E-Lins H680 Series Router

Quick Start

E-Lins Technology Co., Ltd

ADDRESS: Bld22., Longxi Garden, Nonglin RD., Futian District, Shenzhen, 518000, China

PHONE: 86-755-83700465
E-mail: sales@szelins.com support@szelins.com
WEB: http://www.szelins.com

Table of Contents

CHAPTER I PRODUCT PROFILE 4
1.1 PRODUCT SPECIFICATIONS 4
1.2 PACKING LIST 4
1.3 LED INDICATORS AND INTERFACE SPECIFICATIONS 5
CHAPTER II INSTALLATION 6
2.1 HARDWARE INSTALLATION 6
STEP 1： INSERT THE SIM CARD 6
STEP 2: CONNECT TO A PC 6
STEP 3: CONNECT TO A TELEPHONE SET 7
STEP 4: CONNECT THE EXTERNAL ANTENNA (OPTIONAL) 7
STEP 5: CONNECT TO THE POWER ADAPTER 8
CHAPTER III HOW TO LOG INTO THE ROUTER 8
3.1 HOW TO CORRECTLY SET UP YOUR COMPUTER NETWORK CONFIGURATIONS 8
3.2 LOG INTO THE ROUTER 11
STEP 1:OPEN WEB MANAGEMENT 11
STEP 2:INPUT USER AND PASSWORD 11
STEP 3:INTELLIGENT GUIDE 12
CHAPTER IV QUICK START GUIDE 13
STEP 1:INTELLIGENT GUIDE 13
STEP 2:ADMINISTRATOR INFORMATION CONFIGURATION 13
STEP 3:CONFIGURE THE SYSTEM TIME 14
STEP 4:CONFIGURE 3G MODE 15
STEP 5:CONFIGURE LAN INFORMATION 17
STEP 6:CONFIGURE WLAN INFORMATION 18
CHAPTER V SYSTEM STATUS 19
5.1 STATUS (CURRENT WORK CONDITIONS OF THE ROUTER) 19
5.2 STATISTICAL INFORMATION 20
CHAPTER VI NETWORK SETTINGS 21
6.1 WAN SETTINGS 21
6.2 LAN SETTINGS 22
6.3 DHCP CLIENT LIST 24
6.4 ADVANCED ROUTING CONFIGURATIONS 24
CHAPTER VII WIRELESS NETWORK CONFIGURATIONS 26
7.1 BASIC SETTINGS 26
7.2 ADVANCED SETTINGS 29
7.3 SAFETY SETTINGS 31
7.4 WDS CONFIGURATIONS 32
7.5 WPS CONFIGURATIONS 34
CHAPTER VIII FIREWALL 36
8. 1 MAC/IP/PORT FILTERING 36
8.2 PORT TRANSMISSION (VIRTUAL HOST) 38
8. 3 DMZ SETTINGS 39

8.4 SYSTEM SAFETY SETTINGS ····· 39
8.5 CONTENT FILTERING ····· 40
CHAPTER IX SYSTEM MANAGEMENT ····· 40
9.1 MANAGEMENT ····· 40
9. 1. 1 Domain Server ····· 40
9.2 SYSTEM UPGRADE ····· 42
9.3 EQUIPMENT MANAGEMENT ····· 42

Chapter I Product Profile

1.1 Product Specifications

- Supports PSTN Phone
- Supports IEEE802.11b/g/n, speed rate up to 300Mbps.
- NAT & NAPT with VPN pass-through Virtual Server.
- Automatic receipt of IP address with DHCP Server.
- Supports the high-speed gateway and multi-users.
- Security through WEP, WPA and built-in firewall.

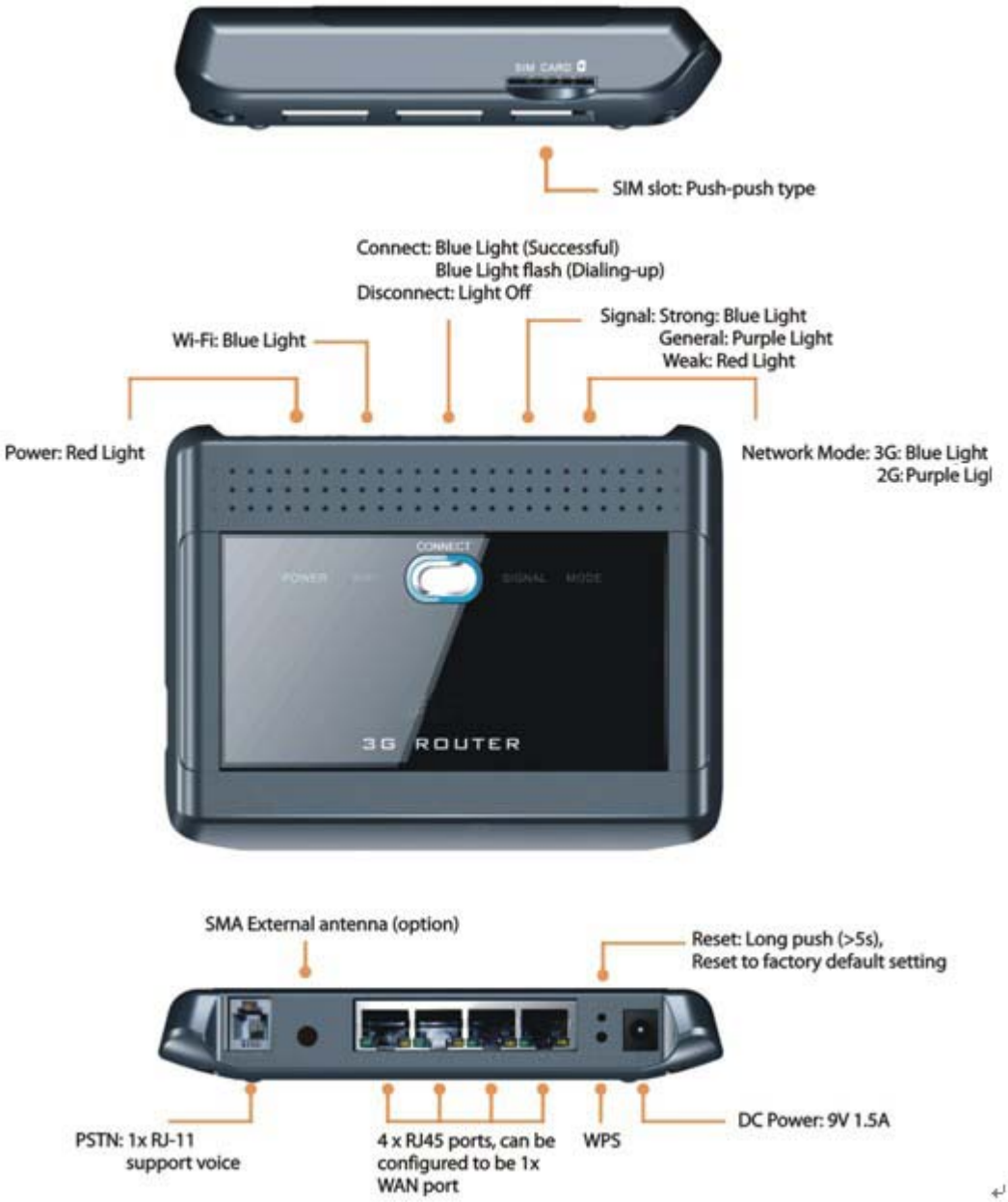
1.2 Packing List

3G Router x1

Power Adapter x1

Quick Start Guide x1

1.3 LED indicators and Interface Specifications



Chapter II Installation

2.1 Hardware Installation

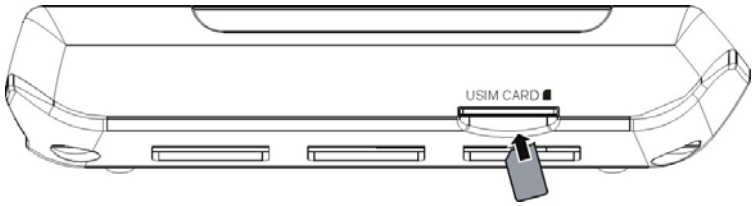
Please make the correct connection as per the following steps before setting up a router. Please place the router in the central part of the coverage area to maximize its wireless performance.

Step 1：Insert the SIM card

Warning *Before inserting or removing the SIM card, you must disconnect the device from the power adapter.*

If you are required to enter the PIN code,enter the correct one. If you fail to enter the correct PIN or PUK code, the network-related functions are unavailable.The SIM card is supplied by the service provider. For details, contact your service provider.

Insert the card into the slot completely, as shown in the following figure.

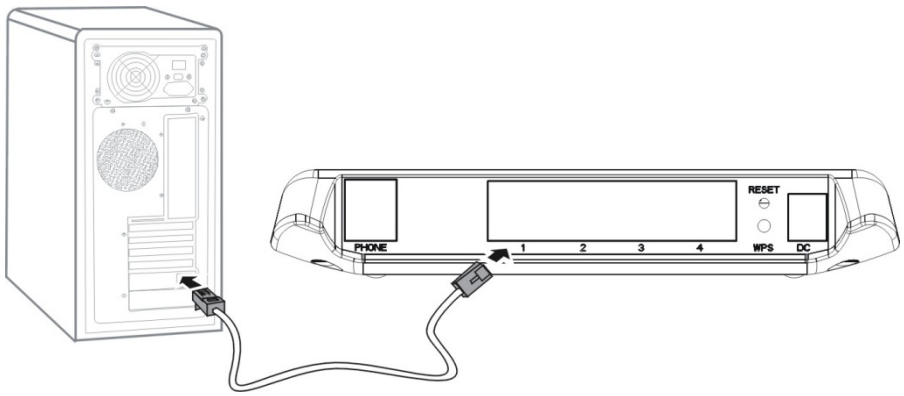


To remove the card, press the card gently. Now the card will pop up automatically.

Step 2: Connect to a PC

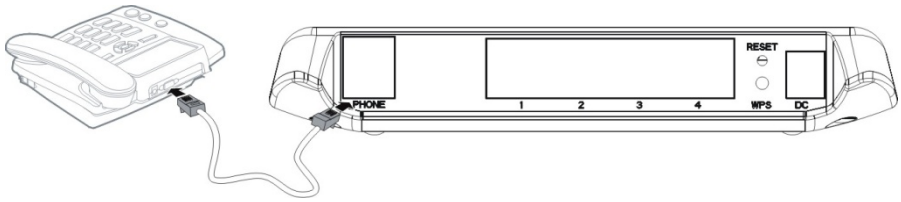
If the indicator of the Ethernet interface connecting with a network cable is on, the connection is successful. The Ethernet cable cannot be longer than 100 meters (328 feet).

To achieve better effect, use the shielded cable.



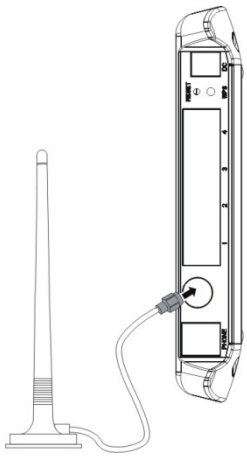
Step 3: Connect to a telephone set

The communication quality of the telephone set can be interfered by the wireless signal. Place the telephone set one meter away from the device.



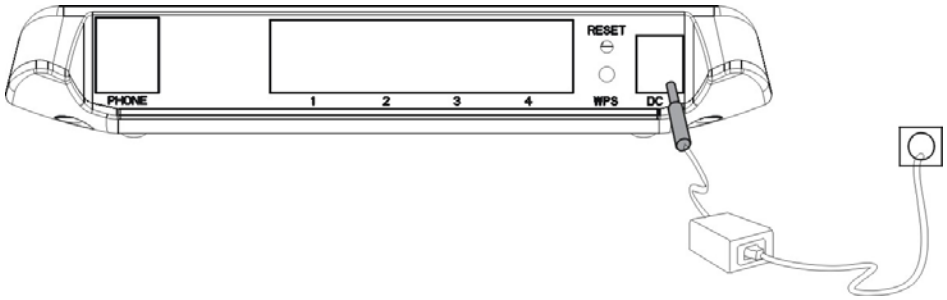
Step 4: Connect the external antenna (optional)

Connect the external antenna cable with the antenna jack on the main unit. Screw the cable to make sure that the antenna is tightly connected with the antenna jack.



Step 5: Connect to the power adapter

Use a power adapter that is compatible with the device; otherwise, the device may be damaged.

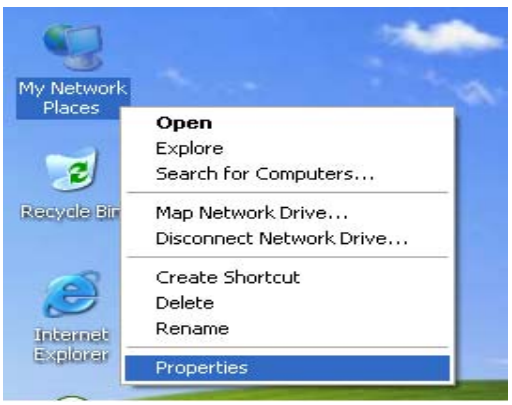


Chapter III How to Log into the Router

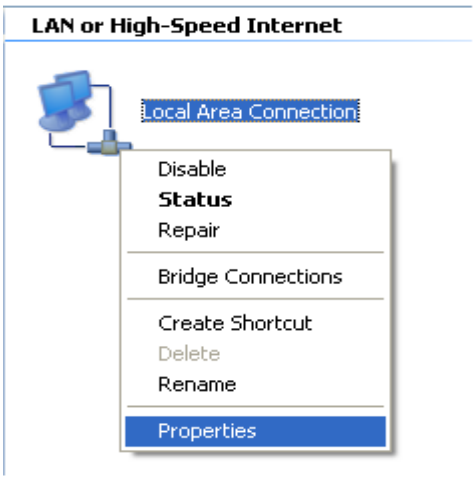
This chapter mainly introduces how to log onto the router set-up page. Please set up your router by reference to the following steps after your router is connected to the device with the cable (refer to Chapter II for the connection steps).

3.1 How to correctly set up your computer network configurations

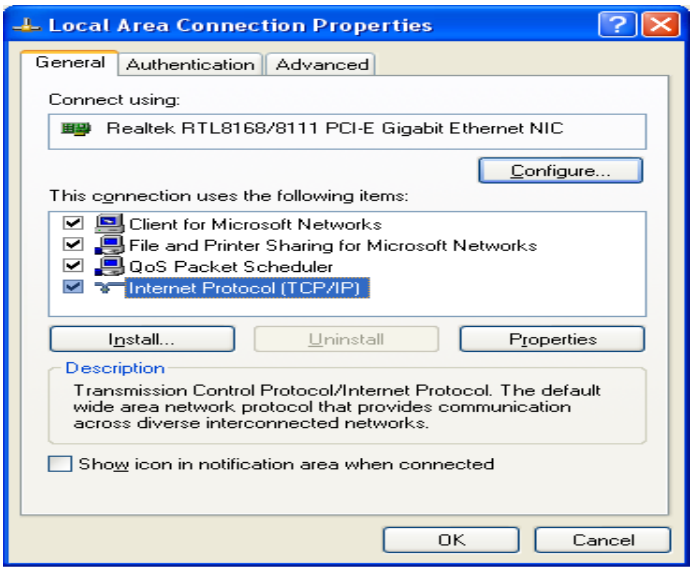
Step1: On the desktop, right-click on “My Network Places”, select “Properties”. (Figure 6)

Step2: In the following  pop-up window, right-click on “Local Area Connection”

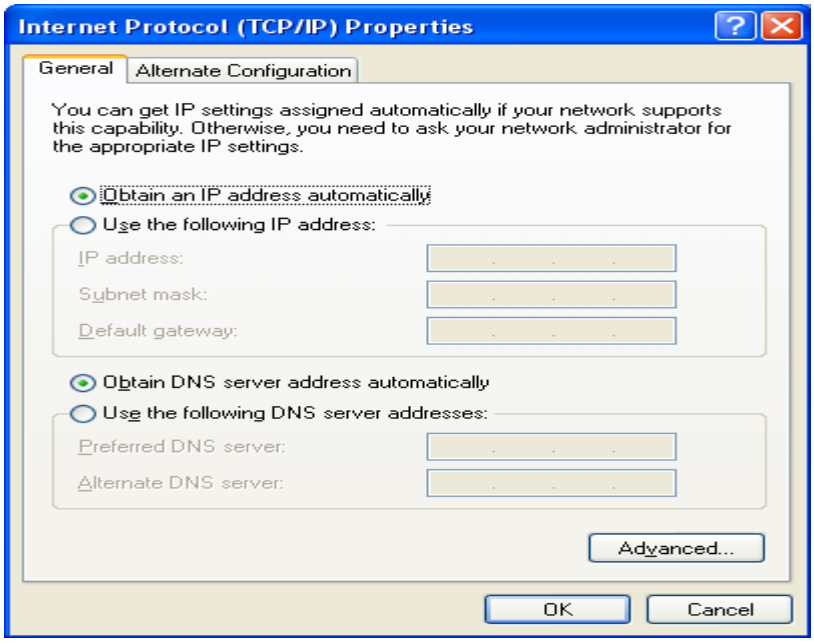
and select “Properties”. (Figure 7)



Step3: In the following window, select “Internet Protocol (TCP/IP)” option, then click “Properties”. (Figure 8)

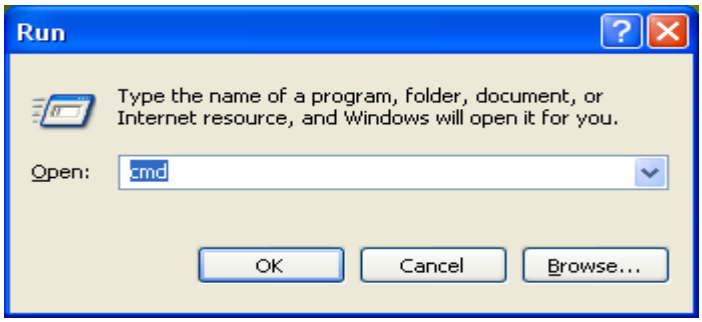


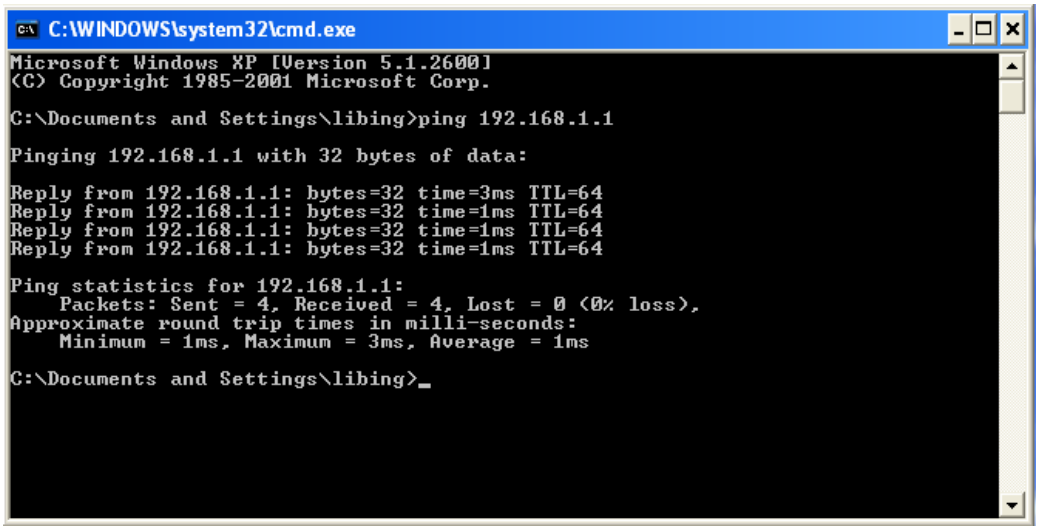
Step4: In the following pop-up window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Then click”OK”. (Figure 9)



Step5: If you selected LAN connection. Please double check if the Gateway is really connected to your computer, when “Local Connection” is showing already connected. Then click “Start” menu and open “Run” program, input “CMD” as figure 10.

[If you selected WIFI connection, Before step5, please click on “Wireless Network Connection” icon in the lower right of desktop, check the wireless network status and select your wireless network. Then connect to it.]

Step6: Input order  “ping 192.168.1.1” and click “Enter”, it will get the following result which is showing the above configuration is successful. (Figure 11)



3.2 Log Into the Router

Step 1:Open Web Management

Open Web browser, input 192.168.1.1 at Address bar, then press “Enter”.

Step 2: input USER and Password

the following pop-up window, both input “admin” at “User name” bar and “Password”

bar, then press “OK”. (Figure 13)

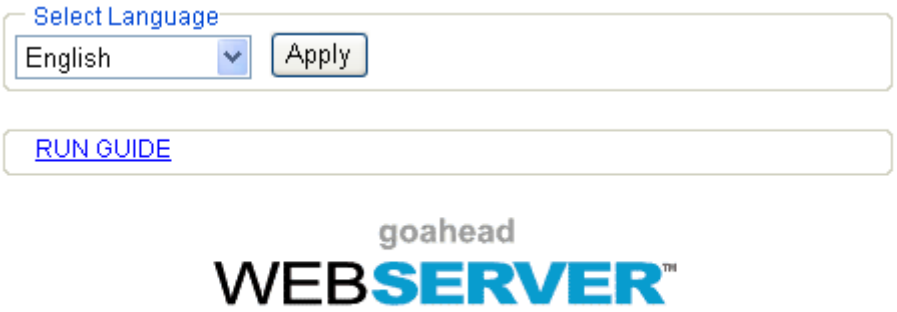
Step 3:Intelligent Guide

Click “RUN GUIDE” as displayed on the major interface and make use of the intelligent guide functions of the router. It enables the one-time configuration of the router’s time, administrator information, internal and external network ports.

Chapter IV Quick Start Guide

Step 1:Intelligent Guide

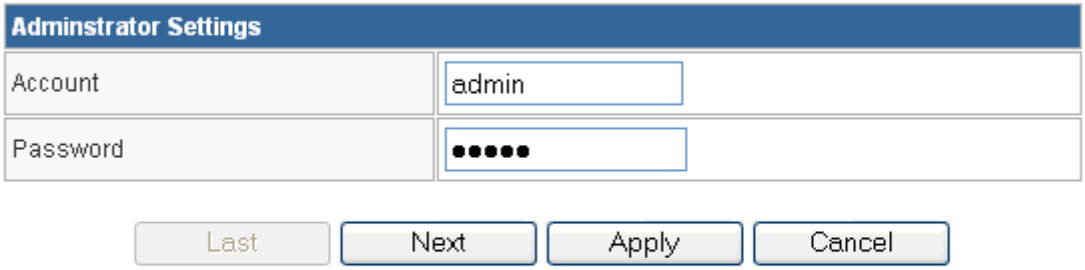
Click “RUN GUIDE” as displayed on the major interface and make use of the intelligent guide functions of the router. It enables the one-time configuration of the router’s time, administrator information, internal and external network ports.



Step 2:Administrator Information Configuration

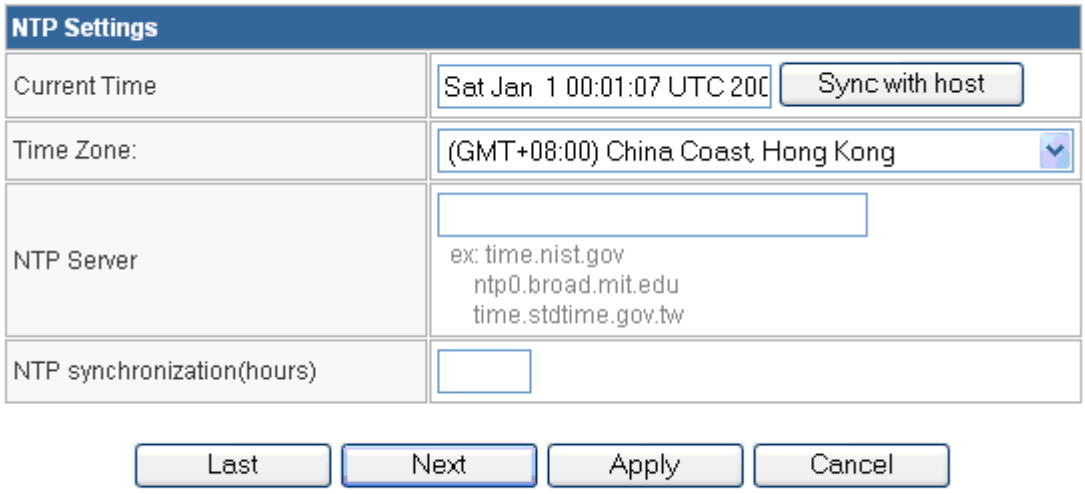
Account: an account (user name) to log into the management interface. The default system account is admin.

Password: a password to log on the management interface. The default system password is admin.



Click “Next” to Configure the System Time

Step 3:Configure the System Time



Current time: display the system time of the router.

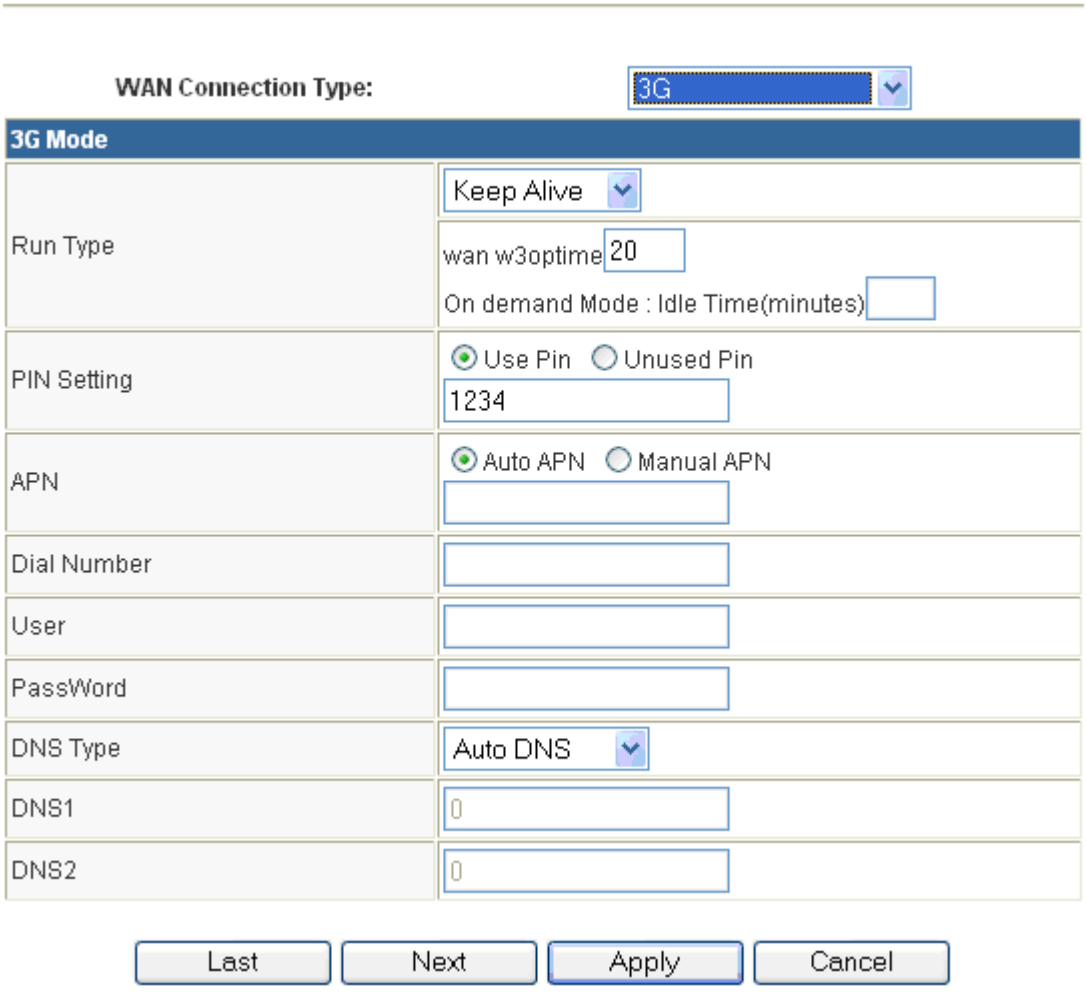
Sync with host: make sure that the router’s time settings are consistent with those of the PC.

NTP Server: set up an Internet-based time server. Every once in a while, the router sets up its time and makes sure that its time is consistent with that of the server.

NTP synchronization(hours): intervals for the router to obtain data from the time server.

Click “Next” to Configure 3G Mode

Step 4:Configure 3G Mode



（图 10）

Run Type: under the “Keep Alive “mode, the router will dial up automatically and get connected to the Internet when 3G equipment is plugged in. Under the “Manual” mode, the access internet through dial-up will not be launched until the user clicks

“Connection” on the status page. Under the “On-Demand” mode, the system will be connected to the network automatically in case of WAN access requests. If there are no network access requests within the specific period (idle time), the system will disconnect to the network automatically. This connection mode could effectively save network access fees for users that select to make payment by the time actually consumed.

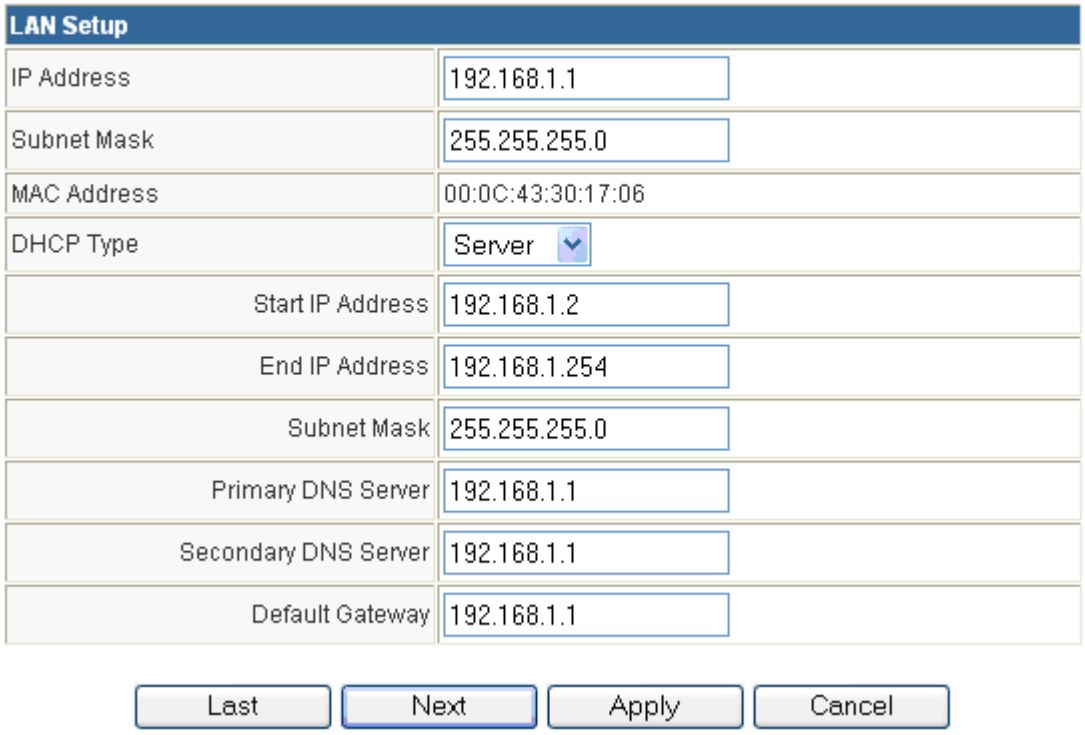
PIN settings: If your 3G Internet access equipment has a PIN code, you shall select “Use PIN” and fill in the PIN code in the following Input Box. Otherwise, you shall select “Unused PIN”.

APN: If you select “Auto APN”, then information such as “APN Information”, “Dial Number”, “User” and “Password” shall be filled by the router automatically. If you select “Manual APN”, then you have to fill in such Internet access information by yourself.

DNS type: If you select “Automatic DNS”, the router will use the DNS obtained by 3G dial-up. If the “Manual DNS” is selected, the router will use the DNS information entered by the user.

Click “Next” to Configure LAN Information

Step 5:Configure LAN Information



Intranet ports and DHCP settings

IP address: set up IP address for Intranet ports.

Subnet mask: set up masks for the Intranet.

MAC address: display the physical address of Intranet ports.

DHCP type: Select “Server” to open DHCP services and then the host in the Intranet could obtain IP dynamically.

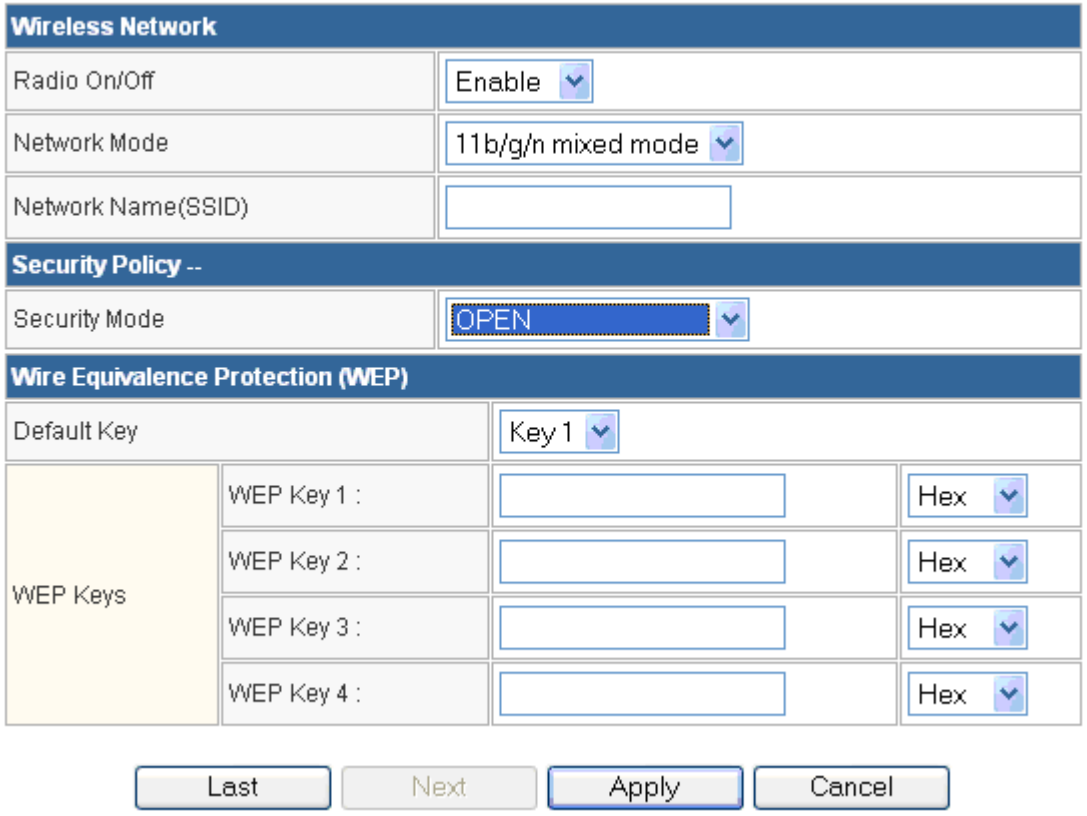
Start IP address-End IP address: IP obtained by the host in the Intranet via DHCP mode are included in this range.

Default gateway: set up the gateway for the host in the Intranet.

DNS server: set up DNS server for the host in the Intranet.

Click “Next” to Configure WLAN Information

Step 6: Configure WLAN Information



Radio On/Off: switch on or Off wireless networks. If Intranet clients do not select "Enable", they could not get Wi-Fi connectivity to the Intranet of the router.

Network mode: select standards used by wireless networks. Options are 802.11b, 802.11g and 802.11n, or mix standards 802.11b/g,802.11b/g/n.

Network Name（SSID）：Enter a name for your wireless local area network (WLAN).

Security Mode： If "Disable" is selected, Intranet clients could have Wi-Fi connection to the router's Intranet without entering key information.

If "OPEN", "SHARED" or "WEPAUTO" is selected, there is a need to set up the key information. Wireless clients in the Intranet cannot gain access to the router's Intranet until correct key information is entered.

You can fill in four (ASCII or Hex, with a length of 10 to 26 characters) keys for this router at the most. One of the four groups of pre-set keys can be selected as the current effective key (default key).

Chapter V System Status

5.1 Status (current work conditions of the router)

System Info	
SDK Version	V1.1.0 (Mar 17 2010 22:56:56)
System Up Time	7 mins, 56 secs
System Platform	433R+V1.0
Internet Configurations	
Connected Type	Connect Disconnect
SIGNAL	
NetType	HSPA
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	202.106.195.68
Secondary Domain Name Server	202.106.46.151
MAC Address	00:0C:43:30:58:16
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:0C:43:30:58:17

SDK Version: indicates the router's current software versions and the release date.

System Up Time: indicates the system operation time after the router is loaded with a power supply. Such time will be cleared to zero after the power supply is unloaded.

System Platform: indicated the router's current model and hardware versions.

Internet configurations:

Connected Type: the router's online modes include static IP, dynamic IP, PPPoE, L2TP, PPTP and 3G. If it is the 3G mode,

two buttons, namely "Disconnect" and "Connect" will be displayed on the interface to disconnect and connect the 3G network.

Signal: signal intensity of the 3G network.

NetType: current 3G network that is connected (such as WCDMA, TD or EVDO).

WAN IP address: current WAN IP address of the router. If the router's connection type is dynamic IP, PPPoE, 3G, L2TP or PPTP and not connected to the extranet, the address will be displayed as empty or 0.0.0.0.

Subnet mask: Router's WAN subnet mask.

Default gateway: Router's WAN default gateway.

Domain server: Address of the DNS server that is currently used by the router.

MAC address: MAC address of the router's Extranet ports.

Local Network:

Local IP address: IP address of the router's Intranet ports.

Local net mask: subnet mask of the router's Intranet.

MAC address: Physical address of the router's Intranet ports.

5.2 Statistical Information

(Data packets and bytes that are received and transmitted by each port and the status of memory use)

Memory	
Memory total:	13556 KB
Memory left:	1068 KB
WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	0
WAN Tx bytes:	0
LAN Rx packets:	1071
LAN Rx bytes:	112062
LAN Tx packets:	758
LAN Tx bytes:	319428

Chapter VI Network Settings

6.1 WAN Settings

Please refer to the Extranet configurations of the “Intelligent Guide” for the online configurations.

MAC replication: If MAC address replication is initiated, the MAC address of the Intranet’s Internet access data packet shall be changed to the MAC address of the router while accessing the Internet via the router.

6.2 LAN Settings

LAN Setup	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
LAN 2	○ Enable ◉ Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:0C:43:30:58:17
DHCP Type	Server
Start IP Address	192.168.1.2
End IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.1.1
Secondary DNS Server	192.168.1.1
Default Gateway	192.168.1.1
Lease Time	86400
Statically Assigned	MAC: 00:1D:72:22:C6:20 IP: 192.168.1.200

IP address: set up IP addresses for Intranet ports.

Subnet mask: set up masks for the Intranet.

LAN 2 : Add an IP to the Intranet ports. This way, LAN clients could get connected to the router through LAN.

MAC address: indicated physical addresses of the Intranet ports.

DHCP type: Select “Server” to open DHCP services and then the host in the Intranet could obtain IPs dynamically.

Start IP address-End IP address: IPs obtained by the host in the Intranet via DHCP mode are included in this range.

Default gateway: set up the gateway for the host in the Intranet.

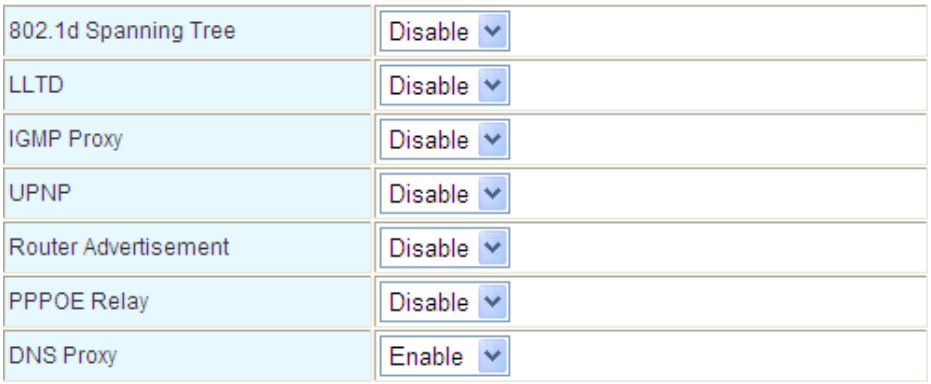
DNS server: set up DNS servers obtained by the host in the Intranet via DHCP (If DNS

Proxy is enabled, we recommend here to describe it as the IP of the Intranet ports. This way, we needn't reset this item when the router's DNS undergoes any changes).

Release time: effective period for the host in the Intranet to obtain IP addresses.

Static designation: Hosts located in specific physical address obtain specific IPs via DHCP.

Introduction of Relevant Intranet Programs



停用： Disable 启用：Enable

802.1d Spanning Tree：Support spanning tree protocols, avoid network loopbacks in the LAN and address broadcast storm issues relating to the looped Ethernet network.

LLTD: Identify whether LLTD (Link-Layer Topology Discovery Responder) protocol is supported. This network protocol could intelligently identify which network equipment or computers are connected in the LAN network.

IGMP Proxy: Confirm whether the router supports the IGMP protocol. This protocol operates between the host and the multicast router that is directed connected to the host. It is a protocol for IP hosts to report the identity of multicast group members.

UPNP: Identify whether UPNP protocols are supported.

Router Advertisement: Identify whether the router supports IPV6.

DNS Proxy: Transmit DNS requests of the Intranet. If this function is enabled, you can configure DNS of the host in the Intranet to IPs of the router's Intranet ports. This way, hosts in the Intranet can diagnose web pages. There is no need to reset the Intranet's DNS after the Internet access method has been changed.

6.3 DHCP client list

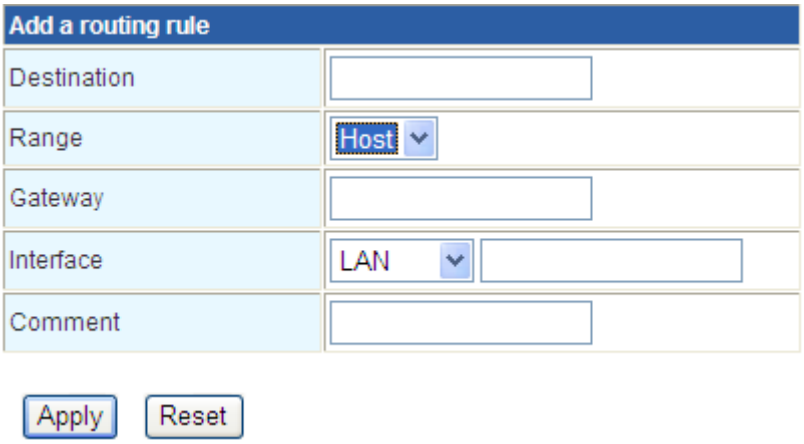
(Display information relevant to the hosts that are connected to the router's Intranet via DHCP)

DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
www-59e926c8637	00:1F:E1:66:51:2E	192.168.1.2	1 days 00:00:00

DHCP client list enables you to check the status of online users such as MAC address, IP address and lease periods of the IP address.

6.4 Advanced Routing Configurations

This function may be used when it is required to add a specific routing for a certain host. The proper use of static routing could reduce routing issues, alleviate the overload of routing data flows and enhance the transmission speed for the data packets. A routing item may be identified by setting targeted IP address, subnet mask and gateway address, among which the targeted IP address and the subnet mask are used to identify a target network/host. Afterwards, the router transmits the data packets to the designated target network/host via the gateway.



Destination: Identify target addresses or networks that are hopefully to be visited.

Host/network: The selection of a host means to designate a certain IP for the host. The network defines a specific network segment by defining a subnet mask.

Gateway: IP address of the router or the host where the data packets are sent.

Interface: Indicate connector information.

Comment: Fill in necessary notes.

Current router table: Display all kinds of information relating to all current router tables that are defined by the user.

Chapter VII Wireless Network Configurations

7.1 Basic Settings

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	3GRouter_jiang Hidden ☐ Isolated ☐
Multiple SSID1	Hidden ☐ Isolated ☐
Multiple SSID2	Hidden ☐ Isolated ☐
Multiple SSID3	Hidden ☐ Isolated ☐
Multiple SSID4	Hidden ☐ Isolated ☐
Multiple SSID5	Hidden ☐ Isolated ☐
Multiple SSID6	Hidden ☐ Isolated ☐
Multiple SSID7	Hidden ☐ Isolated ☐
Broadcast Network Name (SSID)	◉ Enable ○ Disable
AP Isolation	○ Enable ◉ Disable
MBSSID AP Isolation	○ Enable ◉ Disable
BSSID	00:0C:43:30:58:18
Frequency (Channel)	2437MHz (Channel 6)

Radio On/Off: Switch on/off wireless functions of the router.

Network mode: Wireless application standards for the router. The router supports 802.11b, 802.11g, 802.11n or mix modes.

Multiple SSID: Network name of the wireless signals. This router supports multiple wireless networks. If you select “Hiden the Wireless Client”, you cannot scan the router’s SSID. If you select “Isolated”, you can prevent this network from communicating with other networks.

Broadcast network Name: You can select “Disable” to forbid the router to broadcast SSID. After that, the wireless clients cannot scan the router’s SSID. The clients cannot communicate with the router if they fail to know the router’s SSID. The broadcast network identifier is defaulted as “Enable”.

AP Isolation: Isolated at the AP level. After it is enabled, clients at the AP level cannot visit each other, which could prevent the virus from spreading.

MBSSID AP Isolation: Isolated from areas outside this AP. Other clients not belonging to this AP shall not visit clients under this AP.

Basic service set identifier: Business group identifier of the wireless network. In terms of IEEE 802.11, the BSSID is the MAC address of the wireless AP.

Frequency (channel): Channels currently used by the router. Other effective work channels could be selected from the following list and options are 1 to 14.

Operation Mode:

Mix mode: Under this mode, previous wireless network cards are identifiable and connectable to Pre-N AP, but the throughput will be affected to some degree.

Green Field: Be able to reach high throughputs. But it affects the backward compatibility and the system’s safety.

Channel bandwidth: Please select “Default Settings”. It is divided into two types, namely 20MHz and 20/40MHz.

Protection interval: Defaults as “Automatic”. An appropriate protection interval shall be provided to reach good BER performance.

Channel bandwidth: Please select the channel bandwidth to enhance the wireless performance.

MCS: Vertices control signals with the value ranging from zero to thirty-two. The default setting is “Automatic”.

Reverse direction authority: You can choose to “Enable” or “Prohibit” this authority.

Extension channel: Be able to extend specified channel segments.

Aggregation MAC Service Data Unit (A-MSDU): Aggregate multiple Ethernet messages into a comparatively bigger load by taking specific measures.

Automatic confirmation of single blocks: The realization of aggregate exchange sequences could enhance the transmission rate.

Decline requests to confirm single blocks: The default setting is “Prohibit”, which could enhance the transmission rate.

7.2 Advanced Settings

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ◉ Disable
Short Slot	◉ Enable ○ Disable
Tx Burst	◉ Enable ○ Disable
Pkt_Aggregate	◉ Enable ○ Disable
IEEE 802.11H Support	○ Enable ◉ Disable(only in A band)
Country Code	None

Wi-Fi Multimedia	
WMM Capable	◉ Enable ○ Disable
APSD Capable	○ Enable ◉ Disable
WMM Parameters	WMM Configuration
Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ◉ Disable

BG protection mode: You can select “switch-on”, “Switch-off” or “Automatic” to identify the status of BG protection modes.

Beacon interval: Intervals to transmit wireless beacon frames. During this time range, a beacon frame will be transmitted to receive the access information of the peripheral wireless networks.

Data beacon proportion (DTIM): Intervals to transmit specific indication messages. It is a countdown work that notifies the next client window to receive broadcast and multicast.

Fragment Threshold: Specific fragment thresholds of the data packets. When the length of the data packet exceeds such threshold, multiple data packets will be created automatically.

RTS threshold: A RTS (Request to Send) threshold specified by the data packets. When the length of the data packets exceeds this threshold, the router will send RTS to the target sites for negotiation. After the wireless site receives RTS frames, it will respond to the router by sending a CTS (Clear to Send) frame, indicating that the wireless communication is possible.

TX power: Define the correlation between current wireless AP and the SSID's transmission power. The size of the model is in direct proportion with the intensity of the transmission power.

Short preamble: The default status is "Prohibit". The router applies long preambles by the default settings. After it is enabled, the system will no longer be compatible with the operation speed (1Mbps or 2Mbps) of the traditional IEEE802.11.

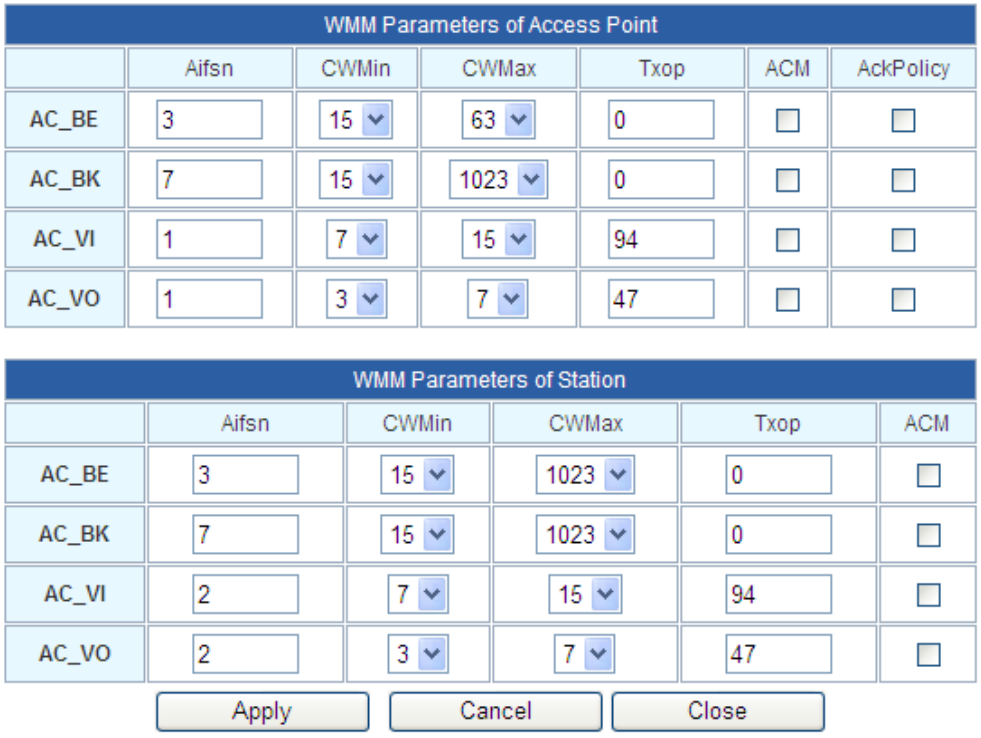
Short slot: The default setting is "Enable" and you can switch it off. The "Enable" could enhance the transmission rate of the wireless communication.

Tx Burst: It belongs to features at the MAC address level, which could enhance TCP transmission fairness for the wireless network.

Pkt_Aggregate: A mechanism to strengthen the LAN and make sure that the data packet could arrive at the destination.

WI-FI Multimedia

It provides configurations for the wireless multimedia parameters. WMM enables the wireless communications to define a priority range according to the data types. Time-sensitive data such as video/audio data have higher priority than that of the normal data. Wireless clients shall support WMM to maintain WMM functions. The client may select “Apply” or “Cancel” based on requirements.



Wi-Fi multimedia capabilities: Enable WMM functions. WMM function will not take effect until the WIFI is enabled.

Direct online capabilities: The enablement will weaken the wireless performance, but could save the energy and electricity.

7.3 Safety Settings

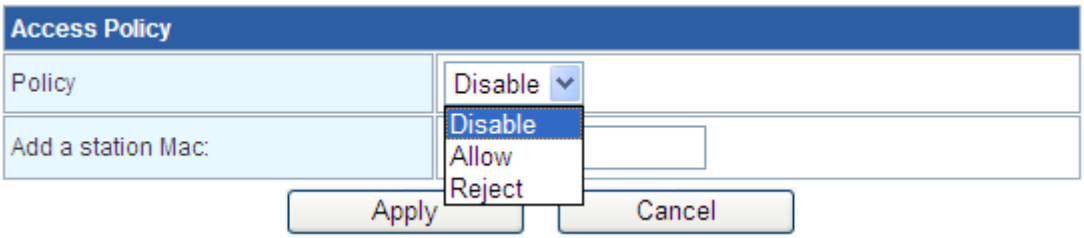
The router supports the safety modes (DisableOpen,SHARED:WEPAUTO,WPA-KEY:(WPA-Personal), WPS2-KEY:(WPA-Personal),

WPA and WPA2).

For specific configurations, refer to relevant configurations for the “Intelligent Guide”.

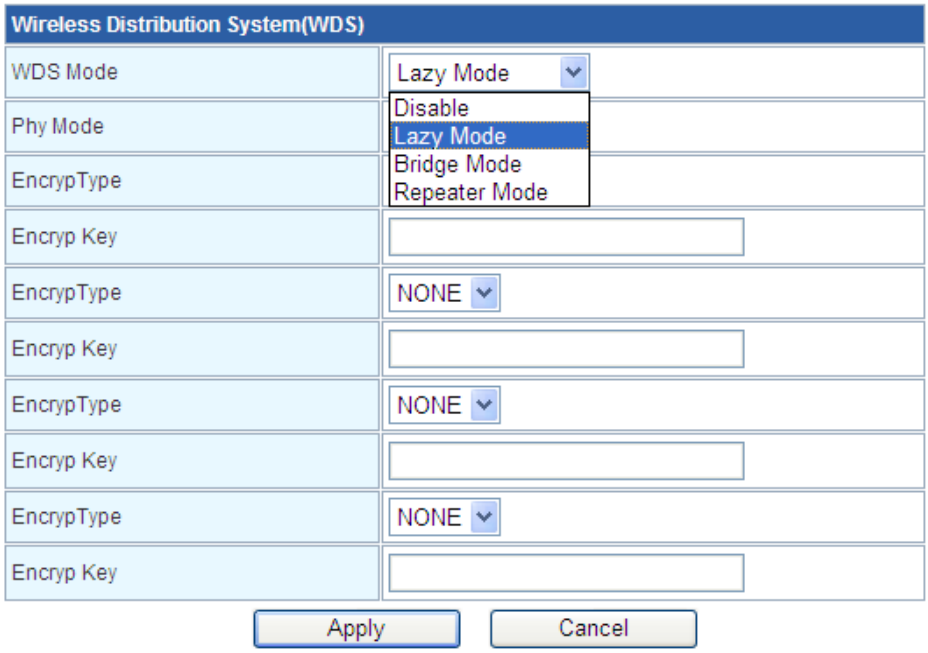
The router selects different encryption and authentication methods for different SSID. Please select a SSID to configure its safety strategy.

“Allow” means that only clients of specific MAC addresses are allowed to gain access. “Reject” means that only clients of specific MAC addresses are forbidden to gain access. “Disable” means that all clients could gain access.



7.4 WDS Configurations

Wireless Distribution System (WDS) is used to expand current wireless network coverage. The router supports three modes, namely Lazy Mode, Bridge Mode and Repeater Mode.



Lazy Mode: Under this mode, wireless equipment on the opposite side could be applicable to the Bridge Mode or Repeater Mode. Wireless connection is available if you enter the router's BSSID to the wireless equipment on the opposite side.

Bridge Mode: Under this mode, you can manually add MAC on the opposite side to corresponding AP MAC address lists or do this through "Scan Options". Then, you click "Save as" to realize the wireless connection for two wire networks.

Repeater Mode: Under this mode, you can manually add MAC on the opposite side to corresponding AP MAC address lists or do this through "Scan Options". This way, you can immediately strengthen and extend signals of the wireless networks.

Encryption type: Three encryption modes are supported, namely WEP, TKIP and AES.

Encrypt Key: Enter the encrypt keys between the wireless equipment.

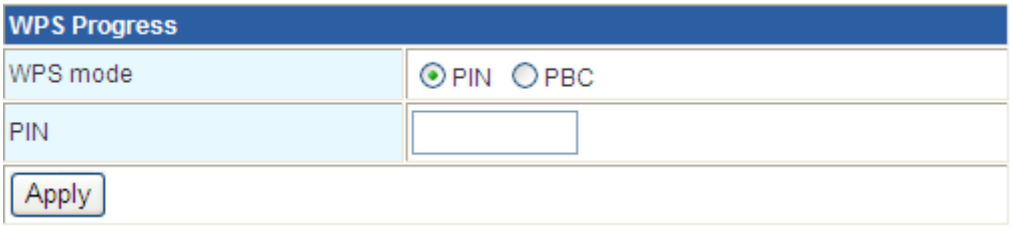
AP MAC Address: Please enter MAC address of the wireless equipment on the opposite side.

7.5 WPS Configurations

Wi-Fi Protection Settings (WPS) can easily and quickly establish an encrypted connection among clients of the wireless network. You have no need to select the encryption mode or configure a key. You just need to enter correct PIN code or select PBC (or press “WLAN/WPS” button indicated on the back panel) to easily configure WPS.

Wi-Fi Protection Settings: Used to disable or enable WPS functions. The default status is “Disable”.

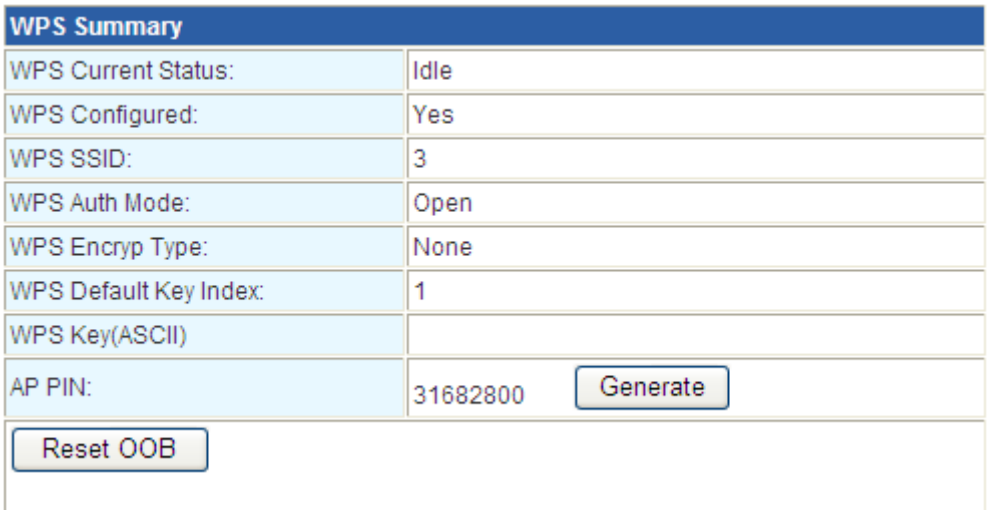
WPS Mode: Support two kinds of simple WPS settings, namely PBC (Push-Button Configuration) and PIN code.



PBC: select PBC and click "Save as" or press WLAN / WPS button on the back panel for about one second while activating WPS / PBC to connect in the client port.

Operation Process: after clicking the WLAN / WPS button for one second, WPS light will blink about 2 minutes, indicating that the function is activated. In this time range, the wireless client ports can activate the WPS / PBC for authentication and consultation. After the connection is successfully connected, WPS indication light will be off and access process of wireless client is completed. If users want to access multiple wireless client ports, users need to repeat the process. It could support up to 32 wireless client ports to access.

PIN: If users want to use the PIN, users must know the PIN code of wireless client ports. Users could just add to the input box and then save while using the same PIN code to make connection in the client ports.



WPS Overview: Display relevant information including current WPS status, authentication modes and encryption types applied, and default private key indexing.

WPS Current Status: “Idle” means the idle status. “Start MSC Process” means that the process is enabled and the access is on the way. “Success” means that the server and the client have reached an agreement during the negotiation.

WPS Configured: “Yes” means taking effect and “Not Used” means not taking effect. Generally, if the AP-Safety Configuration takes effect, this place will be displayed as “Not Used”.

WPS SSID: Display master SSID numbers of the WPS. WPS is only valid for the master SSID.

WPS Auth Mode: The authentication mode used by WPS. WPA/WPA2-Personal mode is commonly seen.

WPS Encryp Type: It means the data encryption type. AES/TKIP encryption type is commonly seen.

WPS Key: Effective keys automatically generated by AP.

APN PIN: Default PIN code.

Reset OOB: When you press this button, the WPS service terminal is indicated as Idle and the WPS indication light turns off. AP will not respond to connection requests from WPS clients and the safety are configured as WPA mode.

Chapter VIII Firewall

8. 1 MAC/IP/Port Filtering

This function is aimed at restricting and managing the client ports of the router. If you need to limit Internet use of the machine of the router, you could use this function. To use this function, you should first activate it and then select a default strategy (accept or reject), which means the data packets that do not comply with the rules to be accepted or rejected. And then fill out the corresponding filter rules. Pay attention that it is not required you to fill out all the items but to fill the appropriate selection according your own requirements. For example, to ban the IP of 192.168.1.146 to use Internet (others can use Internet), you just need to adopt the default strategy as acceptance strategy and fill 192.168.1.146 in the column of the source IP address. To use this function could enhance users' security and manageability of LAN.

MAC/IP/Port Filter Settings	
MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Accept
Comment	

Mac/IP/Port Filtering: This function takes no effect if “Prohibit” is selected. After you click “Enable”, this function will take effect.

Default Strategy: Select “Abandon” or “Accept”. This strategy shall be implemented if rules are not matched as what is defined below.

MAC Address: Fill in MAC addresses that you plan to define rules.

Source IP Address: Enter local IP address that needs filtering. You shall fill in rules that correspond to this IP.

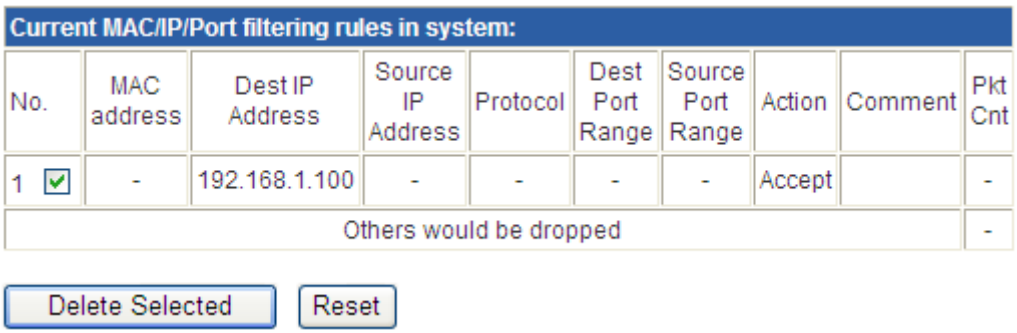
Dest IP Address: Enter destination IP address that needs filtering. You shall fill in rules that correspond to this IP.

Port range: Ranges for ports that need to be abandoned or accepted.

Protocol: Select protocols that are used by controllable data packets.

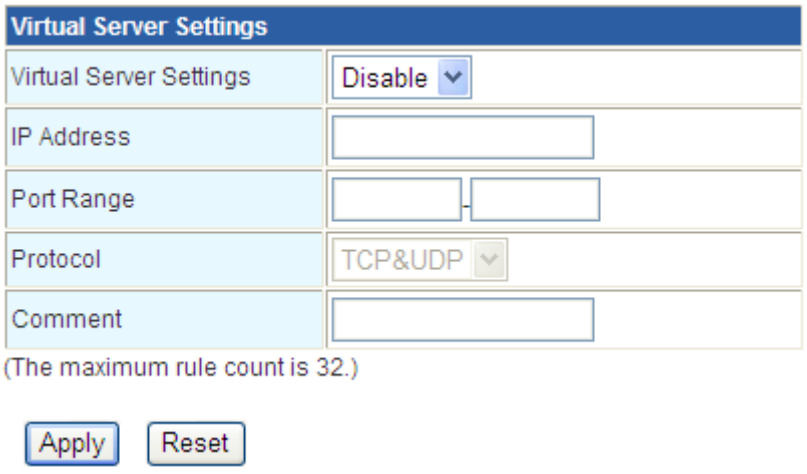
Action: Identify whether the defined rules are “Abandon” or “Accept”. It is in the opposite side of the default strategy.

Comment: Indicate the rules defined by you to differentiate such rules.



8.2 Port Transmission (Virtual Host)

The virtual host enables remote users who gain access to web or FTP services via public network IP addresses to automatically shift to local servers of the LAN. The virtual server can define a service port. All service requests to such port from the Extranet shall be transmitted to LAN servers specified by the router (based on IP address). This way, the user could successfully access LAN servers without any influences on the internal network safety of the LAN.



Virtual Server Settings: Enable or disable functions of the virtual servers.

IP Address: It is used to input necessary IP addresses, such as192.168.1.103.

Port Range: It is used to input necessary port ranges, such as 80-80.

Protocol: Select protocols that are used by controllable data packets.

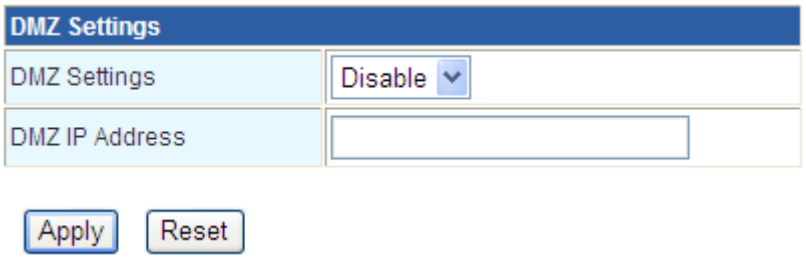
Comment: Fill in necessary notes. In terms of the configurations described above, all

data will be transmitted to a computer with the IP address of 192.168.1.103 within the LAN if some program accesses the 80 port of the router.

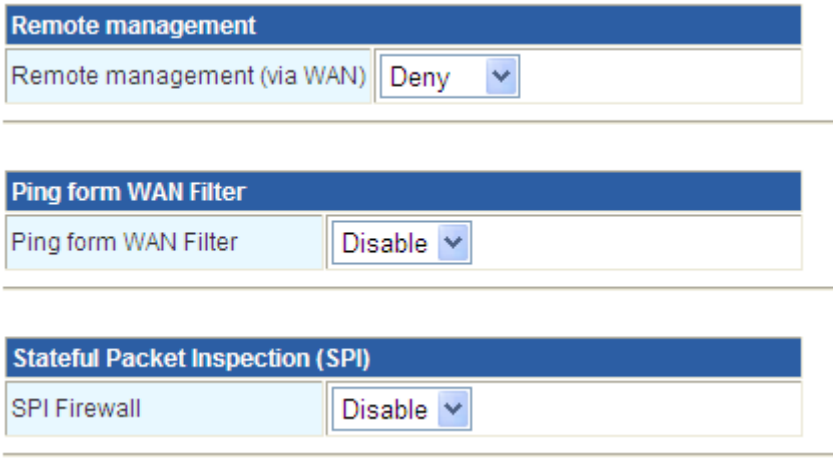
List of current virtual hosts: Indicate the list of current virtual servers.

8. 3 DMZ Settings

(transfer all data received by the router's Extranet ports to "DMZ IP Address")



8.4 System Safety Settings



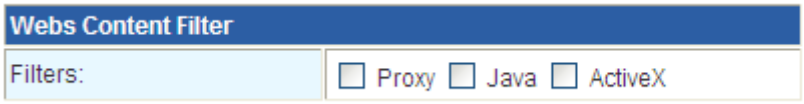
Remote management: Identify whether it is permitted to access WEB management pages via Extranet ports.

Ping form WAN Filter: Identify whether it is permitted to PING the router via Extranet port

SPI firewall: Identify whether to enable the SPI firewall.

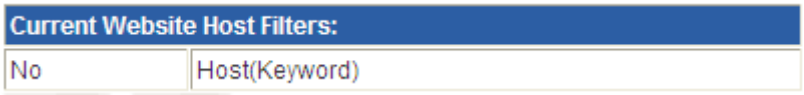
8.5 Content Filtering

Webpage content filtering: Filter the part “Proxy Java ActiveX” of the web pages.



URL filtering: Filter out the entire content of the webpage of URL

Web host filtering: URL webpages including keywords are filtered.



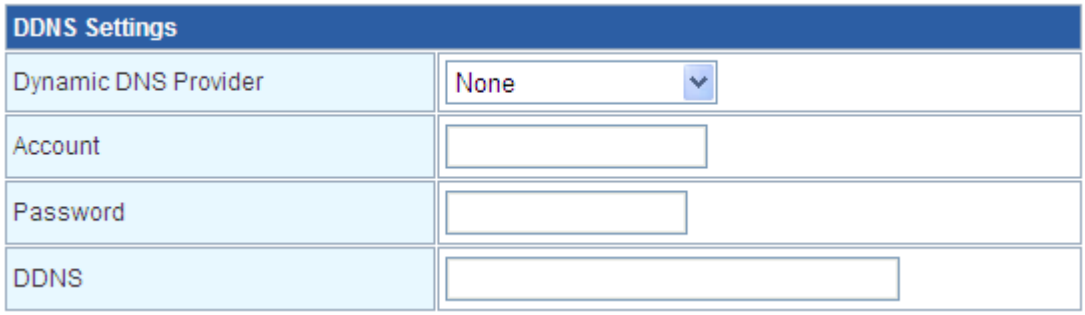
Chapter IX System Management

9.1 Management

9.1.1 Domain Server

DDNS has another name of dynamic DNS whose main function is to achieve parse between the fixed domain name and dynamic IP. For users who use dynamic IP addresses, the dynamic name software installed in the host would send the IP address to the

dynamic parse server provided by DDNS servers every time when getting a new IP from Internet and database of dynamic name parse. When other users in the Internet need to access the domain name, dynamic name parse server would go back to the correct IP address. Thus the majority of users that do not use fixed IP can also build network via fixed domain name.



Dynamic DNS Providers: select websites that provide dynamic domain name service.

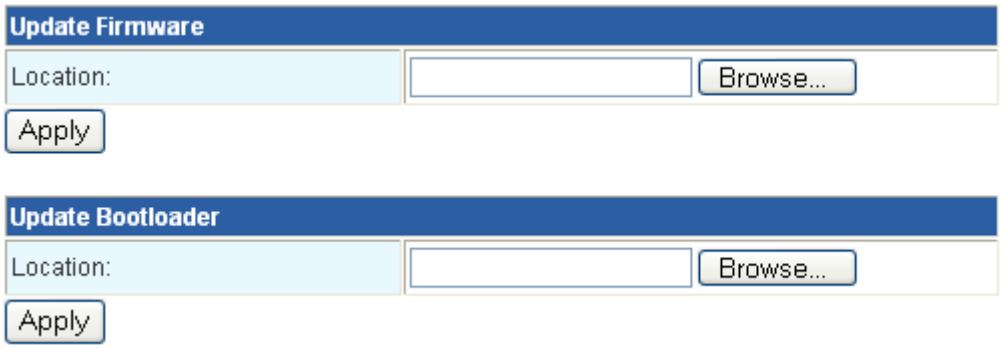
Account: the login name you register in the websites that provide dynamic domain name service.

Password: the password you register in the websites that provide dynamic domain name service.

DDNS: the domain name you register in the websites that provide dynamic domain name service

Note: before using Dynamic Domain Name function, please register the dynamic DNS address services in the website listed in drop-down box of service providers and ensure that this account is effective.

9.2 System Upgrade



If you want to upgrade the software for the router, the first step is to obtain our upgrade files and save them in the computer. Then click “Browse” in the “Upgrade Firmware” to select upgrade files, then click “Apply” and keep waiting until the upgrade is done (generally within one minute).

The “Updates Bootloader” is used to upgrade the system booting programs. it is unnecessary for the user to apply this function.

9.3 Equipment Management

Export system configurations: Save system configuration files in the computer for further recoveries.

Import system configurations: Introduce local configuration files to the router. The configuration of the router will be update to the setting which been imported

Reset: All the configurations will reset to the factory original settings