NSW-R4

USER MANUAL
HANDBUCH
HANDLEIDING
MANUEL DESCRIPTIF
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
КЕРІВНИЦТВО КОРИСТУВАЧА

GEMBIRD®

WIRELESS BROADBAND ROUTER, 300 M
WLAN BREITBAND ROUTER, 300 M
DRAADLOZE BREEDBAND ROUTER, 300M
ROUTEUR SANS FIL, 300M
БЕСПРОВОДНОЙ МАРШРУТИЗАТОР, СКОРОСТЬ ДО 300 МБИТ/С
БЕЗДРОТОВИЙ МАРШРУТИЗАТОР, ШВИДКІСТЬ ДО 300 МБІТ / С

Features

- Wireless 300M router with 4-port 10/100Mbps LAN switch and 802.11n access point
- Supports all IEEE802.11b/g/n WiFi standards
- Up to 300 Mbps data transfer rate via the wireless 802.11n protocol
- Built-in DHCP server automatically assigns and manages all IP addresses within your LAN
- Advanced firewall, 64/128-bit WEP encryption and WPA-PSK, WPA2-PSK security
- Supports Wi-Fi Protected Setup (WPS) with reset button
- Supports MAC/IP filtering and URL blocking (family filter)
- Easy to use Web-interface for all router management options

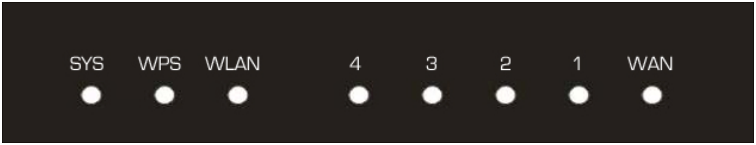
Specifications

- Supported standards: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, CSMA/CA,CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE, PPTP
- Ports: - LAN: 4 x 10/100M Auto MDI/MDIX RJ45 ports
- WAN: 1 x 10/100M Auto MDI/MDIX RJ45 port
- Frequency band 2.4 ~ 2.4835GHz
- Channels: 1 ~ 11 (US, Canada), 1 ~ 13 (Europe)
- Supports Virtual Server and DMZ
- Supports DDNS (DynDNS, TZO) and QoS
- Data transfer rates: max 300 Mbps (11n), 54 Mbps (11g), 11 Mbps (11b)
- Encryption standards: WPS, WPA, WPA2, WPA2/WPA Mixed
- Antenna: 2 x 3 Dbi omni-directional antenna
- RF power: 20 dBm (max)
- Transmission distance: indoors up to 120 m, outdoors up to 360 m (distance is dependent of environmental conditions, obstructions, walls, ceilings, etc)
- Dimensions: 153 x 100 x 30 mm (W x D x H)
- Operating temperature: 0 ~ 40 °C
- Storage temperature: -40 ~ 70 °C
- Operating humidity: 10 ~ 90 % non-condensing;
- Storage humidity: 5 ~ 95 % non-condensing

CE RoHS MADE IN CHINA

1. Wireless router overview

1.1 Front panel (LED indicators)



SYS (Red): Flickering light indicates a proper connection to the power supply.

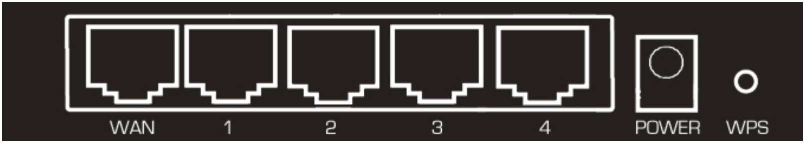
WPS (Green): The LED is flash about two minutes during WPS working.

WLAN (Green): The LED is flickering during wireless activity.

LAN 1, 2, 3, 4(Green): The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

WAN (Green): The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

1.2 Back panel (sockets description)



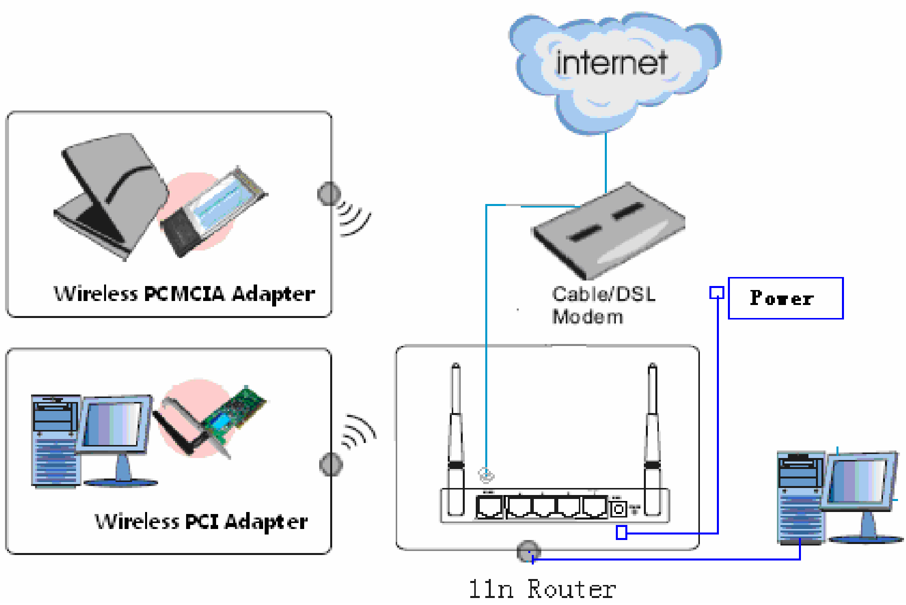
WAN: 10/100Mbps RJ45 port. The WAN port is where you will connect Cable/DSL Modem or other LAN.

LAN (1, 2, 3, 4): 10/100Mbps RJ45 Auto-sensing. These four LAN ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network. If you connect this product with the Hub (or Switchboard) correctly, the Router's corresponding LED and the Hub's (or the Switchboard's) must be illuminates.

POWER: Power inlet.

RESET (WPS): The Reset Button has two functions, WPS and Factory Default. When press it less than 2 seconds, it is WPS function and the Reset LED will flash two minutes, than 6 seconds, the router will restore to factory default.

2 Hardware Installation



1. Make sure that all devices including your PCs, modem and router are powered off.

2. Connect your Internet access device such as cable or DSL modem to the router WAN port using a cat 5e patch cord.

3. Turn all the devices on.
4. Power the router up.

3 Quick Installation Guide

3.1 TCP/IP Settings

Before you can access and configure router, you have to setup your PC network adapter IP address. Connect your PC to the router LAN port. Follow the steps below to access the built-in router web-interface (for Windows OS).

Note: The router default IP address is: **192.168.1.1**

1. Choose Network connections from the Control Panel.

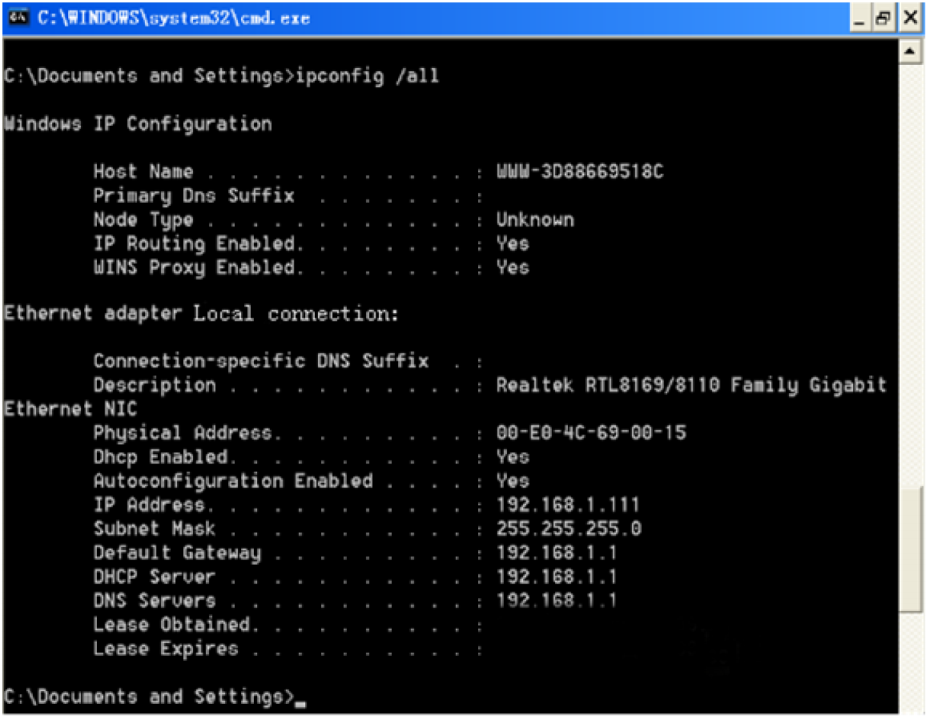
2. Click with the right mouse button over the Network adapter connected to the router. Choose properties from the popup menu which would then appear.

3. Select TCP/IP v.4 from the next window and click Properties

4. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” in the IP Address tab.

5. Click OK to complete the install procedure. You might need to restart your PC to activate these settings.

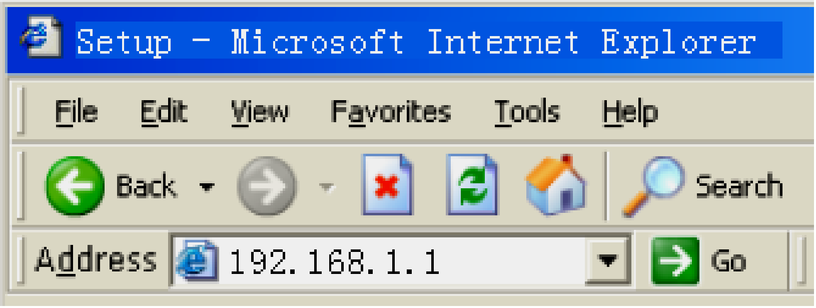
You can verify that your PC got correct IP address selecting Start → Run → cmd and then entering command: ipconfig /all.



```
C:\Documents and Settings>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : WWW-3D88669518C
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : Yes

Ethernet adapter Local connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8169/8110 Family Gigabit
Ethernet NIC
        Physical Address. . . . . . . . . : 00-E0-4C-69-00-15
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.111
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
        Lease Obtained. . . . . . . . . . :
        Lease Expires . . . . . . . . . . :

C:\Documents and Settings>_
```

3.2 Getting Started

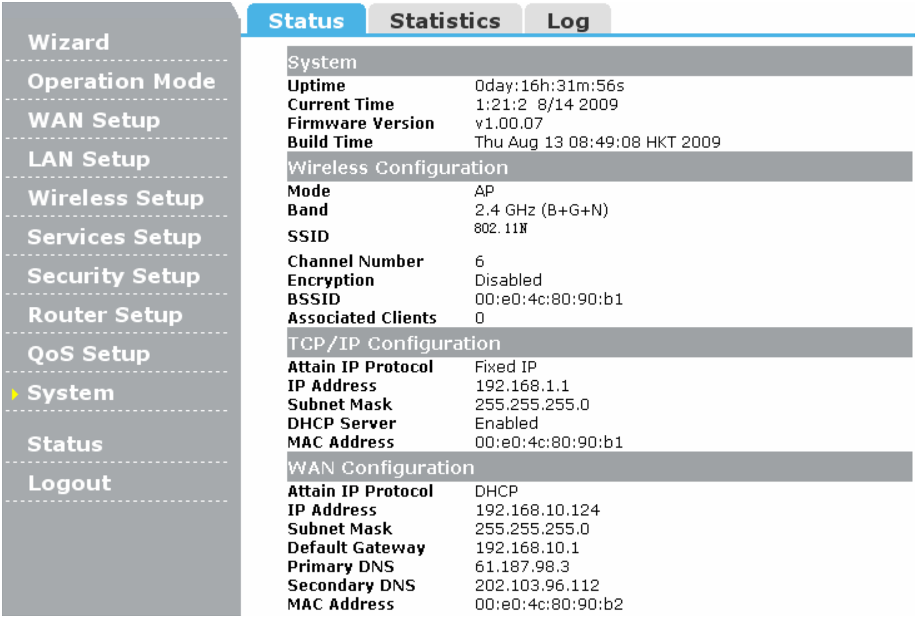
To access the router web-interface, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.1.1).



192.168.1.1

You will be prompted to enter the login and password. The default Login/Password is: *admin/admin*

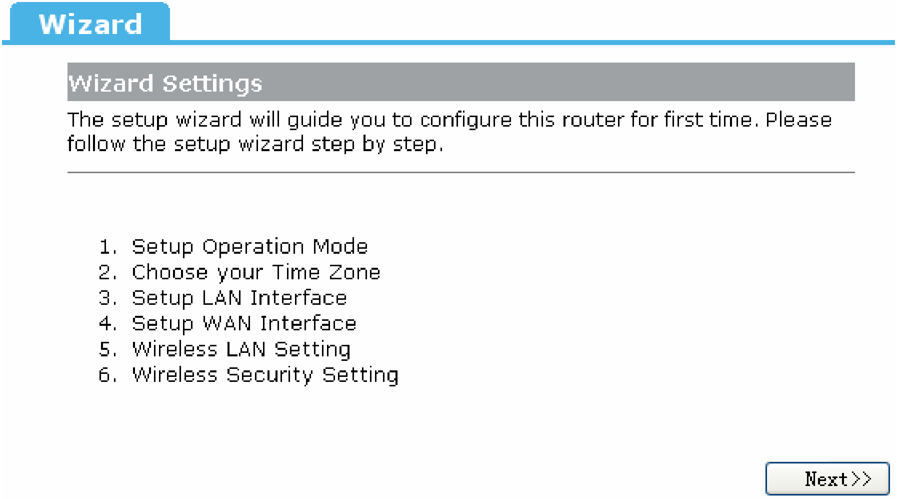
Upon a successful login you will see the status page.



System	
Uptime	0day:16h:31m:56s
Current Time	1:21:2 8/14 2009
Firmware Version	v1.00.07
Build Time	Thu Aug 13 08:49:08 HKT 2009
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	802.11N
Channel Number	6
Encryption	Disabled
BSSID	00:e0:4c:80:90:b1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:e0:4c:80:90:b1
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.124
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	61.187.98.3
Secondary DNS	202.103.96.112
MAC Address	00:e0:4c:80:90:b2

3.3 Setup Wizard

Click on the “Wizard” option to setup your router step by step in a simple way. There are six steps to follow:



Wizard

Wizard Settings

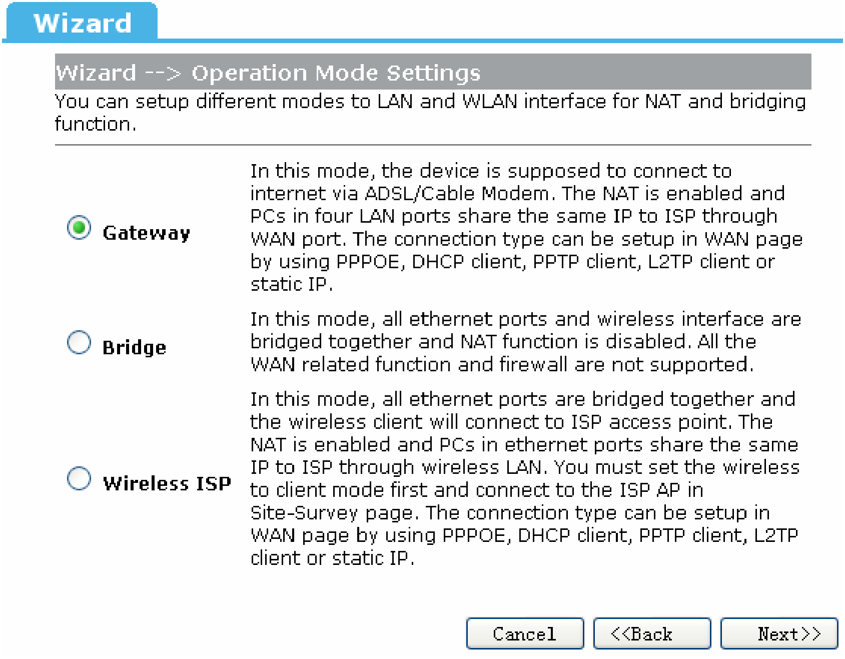
The setup wizard will guide you to configure this router for first time. Please follow the setup wizard step by step.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Please follow the steps to complete the router configuration.

Step 1 – Operation Mode Settings

The router supports three operation modes: Gateway, Bridge and Wireless ISP. Each mode is suitable for different purpose, please choose the correct mode.



Wizard

Wizard --> Operation Mode Settings

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

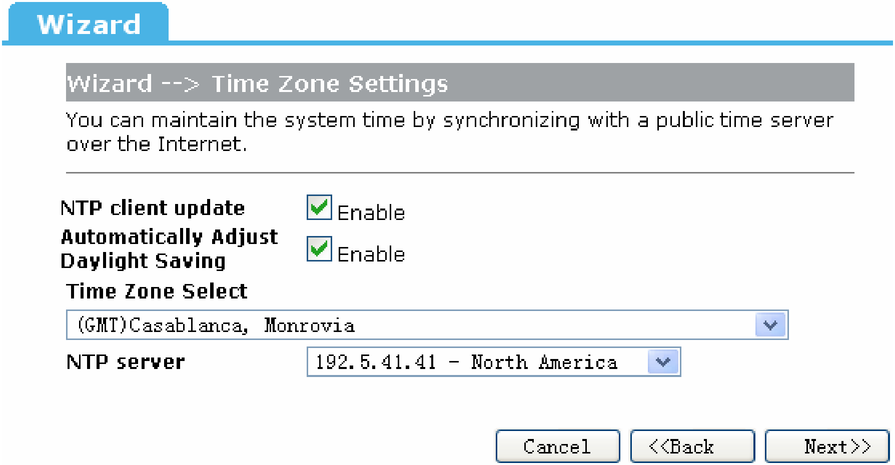
● **Gateway** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

○ **Bridge** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Step 2 – Time Zone Settings

The Time Configuration option allows you to configure, update, and maintain the correct time for the internal system clock. Daylight Saving can also be configured to automatically adjust the time when needed.



Wizard --> Time Zone Settings

You can maintain the system time by synchronizing with a public time server over the Internet.

NTP client update ☑ Enable

Automatically Adjust Daylight Saving ☑ Enable

Time Zone Select: (GMT)Casablanca, Monrovia

NTP server: 192.5.41.41 - North America

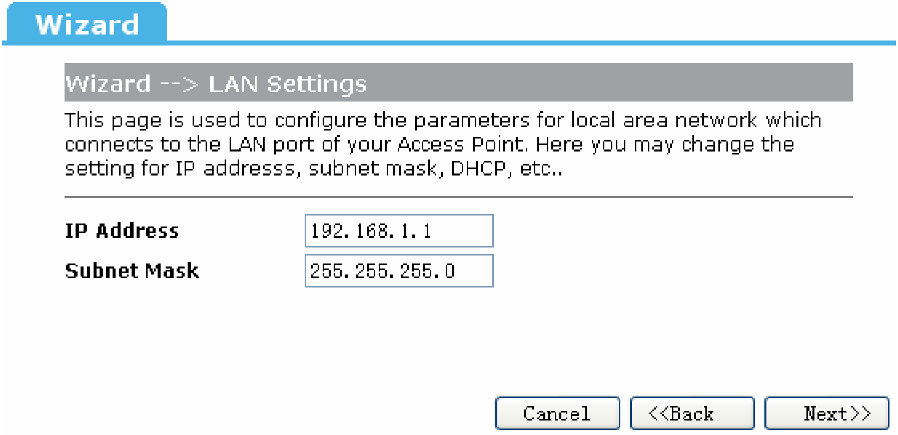
NTP client update: Check this box to connect to the NTP Server and synchronize Internet time.

Automatically Adjust Daylight Saving: If you check this box the system will take the summer time into consideration.

Time Zone Select: Select the Time Zone from the drop-down menu.

NTP Server: Select the NTP Server from the drop-down menu.

Step 3 – LAN Settings
Setup the IP address and network mask for the LAN interface.



Wizard --> LAN Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

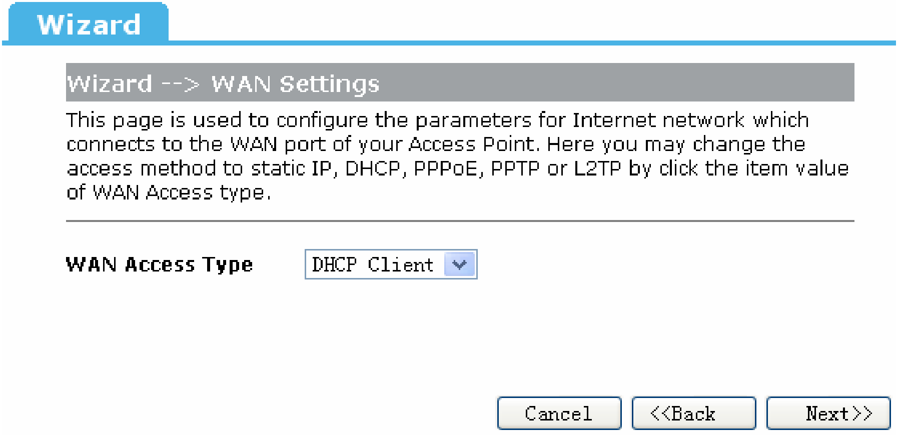
IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Step 4 – WAN Settings

The router supports five access modes for the WAN, please choose the correct mode according to your Internet Service Provider (ISP).

Mode 1: DHCP Client



Wizard --> WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Select DHCP Client to obtain IP Address automatically from your ISP. This mode is commonly used for Cable modem services.

Mode 2: Static IP

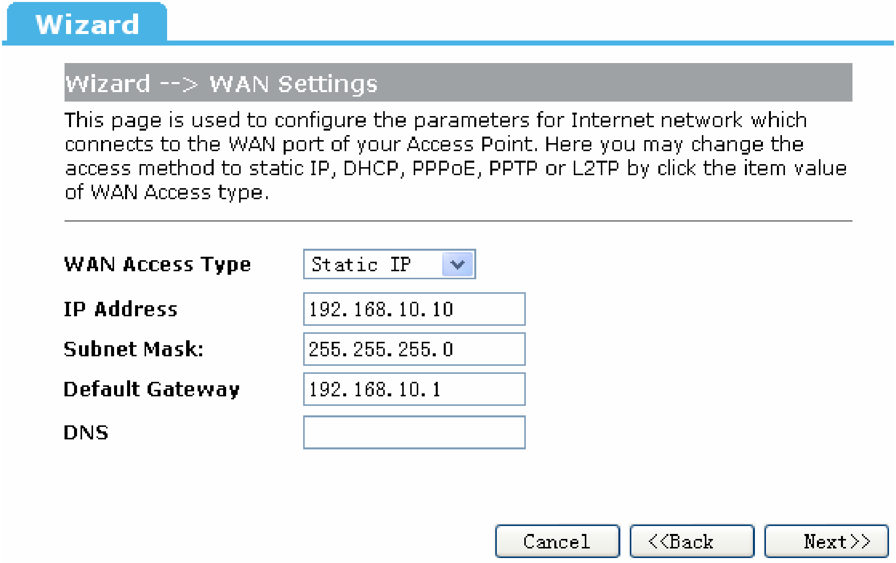
Select Static IP Address if the IP information is provided to you by your ISP. You will need to enter the IP address, subnet mask, gateway address, and DNS address (-es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format.

IP Address: Enter the IP address assigned by your ISP

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DNS: The DNS server information will be supplied by your ISP (Internet Service Provider.)



Wizard --> WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 192.168.10.10

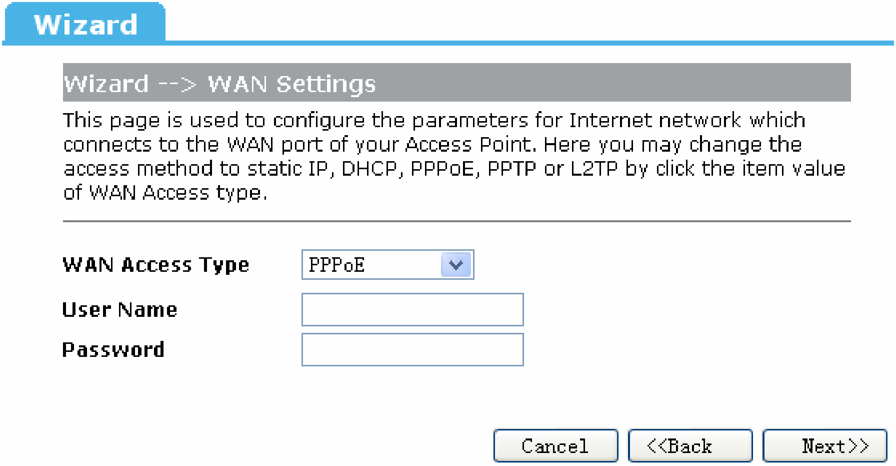
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DNS:

Mode 3: PPPoE

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Wizard --> WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name:

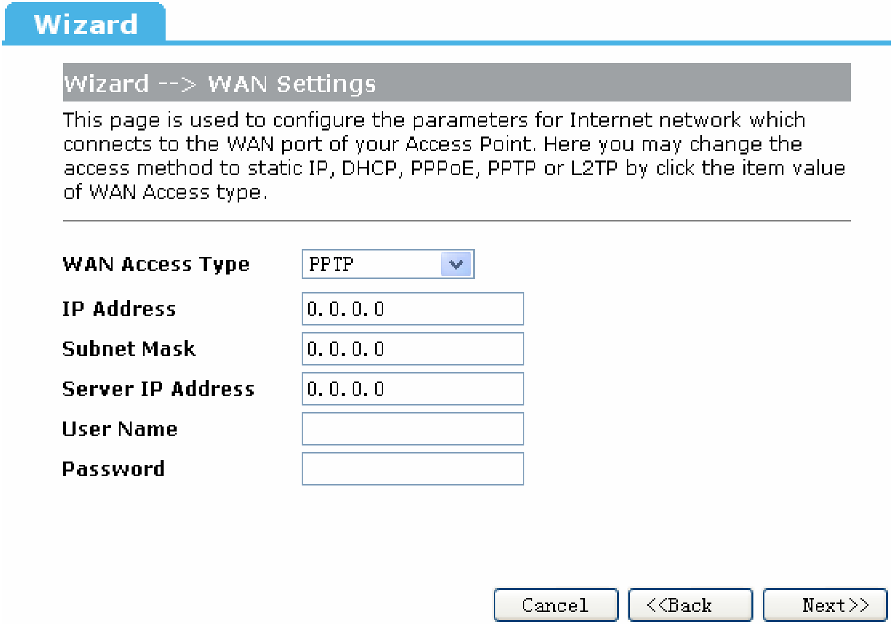
Password:

User Name: Enter your PPPoE user name.
Password: Enter your PPPoE password.

Mode 4: PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with IP information and PPTP

Server IP Address, of course it also includes a username and password. This mode is typically used for DSL services.



Wizard

Wizard --> WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type	PPTP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Server IP Address	0.0.0.0
User Name	
Password	

IP Address: Enter the IP address.

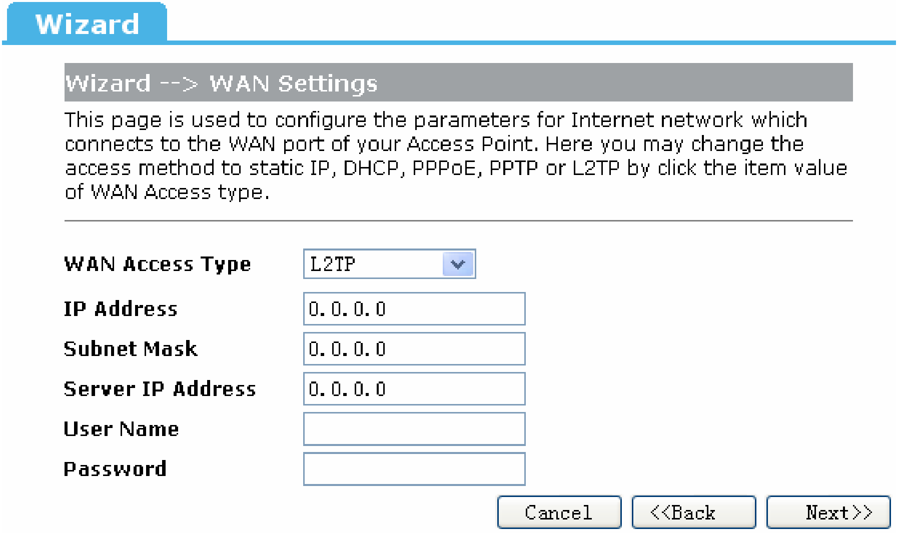
Subnet Mask: Enter the subnet Mask.

Server IP Address: Enter the PPTP Server IP address provided by your ISP.

User Name: Enter your PPTP username.
Password: Enter your PPTP password.

Mode 5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.



Wizard

Wizard --> WAN Settings

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type	L2TP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Server IP Address	0.0.0.0
User Name	
Password	

IP Address: Enter the IP address.

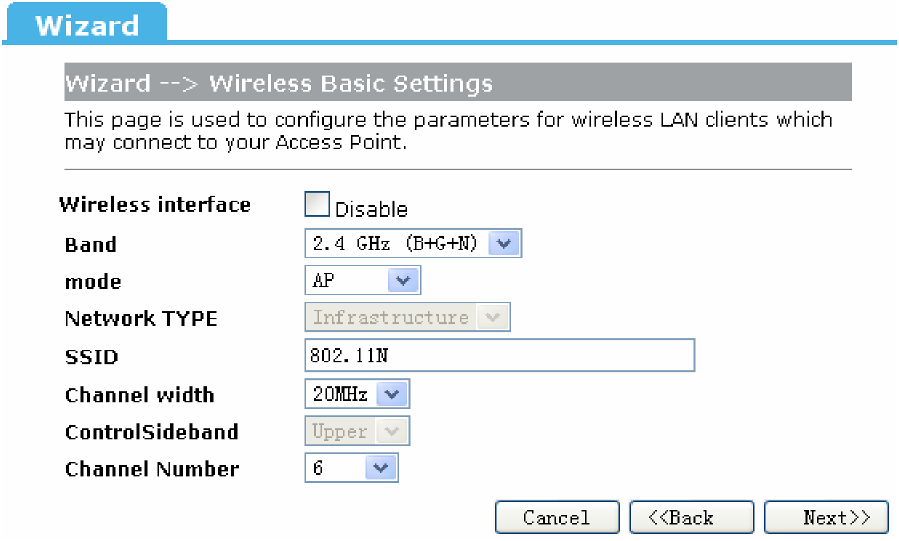
Subnet Mask: Enter the subnet Mask.

Server IP Address: Enter the PPTP Server IP address provided by your ISP.

User Name: Enter your PPTP username.

Password: Enter your PPTP password.

Step 5 – WLAN Settings



Wizard --> Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Wireless interface	□ Disable
Band	2.4 GHz (B+G+N)
mode	AP
Network TYPE	Infrastructure
SSID	802.11N
Channel width	20MHz
ControlSideband	Upper
Channel Number	6

Wireless Interface: If you do not want to use the wireless interface, uncheck the box to disable all the wireless functions.

Band: Supported 802.11B, 802.11G, 802.11N and mixed.

Mode: Supported AP, Client, WDS and AP+WDS mode.

Network TYPE: This type is only valid in client mode.

SSID: Service Set Identifier, external name of your wireless network.

Channel width: Select 40MHz if you use 802.11n or 802.11n mixed mode, otherwise 20MHz, it is default value.

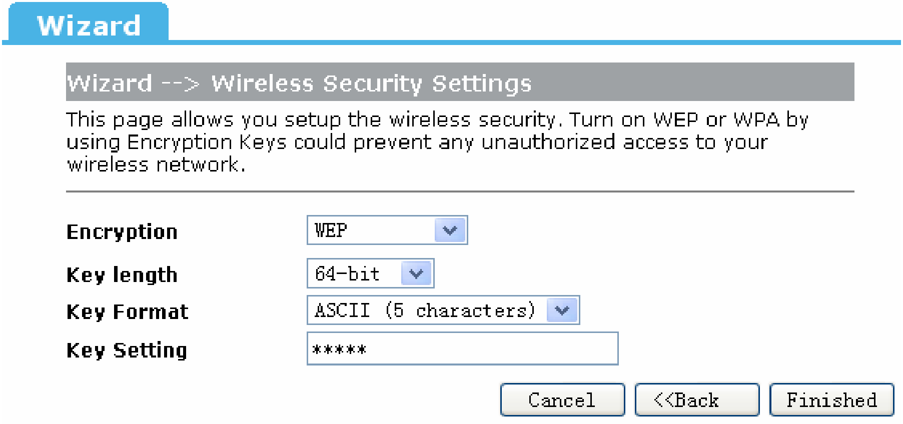
Control Sideband: it is only valid when you choose channel width 40MHz.

Channel Number: Indicates the channel setting for the router. By default the channel is set to 6.

Step 6 – WLAN Security Settings

Secure your wireless network by turning on the WPA or WEP security feature of the router. You can set WEP and WPA-PSK security mode.

The following picture shows how to set the WEP security.



Wizard

Wizard --> Wireless Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WEP

Key length: 64-bit

Key Format: ASCII (5 characters)

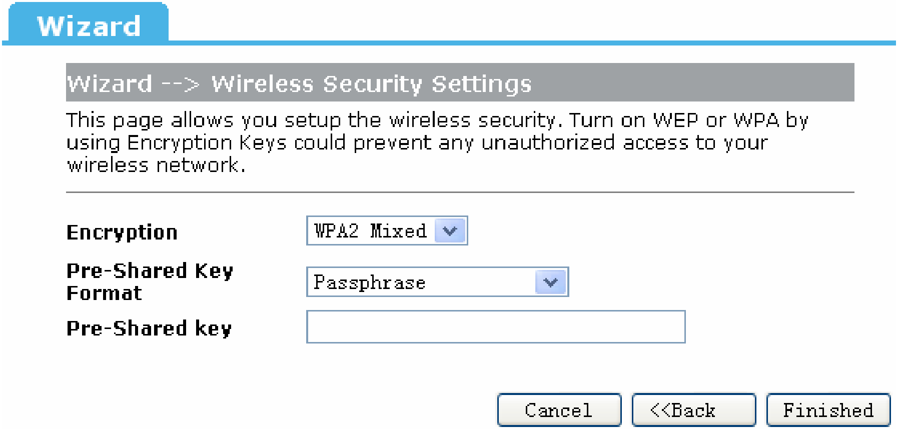
Key Setting: *****

Key length: WEP supports 64-bit or 128-bit security key.

Key Format: The key can be entered in ASCII (as symbols) or Hex (hexadecimal) format.

Key Setting: Enter the key as ASCII or Hex.

The following picture shows how to set the WPA-PSK security; you can also select WPA (TKIP), WPA2 (AES) and Mixed mode.



Wizard

Wizard --> Wireless Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption	WPA2 Mixed
Pre-Shared Key Format	Passphrase
Pre-Shared key	

Pre-Shared Key Format: Specify the format of the key, pass phrase or hex.

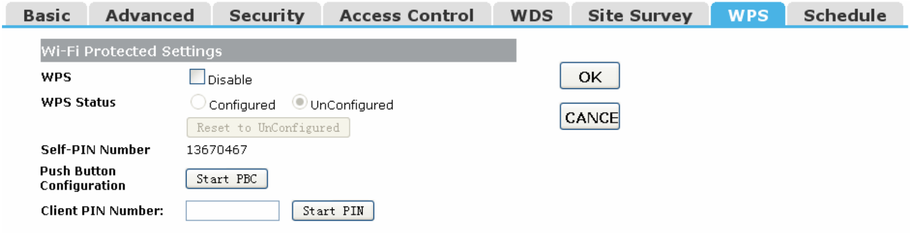
Pre-Shared Key: Enter the key here (phrase or hexadecimal).

4 Advanced Setup

4.1 Wireless Advanced setup

4.1.1 WPS

WPS is designed to set up the password-protected Wi-Fi networks and to simplify the network management. This router supports WPS features for AP mode (access point), AP+WDS mode, Infrastructure-Client mode, and the wireless root interface of Universal Repeater mode.



Wi-Fi Protected Settings

WPS ☐ Disable

WPS Status ○ Configured ● UnConfigured

Self-PIN Number 13670467

Push Button Configuration

Client PIN Number:

WPS: Checking this box and clicking “OK” will disable the WPS function. WPS is turned on by default.

WPS Status: After you set up all security settings the checkbox “Configured” will be highlighted

Self-PIN Number: It is AP’s PIN number.

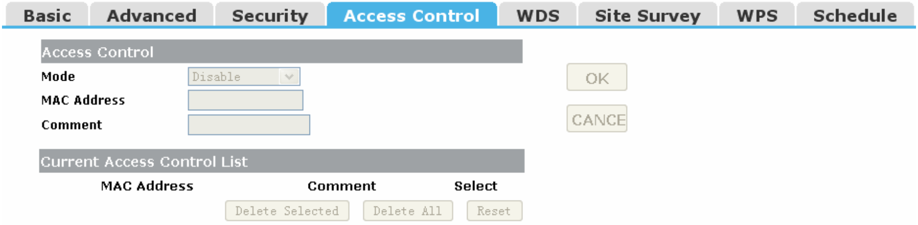
Start PBC: Clicking this button will invoke the Pus Button Configuration of WPS. If one station wants to connect to the AP, it must click its PBC button within two minutes. You will see the reset LED flashing during this time.

Note: This router also has a hardware button, it is the same button with reset. If you keep this button pressed for less than two seconds, the AP will run the PBC function. The reset LED will then flash for two minutes. During this time, the workstations can connect to the AP by using their software or hardware WPS button.

Client PIN Number: The length of PIN can be four or eight digits. If the AP and the workstation use this PIN, they will establish a connection and setup their security key.

4.1.2 Access Control

The Wireless MAC Address Filtering feature allows you to control which wireless stations are allowed to be connected to the router.



Access Control

Mode: Disable

MAC Address:

Comment:

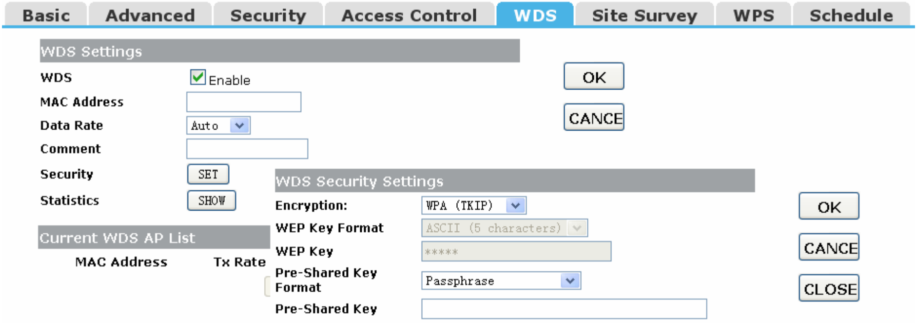
Current Access Control List

MAC Address	Comment	Select

Mode: If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point. The MAC Address format is 001122334455.

4.1.3 WDS

Wireless Distribution System uses wireless media to communicate with the other APs. To do this, you should first set AP Mode to WDS or AP+WDS in the basic settings, then enable WDS function and set another AP MAC address which you would like to communicate with. The WDS supports WEP and PSK security mode. Of course in order to make the APs work, you have to assign for them the same channel and security mode.



WDS Settings

WDS ☑ Enable

MAC Address

Data Rate Auto

Comment

Security SET

Statistics SHOW

Current WDS AP List

MAC Address Tx Rate

WDS Security Settings

Encryption: WPA (TKIP)

WEP Key Format ASCII (5 characters)

WEP Key *****

Pre-Shared Key Format Passphrase

Pre-Shared Key

WDS: Check this box to enable the WDS function.

MAC Address: Enter the remote AP MAC address.

Security: Sets the WDS security settings.

Encryption: You may select WEP 64bits, WEP 128bits, WPA (TKIP), WPA (AES).

WEP Key Format: You may select ASCII Characters or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

WEP Key: Set key to encrypt your data

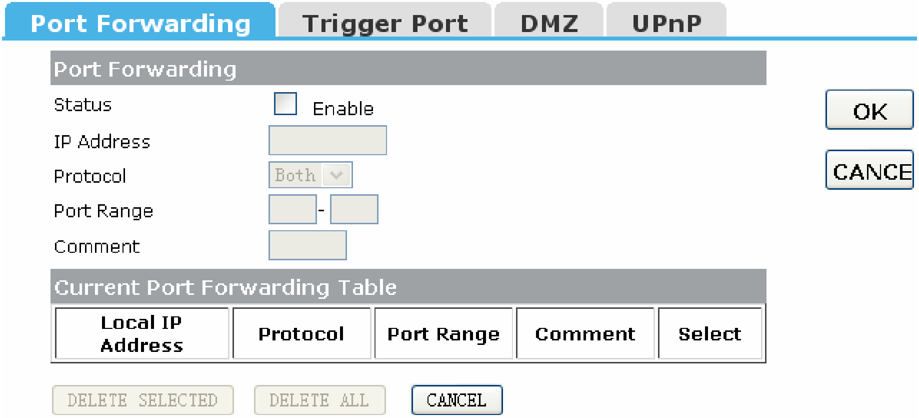
Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).

Pre-Shared Key: Pre-shared key(PSK) is a method to set encryption keys. Commonly used in Wi-Fi Protected Access and WEP.

4.2 Service Setup

4.2.1 Port Forwarding

If you configure the router as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to the local servers with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.



Port Forwarding

Status ☐ Enable

IP Address

Protocol Both

Port Range -

Comment

Current Port Forwarding Table

Local IP Address	Protocol	Port Range	Comment	Select

Status: Clicking this box will enable the Port Forwarding function.

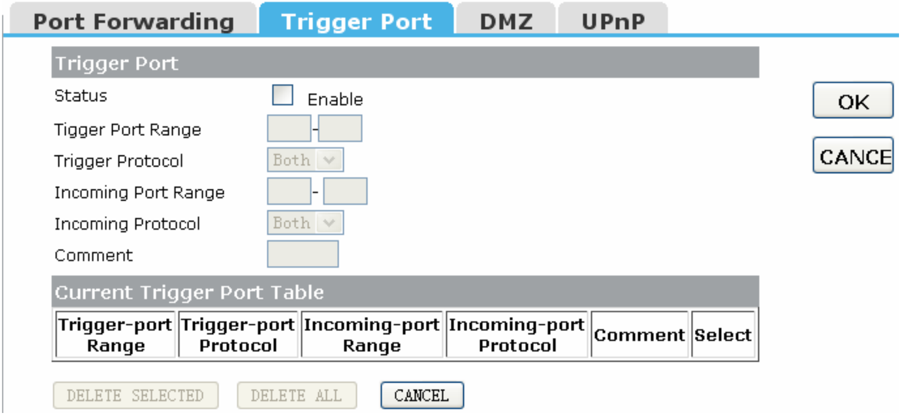
IP Address: The external public IP address to be redirected.

Protocol and Port Range: Select the protocol and port range to be redirected to the local IP.

Current Filter Table: The table shows all forwarding records you have added so far. You can delete any selected record or all records at once.

4.2.2 Trigger Port

Some applications (like Internet games, video conferencing, Internet calling and so on) require multiple connections. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications to let them work with a NAT router.



Trigger Port

Status	□ Enable
Tigger Port Range	-
Trigger Protocol	Both
Incoming Port Range	-
Incoming Protocol	Both
Comment	

Current Trigger Port Table

Trigger-port Range	Trigger-port Protocol	Incoming-port Range	Incoming-port Protocol	Comment	Select

Status: Check on to enable this function.

Trigger Port Range: The port for outgoing traffic. An outgoing connection using this port will “Trigger” this rule.

Trigger Protocol: The protocol used for Trigger Ports, either TCP, UDP or both.

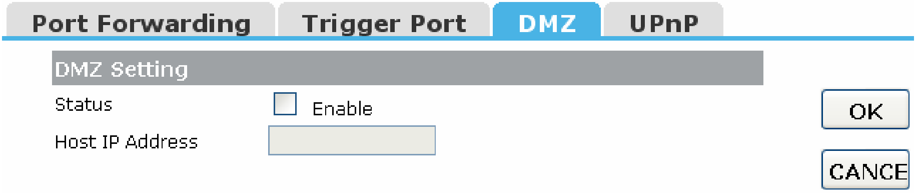
Incoming Port Range: The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule.

Incoming Protocol: The Protocol used for Incoming Ports Ranges, either TCP or UDP, or both.

Comment: You can add some comments for this item.

4.2.3 DMZ

If you have a client PC that cannot run Internet applications properly from behind the NAT firewall or after configuration of the Port Forwarding, then you can open the client to unrestricted two-way Internet access.



DMZ Setting

Status □ Enable

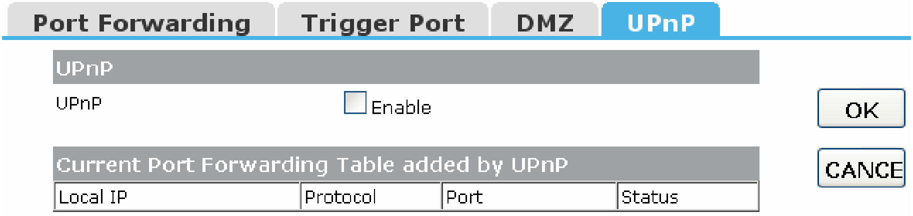
Host IP Address

Status: Clicking this box will enable DMZ function.

Host IP Address: Enter the DMZ host IP Address. Note: this may expose this computer to a variety of security risks.

4.2.4 UPNP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed, UPnP devices can be automatically discovered by the UPnP service application on the LAN.



UPnP

UPnP ☐ Enable

Current Port Forwarding Table added by UPnP

Local IP	Protocol	Port	Status

UPnP: Check to enable UPnP function

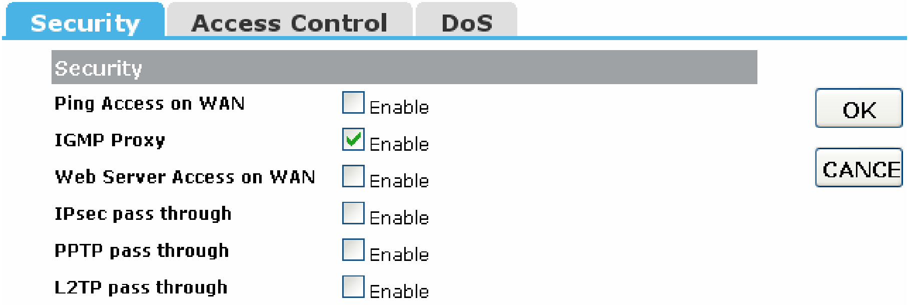
Note: The list will contain the forwarding port added by the UPnP Service.

4.3 Security Setup

The router provides extensive firewall settings to limit the risk of intrusion and protect your computer from hacker attacks.

4.3.1 Security

The firewall will allow or block some services according to the following settings.



Security

Ping Access on WAN □ Enable

IGMP Proxy ☑ Enable

Web Server Access on WAN □ Enable

IPsec pass through □ Enable

PPTP pass through □ Enable

L2TP pass through □ Enable

Ping Access on WAN: allows or blocks the Ping WAN interface.

IGMP Proxy: IGMPproxy is a simple dynamic Multicast Routing Daemon using only IGMP signaling. It's intended for simple forwarding of Multicast traffic between networks.

Web Server Access on WAN: allow or blocks access to the Web Server from WAN interface.

VPN pass through: allows or blocks the VPN Pass through the router NAT.

4.3.2 Access Control

You can set up some rules, for example MAC filter, IP filter, URL filter and Port filter. You can also add some extra conditions for these rules (the date and time), but then you should enable the NTP-client first.

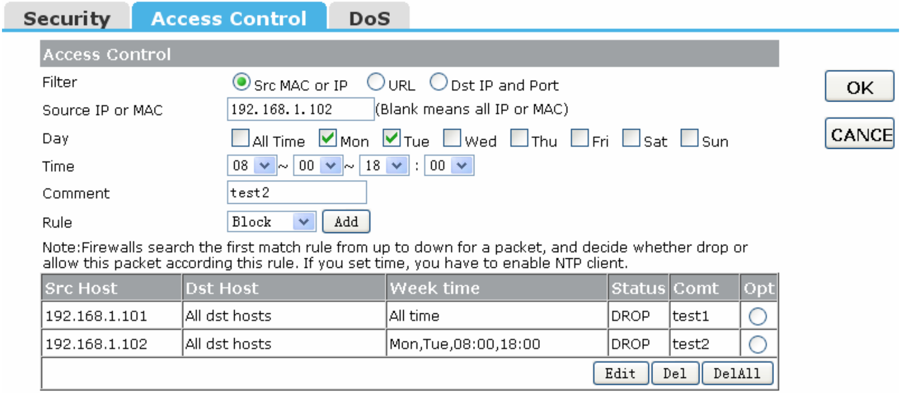
Note 1: Whenever a network packet arrives, the firewall will try to find a suitable rule from this table. The search goes from up to down and stops when a match has been found. Then the packet will be either forwarded or dropped according to the rule. If no rule matching the packet is found, then the firewall will let it go to the destination.

Note 2: If you set the date and time in your rule then the NTP client has to be enabled.

Note 3: Click “Add” button to add this rule to the table and click “OK” to make it effective. You also can edit or delete the records:

1. IP Filter

Allow or block the computers according to their IP addresses.



Access Control

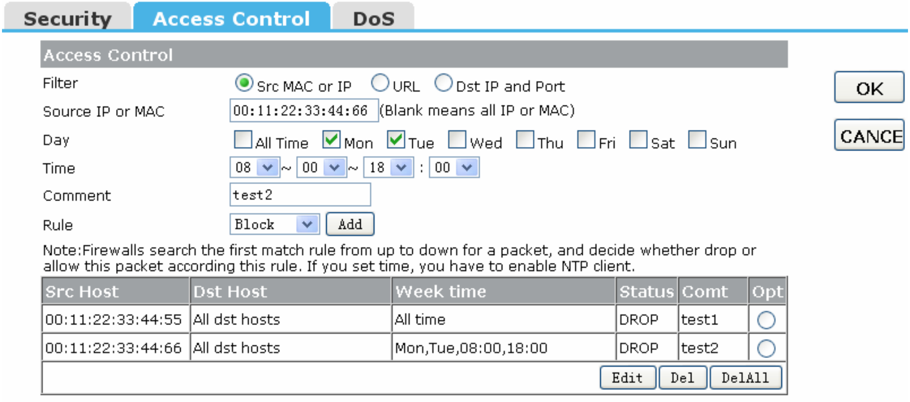
Filter	● Src MAC or IP ○ URL ○ Dst IP and Port
Source IP or MAC	192. 168. 1. 102 (Blank means all IP or MAC)
Day	□ All Time ☑ Mon ☑ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	08 ~ 00 ~ 18 : 00
Comment	test2
Rule	Block Add

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
192.168.1.101	All dst hosts	All time	DROP	test1	○
192.168.1.102	All dst hosts	Mon,Tue,08:00,18:00	DROP	test2	○

2. MAC filter

Allow or block the computers according to their MAC addresses.



Access Control

Filter	● Src MAC or IP ○ URL ○ Dst IP and Port
Source IP or MAC	00:11:22:33:44:66 (Blank means all IP or MAC)
Day	□ All Time ☑ Mon ☑ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	08 ~ 00 ~ 18 : 00
Comment	test2
Rule	Block Add

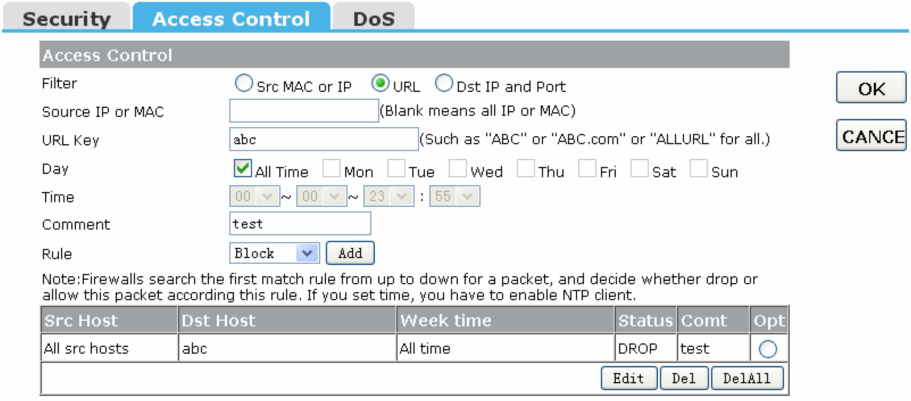
Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
00:11:22:33:44:55	All dst hosts	All time	DROP	test1	○
00:11:22:33:44:66	All dst hosts	Mon,Tue,08:00,18:00	DROP	test2	○

3. URL filter

You can block some URLs using the URL Key string. If Source IP or MAC address fields are blank, then all computers can not access this URL, otherwise the rule only applies to the computer with the given IP or MAC address.

Example 1: block “abc.com”, “abc.net” or “www.abc.com” to all computers.



Access Control

Filter ○ Src MAC or IP ● URL ○ Dst IP and Port

Source IP or MAC (Blank means all IP or MAC)

URL Key abc (Such as "ABC" or "ABC.com" or "ALLURL" for all.)

Day ☑ All Time □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time 00 ~ 00 ~ 23 : 55

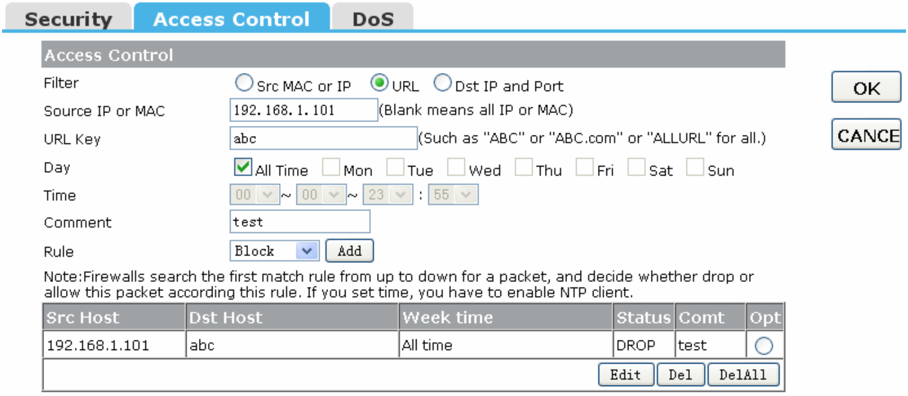
Comment test

Rule Block

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
All src hosts	abc	All time	DROP	test	○

Example 2: block “abc.com”, “abc.net” or “www.abc.com” for the computer with 192.168.1.101 IP address.



Access Control

Filter ○ Src MAC or IP ● URL ○ Dst IP and Port

Source IP or MAC 192. 168. 1. 101 (Blank means all IP or MAC)

URL Key abc (Such as "ABC" or "ABC.com" or "ALLURL" for all.)

Day ☑ All Time □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time 00 ~ 00 ~ 23 : 55

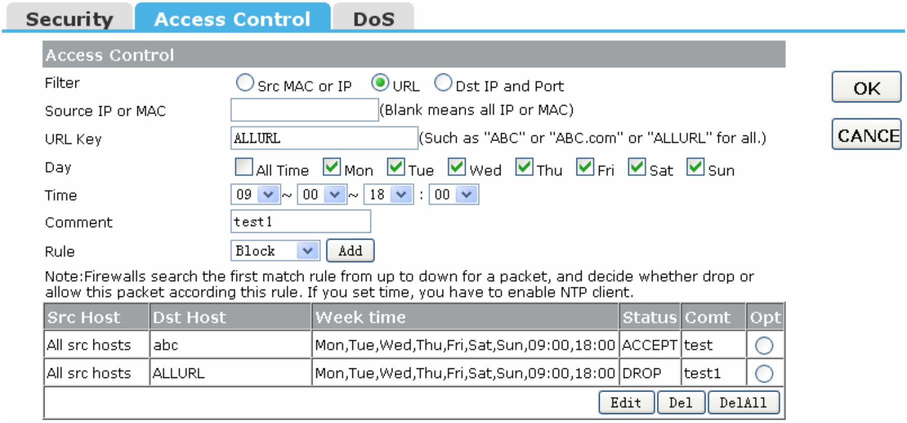
Comment test

Rule Block

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
192.168.1.101	abc	All time	DROP	test	○

Example 3: allow to access “abc.com”, “abc.net” or “www.abc.com” for all computers from 09:00 to 18:00 during the working days only.



Access Control

Filter	○ Src MAC or IP ● URL ○ Dst IP and Port
Source IP or MAC	(Blank means all IP or MAC)
URL Key	ALLURL (Such as "ABC" or "ABC.com" or "ALLURL" for all.)
Day	□ All Time ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun
Time	09 ~ 00 ~ 18 : 00
Comment	test1
Rule	Block Add

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

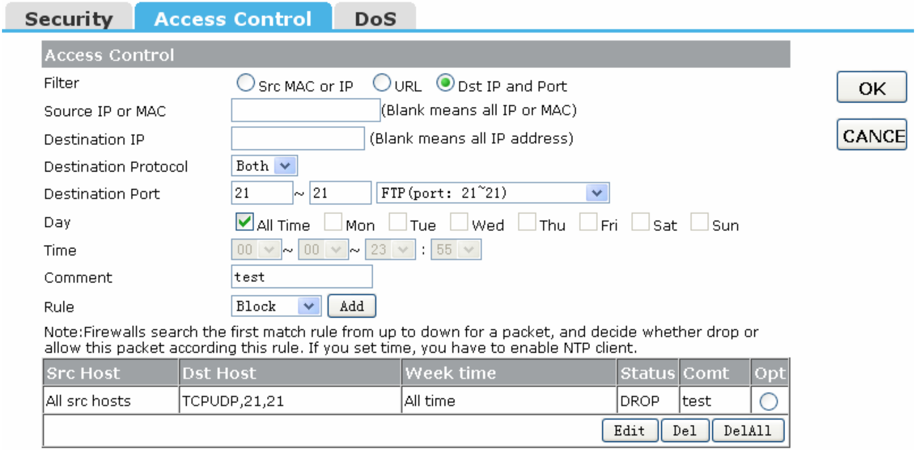
Src Host	Dst Host	Week time	Status	Comt	Opt
All src hosts	abc	Mon,Tue,Wed,Thu,Fri,Sat,Sun,09:00,18:00	ACCEPT	test	○
All src hosts	ALLURL	Mon,Tue,Wed,Thu,Fri,Sat,Sun,09:00,18:00	DROP	test1	○

Edit Del DelAll

4. Port filter

You can limit some or all computers to access a certain destination IP and/or port.

Example 1: block all computers to access port 21.



Access Control

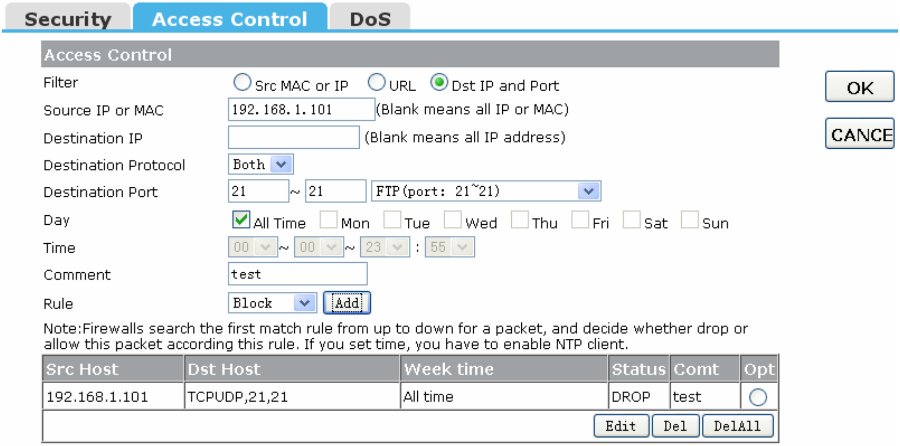
Filter	○ Src MAC or IP ○ URL ● Dst IP and Port
Source IP or MAC	(Blank means all IP or MAC)
Destination IP	(Blank means all IP address)
Destination Protocol	Both
Destination Port	21 ~ 21 FTP(port: 21~21)
Day	☑ All Time □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	00 ~ 00 ~ 23 : 55
Comment	test
Rule	Block Add

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
All src hosts	TCPUDP,21,21	All time	DROP	test	○

Edit Del DelAll

Example 2: block the computer with IP address 192.168.1.101 to access port 21.



Access Control

Filter ○ Src MAC or IP ○ URL ● Dst IP and Port

Source IP or MAC 192.168.1.101 (Blank means all IP or MAC)

Destination IP (Blank means all IP address)

Destination Protocol Both

Destination Port 21 ~ 21 FTP(port: 21~21)

Day ☑ All Time □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time 00 ~ 00 ~ 23 : 55

Comment test

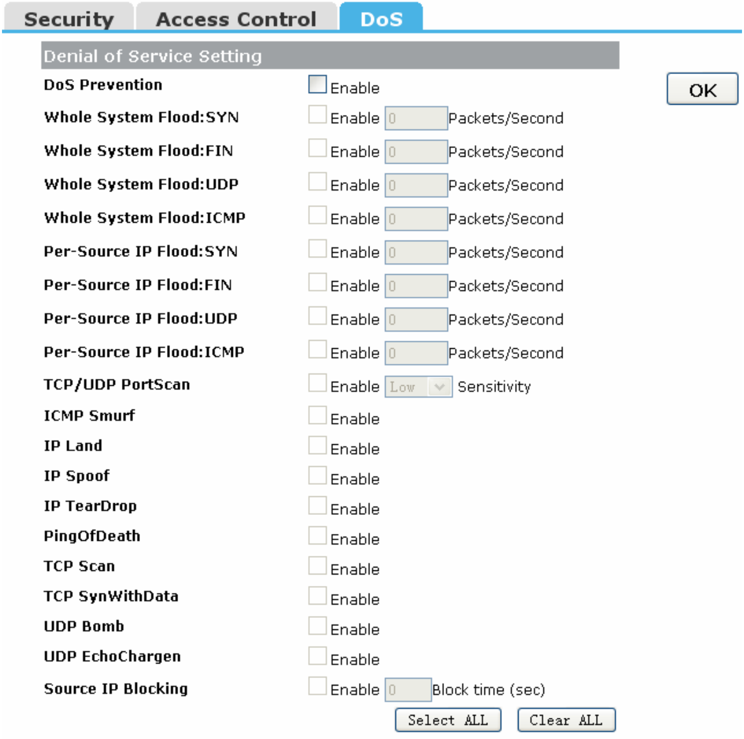
Rule Block Add

Note:Firewalls search the first match rule from up to down for a packet, and decide whether drop or allow this packet according this rule. If you set time, you have to enable NTP client.

Src Host	Dst Host	Week time	Status	Comt	Opt
192.168.1.101	TCPUDP,21,21	All time	DROP	test	○

4.3.3 DoS

With settings on this page you can block the DoS attack.



Denial of Service Setting

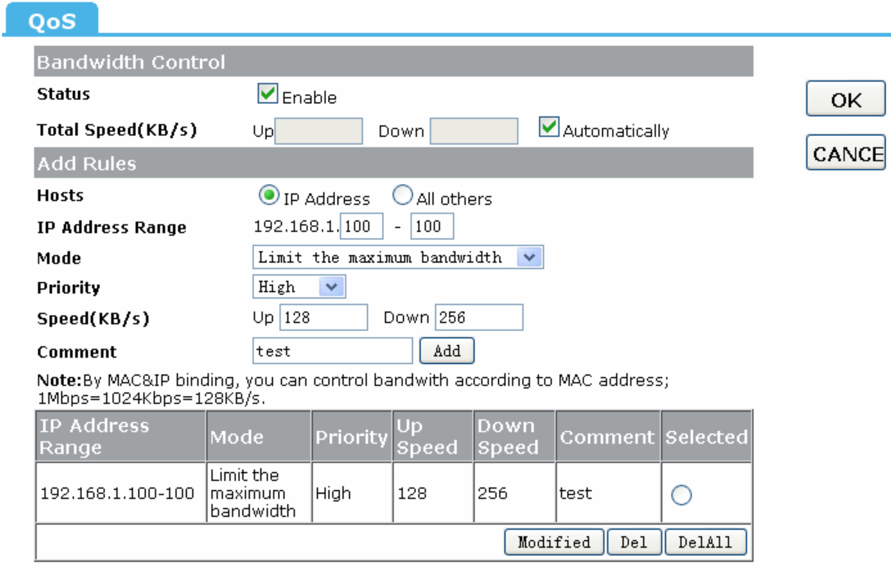
DoS Prevention	☐ Enable	
Whole System Flood:SYN	☐ Enable	0 Packets/Second
Whole System Flood:FIN	☐ Enable	0 Packets/Second
Whole System Flood:UDP	☐ Enable	0 Packets/Second
Whole System Flood:ICMP	☐ Enable	0 Packets/Second
Per-Source IP Flood:SYN	☐ Enable	0 Packets/Second
Per-Source IP Flood:FIN	☐ Enable	0 Packets/Second
Per-Source IP Flood:UDP	☐ Enable	0 Packets/Second
Per-Source IP Flood:ICMP	☐ Enable	0 Packets/Second
TCP/UDP PortScan	☐ Enable	Low Sensitivity
ICMP Smurf	☐ Enable	
IP Land	☐ Enable	
IP Spoof	☐ Enable	
IP TearDrop	☐ Enable	
PingOfDeath	☐ Enable	
TCP Scan	☐ Enable	
TCP SynWithData	☐ Enable	
UDP Bomb	☐ Enable	
UDP EchoChargen	☐ Enable	
Source IP Blocking	☐ Enable	0 Block time (sec)

4.4 QoS Setup

The QoS helps improving your network gaming performance by setting priorities for applications. By default the bandwidth control is disabled and the application priority is not specified.

In order to complete these settings, please follow the steps below.

- Enable this function.
- Enter the total speed or choose automatic mode.
- Enter the IP address of the user which you'd like to control.
- Specify how to control the PC with this IP address: Maximum or minimum bandwidth, priority and its up/download speed.
- Click Add button to add this record to the control table, click OK button to make it effective.



QoS

Bandwidth Control

Status	☑ Enable	
Total Speed(KB/s)	Up [ ] Down [ ]	☑ Automatically

Add Rules

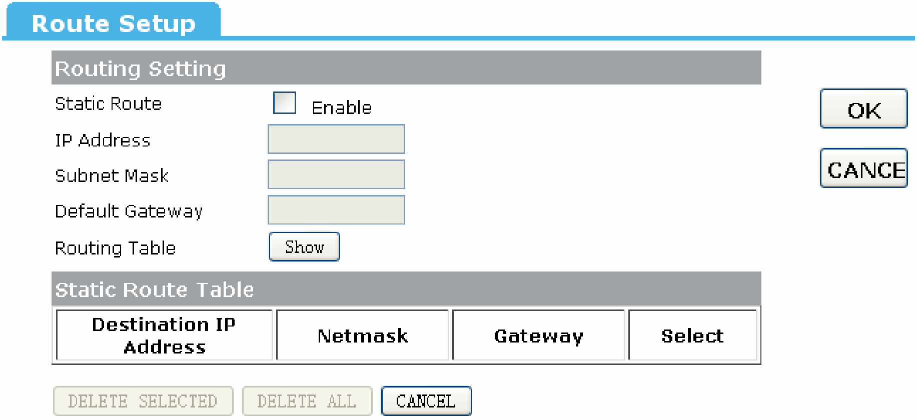
Hosts	● IP Address ○ All others
IP Address Range	192.168.1. 100 - 100
Mode	Limit the maximum bandwidth
Priority	High
Speed(KB/s)	Up 128 Down 256
Comment	test

Note: By MAC&IP binding, you can control bandwith according to MAC address; 1Mbps=1024Kbps=128KB/s.

IP Address Range	Mode	Priority	Up Speed	Down Speed	Comment	Selected
192.168.1.100-100	Limit the maximum bandwidth	High	128	256	test	○

4.5 Router Setup

A static route is a pre-determined pathway that the network information should travel to reach a specific host or network.



Route Setup

Routing Setting

Static Route □ Enable

IP Address

Subnet Mask

Default Gateway

Routing Table [Show]

Static Route Table

Destination IP Address	Netmask	Gateway	Select

Static Route: Click this box to enable the static route.

IP Address: The network or host IP address wished to be accessed.

Subnet Mask: The subnet mask of the destination IP.

Default Gateway: the router or host IP address where the network packet was originally sent. It must be on the same network segment with the WAN or LAN port.

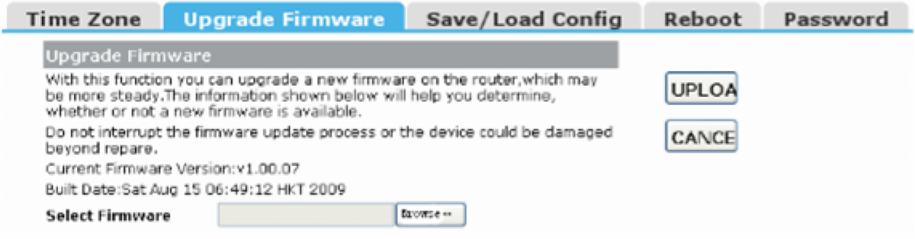
Routing Table: Clicking the Show button will let you see the whole routing table.

Static Route table: shows all the records in the static routing table. You can delete the selected record or all records at once.

4.6 System

4.6.1 Upgrade Firmware

You can upgrade the Firmware by selecting the file and pressing the button “upload”.



Upgrade Firmware

With this function you can upgrade a new firmware on the router,which may be more steady.The information shown below will help you determine, whether or not a new firmware is available.

Do not interrupt the firmware update process or the device could be damaged beyond repare.

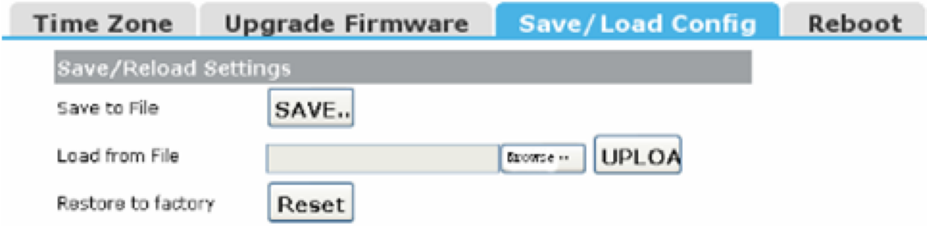
Current Firmware Version:v1.00.07

Built Date:Sat Aug 15 06:49:12 HKT 2009

Select Firmware

4.6.2 Save/Load Config

Here you can backup or restore the whole system configuration.



Save/Reload Settings

Save to File

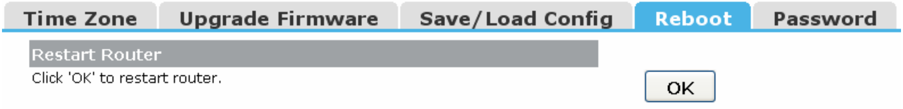
Load from File

Restore to factory

Save to File: Get the router's settings and store it on your local computer.
Load from File: Restore the settings from the file you saved before.
Restore to factory: Restore the system settings to the factory default.

4.6.3 Rebooting the device

You can reboot the device by clicking on the Reboot button.

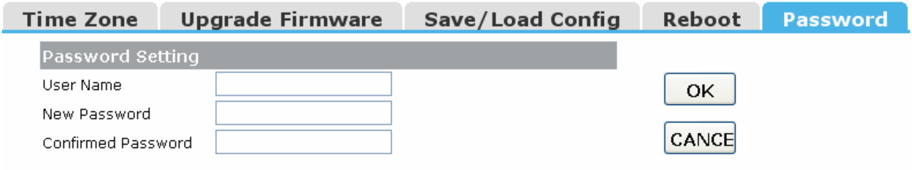


Restart Router

Click 'OK' to restart router.

4.6.4 Setting Password

To ensure the Router's security it is recommended to change the login and password after the first login.

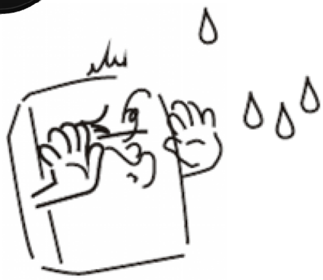


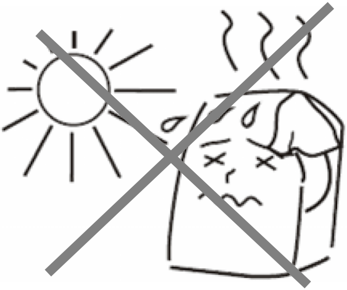
Password Setting

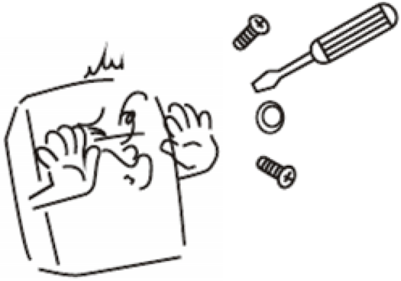
User Name

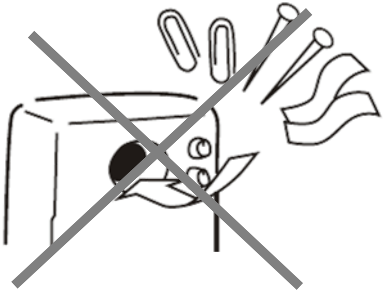
New Password

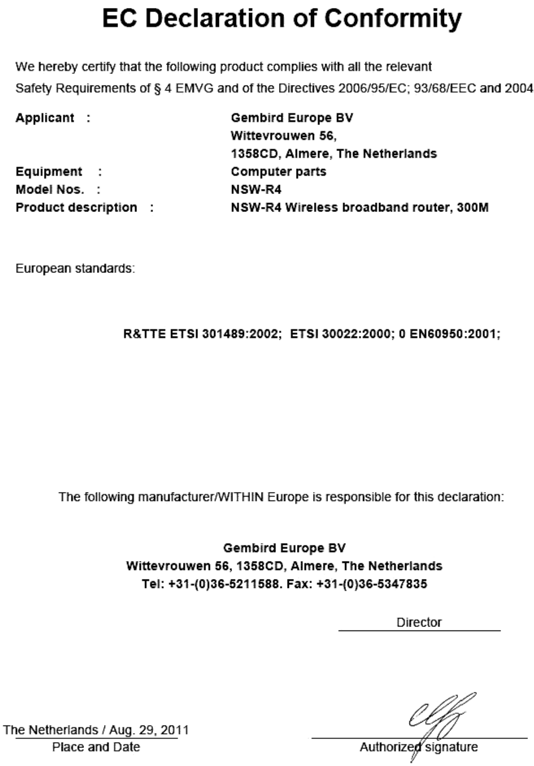
Confirmed Password











EC Declaration of Conformity

We hereby certify that the following product complies with all the relevant
Safety Requirements of § 4 EMVG and of the Directives 2006/95/EC; 93/68/EEC and 2004/108/EC.

Applicant :	**Gembird Europe BV** **Wittevrouwen 56,** **1358CD, Almere, The Netherlands**
Equipment :	**Computer parts**
Model Nos. :	**NSW-R4**
Product description :	**NSW-R4 Wireless broadband router, 300M**

European standards:

R&TTE ETSI 301489:2002; ETSI 30022:2000; 0 EN60950:2001;

The following manufacturer/WITHIN Europe is responsible for this declaration:

Gembird Europe BV
Wittevrouwen 56, 1358CD, Almere, The Netherlands
Tel: +31-(0)36-5211588. Fax: +31-(0)36-5347835

Director

The Netherlands / Aug. 29, 2011
Place and Date

Authorized signature

Waste disposal:

Do not deposit this equipment with the household waste. Improper disposal can harm both the environment and human health. For Information about waste collection facilities for used electrical and electronic devices, please contact your city council or an authorized company for the disposal of electrical and electronic equipment.

Entsorgungshinweise:

Werfen Sie dieses Gerät nicht in den Hausmüll. Unsachgemäße Entsorgung kann sowohl der Umwelt als auch der menschlichen Gesundheit schaden. Informationen zu Sammelstellen für Altgeräte erhalten Sie bei Ihrer Stadtverwaltung oder einer autorisierten Stelle für die Entsorgung von Elektro-und Elektronikgeräten.

Richtlijnen m.b.t. afvalverwerking

Batterijen en accu's dienen als klein-chemisch afval afgeleverd te worden bij toegewezen afvalverzamelpunten (zie www.afvalgids.nl). U dient ervoor te zorgen dat de batterijen/accu's leeg zijn en dus geen stroom meer kunnen leveren. Let op, de batterijen/accu's dienen onbeschadigd ingeleverd te worden.

Gooi dit product niet weg in uw vuilnisbak. Dit kan zowel het milieu als de menselijke gezondheid schade toebrengen. Informatie over het inleveren van dit product kunt u inwinnen bij uw gemeentelijke vuilnisdienst of andere geautoriseerde instelling in uw buurt.

Traitement des déchets:

Ne jetez pas cet appareil dans les déchets domestiques. Un traitement inapproprié peut être dommageable à l'environnement et à la santé humain.

Vous trouvez des informations sur les centres de rassemblement des appareils vieux chez l'administration municipale ou

chez un centre autorisé pour le traitement des appareils électriques ou électroniques.

WARRANTY CONDITIONS 🇪🇺	**GARANTIE BEDINGUNGEN** 🇩🇪 🇨🇭 🇦🇹
The warranty period is 36 months and begins with the sale to the end user. The receipt must clearly list the date of purchase and the part number, in addition it should be printed. Keep the receipt for the entire warranty period since it is required for all warranty claims. During the warranty period the defective items will be credited, repaired or replaced at the manufacturer's expense. Work carried out under the warranty neither extends the warranty period nor starts a new warranty period. The manufacturer reserves the right to void any warranty claim for damages or defects due to misuse, abuse or external impact (falling down, impact, ingress of water, dust, contamination or break). Wearing parts (e.g. rechargeable batteries) are excluded from the warranty. Upon receipt of the RMA goods, Gembird Europe B.V. reserves the right to choose between replacement of defective goods or issuing a credit note. The credit note amount will always be calculated on the basis of the current market value of the defective products	Die Garantie beträgt 36 Monate ab Verkaufsdatum an den Endverbraucher. Das Kaufdatum und der Gerätetyp sind durch eine maschinell erstellte Kaufquittung zu belegen. Bitte bewahren Sie Ihren Kaufbeleg daher für die Dauer der Garantie auf, da er Voraussetzung für eine eventuelle Reklamation ist. Innerhalb der Garantiezeit werden alle Mängel, wahlweise durch den Hersteller entweder durch Instandsetzung, Austausch mangelhafter Teile oder im Austausch, behoben. Die Ausführung der Garantieleistung bewirkt weder eine Verlängerung noch einen Neubeginn der Garantiezeit. Eine Garantieleistung entfällt für Schäden oder Mängel die durch unsachgemäße Handhabung oder durch äußere Einwirkung (Sturz, Schlag, Wasser, Staub, Verschmutzung oder Bruch) herbeigeführt wurden. Verschleißteile (z.B. Akkus) sind von der Garantie ausgenommen.
Gembird Europe B.V. Wittevrouwen 56, 1358CD Almere The Netherlands www.gembird.nl/support support@gmb.nl Tel. +31-36-5211588 (0900-4362473 inside The Netherlands, € 0,15 p/m, mobile costs not included)	GEMBIRD Deutschland GmbH Coesterweg 45, 59494 Soest Deutschland www.gembird.de/support support@gembird.de Tel. +49-180 5-436247 0,14 € pro Minute aus dem deutschen Festnetz. Mobilfunkpreise können abweichen

GARANTIE VOORWAARDEN	CONDITIONS DE GARANTIE
🇳🇱 🇧🇪 🇱🇺	🇫🇷
De garantietermijn bedraagt 36 maanden en gaat in op de aankoopdatum van het product door de eindgebruiker. Op de aankoopbon moeten de aankoopdatum en productomschrijving duidelijk vermeld staan. Gelieve de aankoopbon de gehele garantieperiode te bewaren, deze is ten alle tijden benodigd voor alle garantie aanspraken. Tijdens de garantieperiode zullen alle gebreken verholpen of vervangen worden door de fabrikant d.m.v. reparatie, omruiling van het defecte onderdeel of het gehele apparaat. Aanspraken tijdens de garantieperiode leiden niet tot verlenging hiervan. Garantieaanspraak vervalt bij schade of gebreken die ontstaan zijn door oneigenlijk gebruik, misbruik of invloeden van buitenaf (vallen, stoten, water, stof, vuil of breken). Slijtagegevoelige onderdelen (b.v. batterijen) zijn uitgesloten van garantie. Bij ontvangst van de RMA goederen behoudt Gembird zich het recht om te kiezen tussen vervanging van de defecte waren of het uitgeven van een kreditnota. Het bedrag van de kreditnota zal altijd gecalculeerd zijn op basis van de huidige marktprijs voor het defecte produkt.	Garantie est de 36 mois a partir de la date d’achat de l'utilisateur final. Le talon de garantie doit énumérer clairement la date d'achat et le type d'appareil. Conservez le reçu d'achat pendant toute la durée de la garantie car elle est nécessaire pour toute réclamation. Au cours de la période de garantie tous les défauts doivent être remplacé aux frais du fabricant, soit par la réparation ou la remplacement de la pièce défectueuse ou l'ensemble du produit. Les travaux effectués sous garantie ne prolongent pas la période de garantie ni ne commencent pas une nouvelle période de garantie. Le fabricant se réserve le droit d'annuler toute demande de garantie pour les dommages ou défauts dus à une mauvaise utilisation, abus ou les effets externes (chute, choc, pénétration de l'eau, la poussière, etc..). Les pièces d'usure (par exemple les piles rechargeables) sont exclus de la garantie. Dès réception de la marchandise sous garantie, le SAV de Gembird Europe BV se réserve le droit de choisir entre le remplacement des produits défectueux ou de délivrer un avoir. Le montant d’avoir sera toujours calculée sur la base de la valeur actuelle du marché des produits défectueux.
Gembird Europe B.V. Wittevrouwen 56, 1358CD Almere The Netherlands www.gembird.nl/support support@gmb.nl Tel. +31-36-5211588 € 0,15 p/m binnen Nederland Exclusief mobiele telefoonkosten	Gembird Europe B.V. Wittevrouwen 56 1358CD Almere, The Netherlands www.gembird.nl/support gembird@letmerepair.fr +33(0) 251 404849 Prix d'appel depuis telephone fixe Pays-Bas : 0.15 euro / min Prix d'appel depuis telephone mobile / autre pays - selon operateur

ГАРАНТИЙНЫЙ ТАЛОН

1. Гарантийное обслуживание предоставляется в течение срока гарантии, при наличии правильно и четко заполненного гарантийного талона, и изделия в полной комплектации. Серийный номер и модель изделия должны соответствовать указанным в гарантийном талоне.
2. Гарантийное обслуживание представляет собой бесплатное устранение всех неполадок (ремонт), или замену изделия на новое (аналогичное).
3. Гарантия не распространяется на неисправности, вызванные следующими причинами:
- использование изделия не по назначению.
- нарушение условий эксплуатации, хранения или перевозки изделия, которые указаны в настоящей инструкции.
- подключение нестандартных или неисправных периферийных устройств, аксессуаров.
- механические повреждения, попадание внутрь изделия посторонних предметов, веществ, жидкостей, насекомых.
- ремонт изделия не уполномоченными на то лицами.

4. Комплектность и внешний вид изделия проверяются Покупателем при получении товара в присутствии персонала фирмы.

Послепродажные претензии по укомплектованности и внешнему виду не принимаются.

Наименование изделия: ___________________________

Модель ____

Серийный номер _________________________________

Срок гарантии ___________________________________

Дата продажи «____» __________________ 20____ года

Фирма-продавец: _________________________________
Адрес и телефон фирмы-продавца:

____

М.П. С условиями гарантии ознакомлен и согласен:

Продавец: _____________ Покупатель: _____________

УМОВИ ГАРАНТІЙНОГО ОБСЛУГОВУВАННЯ

1. Гарантійне обслуговування надається протягом терміну гарантії, при наявності Гарантійного талону, заповненого належним чином, та виробу в повній комплектації.
2. Гарантійне обслуговування не підтримується в разі порушення правил експлуатації, зберігання або перевезення виробу, що зазначені в інструкції по експлуатації виробу.
3. Гарантійне обслуговування скасовується у випадках:
- наявності механічних пошкоджень або слідів стороннього втручання;
- пошкодження викликані стихійним лихом або нещасним випадком, включаючи й блискавку, потраплянням у виріб сторонніх предметів, рідин, комах, тощо;
- пошкодження викликані застосуванням або підключенням нестандартних або несправних периферійних пристроїв, аксесуарів;

4. Гарантія не поширюється на витратні матеріали та додаткові аксесуари;

З гарантійними умовами згоден.

Підпис покупця: ____________________

ГАРАНТІЙНИЙ ТАЛОН № __________________________

Товар/модель ___________________________________

Серійний номер _________________________________

Термін гаранії ___________________________________

Дата продажу ___________________________________

Продавець (назва, телефон)

____

Печатка та підпис продавця

____

З гарантійних питань звертайтесь до сервісних центрів Gembird. Про адреси та контакти Ви можете дізнатись на сайті www.gembird.ua або по телефону 044-4510213.