Wireless Broadband Router

User`s Manual

SOLARIS 300

Copyright Statement

NEXXT SOLUTIONS is the registered trademark of Nexxt Solutions LLC. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Nexxt Solutions LLC. Without the permission of Nexxt Solutions LLC, any individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages.

All the photos and product specifications mentioned in this manual are for references only. As the upgrade of software and hardware, there will be changes. And if there are changes, Nexxt is not responsible for informing in advance. If you want to know more about our product information, please visit our website at www.nexxtsolutions.com.

Contents

Chapter 1 Introduction

Thank you for purchasing NEXXT SOLARIS 300 11N Wireless Broadband Router!

SOLARIS 300 utilizes advanced MIMO technology and increases over 8 times transmission range of ordinary 802.11g products. Compatible with IEEE802.11n (Draft 4.0) and IEEE802.11g/b standards, it can provide up to 300Mbps stable transmission rate. Additionally, it includes router, wireless access point, four-port switch and firewall in one, dedicated to SOHOs (Small Office/Home Office) and family networking.

It supports WDS (Wireless Distribution System) function for repeating and amplifying the signals to extend the wireless network coverage. Besides, the Router also supports all of the latest wireless security features, such as 64/128-bit WEP, WPA, WPA2, WPA&WPA and WPS (PBC and PIN) encryption methods, packet filtering and port forwarding, to prevent unauthorized access and protect your network against malicious attack.

In addition, URL and MAC address filtering can take it easy for parents and network administrator to manage network life and QoS bandwidth control over specific computer's downloading speed is supported as well. Moreover, UPnP and WMM support can smooth your MSN voice better, and the included Setup Wizard on CD-ROM will be easy and fast for non-savvy users to install the device and access to the Internet.

1.1 Product Features

- Includes router, wireless access point, four-port switch and firewall in one
- Provides up to 300Mbps uploading and downloading speed
- Supports two WPS (Wi-Fi Protected Setup) encryption methods: PBC and PIN
- Compliant to IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3 and IEEE802.3u standards
- Supports over 8 times transmission range of 11G products
- Supports 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- Supports RTS/CTS protocol and data partitioning function
- Provides one 10/100Mbps Auto-Negotiation Ethernet WAN port
- Provides four 10/100Mbps Auto-Negotiation Ethernet LAN ports

- Supports xDSL/Cable MODEM, static and dynamic IP in community networking
- Supports remote/local Web management
- Supports WMM to better smooth your voice and video
- Supports SSID stealth mode and access control based over MAC address (up to 30 entries)
- Supports Auto MDI/MDIX
- Supports wireless Roaming technology for high-efficient wireless connections
- Supports auto negotiation/manual mode for 802.11b/802.11g/802.11n
- Supports UPnP and DDNS
- Supports Firefox 1.0, IE5.5 or above
- Supports SNTP
- Supports virtual server, DMZ host
- Built-in firewall for hacker's attack prevention
- Supports DHCP server/client
- Supports auto wireless channel selection
- Supports LAN access control to the Internet
- Provides syslog to record the status of the router
- Supports WDS wireless network extension
- Supports QoS function
- Detachable antennas provided

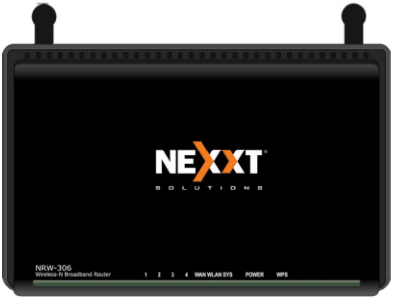
1.2 Package Contents

Please unpack the box and check the following items:

- One SOLARIS 300 11N Wireless Broadband Router
- One Quick Installation Guide
- One Power Adapter
- One CD-ROM
- Two detachable antennas

If any of listed items are missing or damaged, please contact the Nexxt Solutions LLC reseller from whom you purchased for replacement immediately.

1.3 LED Indicator and Port Description



Front Panel and LED Indicator Show

LED indicator description on front panel: (from L to R)

- **POWER**

  When turns orange, Always ON indicates the power connects well.

- **SYS**

  When turns orange, blinking indicates the system runs well.

- **WPS**

  When blinking, it indicates the device is negotiating with client in WPS mode.

- **WLAN**

  Wireless signal LED indicator. When turns orange, blinking indicates the wireless function is enabled.

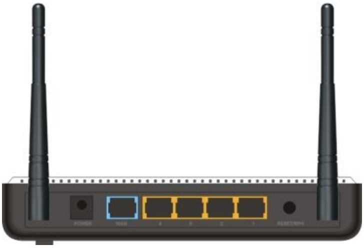
- **LAN (4,3,2,1)**

  Wired local network LED indicator. Always ON indicates it is connected with Ethernet device; blinking indicates the device is transmitting and/or receiving data.

- **WAN**

  Wide area network indicator. Always ON indicates the Router’s WAN Port.

Back Panel Show :



Rear Panel：（From L to R）

- **POWER**

  The jack is for power adapter connection. Please use the included 9V DC power adapter.

- **WAN**

  A 100Mbps Ethernet port, can be connected with MODEM, Switch, Router and other Ethernet device for Internet connecting to DSL MODEM, Cable MODEM and ISP.

- **LAN (1, 2, 3, 4)**

  4 10/100Mbps Ethernet ports can be connected with Ethernet switch, Ethernet router and NIC card.

- **RESET/WPS**

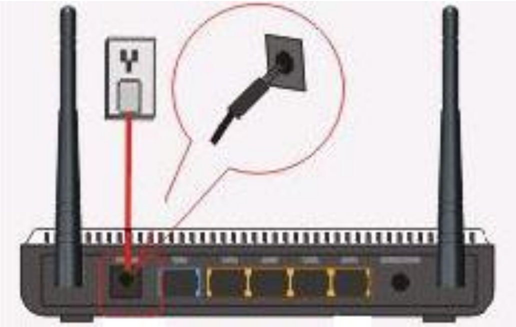
  The combination button for system reset and WPS features. Press this button for 7 seconds, the settings configured in this device will be deleted and it will restore the settings to the default one. Press it for one second, the WPS feature will be enabled.

Chapter 2 Hardware Installation

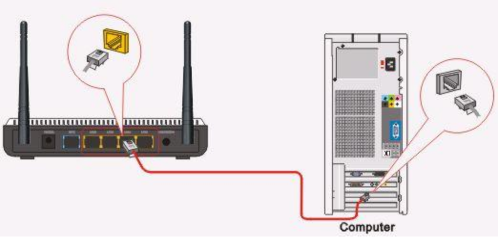
2.1 How to Install the Router

After you unpack the box, please follow the steps below to connect. For better wireless performance, please put the device in the middle of wireless coverage area.

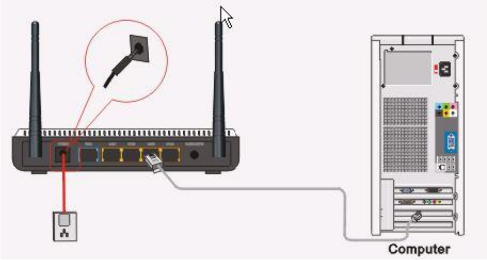
Please use the included power adapter to power on the Router. IMPORTANT: Use of a different power adapter could cause damage and voids the warranty for this product.



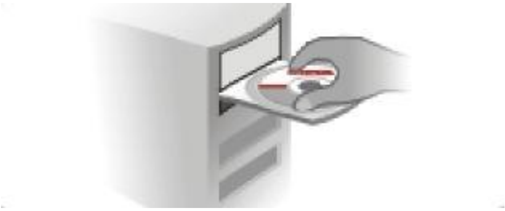
Please connect the LAN port of the Router to the network adapter of your computer with a cable.



Please connect your broadband line provided by your ISP to the WAN port.

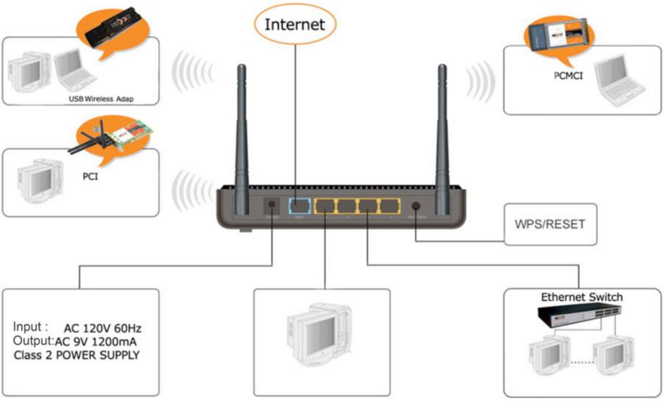


Insert the included CD-ROM into the CD-ROM drive, double click the “Setup” icon and follow the instructions to complete the installation. Or you can enter the Router’s Web page to configure it. (More details please refer to Chapter 3.)



2.2 Network Application Plan

Usually wireless LAN Network is deployed in a planned environment where each access point is located in a steady place with certain wireless coverage area for communication service. Generally speaking, it is in the center of the area to reduce “dead spot”.



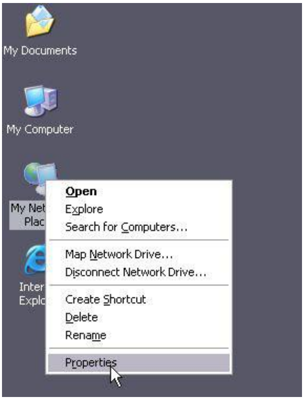
Chapter 3 How to Login to the Router

The chapter mainly presents how to enter the Router's Web page. After you have finished the hardware installation, the following steps will assist you to set the network configurations for your computer.

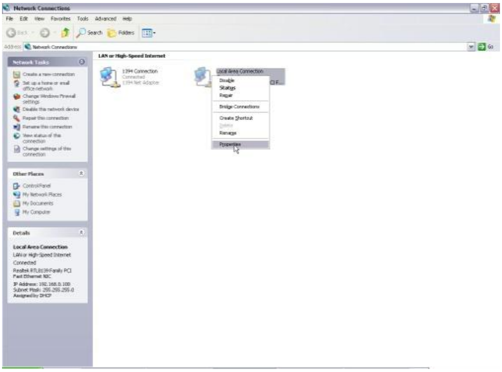
3.1 How to Set the Network Configurations

3.1.1 Windows XP Procedure

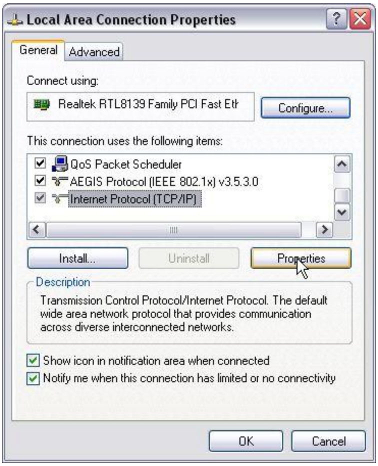
1. On your computer desktop right click "My Network Places" and select "Properties".



2. Right click "Local Area Network Connection" and select "Properties".



3 . Select "Internet Protocol (TCP/IP)" and click "Properties".



Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

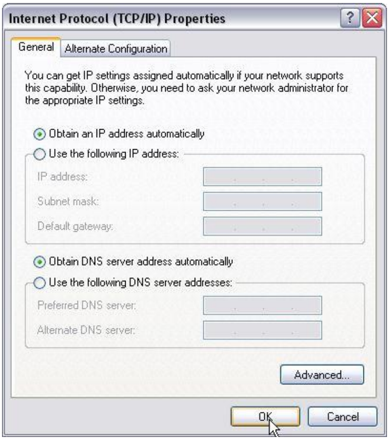
☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.5.3.0
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4 . Select "Obtain an IP address automatically" and "Obtain DNS server address automatically". Click "OK" to save the configurations.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

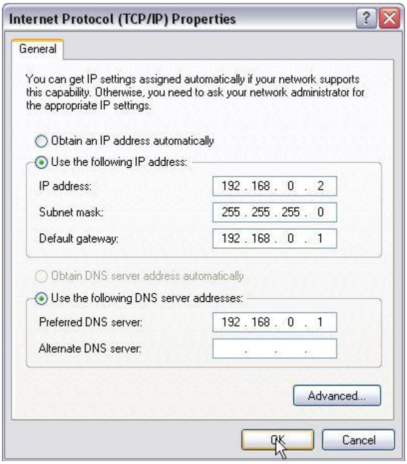
Or select "Use the following IP address" and enter the IP address, Subnet mask, Default gateway as follows:

IP Address: 192.168.0.XXX : (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

Certainly you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router's default gateway as the DNS proxy server. Click "OK" to save the configurations.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

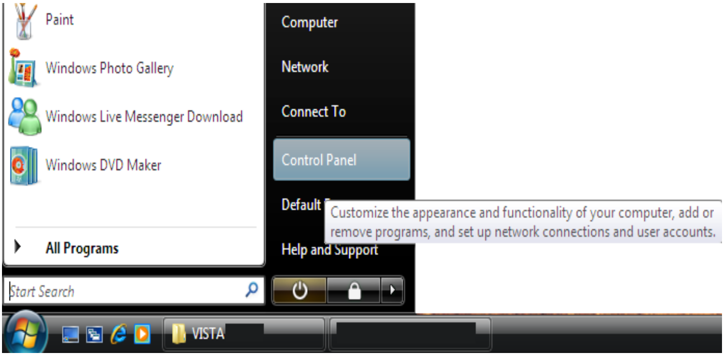
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

3.1.2 Windows Vista Procedure

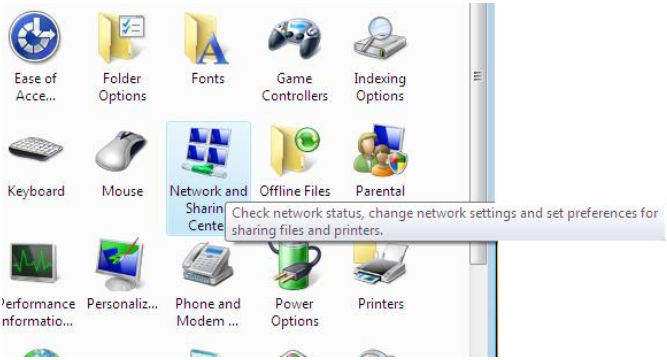
How to Set the Network Configurations

1. Click on the Vista Pearl, start button, then go to "Control Panel"



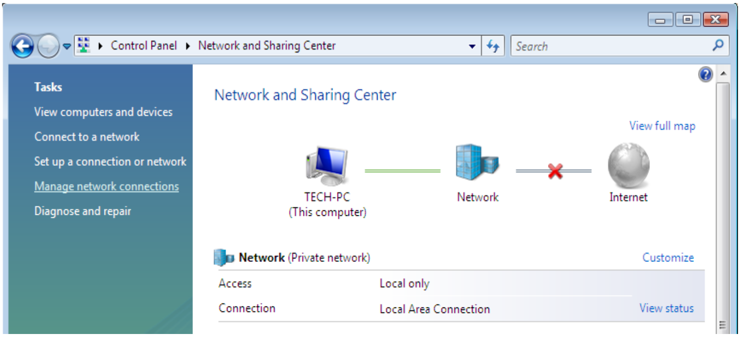
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

2. Go to the Network and Sharing Center icon,



Check network status, change network settings and set preferences for sharing files and printers.

then go to the "Manage network connections" on the left panel.

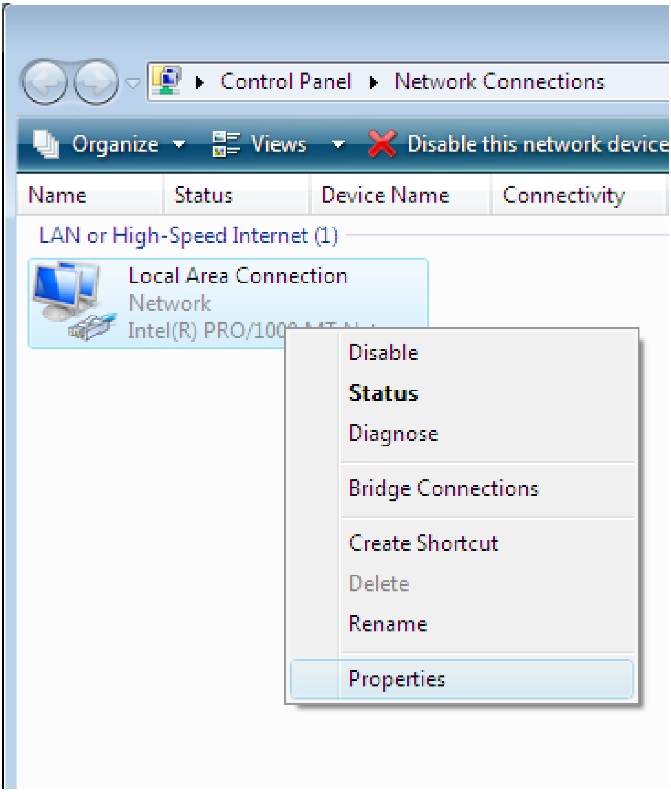

Control Panel ▸ Network and Sharing Center
Search
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
View full map
TECH-PC
(This computer)
Network
Internet
Customize
View status

Network (Private network)

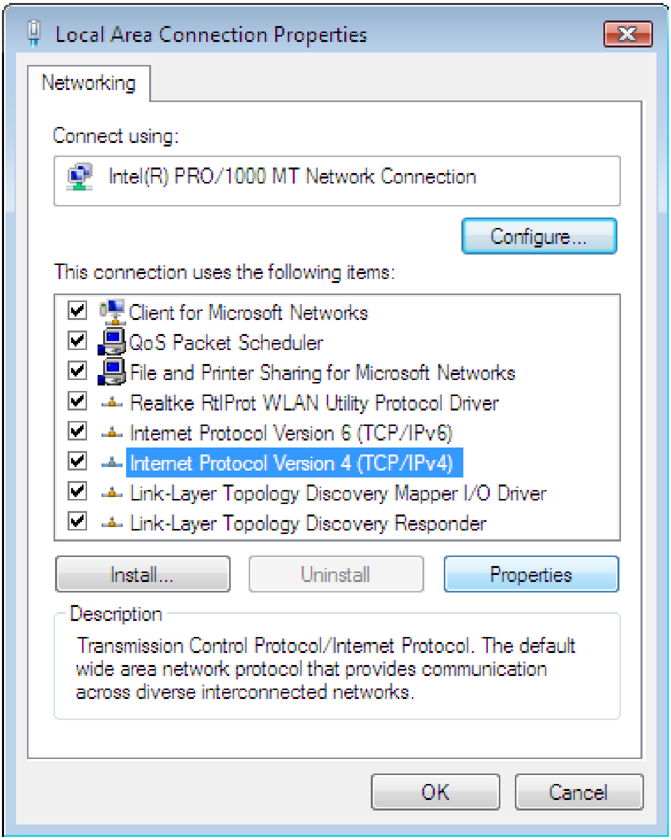
Access Local only

Connection Local Area Connection

3. On the “Local Area connection” option right click and select “properties”.



4. Select "Internet Protocol version 4(TCP/IPv4)" and click "Properties".



Connect using:

Intel(R) PRO/1000 MT Network Connection

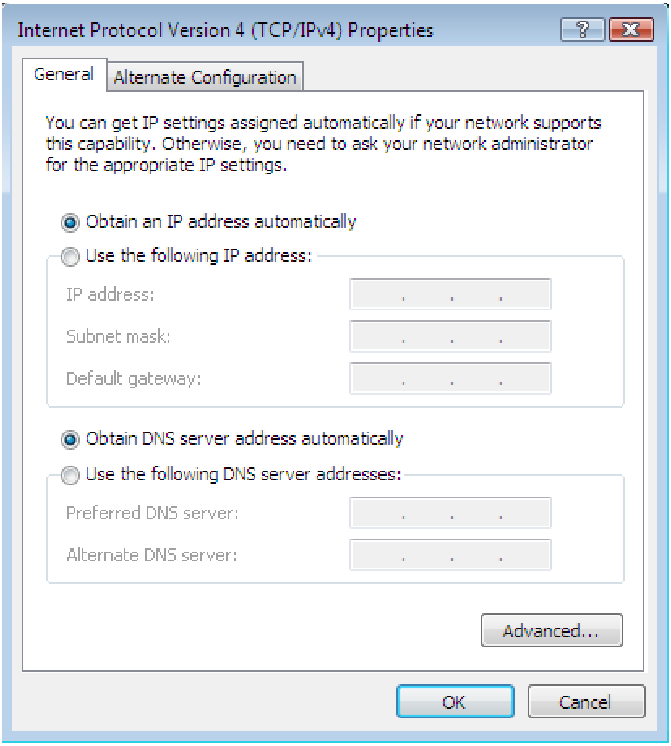
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Realtke RtlProt WLAN Utility Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically". Click "OK" to save the configurations.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

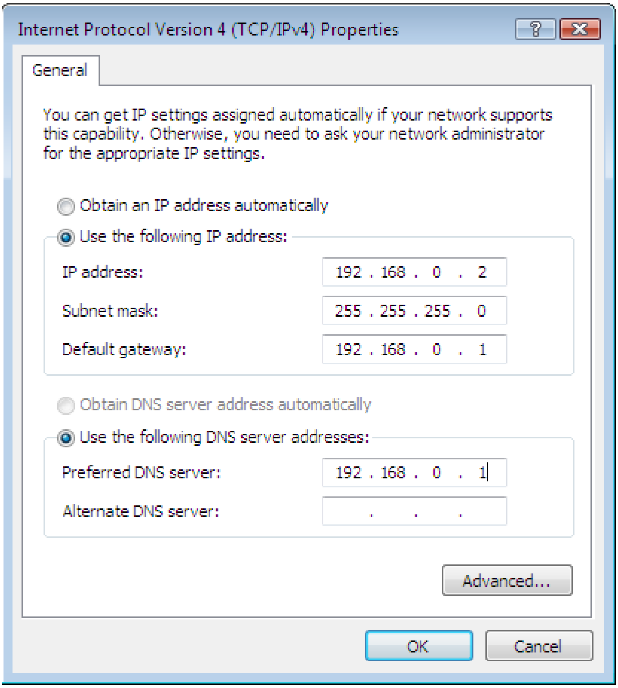
Or select "Use the following IP address" and enter the IP address, Subnet mask, Default gateway as follows:

IP Address: 192.168.0.XXX : (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

Certainly you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router's default gateway as the DNS proxy server. Click "OK" to save the configurations.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

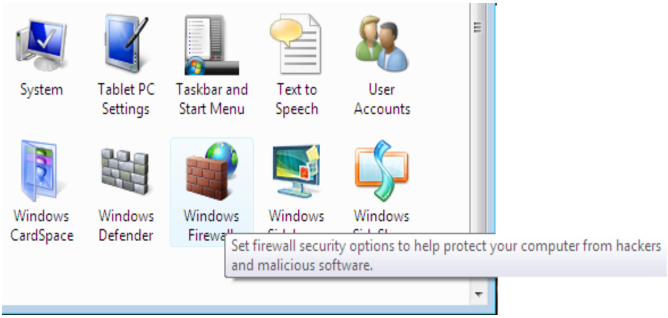
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

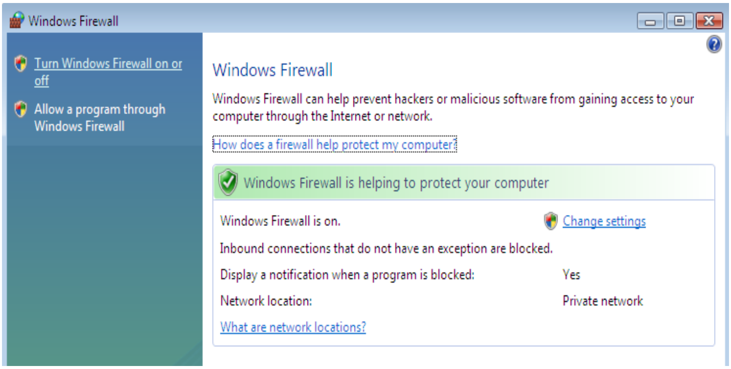
Notice: Sometimes Windows VISTA´s firewall blocks the connection to your router, to perform the above steps you need to disable the firewall during the process.

Go to "Control Panel" then select the option Windows Firewall



Set firewall security options to help protect your computer from hackers and malicious software.

Then on the left panel select "Turn Windows firewall on or off"


Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall

Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

How does a firewall help protect my computer?

Windows Firewall is helping to protect your computer

Windows Firewall is on. Change settings

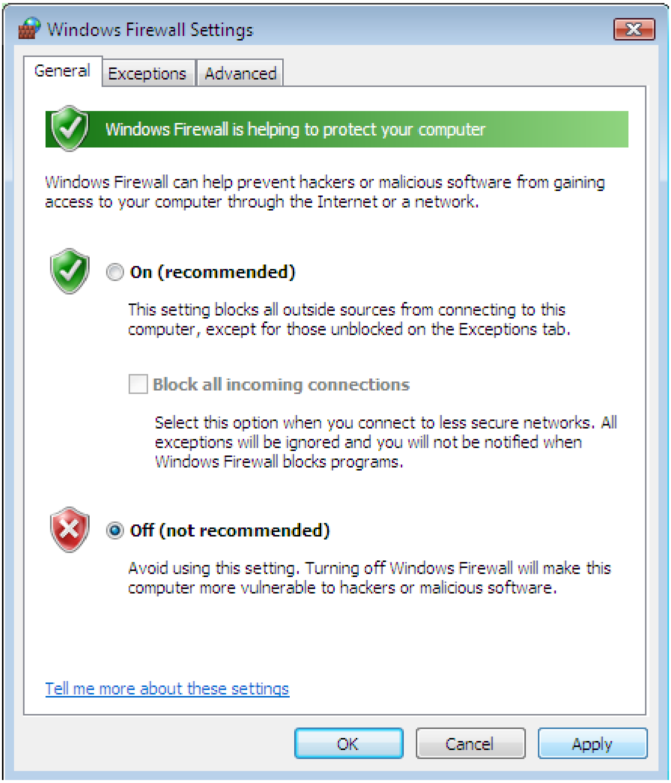
Inbound connections that do not have an exception are blocked.

Display a notification when a program is blocked: Yes

Network location: Private network

What are network locations?

Then select “OFF” and click apply and Ok.



Windows Firewall Settings

Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

○ **On (recommended)**

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

☐ **Block all incoming connections**

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

● **Off (not recommended)**

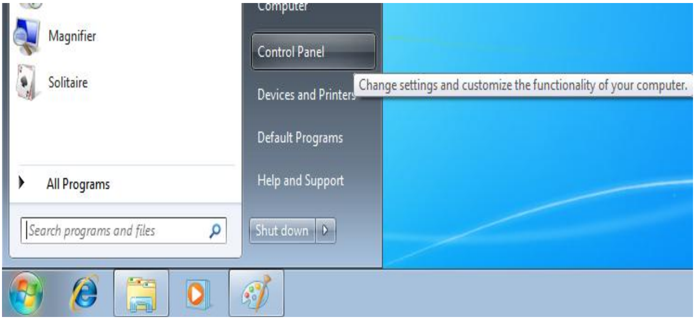
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings

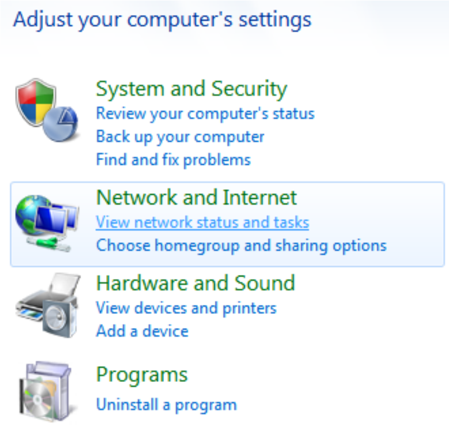
Remember to enable the firewall once you have finish installing your router.

3.1.3 Window 7 Procedure

How to Set the Network Configurations
1. Click on the Windows 7 start button, and then go to "Control Panel"



2. Go to the Network and Internet icon select option "View networks status and task",


Adjust your computer's settings

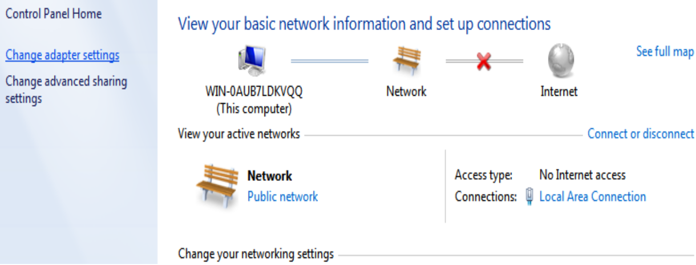
System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

then go to the “Change adapter settings” on the left panel



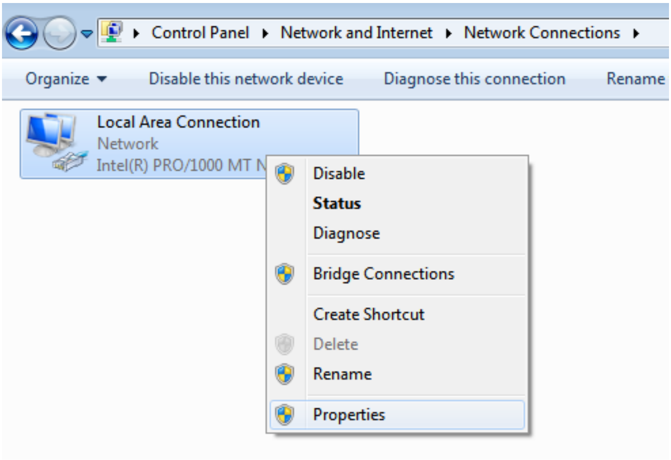
View your basic network information and set up connections

View your active networks

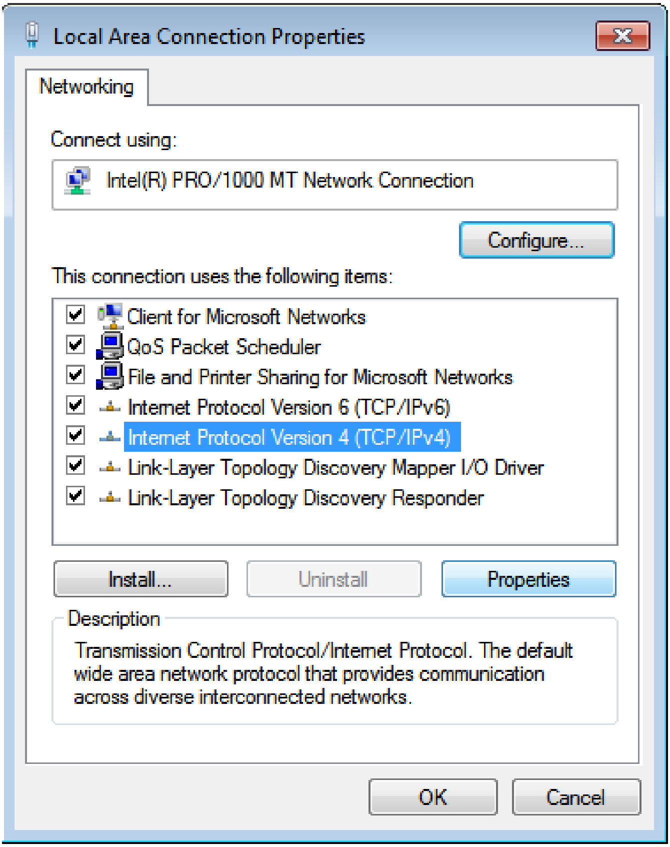
Network
Public network

Access type: No Internet access
Connections: Local Area Connection

3. On the “Local Area connection” option right click and select “properties”.



4. Select "Internet Protocol version 4(TCP/IPv4)" and click "Properties"



Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

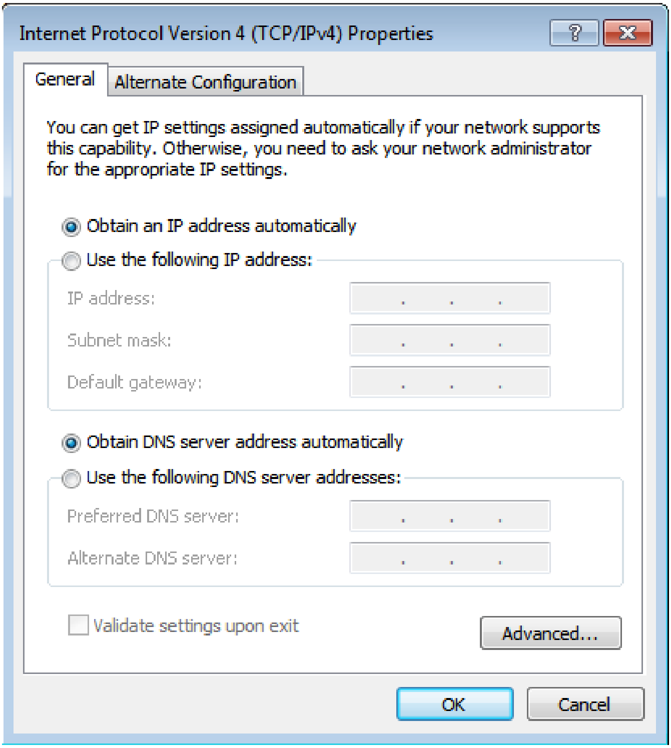
This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically". Click "OK" to save the configurations.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

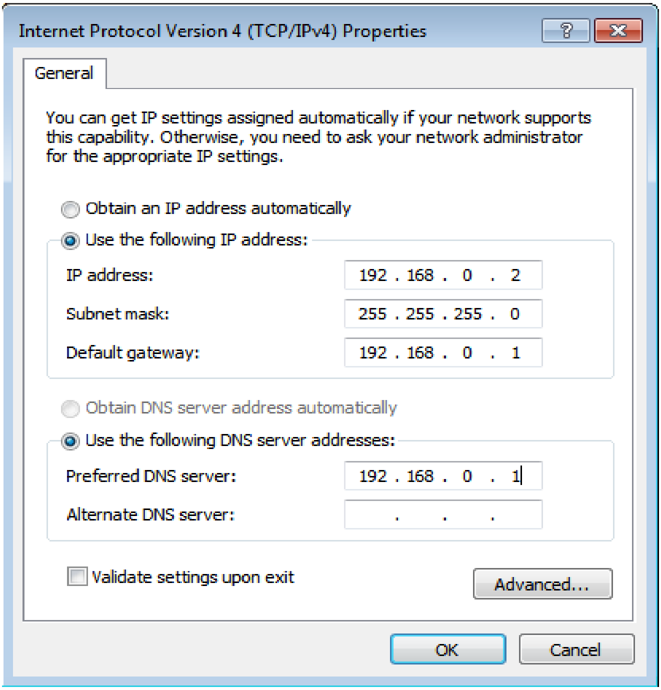
Or select "Use the following IP address" and enter the IP address, Subnet mask, Default gateway as follows:

IP Address: 192.168.0.XXX : (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

Certainly you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router's default gateway as the DNS proxy server. Click "OK" to save the configurations.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

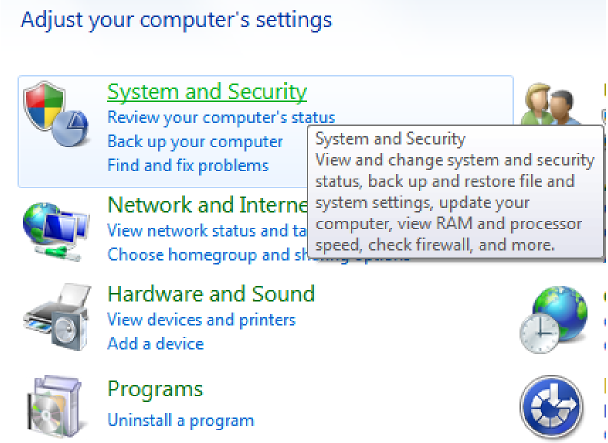
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Notice: Sometimes Windows 7 firewall blocks the connection to your router, to perform the above steps you need to disable the firewall during the process.
Go to "Control Panel" then select the option System and Security

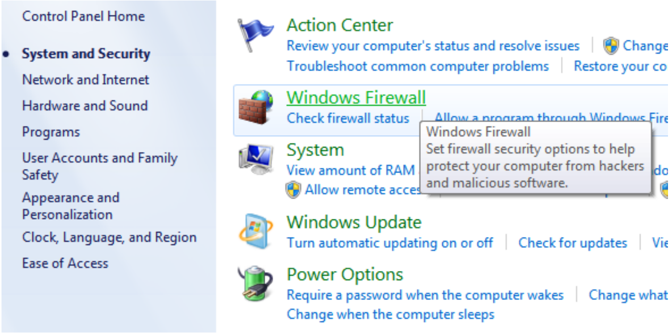


Adjust your computer's settings

System and Security
Review your computer's status
Back up your computer
Find and fix problems

System and Security
View and change system and security status, back up and restore file and system settings, update your computer, view RAM and processor speed, check firewall, and more.

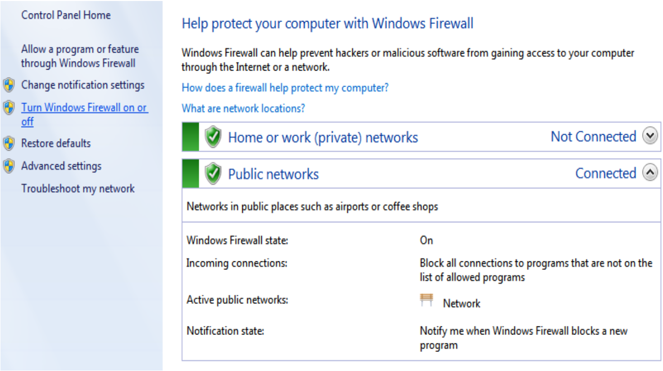
Then select "Windows Firewall"



Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change
Troubleshoot common computer problems
Restore your co
Windows Firewall
Check firewall status
Allow a program through Windows Fire
System
View amount of RAM
Allow remote acces
Windows Update
Turn automatic updating on or off
Check for updates
Vie
Power Options
Require a password when the computer wakes
Change what
Change when the computer sleeps

Windows Firewall
Set firewall security options to help protect your computer from hackers and malicious software.

Then on the left panel select "Turn Windows firewall on or off"



Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

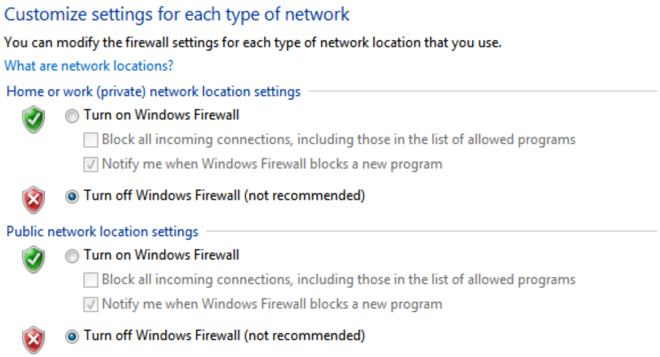
Home or work (private) networks — Not Connected

Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Then select "OFF" on both options and click Ok.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

○ Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

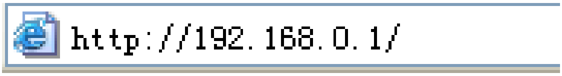
● Turn off Windows Firewall (not recommended)

Remember to enable the firewall once you have finish installing your router.

3.2 Login to the Router

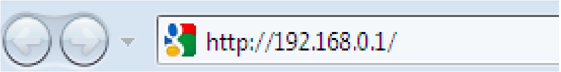
1 . To access the Router's Web-based interface, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, http://192.168.0.1. Press "Enter".

Windows XP:



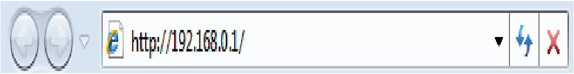
http://192.168.0.1/

Windows Vista:



http://192.168.0.1/

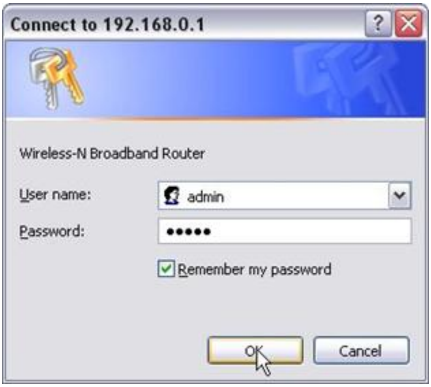
Windows 7:



http://192.168.0.1/

2. Input the "admin" in both User Name and Password. Click "OK".

Windows XP:



Connect to 192.168.0.1

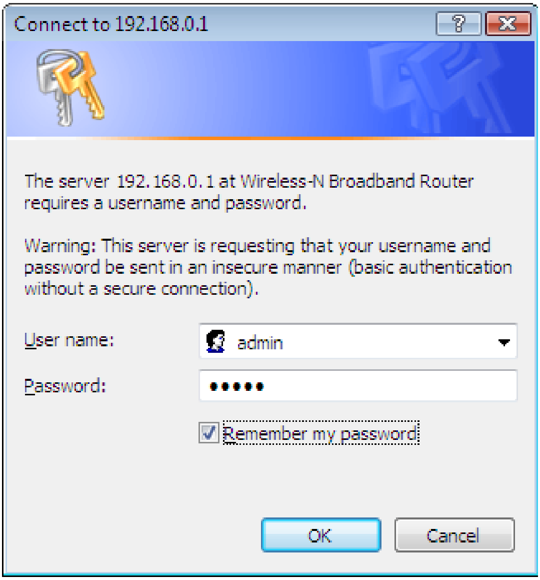
Wireless-N Broadband Router

User name: admin

Password: •••••

☑ Remember my password

Windows Vista:



Connect to 192.168.0.1

The server 192.168.0.1 at Wireless-N Broadband Router requires a username and password.

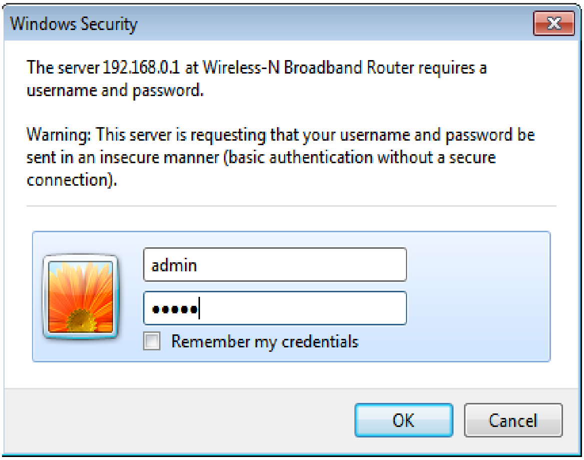
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

☑ Remember my password

Windows 7:



The server 192.168.0.1 at Wireless-N Broadband Router requires a username and password.

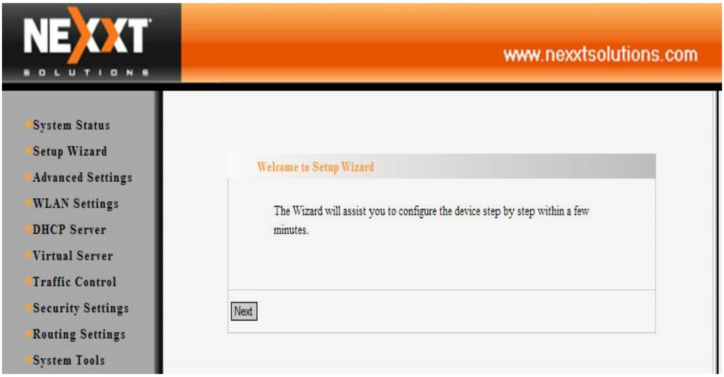
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

•••••

☐ Remember my credentials

3. If you enter the correct user name and password, the screen will show as follows:



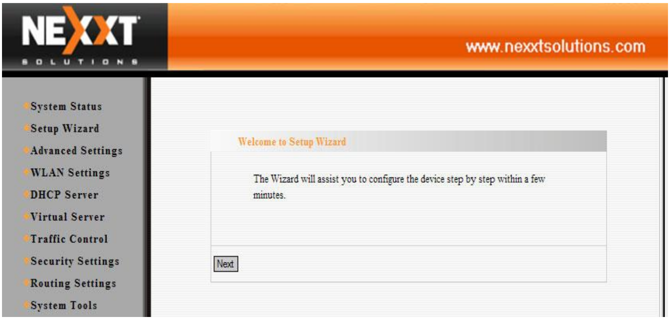
The Wizard will assist you to configure the device step by step within a few minutes.

Chapter 4 Quick Setup Guide

This chapter deals with how to access the Internet quickly. Please follow this guide to connect your Router to the Internet.

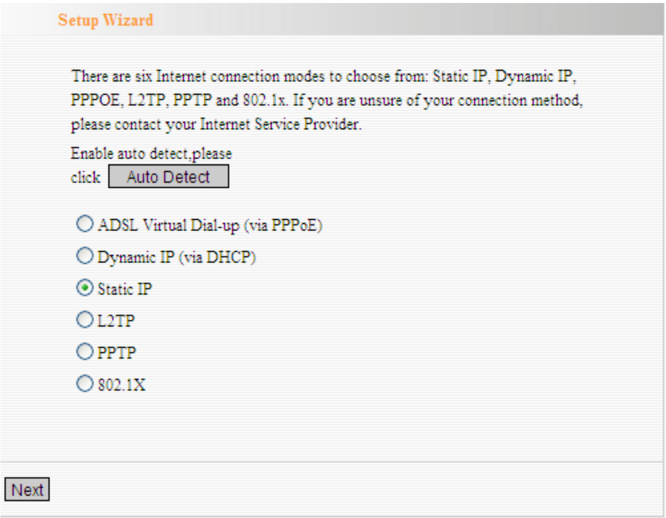
4.1 Setup Wizard

Here is the “Welcome to Setup Wizard” for configuring your Router quickly. Click “Next”.



The Wizard will assist you to configure the device step by step within a few minutes.

In this screen, select one mode of your Internet connection you use. If you are not clear, press the “Detect” button or contact your Internet Service Provider, and click “Next”.



There are six Internet connection modes to choose from: Static IP, Dynamic IP, PPPOE, L2TP, PPTP and 802.1x. If you are unsure of your connection method, please contact your Internet Service Provider.

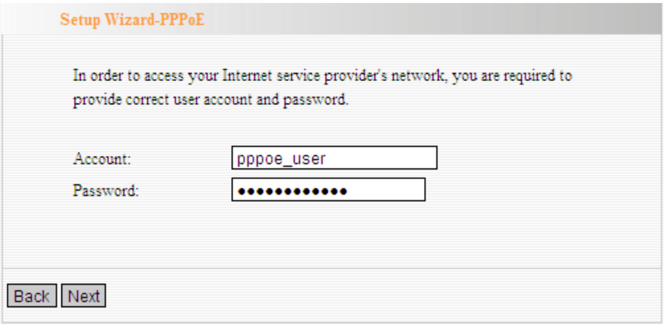
Enable auto detect,please click

○ ADSL Virtual Dial-up (via PPPoE)
○ Dynamic IP (via DHCP)
● Static IP
○ L2TP
○ PPTP
○ 802.1X

ADSL Virtual Dial-up (Via PPPoE)

Enter the Account and Password provided by your ISP, and click "Next".

For example :

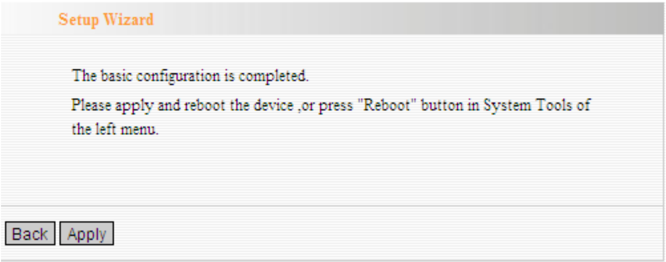


In order to access your Internet service provider's network, you are required to provide correct user account and password.

Account: pppoe_user
Password: ●●●●●●●●●●●●●

Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like other modes. Click "Next" and "Save" to finish the settings.



The basic configuration is completed.

Please apply and reboot the device ,or press "Reboot" button in System Tools of the left menu.

Static IP

In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click "Next".

For example :

ISP provides the following TCP/IP parameters as follows

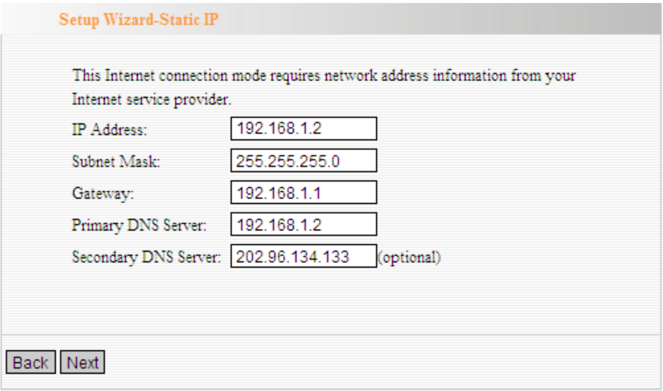
IP Address : 192.168.1.2

Subnet Mask : 255.255.255.0

Gateway : 192.168.1.1

Primary DNS Server : 202.96.128.86

Alternate DNS Server : 202.96.134.133

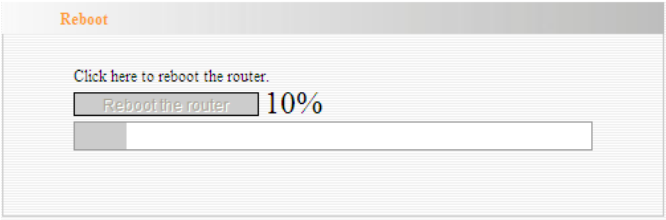


Setup Wizard-Static IP

This Internet connection mode requires network address information from your Internet service provider.

IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Primary DNS Server: 192.168.1.2
Secondary DNS Server: 202.96.134.133 (optional)

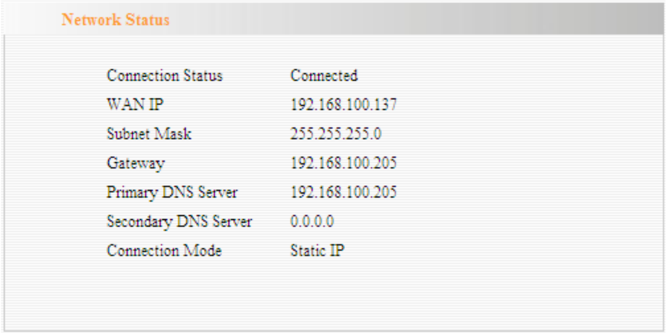
Click "Save" to complete the setup wizard. The Router will record the settings you made. To activate the settings, it is recommended to select "Reboot the Router" from "System Tool" of the left menu. It is rebooting now, please wait for a few minutes and **DO NOT** power it off.



Reboot

Click here to reboot the router.

Click the "System Status" in the left menu of the Web-based Utility to find out the current network and system information. If the "Connection Status" is "Connected", Congratulations you on completing the Router's basic settings. You are on the Internet now. If you want to configure more, please proceed to the following explanations for Advanced Settings.



Network Status

Connection Status	Connected
WAN IP	192.168.100.137
Subnet Mask	255.255.255.0
Gateway	192.168.100.205
Primary DNS Server	192.168.100.205
Secondary DNS Server	0.0.0.0
Connection Mode	Static IP

L2TP

L2TP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter L2TP username.

Password: Enter L2TP password.

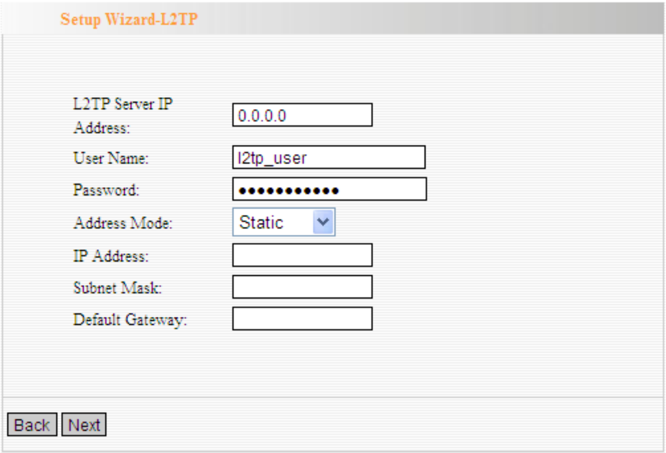
MTU: Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1400 is the default MTU.

Address Mode: Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the L2TP IP address supplied by your ISP.

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

Default Gateway: Enter the Default Gateway supplied by your ISP.



Setup Wizard-L2TP

L2TP Server IP Address: 0.0.0.0

User Name: l2tp_user

Password: ●●●●●●●●●●●

Address Mode: Static

IP Address:

Subnet Mask:

Default Gateway:

PPTP

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

User Name: Enter PPTP username provided by your ISP.

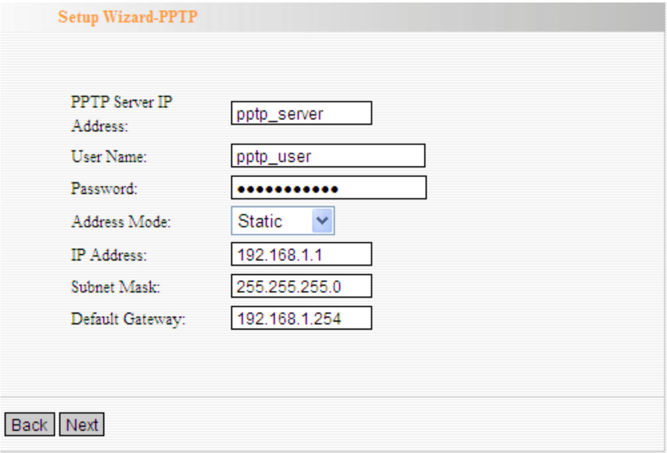
Password: Enter PPTP password provided by your ISP.

Address Mode: Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the PPTP IP address supplied by your ISP.

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

Default Gateway: Enter the Default Gateway supplied by your ISP.



PPTP Server IP Address: pptp_server

User Name: pptp_user

Password: ●●●●●●●●●●●

Address Mode: Static

IP Address: 192.168.1.1

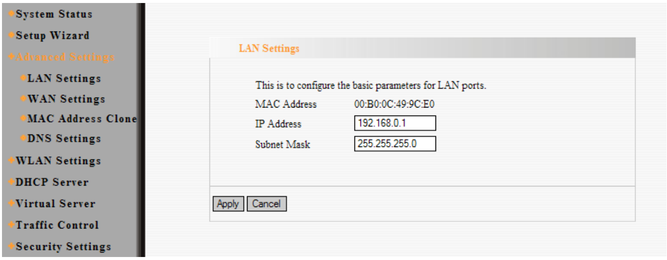
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Chapter 5 Advanced Settings

5.1 LAN Settings

LAN Settings are for the basic TCP/IP parameters of LAN ports.



This is to configure the basic parameters for LAN ports.

MAC Address 00:B0:0C:49:9C:E0

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

- **MAC Address:** The Router's physical MAC address as seen on your local network, which is unchangeable.
- **IP Address:** The Router's LAN IP address (not your PC's IP address). 192.168.0.1 is the default value.
- **Subnet Mask:** It shows the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value.

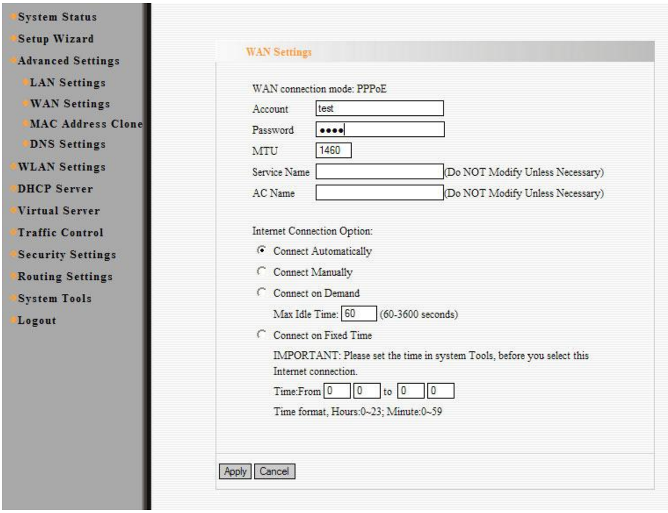
IMPORTANT:

Once you modify the IP address, you need to remember it for the Web-based Utility login next time.

5.2 WAN Settings

After you have selected the ISP connection type in "Setup Wizard" and you want to modify the related settings, here you can modify and configure the settings in details.

Virtual Dial-up (PPPoE)



WAN Settings

WAN connection mode: PPPoE

Account: test

Password: ••••

MTU: 1460

Service Name: (Do NOT Modify Unless Necessary)

AC Name: (Do NOT Modify Unless Necessary)

Internet Connection Option:

● Connect Automatically

○ Connect Manually

○ Connect on Demand

Max Idle Time: 60 (60-3600 seconds)

○ Connect on Fixed Time

IMPORTANT: Please set the time in system Tools, before you select this Internet connection.

Time:From 0 0 to 0 0

Time format, Hours:0~23; Minute:0~59

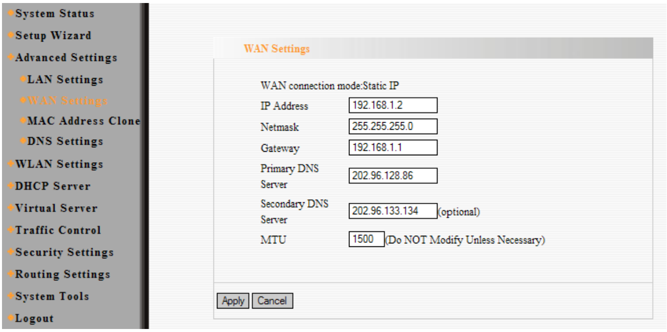
- **Connection Mode:** Show your current connection mode.
- **Account:** Enter the information provided by your ISP.

- **Password:** Enter the information provided by your ISP.
- **MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1492. Do NOT modify it unless necessary. But if when some specific website or web application software can not be open or enabled, have a try to change the MTU value as 1450, 1400, etc.
- **Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- **AC Name:** Enter it if provided. Do NOT modify it unless necessary.
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect Manually:** Connect to the Internet by users manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix.

Notice:

The "Connect on Fixed Time" can be deployed only when you have set the current time in "Time Settings" from "System Tools".

Static IP



WAN Settings

WAN connection mode:Static IP

IP Address: 192.168.1.2

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS Server: 202.96.128.86

Secondary DNS Server: 202.96.133.134 (optional)

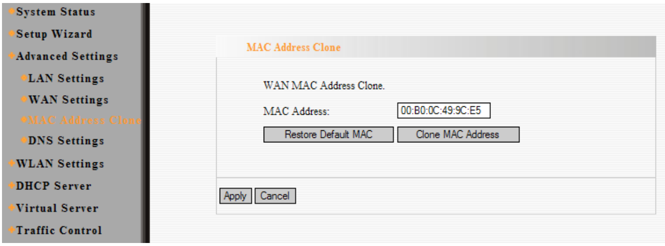
MTU: 1500 (Do NOT Modify Unless Necessary)

If the connection mode static IP is chosen, you can modify the following addressing information.

- **IP Address:** Here enter the WAN IP address provided by your ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask here.
- **Gateway:** Enter the WAN Gateway here.
- **Primary DNS Server:** Enter the Primary DNS server provided by your ISP.
- **Secondary DNS Server:** Enter the secondary DNS.
-

5.3 MAC Address Clone

This page is for the Router’s WAN MAC address.



WAN MAC Address Clone.

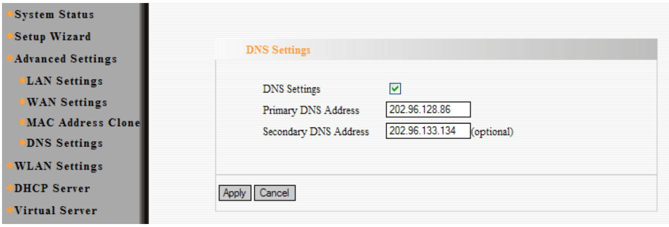
MAC Address: 00:B0:0C:49:9C:E5

Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

- **MAC Address:** The MAC address to be registered with your Internet service provider.
- **Clone MAC Address:** Register your PC's MAC address.
- **Restore Default MAC Address:** Restore to the default hardware MAC address.

5.4 DNS Settings

DNS is short for Domain Name System (or Service), an Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.



DNS Settings ☑

Primary DNS Address 202.96.128.86

Secondary DNS Address 202.96.133.134 (optional)

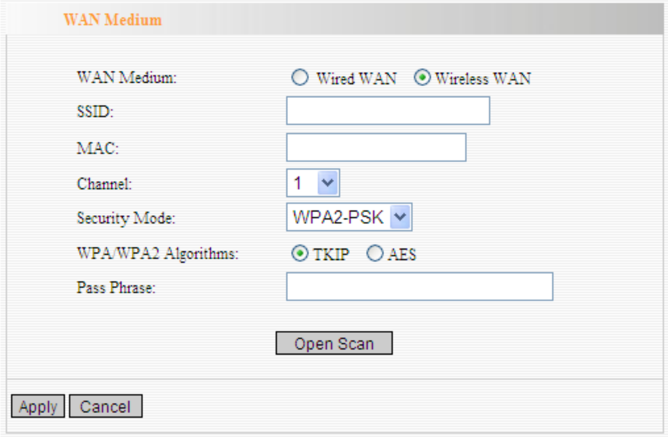
- **DNS:** Click the checkbox to enable the DNS server. The Router’s DHCP sever will answer the client’s requests and distribute DNS address.
- **Primary DNS Address:** Enter the necessary address provided by your ISP.
- **Secondary DNS Address:** Enter the second address if your ISP provides, which is optional.

Notice:

After the settings are completed, reboot the device to activate the modified settings.

5.5 WAN Media Type

In most cases, ISP provides wired WAN access (ADSL MODEM, Cable MODEM, etc.) and you only need to insert the line into the Router's WAN port. Sometime, wireless WAN access type, more flexible and convenient, is also provided by some ISP.



WAN Medium

WAN Medium: ○ Wired WAN ● Wireless WAN
SSID:
MAC:
Channel: 1
Security Mode: WPA2-PSK
WPA/WPA2 Algorithms: ● TKIP ○ AES
Pass Phrase:

- **Wired WAN:** In this type, WAN port should be connected by wired cable. This type is the device's default option.
- **Wireless WAN:** When your ISP provides wireless access service, you can enable this WAN access type.
- **SSID:** SSID (Service Set Identifier) is the ID name of the wireless device. You must input the correct

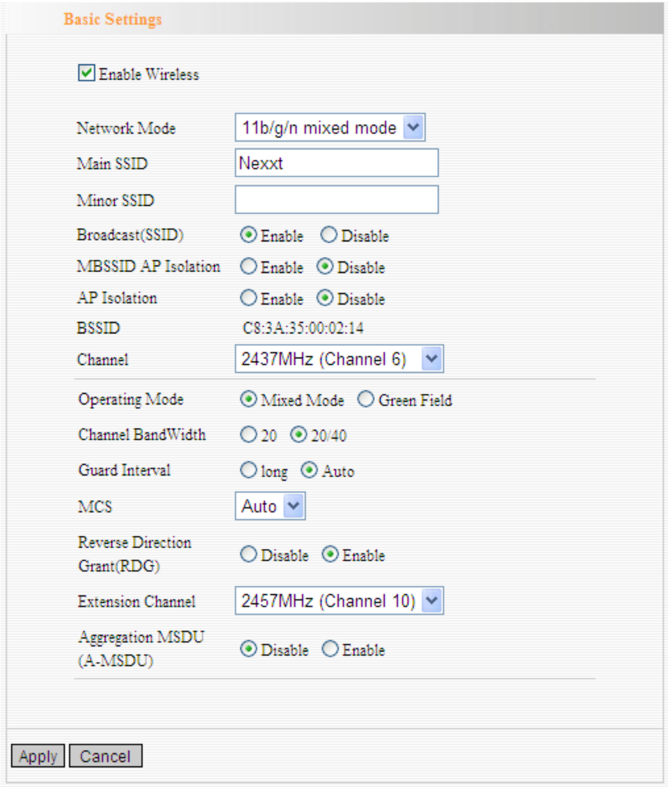
SSID and keep it the same SSID with your ISP's wireless device. Otherwise, it is not allowed to have access to your ISP network. Click "Open Scanner' to search the available SSID.

- **MAC:** Enter the MAC address of ISP wireless device. Click "Open Scanner" to search the MAC address.
- **Channel:** Wireless device's communication channel. Keep it the same channel with your ISP's wireless device. Click "Open Scanner' to search the available AP channel.
- **Security Mode:** If your ISP has set the security parameters, the receiving station must set the same security mode, encryption method and key with ISP's device.

If you know the ISP wireless device's SSID, enter the SSID, Wireless MAC address, Channel and Encryption method into the corresponding fields. Certainly you can click the "Open Scanner" button to fill these fields automatically. After you apply the settings, In "Setup Wizard" page select the corresponding WAN connection type to connect the Internet. For example: If your ISP wireless device provides Dynamic IP access type, you need to select "Dynamic IP (Via DHCP)".

Chapter 6 Wireless Setting

6.1 Basic Settings



Basic Settings

☑ Enable Wireless

Network Mode	11b/g/n mixed mode
Main SSID	Nexxt
Minor SSID	
Broadcast(SSID)	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	C8:3A:35:00:02:14
Channel	2437MHz (Channel 6)
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU (A-MSDU)	● Disable ○ Enable

- **Enable Wireless:** Check to enable the Router’s wireless features; uncheck to disable it.
- **Network Mode** : Select one mode from the

following. The default is 11b/g/n mode.

11b mode: Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.

11g mode: Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

11b/g mode: Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.

11b/g/n mode: Allow 11b/g/n-compliant client device to connect with the AP with auto-negotiation speed.

- **Main SSID**: SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- **Minor SSID**: It is optional.
- **Broadcast (SSID):** Select “Enable” to enable the device's SSID to be visible by wireless clients. The default is enabled.
- **MBSSID AP Isolation**: One access control feature based on wireless MAC address. When this feature is enabled, wireless clients connected with the same SSID can not communicate with each other. For example, configure main SSID as AP1,

minor SSID as AP2. PC1 and PC2 connect to AP1 via wireless adapter, and configure PC1 and PC2 in the same segment. After the feature is enabled, two PCs can not communicate and share network resource each other, but they can communicate with wireless clients connected with AP2. This feature is to isolate the communication of wireless clients connected with the same SSID.

- **AP Isolation:** One access control feature based on SSID. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. When this feature is enabled, wireless clients connected with the Main SSID and Minor SSID can not communicate with each other, which can secure the wireless network strongly. For example, configure main SSID as AP1, minor SSID as AP2. PC1 connects to AP1 via wireless adapter; PC2 connecting to AP2. After the feature is enabled, two PCs can not communicate and share network resource each other. This feature is to isolate the communication of wireless clients connected with different SSID.
- **Tip:** If you want to isolate all connected wireless client's communication, please enable MBSSID AP Isolation and AP Isolation simultaneously.
- **BSSID** : Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.

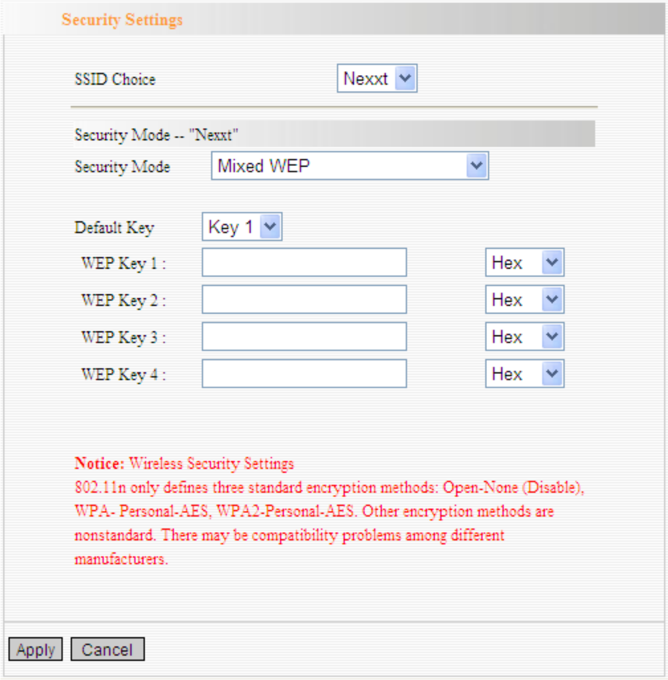
- **Channel**： Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- **Extension Channel** : To increase data throughput of wireless network, the extension channel range is used in 11n mode.
- **Channel Bandwidth** : Select the channel bandwidth to improve the wireless performance. When the network has 11b/g and 11n clients, you can select the 40M; when it is an 11n network, select 20/40M to improve its throughput.

6.2 Wireless Security Setting

It is used to configure the AP network's security setting. Here presents the common encryption methods, including Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window:

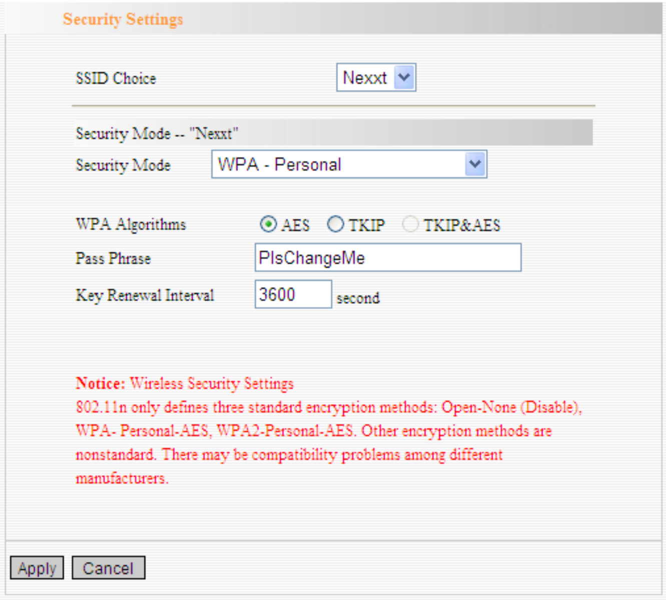


Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **Security Mode** : From the drop-down menu select the corresponding security encryption modes.
- **WEP Key1~4** : Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.
- **Default Key** : Select one key from the four configured keys as the current available one.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.



SSID Choice: Nexxt

Security Mode -- "Nexxt"

Security Mode: WPA - Personal

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Pass Phrase: PlsChangeMe

Key Renewal Interval: 3600 second

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

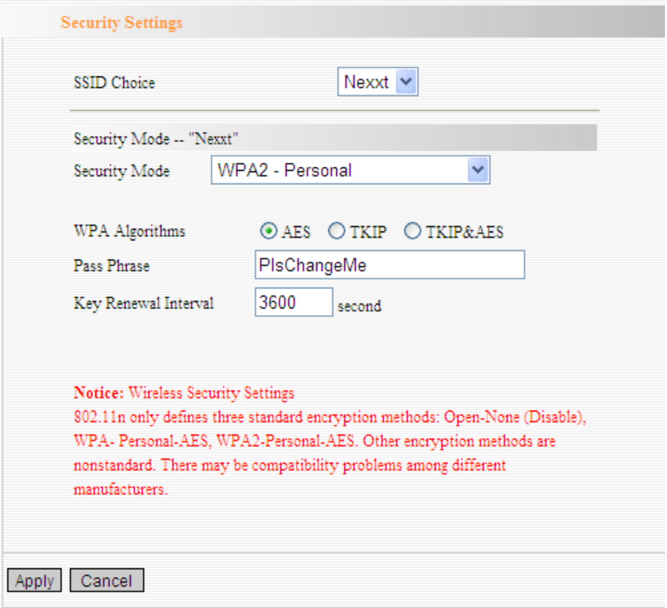
- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **WPA Algorithms** : Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption

Standard]. The default is TKIP mode.

- **Pass Phrase** : Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval** : Set the key's renewal period.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access).



SSID Choice: Nexxt

Security Mode -- "Nexxt"

Security Mode: WPA2 - Personal

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Pass Phrase: PlsChangeMe

Key Renewal Interval: 3600 second

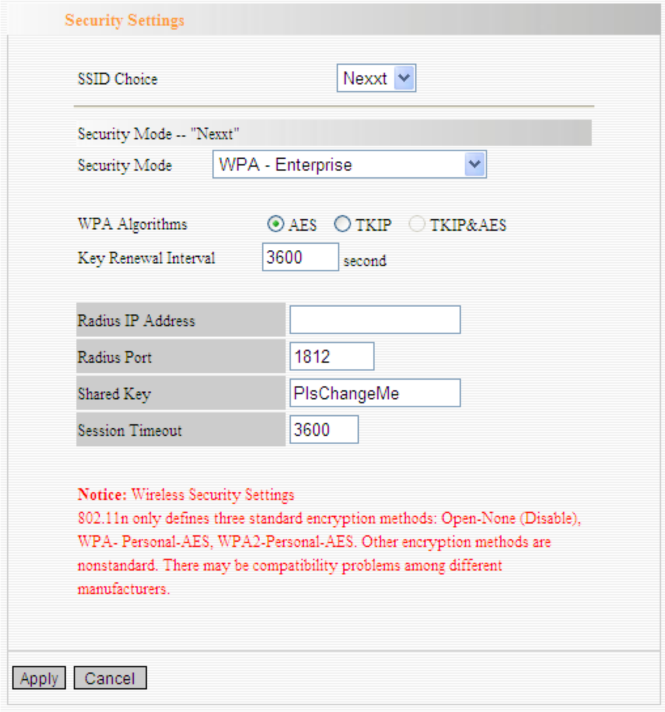
Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.

- **WPA Algorithms** : Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Pass Phrase** : Enter the encrypted characters with 8-63 ASCII characters.
- **Key renewal Interval** : Set the key's renewal period.

6.2.4 WPA- Enterprise

This security mode is used when a RADIUS server is connected to the device. Select "WPA-Enterprise" from the drop-down menu to enter the following window:



SSID Choice: Nexxt

Security Mode -- "Nexxt"

Security Mode: WPA - Enterprise

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Key Renewal Interval: 3600 second

Radius IP Address	
Radius Port	1812
Shared Key	PlsChangeMe
Session Timeout	3600

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

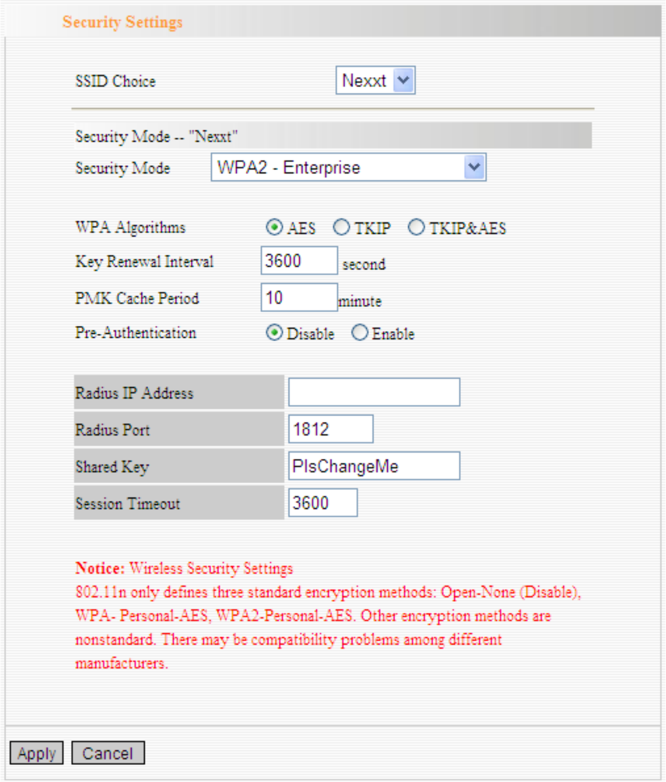
- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **WPA Algorithms** : Provides TKIP [Temporal Key

Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.

- **Key Renewal Interval** : Set the key’s renewal period.
- **Radius Server** : Enter the IP address of the Radius server.
- **Radius Server port** : Enter the authentication port of the Radius server. The default is 1812.
- **Shared Secret** : Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout** : The authentication interval period between AP and authentication server.

6.2.5 WPA2-Enterprise

This security mode is based on Radius authentication server and WPA2 encryption method. WPA2 is used when a RADIUS server is connected to the device. Select "WPA2-Enterprise" from the drop-down menu to enter the following window:



SSID Choice: Nexxt

Security Mode -- "Nexxt"

Security Mode: WPA2 - Enterprise

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Key Renewal Interval: 3600 second

PMK Cache Period: 10 minute

Pre-Authentication: ● Disable ○ Enable

Radius IP Address	
Radius Port	1812
Shared Key	PlsChangeMe
Session Timeout	3600

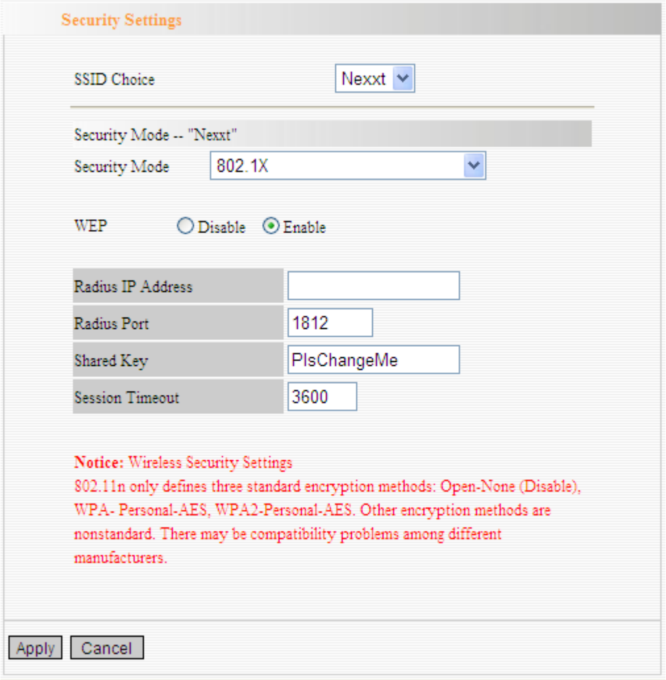
Notice: Wireless Security Settings

802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **WPA Algorithms** : Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Key Renewal Interval** : Set the key’s renewal period.
- **Radius Server** : Enter the IP address of the Radius server.
- **Radius Server port** : Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key** : Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout** : The authentication interval period between AP and authentication server. The default is 3600s.

6.2.6 802.1X

This security mode is used when a RADIUS server is connected to the device. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass. Select "802.1x" from the drop-down menu to enter the following window:



Security Settings

SSID Choice: Nexxt

Security Mode -- "Nexxt"

Security Mode: 802.1X

WEP ○ Disable ● Enable

Radius IP Address:

Radius Port: 1812

Shared Key: PlsChangeMe

Session Timeout: 3600

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **Select SSID** : Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **WEP** : Click "Enable/Disable" to enable or disable

the WEP algorithm.

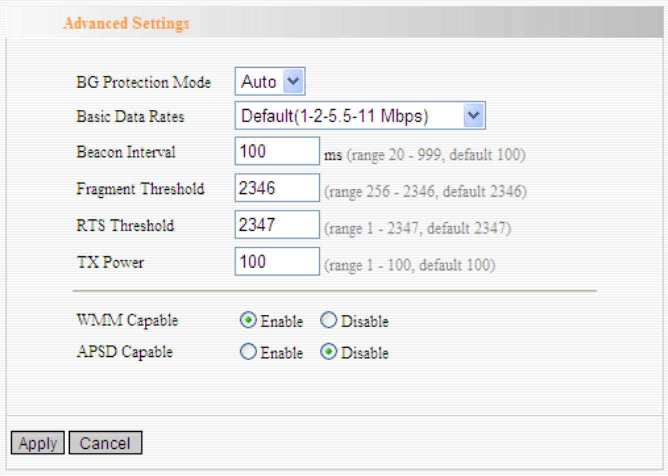
- **Radius Server** : Enter the IP address of the Radius server.
- **Radius Server Port** : Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key** : Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout** : The authentication interval period between AP and authentication server. The default is 3600s.

Note:

To improve security level, do not use too easy characters. If you are not familiar with these ten security modes, it is recommended to use “WPA-Personal” mode.

6.3 Advanced Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, etc.



Advanced Settings

BG Protection Mode: Auto
Basic Data Rates: Default(1-2-5.5-11 Mbps)
Beacon Interval: 100 ms (range 20 - 999, default 100)
Fragment Threshold: 2346 (range 256 - 2346, default 2346)
RTS Threshold: 2347 (range 1 - 2347, default 2347)
TX Power: 100 (range 1 - 100, default 100)

WMM Capable: ● Enable ○ Disable
APSD Capable: ○ Enable ● Disable

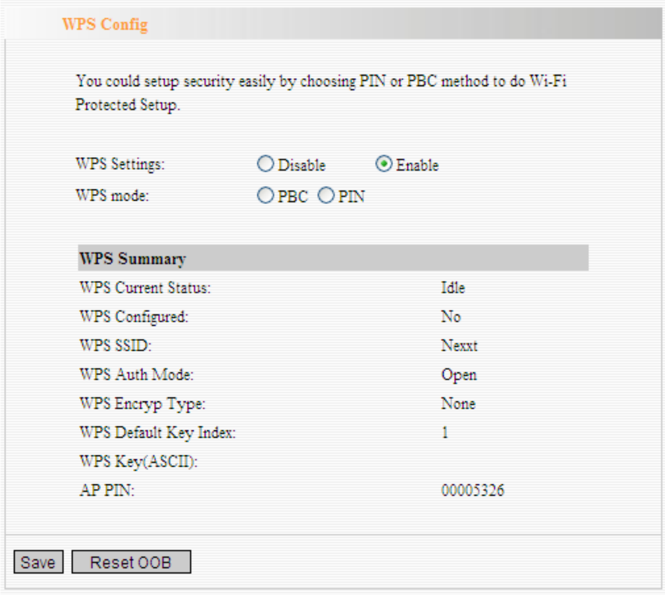
- **BG protection Mode:** Auto by default. It is for 11b/g wireless client to connect 11n wireless network smoothly in a complicated wireless area.
- **Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Here, default value is (1-2-5.5.-11Mbps…). It is recommended not to modify this value.
- **Beacon Interval:** Set the beacon interval of wireless radio. Default value is 100. It is

recommended not to modify this value.

- **Fragment Threshold:** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes. It is recommended not to modify this value.
- **RTS Threshold**: RTS stands for “Request to Send”. This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2346. It is recommended not to modify this value in SOHO environment.
- **TX Power:** Set the output power of wireless radio. The default value is 100.
- **WMM Capable:** It will enhance the data transfer performance of multimedia data when they’re being transferred over wireless network. It is recommended to enable this option.
- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

6.4 WPS Settings

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the device through encrypted contents. The users only enter PIN code or press WPS button on the panel to configure it without selecting encryption method and secret keys by manual. In the "Wireless settings" menu, click "WPS settings" to enter the next screen.



WPS Config

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Settings: ○ Disable ● Enable

WPS mode: ○ PBC ○ PIN

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	Nexxt
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII):	
AP PIN:	00005326

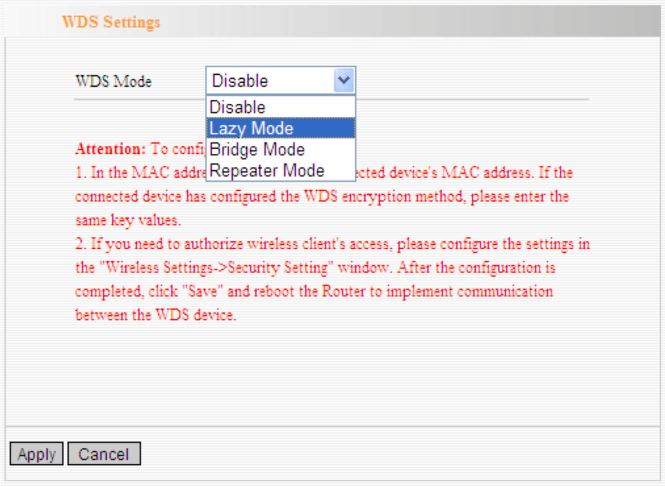
- **WPS settings**: To enable or disable WPS function. The default is "disable".

- **WPS mode** : Provide two ways: PBC (Push-Button Configuration) and PIN code.
- **PBC** : Select the PBC or press the WPS button on the front panel of the device for about one second (Press the button for about one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports up to 32 clients access.)
- **PIN** : If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client.
- **WPS Summary** : Show the current state of Wi-Fi protected setting, including authorized mode, encryption type, default key and other information.
- **WPS Current Status** : Idle means WPS in idle state. Start MSC process means the process has been started and waits for being connected. Configured means the negotiation is successful between server and clients.
- **WPS Configured** : "yes" means WPS feature is enabled and goes into effect. "not used" means it is not used. Usually the AP-security has been enabled, here will displayed "not used".
- **WPS SSID** : Show the main SSID set by WPS.

- **WPS Auth. Mode** : The authorization mode deployed by WPS, generally WPA/WPA2-personal mode.
- **WPS Encrypt Type** : The encryption type used by WPS, generally AES/TKIP.
- **WPS key** : The effective key generated by AP automatically.
- **AP PIN (KEY)** : The PIN code used by default.
- **Reset OOB** : When this button is pressed, the WPS client will be idle state, and WPS indicator will be turned off. AP will not respond the WPS client's requests and the set the security mode as WPA mode.

6.5 WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.



WDS Mode: Disable

Attention: To confi

1. In the MAC addre … cted device's MAC address. If the connected device has configured the WDS encryption method, please enter the same key values.

2. If you need to authorize wireless client's access, please configure the settings in the "Wireless Settings->Security Setting" window. After the configuration is completed, click "Save" and reboot the Router to implement communication between the WDS device.

Lazy: In this mode, the connected device can be Bridge mode or Repeater mode and enter the Router's BSSID to establish the connection.

Bridge: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table.

Repeater Mode : In this mode, add the opposing MAC address into each own AP MAC address table by manual or scanner to enlarge and extend the wireless radio.

Encrypt Type: Select one from WEP, TKIP, AES for security here.

Pass phrase: Enter the encrypted key for wireless devices.

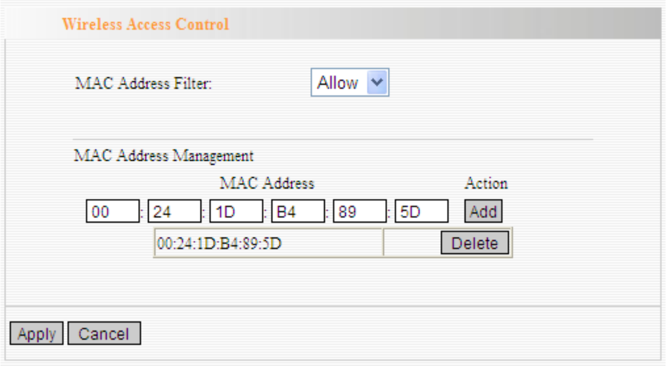
AP MAC: Input the MAC address of another (opposing) wireless router you want to connect.

⚠**NOTE:**

It is recommended that two wireless routers keep the same bandwidth, channel number, and security settings. Apply the settings and reboot the Router to activate it.

6.6 Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management to allow or block the specific clients to access the wireless network. Select "Wireless Setting->Access Control" to display the following screen:



Wireless Access Control

MAC Address Filter: Allow

MAC Address Management

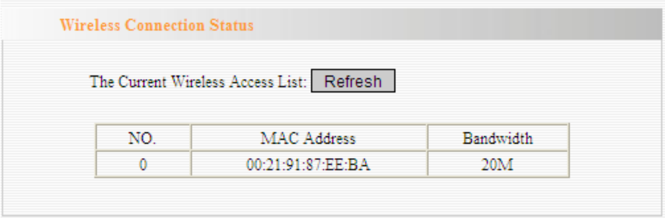
MAC Address	Action
00 : 24 : 1D : B4 : 89 : 5D	Add
00:24:1D:B4:89:5D	Delete

- **MAC Address Filter** : Enable/disable MAC address filter. Select "Close" to malfunction MAC address; "disable" to prevent the MAC addresses in the list from accessing the wireless network; "Allow" to allow the MAC address in the list to access the wireless network.
- **MAC Address Management** : Input the MAC address to implement the filter policy. Click "Add" to finish the MAC add operation.

- **MAC list** : Show the added MAC addresses. You can add or delete them.

6.7 Connection Status

This page shows wireless client's connection status, including MAC address, Channel bandwidth, etc. Select "Wireless Setting->connection status" to enter the following screen:



Wireless Connection Status

The Current Wireless Access List:

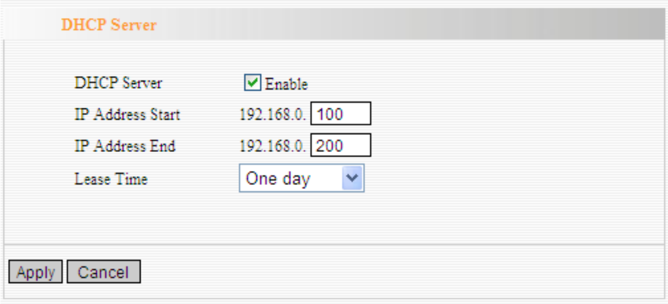
NO.	MAC Address	Bandwidth
0	00:21:91:87:EE:BA	20M

- **MAC Address** : Shows current MAC addresses of the hosts connecting to the Router.
- **Bandwidth** : Shows current bandwidth of the hosts (wireless client).

Chapter 7 DHCP Server

7.1 DHCP Settings

DHCP (Dynamic Host Control Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating "Obtain an IP Address Automatically". So specifying the starting and ending address of the IP Address pool is needed.



DHCP Server ☑ Enable

IP Address Start 192.168.0. 100

IP Address End 192.168.0. 200

Lease Time One day

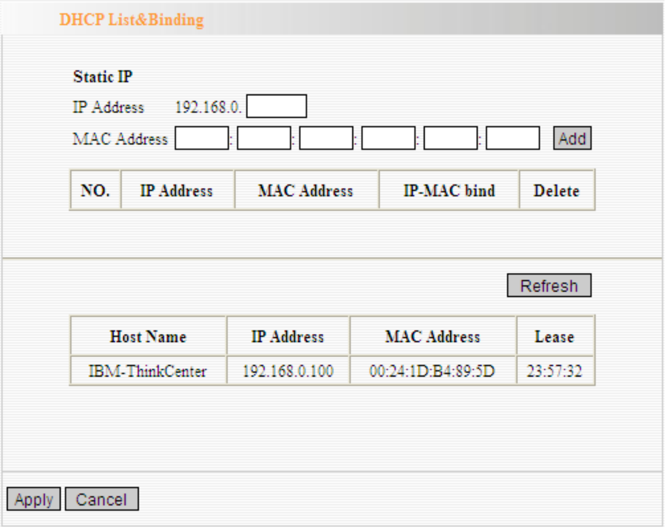
- **DHCP Server:** Activate the checkbox to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP address for DHCP server distribution.
- **Lease Time:** The length of the IP address lease.

For example :

If the lease time is an hour, then DHCP server will reclaim the IP address in each hour.

7.2 DHCP List and Binding

The Static IP assignment is to add a specifically static IP address to the assigned MAC address. You can view the related information in the DHCP server list.



NO.	IP Address	MAC Address	IP-MAC bind	Delete

Host Name	IP Address	MAC Address	Lease
IBM-ThinkCenter	192.168.0.100	00:24:1D:B4:89:5D	23:57:32

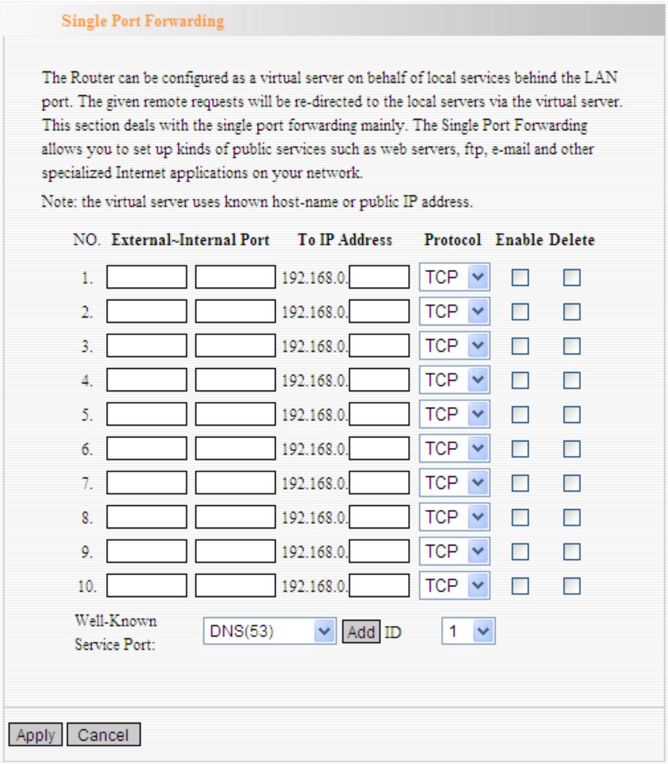
- **IP Address:** Enter the IP address which needs to be bound.
- **MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click “Add” to add the entry in the list.

- **Hostname:** The name of the computer which is added a new IP address.
- **Lease Time:** The left time length of the corresponding IP address lease.

Chapter 8 Virtual Server

8.1 Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.



Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port		To IP Address	Protocol	Enable	Delete
1.			192.168.0.	TCP	☐	☐
2.			192.168.0.	TCP	☐	☐
3.			192.168.0.	TCP	☐	☐
4.			192.168.0.	TCP	☐	☐
5.			192.168.0.	TCP	☐	☐
6.			192.168.0.	TCP	☐	☐
7.			192.168.0.	TCP	☐	☐
8.			192.168.0.	TCP	☐	☐
9.			192.168.0.	TCP	☐	☐
10.			192.168.0.	TCP	☐	☐

Well-Known Service Port: DNS(53)

- **External Port:** This is the external (WAN) port number for server or Internet application, for example, port 21 for ftp service.
- **Internal Port:** This is the port number of LAN computer set by the Router. The Internet traffic from the external port will forward to the internal port. For example : you can set the internal port NO.66 to act as the external port NO.21 for ftp

service.

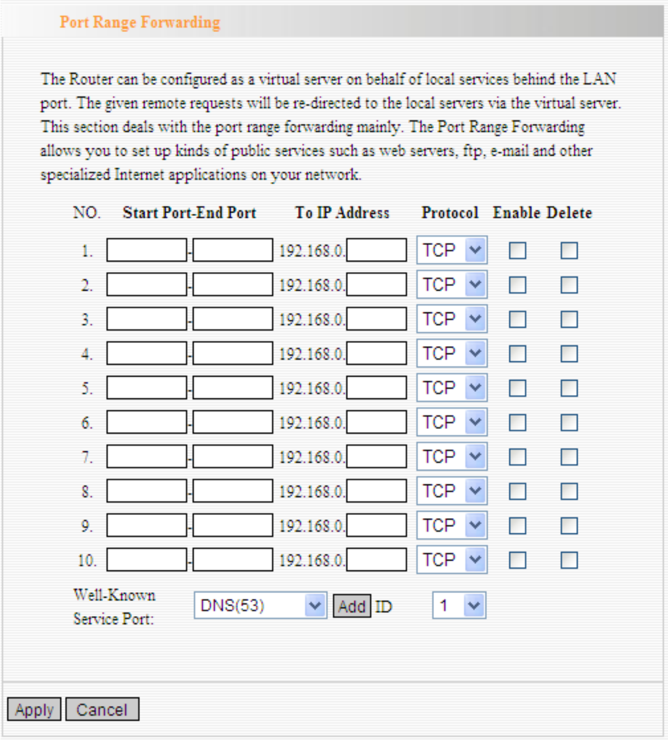
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:**Click to check it for corresponding operation.
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

⚠**NOTE:**

If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.2 Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.



Port Range Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.	-	192.168.0.	TCP	☐	☐
2.	-	192.168.0.	TCP	☐	☐
3.	-	192.168.0.	TCP	☐	☐
4.	-	192.168.0.	TCP	☐	☐
5.	-	192.168.0.	TCP	☐	☐
6.	-	192.168.0.	TCP	☐	☐
7.	-	192.168.0.	TCP	☐	☐
8.	-	192.168.0.	TCP	☐	☐
9.	-	192.168.0.	TCP	☐	☐
10.	-	192.168.0.	TCP	☐	☐

Well-Known Service Port: DNS(53) Add ID 1

- **Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.

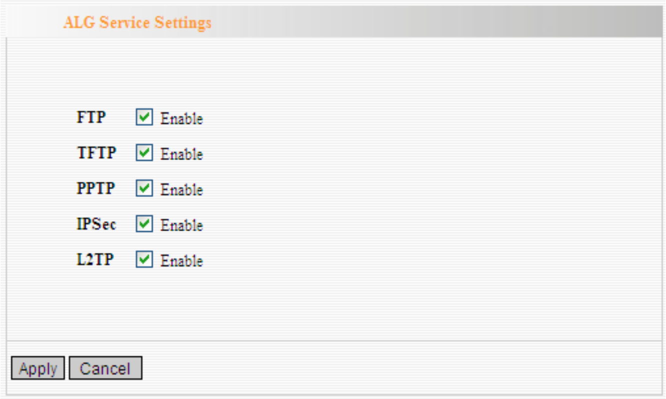
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Add:** Add the selected well-known port to the policy ID.

⚠**NOTE:**

If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.3 ALG Service Settings

In the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications etc.



ALG Service Settings

FTP ☑ Enable

TFTP ☑ Enable

PPTP ☑ Enable

IPSec ☑ Enable

L2TP ☑ Enable

In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

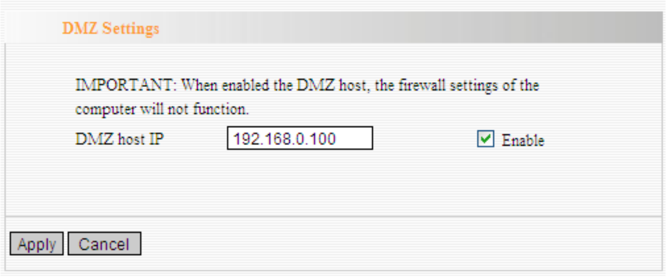
Usually allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.

In the default ALG settings, the following protocols have enabled. It is recommended to keep the settings unchanged.

1. FTP
2. TFTP
3. PPTP
4. IPSec
5. L2TP

8.4 DMZ Settings

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.



IMPORTANT: When enabled the DMZ host, the firewall settings of the computer will not function.

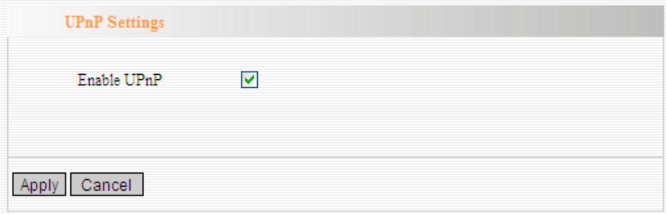
DMZ host IP 192.168.0.100 ☑ Enable

- ➢ **DMZ Host IP Address:** The IP address of the computer you want to expose.
- ➢ **Enable:** Click the checkbox to enable the DMZ host.

IMPORTANT: When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

8.5 UPNP Settings

It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.



UPnP Settings

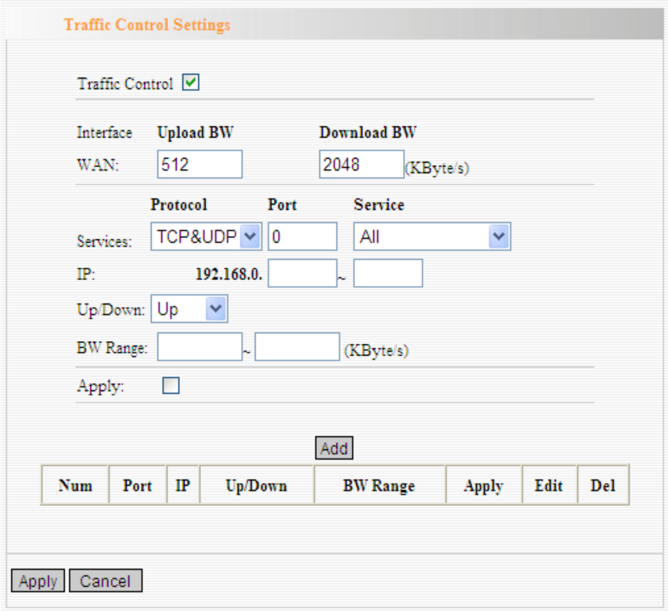
Enable UPnP ☑

- **Enable UPnP:** Click the checkbox to enable the UPnP.

Chapter 9 Traffic Control

9.1 Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.



Traffic Control Settings

Traffic Control ☑

Interface	Upload BW	Download BW
WAN:	512	2048 (KByte/s)

	Protocol	Port	Service
Services:	TCP&UDP	0	All

IP: 192.168.0. ~

Up/Down: Up

BW Range: ~ (KByte/s)

Apply: ☐

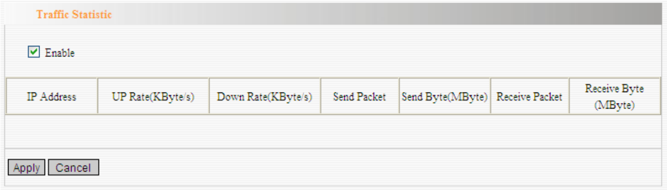
Num	Port	IP	Up/Down	BW Range	Apply	Edit	Del

- **Enable Traffic Control:** To enable or disable the internal IP bandwidth control. The default is disabled.

- **Interface:** To limit the uploading and downloading bandwidth in WAN port.
- **Service:** To select the controlled service type, such as HTTP service.
- **IP Starting Address:** The first IP address for traffic control.
- **IP Ending Address:** The last IP address for traffic control.
- **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- **Bandwidth:** To specify the uploading/downloading Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.
- **Apply:** To enable the current editing rule. If not, the rule will be disabled.
- **Add:** After edit the rule, click the “add to list” button to add the current rule to rule list.
- **Apply:** Click “Save” to activate the current rule.
- **Cancel:** Click “Cancel” to drop all setting saved last time.

9.2 Traffic Statistics

Traffic statistics is used to show the LAN PC’s traffic information.



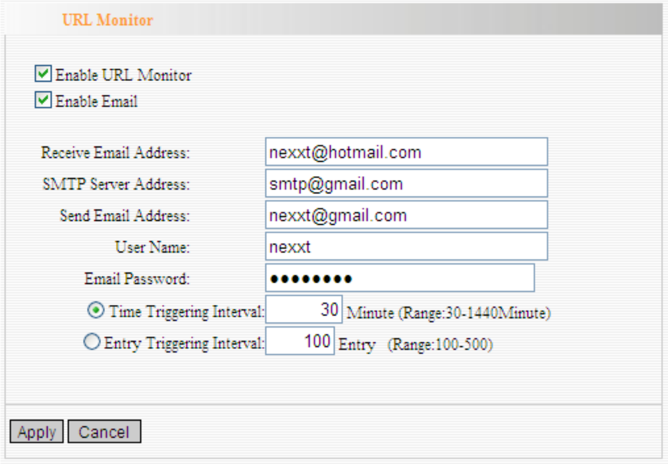
IP Address	UP Rate(KByte/s)	Down Rate(KByte/s)	Send Packet	Send Byte(MByte)	Receive Packet	Receive Byte (MByte)

- **Enable traffic statistics:** check to enable traffic statistics. Usually traffic statistics is disabled, which can improve the Router’s data handling. The default is disabled. If it is enabled, the page will update the PC’s traffic information automatically and be refreshed every 5 seconds.
- **IP address:** The IP address to be shown.
- **Upstream rate:** the speed of upstream data per second (Kbyte/S).
- **Downstream rate:** the speed of downstream data per second (Kbyte/S).
- **Sending packet:** The PC’s packets sending from the PC.
- **Sending byte:** The byte (Mbyte) sending from the PC.
- **Receiving packet:** The PC’s packets received from the Router.
- **Receiving byte:** The PC’s byte (Mbyte) received from the Router.

Chapter 10 URL Monitor

10.1 URL Monitor

This feature is used to record user's Internet activity, so in terms of this feature, the administrator can check out and control what they can do and have done.



☑ Enable URL Monitor

☑ Enable Email

Receive Email Address: nexxt@hotmail.com

SMTP Server Address: smtp@gmail.com

Send Email Address: nexxt@gmail.com

User Name: nexxt

Email Password: ●●●●●●●●●

● Time Triggering Interval: 30 Minute (Range:30-1440Minute)

○ Entry Triggering Interval: 100 Entry (Range:100-500)

- **Enable URL Monitor:**

  After checking this feature, the Router will record LAN computer's URL information, including the visiting Website, your LAN IP address and the time. The Router can record up to 500 entries. If the record is more than 500 entries, the counter will clean all records and restart the URL record again.

If the Router is powered off and restarts the device, the records will be also lost. The default setting is disabled.

- **Enable Email:** To enable this feature, the URL records will be sent to specified e-mail, which can be solved the problem that the records will be lost when it is over 500 entries.
- **Receive E-mail Address:** Input the received E-mail's address here. For example: nexxt@gmail.com
- **SMTP Server Address:** Input the SMTP server address here. If you are not clear what your SMTP server's address is, you can find them from Help page of the registered e-mail. For example: smtp.sohu.com, smtp.163.com, etc.
- **Send Email Address:** Input the sending email address here.
- **User Name:** Input the sending e-mail's user name.
- **Email Password:** Input the sending e-mail's password.
- **Time Triggering Interval:** To set sending e-mail's time interval. The time ranges from 30 to 1440 minutes. For example: if you input 30 here, it means the Router will send a email from "Send Email Address" to "Receive Email Address" in every 30 minutes. And then the device will clean all

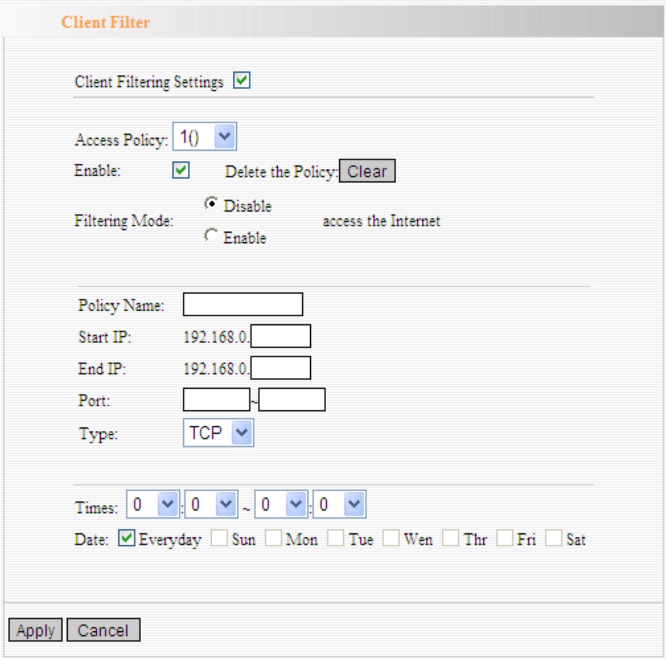
records and start the recording again.

- **Entry Triggering Interval:** To set sending e-mail’s entry interval. The entry ranges from 100 to 500. For example: if you input 100 here, it means the Router will send a email from “Send Email Address” to “Receive Email Address” in every 100 entries. And then the device will clean all records and start the recording again.

Chapter 11 Security Settings

11.1 Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.



Client Filter

Client Filtering Settings ☑

Access Policy: 1()

Enable: ☑ Delete the Policy: Clear

Filtering Mode: ● Disable ○ Enable access the Internet

Policy Name:

Start IP: 192.168.0.

End IP: 192.168.0.

Port: ~

Type: TCP

Times: 0 : 0 ~ 0 : 0

Date: ☑ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

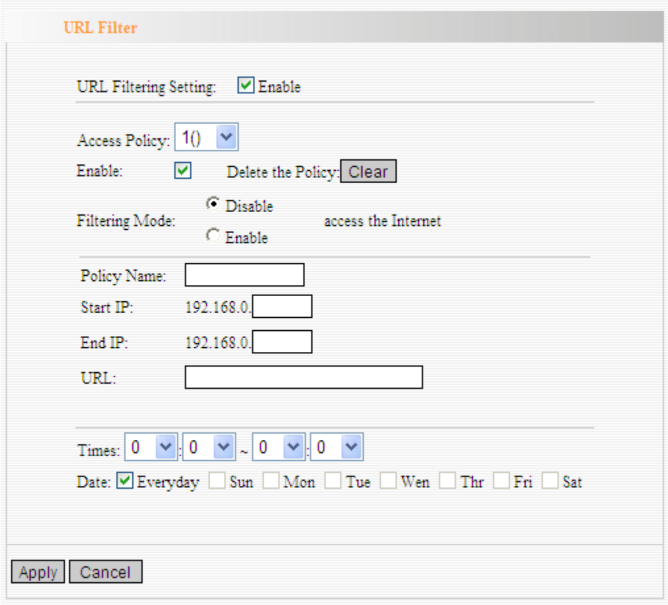
- **Client Filter:** Check to enable client filter.
- **Access Policy:** Select one number from the

drop-down menu.

- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **IP Start/End:** Enter the starting/ending IP address.
- **Port No.:** Enter the port range based over the protocol for access policy.
- **Protocol:** Select one protocol (TCP/UDP/Both) from the drop-down menu.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.

11.2 URL Filter Settings

In order to control the computer to have access to websites, you can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.



URL Filter

URL Filtering Setting: ☑ Enable

Access Policy: 1()

Enable: ☑

Delete the Policy:

Filtering Mode: ● Disable ○ Enable access the Internet

Policy Name:

Start IP: 192.168.0.

End IP: 192.168.0.

URL:

Times: 0 : 0 ~ 0 : 0

Date: ☑ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

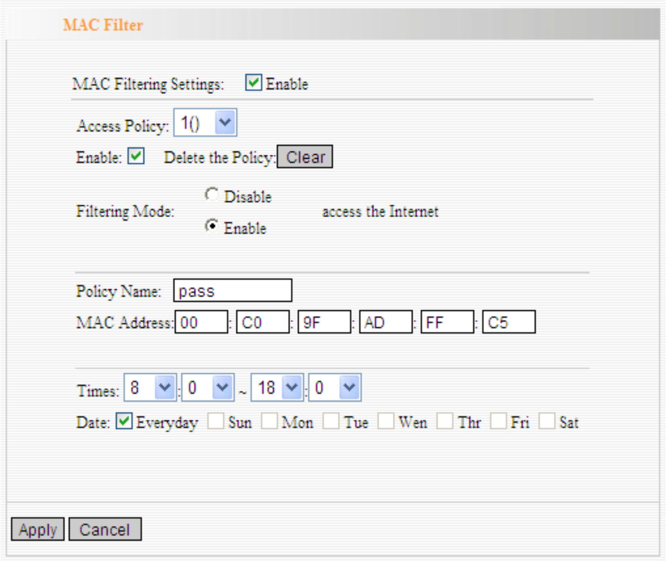
- **URL Filter:** Check to enable URL filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click "Clear" button to clear all

settings for the policy.

- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **Start/End IP:** Enter the starting/ending IP address.
- **URL Strings:** Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.
- **Apply** : Click "Apply" to activate the configuration.

11.3 MAC Address Filter

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.



MAC Filter

MAC Filtering Settings: ☑ Enable

Access Policy: 1()

Enable: ☑ Delete the Policy: Clear

Filtering Mode: ○ Disable ● Enable access the Internet

Policy Name: pass

MAC Address: 00 : C0 : 9F : AD : FF : C5

Times: 8 : 0 ~ 18 : 0

Date: ☑ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

- **MAC Address Filter:** Check to enable MAC address filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click "Clear" button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or

disable to access the Internet.

- **Policy Name:** Enter a name for the access policy selected.
- **MAC Address:** Enter the MAC address you want to run the access policy.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.
- **Apply** : Click to make the settings go into effect.

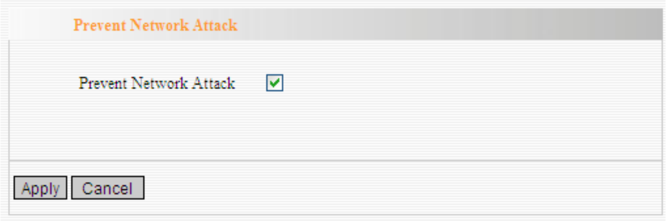
For example:

If you want to configure the host with MAC address 00:C0:9F: AD:FF:C5 not to access the Internet at 8 : 00-18 : 00, you need to set it as above.

11.4 Prevent Network Attack

This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically.

The attacker's IP address can be found from the "System Log".

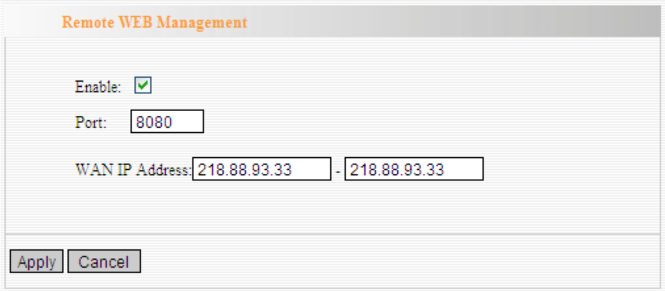


Prevent Network Attack ☑

- **Prevent Network Attack:** Check to enable it for attack prevention.

11.5 Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the "Enable".



Enable: ☑

Port: 8080

WAN IP Address: 218.88.93.33 - 218.88.93.33

- **Enable:** Check to enable remote web management.
- **Port:** The management port open to outside access. The default value is 80.
- **WAN IP Address:** Specify the range of the WAN IP address for remote management.

Note :

1. If you want to login the device's Web-based interface via port 8080, you need use the format of WAN IP address: port (for example

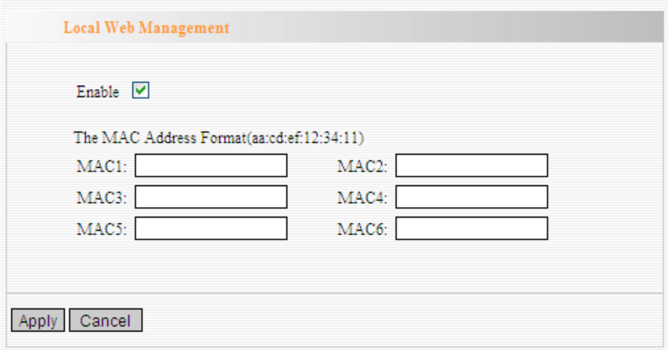
http://219.134.32.101: 8080) to implement remote login.

2. If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 218.88.93.33-218.88.93.35, then only the IP addresses as 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the Router.

For example: If you want to configure the IP address 218.88.93.33 to access the device’s web interface, please set it as follows:

11.6 Local Web Management

Local web management, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.



- **Enable:** Check to enable the local web management.
- **MAC1/2/3…:** Enter the MAC addresses of LAN computers.

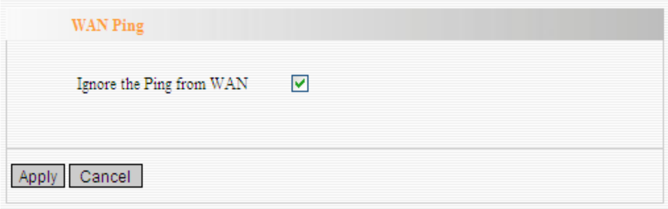
Note :

1. In the default state, this feature is not enabled. All computers in the LAN can login the Web.
2. For example, if you only allow the MAC address

with 00:11:22:33:E4:F5 to access the Web, please set it as above.

11.7 WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.



WAN Ping

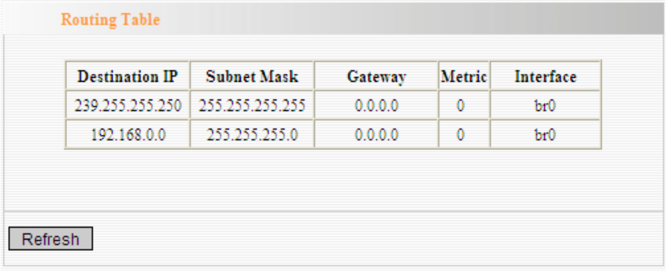
Ignore the Ping from WAN ☑

- **Ignore Ping from WAN:**
  Check to ignore the ping request and give no reply.

Chapter 12 Routing Setting

12.1 Routing Table

The main duty for a router is to look for a best path for every data frame, and transfer this data frame to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.

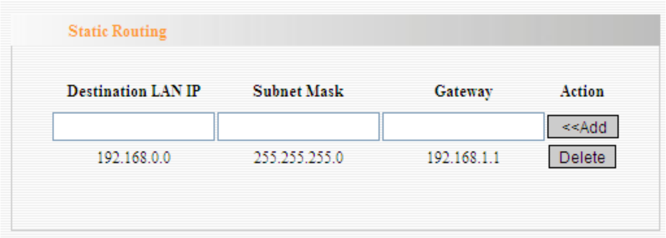


Routing Table

Destination IP	Subnet Mask	Gateway	Metric	Interface
239.255.255.250	255.255.255.255	0.0.0.0	0	br0
192.168.0.0	255.255.255.0	0.0.0.0	0	br0

12.2 Static Routing

This page is used to configure the Router's static routing.



Destination LAN IP	Subnet Mask	Gateway	Action
192.168.0.0	255.255.255.0	192.168.1.1	Delete

- **Destination LAN IP:** The address of the remote host with which you want to construct a static route.
- **Subnet Mask:** The network portion of the Destination LAN IP.
- **Gateway:** The gateway of the next hop, usually the Router or host's IP address.

Note :

1. The gateway must keep the same segment with the Router's LAN IP address.

2. If the destination IP address is one host's IP address, the Subnet mask should be 255.255.255.255.

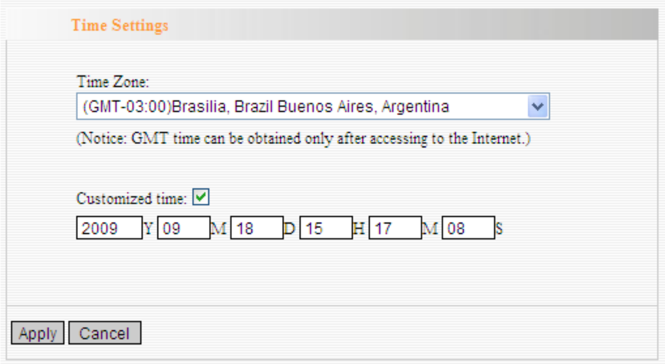
3. If the destination IP address is an IP address

range, the subnet mask should match the IP address. For example, if the IP is 10.0.0.0, subnet mask should be 255.0.0.0; if the IP is 10.1.2.0, subnet mask should be 255.255.255.0.

Chapter 13 System Tools

13.1 Time Settings

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.



Time Settings

Time Zone: (GMT-03:00)Brasilia, Brazil Buenos Aires, Argentina

(Notice: GMT time can be obtained only after accessing to the Internet.)

Customized time: ☑

2009 Y 09 M 18 D 15 H 17 M 08 S

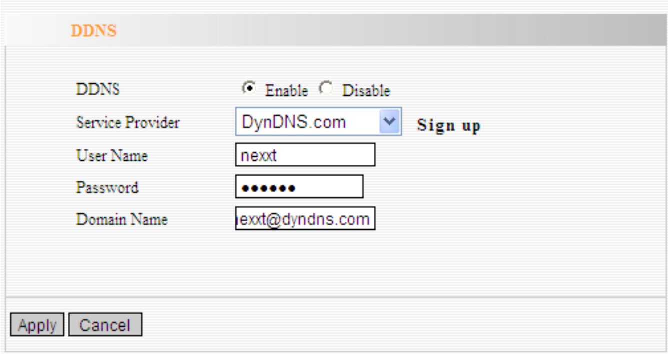
- **Time Zone:** Select your time zone from the drop-down menu.
- **Customized time:** Enter the time you customize.

Note :

When the Router is powered off, the time setting will be lost. Before the Router will obtain GMT time automatically, you need connect with the Internet and obtain the GMT time, or set the time on this page first. Then the time in other features (e.g. firewall) can be activated.

13.2 DDNS

The DDNS (Dynamic Domain Name System) is supported in this Router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select "Enable" and a DDNS service provider to sign up.



DDNS ● Enable ○ Disable

Service Provider DynDNS.com

User Name nexxt

Password ••••••

Domain Name exxt@dyndns.com

- **Main Features:**

  Owing to ISP most times provides dynamic IP address, DDNS is used to capture the changeable IP address and match the fixed domain. Then users can have access to the Internet to communicate with others.

DDNS can help you establish virtual host in your home and company.

- **DDNS:** Click the radio button to enable or disable the DDNS service.
- **Service Provider:** Select one from the drop-down menu and press “Sign up” for registration.
- **User Name:** Enter the user name the same as the registration name.
- **Password:** Enter the password you set.
- **Domain Name:** Enter the domain name which is optional.

For example :

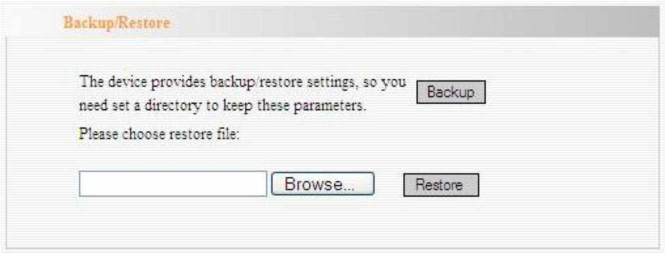
In the local host 192.168.0.10 establish a Web server, and register in 3322.org as follows:

User name	nexxt
Password	mypasswd
Domain Name	nexxt.3322.org

After mapping the port in the virtual server, setting account information in DDNS server and in the address field entering http://nexxt.3322.org, you can access the Web page.

13.3 Backup/Restore Settings

The device provides backup/restore settings, so you need set a directory to keep these parameters.

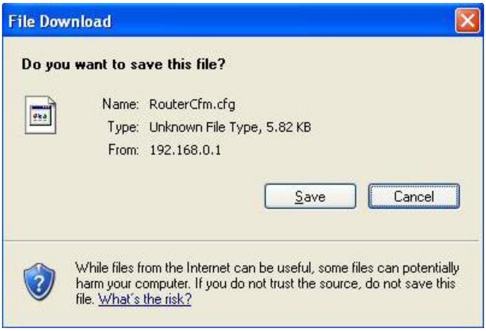


The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

- **Backup Setting** :

  Click "Backup" button to back up the Router's settings and select the path for save.



Do you want to save this file?

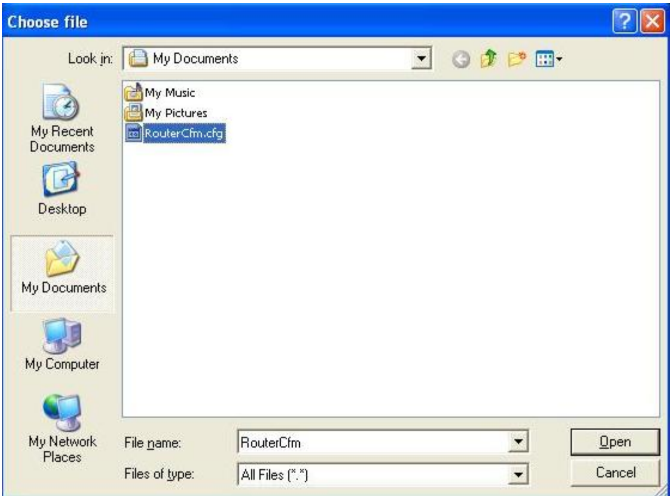
Name: RouterCfm.cfg
Type: Unknown File Type, 5.82 KB
From: 192.168.0.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Click "Save" to save the configuration files.

- **Restore Setting** :

  Click "Browse" button to select the backup files.

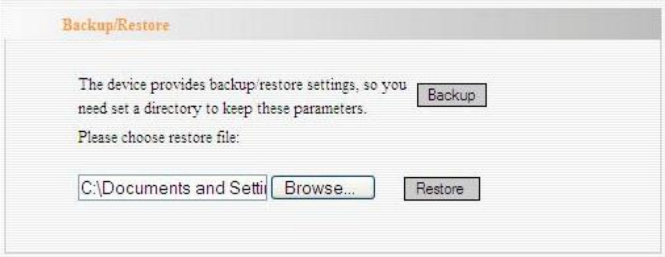


Look in: My Documents

File name: RouterCfm

Files of type: All Files (*.*)

Click "Restore" button to restore previous settings.



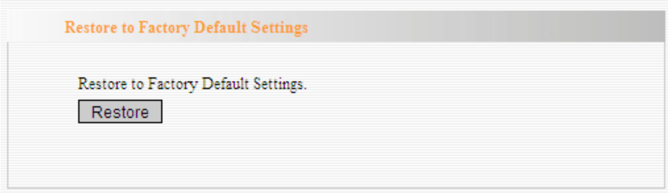
The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

C:\Documents and Setti

13.4 Restore to Factory Default Setting

This button is to reset all settings to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.



Restore to Factory Default Settings

Restore to Factory Default Settings.

- **Restore:** Click this button to restore to default settings.

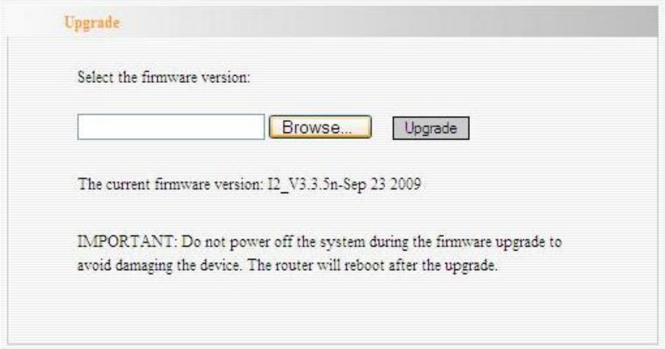
- **Factory Default Settings:**
  User Name: admin
  Password: admin
  IP Address: 192.168.0.1
  Subnet Mask: 255.255.255.0

⚠ **NOTE:**

After restoring to default settings, please restart the device, then the default settings can go into effect.

13.5 Upgrade Firmware

The Router provides the firmware upgrade by clicking the "Upgrade" after browsing the firmware upgrade packet which you can download from www.nexxtsolutions.com



Select the firmware version:

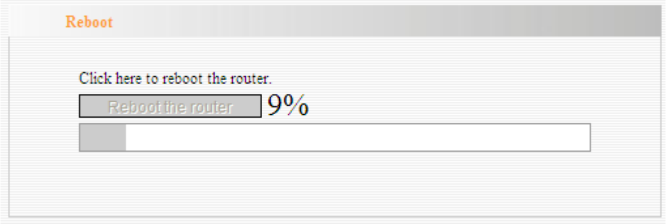
The current firmware version: I2_V3.3.5n-Sep 23 2009

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the device. The router will reboot after the upgrade.

- **Browse:** click this button to select the upgrade file.
- **Upgrade:** click this button to start the upgrading process. After the upgrade is completed, the Router will reboot automatically.

13.6 Reboot the Router

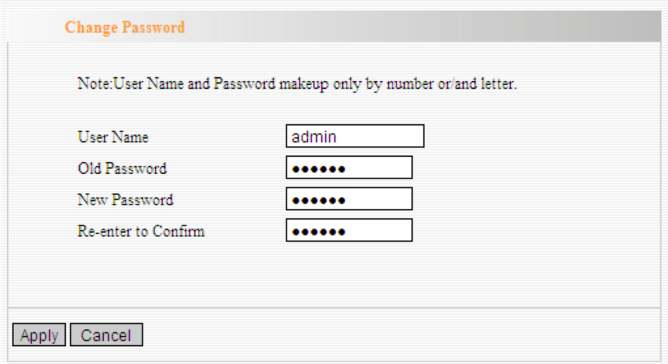
Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.



Reboot the router: Click this button to reboot the device.

13.7 Password Change

This section is to set a new user name and password to better secure your router and network.



Note:User Name and Password makeup only by number or/and letter.

User Name: admin
Old Password: ••••••
New Password: ••••••
Re-enter to Confirm: ••••••

- **User Name:** Enter a new user name for the device.
- **Old Password:** Enter the old password.
- **New Password:** Enter a new password.

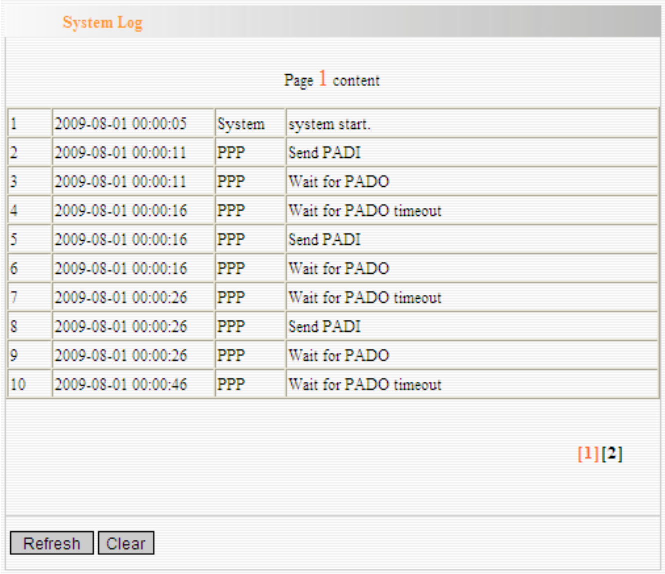
- **Re-enter to Confirm:** Re-enter to confirm the new password.

⚠**NOTE:**

It is highly recommended to change the password to secure your network and the Router.

13.8 System Log

The section is to view the system log. Click the "Refresh" to update the log. Click "Clear" to clear all shown information. If the log is over 150 records, it will clear them automatically.



Page 1 content

1	2009-08-01 00:00:05	System	system start.
2	2009-08-01 00:00:11	PPP	Send PADI
3	2009-08-01 00:00:11	PPP	Wait for PADO
4	2009-08-01 00:00:16	PPP	Wait for PADO timeout
5	2009-08-01 00:00:16	PPP	Send PADI
6	2009-08-01 00:00:16	PPP	Wait for PADO
7	2009-08-01 00:00:26	PPP	Wait for PADO timeout
8	2009-08-01 00:00:26	PPP	Send PADI
9	2009-08-01 00:00:26	PPP	Wait for PADO
10	2009-08-01 00:00:46	PPP	Wait for PADO timeout

- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the current shown log.

13.9 Logout

After you have finished the settings completely, in logout page click “Yes” to logout the web management page.

Appendix 1：Glossary

Access Point (AP):

Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.

Channel:

An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID:

Service Set identifier. An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP:

Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommended using.

WPA/WPA2:

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

Appendix 2: Ask and Question

In this part some questions and problems shown during the Router's usage and installation will be given suggesting answers. If your problems are not in the list, please log into our website www.nexxtsolutions.com or send an E-mail to techsupport@nexxtsolutions.com, and we will reply you in the first time.

1、Can not login to the Web interface of the Router after you enter the IP address in the address field？

Step 1: check the Router if it works well. Once the device is powered on for a few seconds, the SYS indicator on the panel will be turned on. If it is not, please contact us.

Step 2: check the network cables if it is good and the corresponding indicator is "Always ON". Sometimes, the indicator is "Always ON", but it does not mean it gets through.

Run "Ping" command and check if it can ping the Router's LAN IP address 192.168.0.1. If it is OK, please make sure your browser does not access the Internet by proxy server. If the ping fails, you can press the “RESET” button for 7 seconds to restore to default settings. And then repeat the ping operation. If it still does not work, please contact us.

2、Forget the login password and can not enter the setting page. What can I do?

Press the “RESET” button for 7 seconds to restore the Router to default settings.

3、The computer connected with the Router shows IP address conflict. What can I do?

Check if there are other DHCP servers in the LAN. If there have, disable them. The default IP address of the Router is 192.168.0.1 and please maker sure the address is not occupied by other devices. If there are two computers with the same IP addresses, please modify one.

4、I can not use E-mail and access the Internet. What can I do?

It happens in ADSL connection and Dynamic IP users. And you need modify the default MTU value (1492).

Please in the "WAN Setting" modify the MTU value with the recommended value as 1450 or 1400.

5、How to configure and access the Internet via Dynamic IP?

In Setup Wizard of the Web utility interface, select "Dynamic IP" connection type and click "Save" to activate it. As some ISPs bind the user computer's MAC address, you need to clone the Router's WAN MAC address to the bind21ing PC's MAC address. Select "MAC Address Clone" in "Advanced Setting" to input your computer's MAC address and click "Apply" to activate it.

6、How to share my computer's source with other users in Internet？

If you want Internet users to access the internal server via the Router such as e-mail server, Web, FTP, you can configure the "Virtual Server" to come true.

Step 1: create your internal server, make sure the LAN users can access these servers and know related service port. For example, Web server's port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: in the Router's web click "Virtual Server" and select "Single Port Forwarding".

Step 3: input the external service port given by the

Router, for example, 80.

Step 4: input the internal Web service port, for example, 80.

Step 5: Input the internal server’s IP address. If your Web server’s IP address is 192.168.0.10, please input it.

Step 6: select the communication protocol used by your internal host: TCP, UDP, ICMP.

Step 7: click “Apply” to activate the settings.

The following table has listed the well-known application and service port:

Server	Protocol	Service Port
WEB Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503、1720
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice:1863、6901(TCP) Voice:1863、5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110