LAN**

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to known the MAC address of this device, say 00-11-22-33-44-55. To click on “Wake up” button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP address for Ping Test

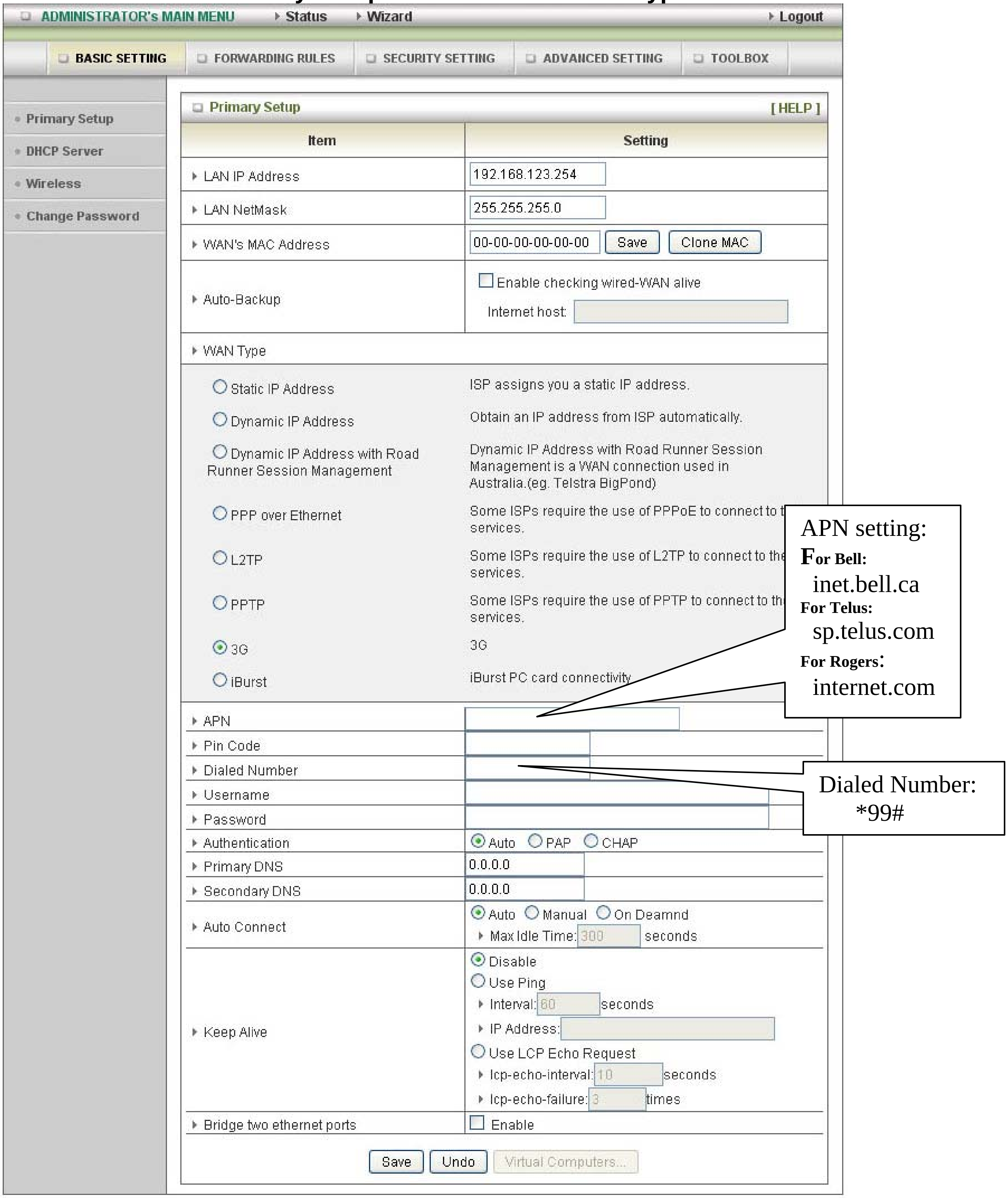
Use ping to test connection of domain name or IP address

Reboot Device in schedule

When clicked on the Enable, device will reboot automatically follow the schedule rule, so you have to setup schedule rule first. Then the schedule time will show in the schedule the list.

Setup 3G Card

BASIC SETTING →Primary Setup → Select 3G in WAN Type



Primary Setup

Item	Setting
LAN IP Address	192.168.123.254
LAN NetMask	255.255.255.0
WAN's MAC Address	00-00-00-00-00-00
Auto-Backup	□ Enable checking wired-WAN alive Internet host:
WAN Type	
○ Static IP Address	ISP assigns you a static IP address.
○ Dynamic IP Address	Obtain an IP address from ISP automatically.
○ Dynamic IP Address with Road Runner Session Management	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. Telstra BigPond)
○ PPP over Ethernet	Some ISPs require the use of PPPoE to connect to t services.
○ L2TP	Some ISPs require the use of L2TP to connect to the services.
○ PPTP	Some ISPs require the use of PPTP to connect to th services.
● 3G	3G
○ iBurst	iBurst PC card connectivity
APN	
Pin Code	
Dialed Number	
Username	
Password	
Authentication	● Auto ○ PAP ○ CHAP
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Auto Connect	● Auto ○ Manual ○ On Deamnd Max Idle Time: 300 seconds
Keep Alive	● Disable ○ Use Ping Interval: 60 seconds IP Address: ○ Use LCP Echo Request lcp-echo-interval: 10 seconds lcp-echo-failure: 3 times
Bridge two ethernet ports	□ Enable

APN setting:
For Bell:
inet.bell.ca
For Telus:
sp.telus.com
For Rogers:
internet.com

Dialed Number:
*99#