

E-TOP 11n Broadband Router

N+ High Power Gigabit Broadband Router - All Broadbands

GR290n

User Manual



Table of Contents

FCC Caution	5
Safe Seating Gestures	6
CE Statement of Conformity	6
Notice	6
Chapter 1 Introduction	7
1.1 Overview	7
1.2 Features	8
1.3 Specifications	9
1.3.1 Product Appearance	11
1.3.2 LED Indicator Status Description	11
1.4 System Requirements	12
1.5 Get Your IP Automatically & Manually	13
1.5.1 Network Testing	16
1.5.2 Testing with Internet Browser	16
1.5.2.1 Testing with DOS (Windows XP Platform)	16
Chapter 2 Hardware Installation	19
2.1 Diagram of Connecting Hardware to 11N Broadband Router	19
2.1.1 Hardware Connection and Application for Router Mode	19
Chapter 3 One Button Setup	20
3.1 One Button Setup configuration for Router Mode	20
Chapter 4 Basic Setup	24
4.1 Router Mode	24
4.1.1 Administrator Setup Instruction	24
4.2 Basic Setup	25
4.2.1 Time Zone Setup	25
4.2.2 LAN Interface Setup	26
4.2.3 WAN Setup	27
4.2.3.1 WAN Interface– Ethernet Port	27
4.2.3.2 WAN Interface– Wireless	27
4.2.3.3 WAN Access Type – Static IP	27
4.2.3.4 WAN Access Type – Dynamic IP	27
4.2.3.5 WAN Access Type – PPPoE	28
4.2.3.6 WAN Access Type – PPTP	28
4.2.3.7 Wireless Setup	28
4.2.3.8 Wireless Security Setup	29
4.2.4 Basic Setup Complete	30

Chapter 5	Advanced Configuration	32
5.1	IP Configuration	32
5.1.1	WAN	32
5.1.1.1	WAN Interface– Ethernet Port.....	32
5.1.1.2	WAN Interface– Wireless	33
5.1.1.3	WAN Access Type – Static IP.....	33
5.1.1.4	WAN Access Type –Dynamic IP	34
5.1.1.5	WAN Access Type –PPPoE.....	35
5.1.1.6	WAN Access Type – PPTP	37
5.1.2	LAN Interface Setup	38
5.1.3	Dynamic DNS Setting.....	40
5.2	Wireless Setup	41
5.2.1	Wireless Basic Settings.....	42
5.2.2	Wireless Advanced Settings	46
5.2.3	Wireless Security Setup	47
5.2.4	Wireless Access Control	49
5.2.5	WDS Settings.....	51
5.2.6	WPS	56
5.3	NAT	60
5.3.1	Visual Server.....	60
5.3.2	Visual DMZ	62
5.4	Firewall.....	63
5.4.1	QoS	63
5.4.2	Port Filtering	65
5.4.3	IP Filtering	67
5.4.4	MAC Filtering	68
5.4.5	URL Filtering	70
5.5	System Management	71
5.5.1	Change Password	71
5.5.2	Upgrade Firmware.....	72
5.5.3	Profiles Save.....	73
5.5.4	Time Zone Setting	78
5.5.5	UPnP Setting.....	80
5.5.6	Language Setting	81
5.6	Log & Status	82
5.6.1	Network Config.....	82
5.6.2	Event Log	83
5.7	Logout.....	85

Chapter 6	DDNS Service Application.....	87
Chapter 7	Q & A	92
7.1	Installation	92
7.2	LED	92
7.3	IP Address.....	93
7.4	OS Setting.....	93
7.5	11n Broadband Router Setup	94
7.6	Wireless LAN	96
7.7	Support	98
7.8	Others.....	99
7.9	USB Device	99
Chapter 8	Appendices	100
8.1	Operating Systems	100
8.2	Browsers.....	100
8.3	Communications Regulation Information	100

FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) Statement

This Equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

1. The device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) this device must accept any interference received, including interference that may cause undesired operation.
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:

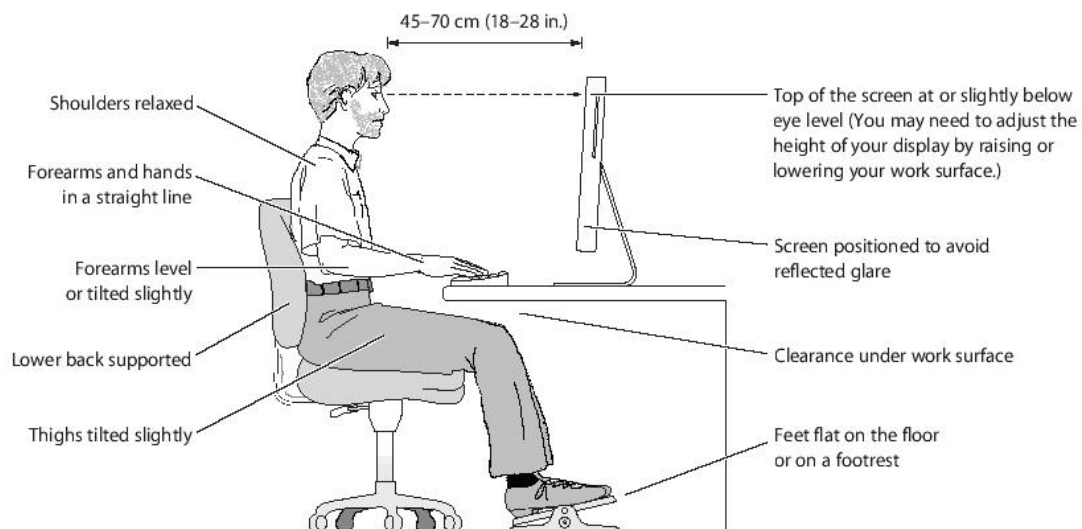
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Safe Seating Gestures

You should follow the manufacturer's instructions for adjusting the backrest to fit your body properly.

- An adjustable chair that provides firm, comfortable support is best.
- Adjust the height of the chair so your thighs are horizontal and your feet flat on the floor.
- The back of the chair should support your lower back (lumbar region).



CE Statement of Conformity

Our product has been tested in typical configuration by Ecom Sertech Corp and was found to comply with the essential requirement of “Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility” (89/336/EEC; 92/31/EEC; 93/68/EEC)

Notice

Changing RF parameter is not allowed.

Chapter 1 Introduction

1.1 Overview

11n Broadband Router is a convenient wireless solution for delivering 802.11n wireless connectivity with a maximum wireless signal rate of up to 300Mbps. Use it in home or company.

1.2 Features

- **WPS button** provides not only an easy and secured wireless network but also a WDS repeater in one push
- **Multiple APs Supported** : adds or limits the properties for classed SSID, increasing the flexibility and efficiency of the network.
- **Superior, reliable performance** : 20000 fast recycling sessions provide a stable network connection for P2P downloading.

1.3 Specifications

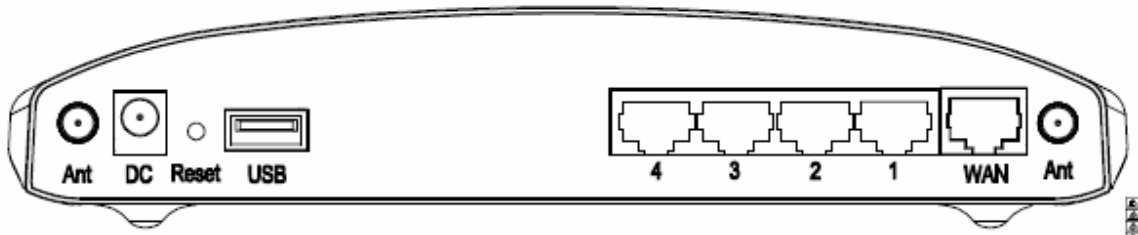
Item	Specification
Key Components	
Main Processor	Realtek RTL8198 (600MHz)
Flash	8Mbytes Serial Flash
RAM	64Mbytes DDR2
Wireless Chip	Realtek RTL8192CE (MAC+BB+RF) 2T2R
Communication Interfaces	
WAN Port	1 x 10/100/1000Mbps RJ45, with auto MDI/MDIX
LAN Port	4 x 10/100/1000Mbps RJ45, with auto MDI/MDIX
USB Port	1 x USB 2.0 host for 3.5G \ WiMAX USB dongle and Smartphone
Wireless	IEEE 802.11 b/g/n
Others	
Wireless Antenna	External 5dBi x 2
Transmission Power	802.11b: 13±1dBm @ normal temp. range 802.11g: 19±1dBm @ normal temp. range 802.11n (20MHz/40MHz): 18.5±1dBm @ normal temp. range
Receive Sensitivity	11Mbps : TYP. -83dBm @ 8% PER 54Mbps: TYP. -70dBm @ 10% PER 11n (20MHz): TYP. -64dBm @ 10% PER 11n (40MHz): TYP. -61dBm @ 10% PER
Button	Reboot button / Reset button – one second for reboot/ten seconds for restore to factory default setting ° WPS button – When WPS button pushed , system will enter WPS connecting mode °

Operation Requirement	Operating Temp. 0°C~40°C (32°F~104°F) Storage Temp. -20°C~70°C (-4°F~158°F) Operating Humidity 10% to 85% Non-Condensing Storage Humidity 5% to 90% Non-Condensing
Power Supply	Power Adapter DC5V/1.5A
Dimensions	198.2(L) x 107(W) x 39.1(H)mm

Notice:

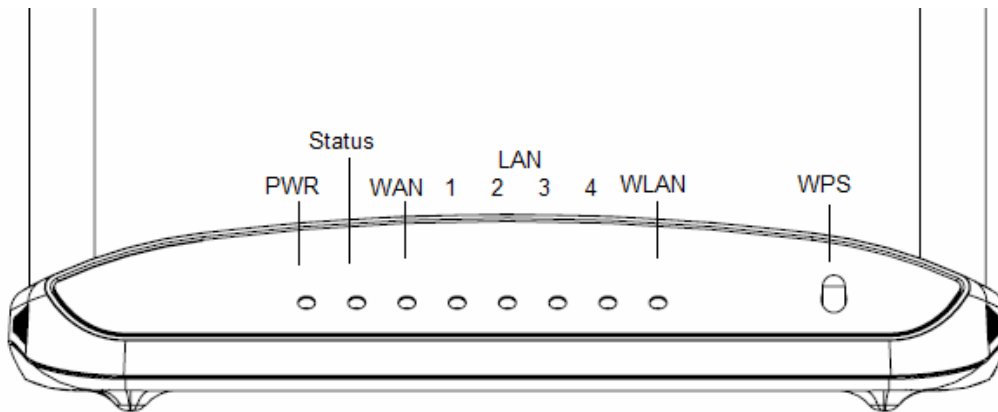
1. USB device with power more than 500mA is not supported

1.3.1 Product Appearance



Power Receptor	Adapter, Input:90-240Vac, Output: 12V/ 1A
WPS	Push “WPS” button to looking for other WPS devices. The security will be set up between these 2 Wi-Fi devices after pairing.
Reset Button	Press “Reset” button over 10 seconds. When status indicator turns from flashing to solid, the process is completed. All settings are back to default.
Ethernet Port	1x WAN port, 4x LAN ports
USB2.0 Ports	1 USB Port

1.3.2 LED Indicator Status Description



LED	Function	Color	Status	Description
Power x 1	Power indication	Green	On	Power is being applied to this product
Status x 1	System status	Green	On	System is ready to work
			Blinking 120ms	Reset / Firmware update in progress
WLAN/ WPS x 1	Wireless activity &	Green	On	Wireless is connected
			Blinking	Wireless Tx/Rx activity

	WPS status		30ms	
		Reddish Orange	Blinking 120ms	WPS function in progress
WAN x 1	WAN port activity	Green	On	100Mbps Ethernet is connected
			Blinking 30ms	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking 120ms	10Mbps Ethernet Tx/Rx activity
LAN x 4	LAN port activity	Green	On	100Mbps Ethernet is connected
			Blinking 30ms	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking 120ms	10Mbps Ethernet Tx/Rx activity

1.4 System Requirements

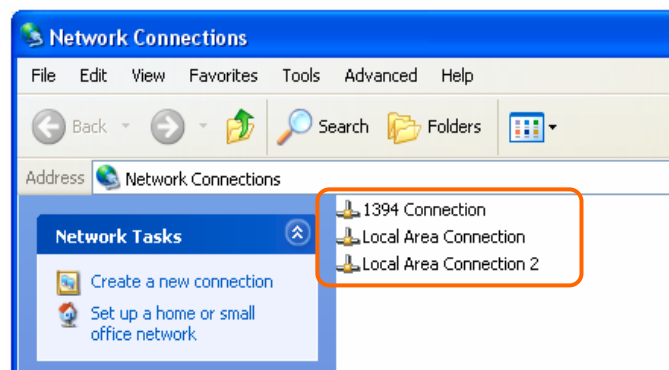
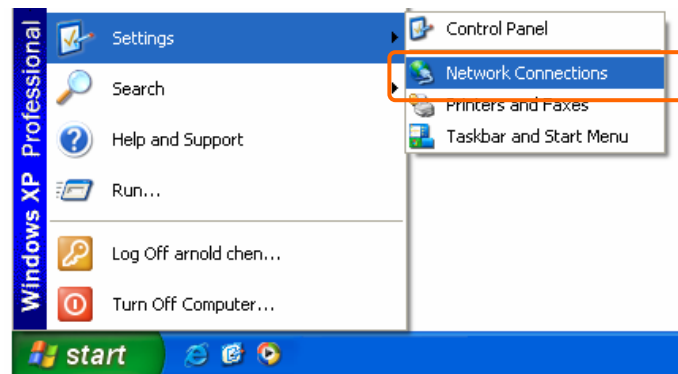
To begin with 11n Broadband Router, you must have the following minimum system requirements. If your system can't correspond to the following requirements, you might get some unknown troubles on your system.

- XDSL/Cable Modem and broadband Internet Account.
- One Ethernet (10 BASE-T or 10/100 BASE-TX) network interface card.
- One PC or Notebook with web browser software installed (E.g.: Internet Explorer 5.0, Netscape Navigator 7.x, Apple Safari 2.03 or higher version).
- At least one 802.11b/g/n wireless adapter for wireless mobile clients.
- Recommended OS: Win2000 or WinXP / Linux.

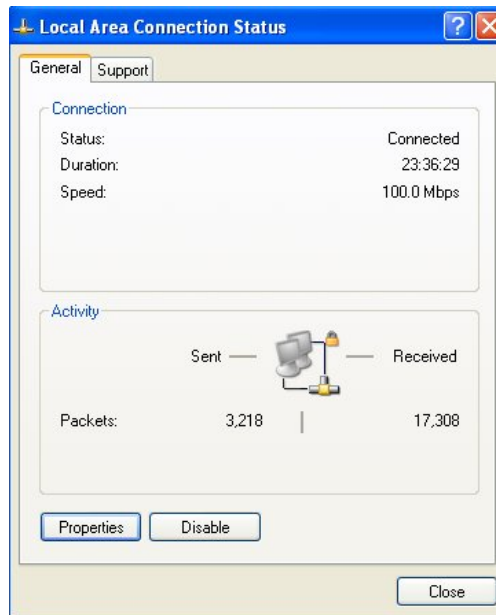
1.5 Get Your IP Automatically & Manually

After 11n Broadband Router connected with your computer, please make sure your IP is in the automatic IP position or you adjust it manually in order to activate the Internet network from home to Internet. If you don't know how to enter the settings, please follow the steps as below.

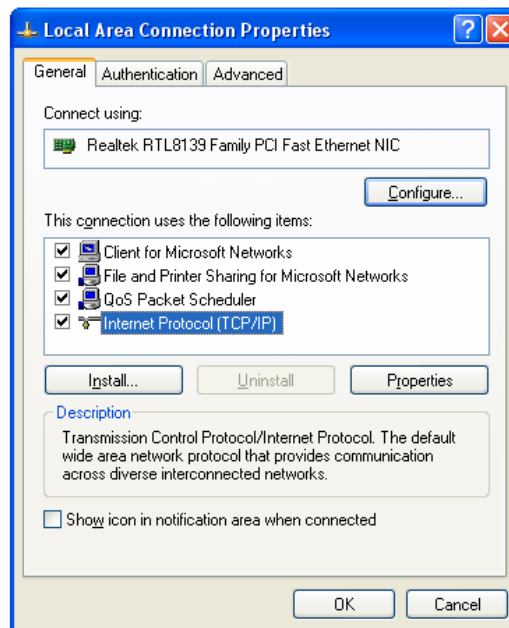
Step 1. Go to **Start>Settings> Network Connections** and then select **Local Area Connection**.



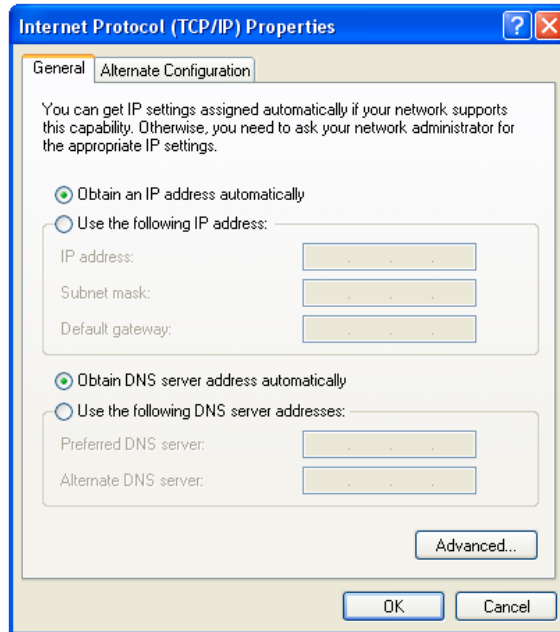
Step 2. Click on Properties



Step 3. Double click on Internet Protocol (TCP/IP).



Step 4-1. For getting IP automatically if you are one of the users under 11n Broadband Router, please skip **Use the following IP address** and then select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and then click on **OK** button.



Step 4-2. For getting IP manually in order to specify a Virtual Server, such as Print Server, FTP Server and so on, please skip **Obtain an IP address automatically** and then select **Use the following IP address**. And the following default setting of 11n Broadband Router should be noted:

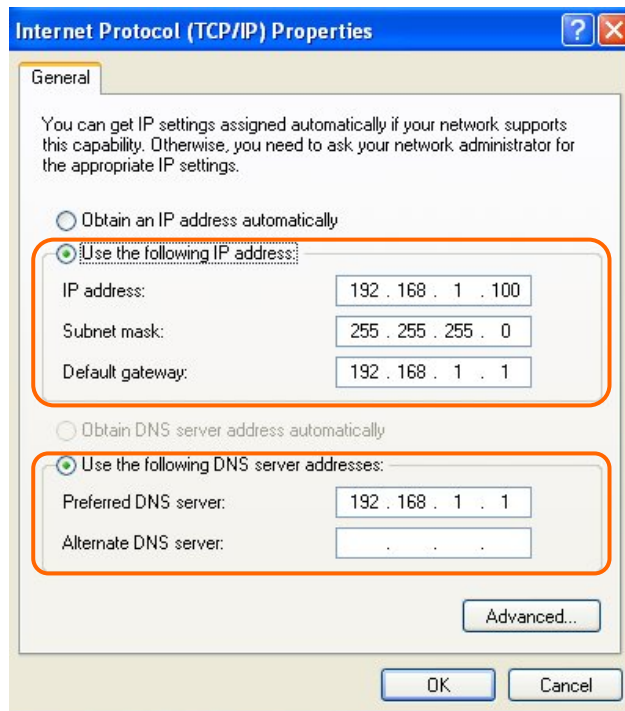
- IP Address: 192.168.1.10 (as your Print Server for example)
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

Note: If you configure your computer's IP Address manually, it needs to be on the same network segment.

For example:

- IP Address: 192.168.1.xxx (xxx can be any number between 2 and 253, but it can't be repeated, we use 100 to be the example.)
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1 (this is the IP address of 11n Broadband Router in Router Mode)
- DNS: 192.168.1.1 (use 11n Broadband Router's IP address or on your own choice)

Note: IP address and Default gateway cannot be the same.



1.5.1 Network Testing

There are two ways to test your Network whether it can work on Internet or not. They are “Testing with Internet Browser” and “Testing with Dos”.

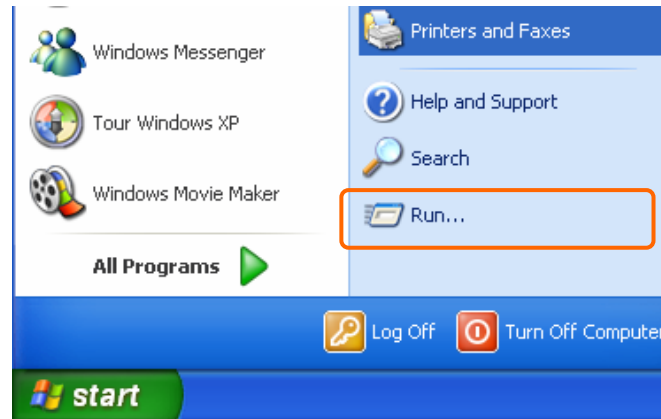
1.5.2 Testing with Internet Browser

Open an Internet Browser, such as Internet Explore or Netscape. Input a valid web address you like, for example, <http://www.yahoo.com> in the web address blank and then press enter. If the website appears, that means your Internet is working under normal situation.

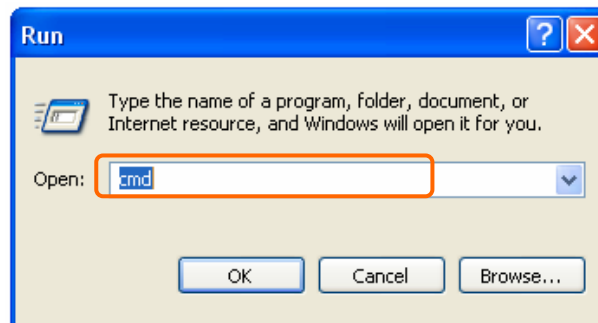


1.5.2.1 Testing with DOS (Windows XP Platform)

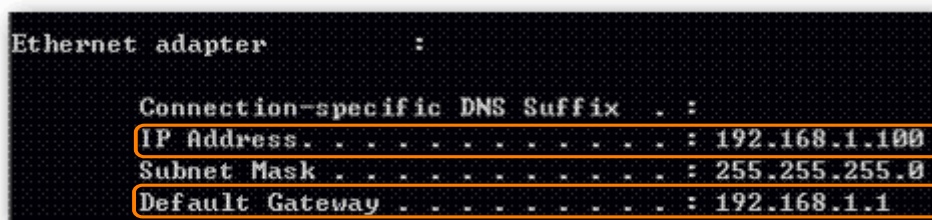
Step 1. Go to start > Run.



Step 2. Input **cmd** in the blank, and then click **OK** button. The Command Prompt window appears.



Step 3. Input **ipconfig** in the flashing area then press enter. You will get an IP Address 192.168.1.100, for example, and Default Gateway as 192.168.1.1.



Step 4. Ping a legal WAN Address such as 192.168.1.1. If Internet works, it will show **Reply from 192.168.1.1: bytes = 32 time = 3ms TTL =64**, for example.

```
C:\Documents and Settings\chou1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

If it can't work, it will show **Request timed out.**

```
C:\Documents and Settings\chou1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

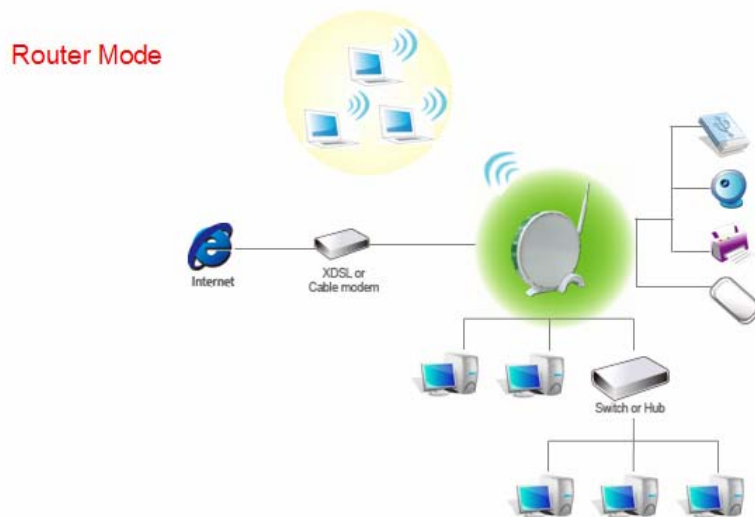
Chapter 2 Hardware Installation

2.1 Diagram of Connecting Hardware to 11N Broadband Router

11n Broadband Router is a portable and convenient wireless solution for delivering 802.11n wireless connectivity with a maximum wireless signal rate of up to 300Mbps. Use it in conference rooms, hotel rooms, or even at hotspots.

2.1.1 Hardware Connection and Application for Router Mode

When 11n Broadband Router switches to Router Mode, there will be each WAN and LAN port existing, the administrator can do the Quick Setup including WAN Setup, LAN Setup, Wireless Setup, Time Server Setup, Password Setup, Firewall Setup, QoS Setup.



Chapter 3 One Button Setup

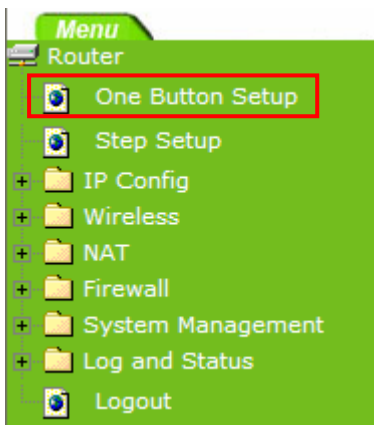
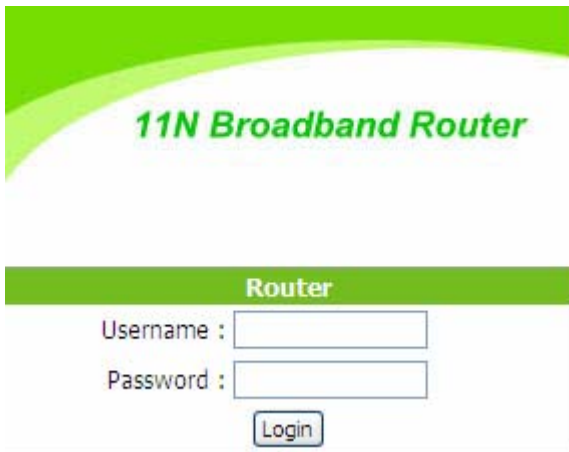
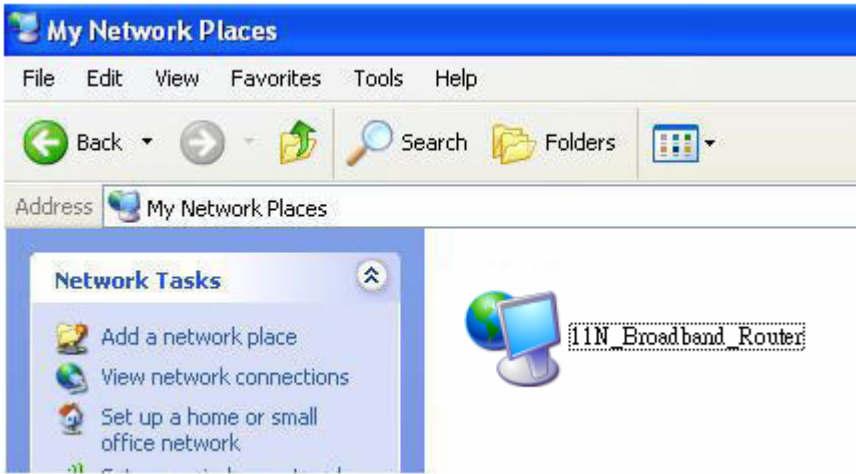
The advanced One Button Setup provides users a simple way to set up the complicated network. Instead of numbers of IPs to be memorized, you just need to fill in some necessary information and then enjoy the secured internet by clicking the “**Finished**” button.

3.1 One Button Setup configuration for Router Mode

The default UPnP of 11n Broadband Router is ON. When users connect 11N Broadband Router to their PC, and icon will show up in the right-down corner.



Step 1. Click the **Internet Gateway Device** to open the login page.



One Button Setup

This page is used to configure all of the server router function for first time.

Time Zone Select

Time Zone Select :

Change Password

New Password:

Device Name

Device Name:

WAN Interface Setup

WAN Interface:

SERVICE:

Connect Speed: Auto Switch 2.5G/2.75G only 3G/3.5G only

SIM PIN: None

Retype SIM PIN:

APN:

Username:

Password:

PHONE Number:

Wireless Setup

SSID:

Encryption:

- **Time Zone Select:** Select your time zone from the Time Zone drop-down list.
- **Change Password:** For changing password, please fill the password information into the blank.

- **Device Name:** Name your device here. The default is “11N_Broadband_Router”.
- **WAN Interface Setup:** Select the WAN Interface from the drop-down list.
- **Connect Speed:** Select connection speed.
- **WAN Type Setup:** Please choose the access type.
- **Wireless Setup:** Define the SSID, and Encryption type.
- **Finished:** Click **finished** button to complete the setting.

Note: One Button Setup is not completed unless users finish all settings and click **Finished** button.

Chapter 4

Chapter 5 Basic Setup

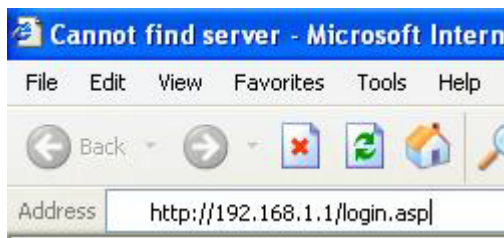
5.1 Router Mode

Under Router Mode, the Router provides a Router/AP function. User can get IP address assigned by ISP wired or wirelessly. It also supports NAT and DHCP functions that enable multiple computers to share an Internet connection at the same time.

5.1.1 Administrator Setup Instruction

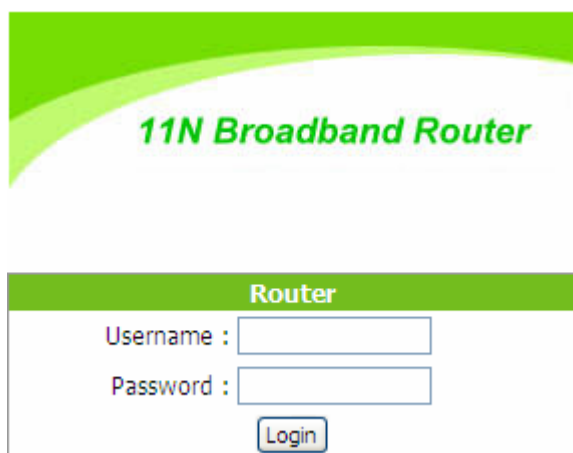
Open a Microsoft Internet Explorer, Mozilla Firefox or Apple Safari browser, and enter <http://192.168.1.1> (Default Gateway) into browser's blank.

Notice: If the homepage doesn't appear, please check if the TCP/IP configuration is obtaining IP address automatically or not. If you don't know how to do it, please refer to "1.5 Get your IP Automatically & Manually".



Homepage

The default values for User Name and Password are **admin** (all in lowercase letters). Click **Login** to enter.



5.2 Basic Setup

Typical Configuration Manager Page consists of two separate frames. The left frame contains all the means available for device configuration. Menus are indicated by file icons, and related menus are grouped into categories, such as LAN, WAN and etc., and indicated by folder icon, depending on whether the group of menus are expanded or not. You can click on any of these to display a specific configuration page.

Select **Step Setup** on the left of the main menu. Then you'll see the full functionality selection screen appears and detailed settings for each item, including "**Basic**" and "**Application**" two parts.

Click **Basic**, you see 4 major items set in Basic Setup Selection. Please click **Next** to the next page.



The screenshot shows a web-based configuration interface for a router. On the left is a green sidebar menu titled 'Router' with the following items: 'One Button Setup', 'Step Setup' (highlighted with a blue box), 'IP Config', 'Wireless', 'NAT', 'Firewall', 'System Management', 'Log and Status', and 'Logout'. The main content area has a blue header 'Router Basic Setup'. Below the header, it says: 'The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.' A horizontal line separates this from the next section: 'Welcome to Setup Wizard .'. Below that, it says: 'The Wizard will guide you the through following steps. Begin by clicking on Next.' followed by a numbered list: 1. Time Zone Setup, 2. LAN Interface Setup, 3. WAN Setup, 4. Wireless Setup. At the bottom right of the main content area is a 'Next' button.

5.2.1 Time Zone Setup

Time Zone Setting

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

Enable NTP client update

Time Zone Select : (GMT+08:00)Taipei

NTP server : 192.5.41.41 - North America

Cancel Back Next

Select **Enable NTP client update** to maintain the system time.

5.2.2 LAN Interface Setup

If you are using 11n Broadband Router with multiple PCs on your LAN, you must connect the LAN via the Ethernet ports on the built-in Ethernet switch. You must assign a unique IP address to each device residing on your LAN. The LAN IP address identifies the router as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN. The default LAN IP for the Internet Security Router is 192.168.1.1.

LAN Interface Setup

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

Device Name: 11N_Broadband_Rou

IP Address: 192.168.1.1

Cancel Back Next

For Gateway IP Address, the IP address 192.168.1.xxx (xxx can be any number between 1 and 254 that is not used by another device.) Please don't change the default LAN IP settings at this section until you have completed the rest of the configurations and confirm that your Internet connection is working.

Click on **Next** button to proceed.

5.2.3 WAN Setup

The WAN settings can be referred to as the Public setting. All IP information in the WAN settings is public IP addresses which are accessible on the Internet. 11n Broadband Router supports 4 interfaces and 4 access types to WAN. Select one of the WAN connection modes required by your ISP in the following WAN Setup Configuration page, the WAN setup pages will vary depending on what kind of WAN Type you select.

Choose your WAN Interface and Access WAN type as the above mentioned, and click **Next**, its associated settings will show up.

5.2.3.1 WAN Interface– Ethernet Port

If you are using an Ethernet cable to connect the Internet, please select **Ethernet port**.

5.2.3.2 WAN Interface– Wireless

If you are connecting the internet via wireless, please select **Wireless** and its associated settings will show up underneath at the same time.

You can see a list of available Wireless networks. Select you preferred one to connect and the Encryption type form the drop-down list.

5.2.3.3 WAN Access Type – Static IP

Choose Static IP Address if all WAN IP information is provided to you by your ISP. You will need to enter the IP address, IP netmask and IP gateway as provided. Each entered fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. Fill in the DNS information provided by your ISP; otherwise, **Domain Name** can't be used.

Click on **Next** button to go on next setting page.

5.2.3.4 WAN Access Type – Dynamic IP

Choose Dynamic IP to obtain IP address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

Click on **Next** button to go on next setting page.

5.2.3.5 WAN Access Type – PPPoE

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

Click on **Next** button to go on next setting page.

5.2.3.6 WAN Access Type – PPTP

This option is typically used for DSL services. Some DSL service providers supply a special DSL modem. This kind of modem only supports the PPTP tunnel to access the Internet, you should create a PPTP tunnel that carries a PPP session and terminates on the DSL model. Once the tunnel has been established, this kind of DSL modem will forward the PPP session to the ISP. As long as the PPP session is connected, all the local users will be able to share this PPP session to access to the Internet.

Click on **Next** button to go on next setting page.

5.2.3.7 Wireless Setup

First step is to name your SSID, and the default value is Download Server Router. Please follow the illustrations below to proceed.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

SSID:

Channel Number:

Encryption:

5.2.3.8 Wireless Security Setup

The security function is provided to prevent the connection requests from unauthorized wireless clients. As the **Encryption Type**, select WEP or WPA can protect your data from eavesdroppers, if you do not need the encryption, select “None” to skip the following setting.

a. Encrypt Type - WEP

11n Broadband Router supports both 64-bit and 128-bit encryption using the Wired Equivalent Privacy (WEP) algorithm. Select the type of encryption you want to use (64 or 128 bit) and configure one to four WEP Keys. The “1280bit” method is more secure than the “64-bit”.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

SSID:

Channel Number:

Encryption:

Key Length:

Key Format:

Key Setting:

Key Length: For 64bits WEP key, 10 hexadecimal digitals leading by **0x** can be entered. For 128bits WEP key, 26 hexadecimal digits leading by **0x** can be entered.

Key Format: The keys can be entered in ASCII or Hexadecimal. Select the item from drop-down list you wish to use.

Key Setting: A password is requested here.

Note: 128 bits WEP is most secure, but has more encryption/decryption overhead. Note that all wireless devices must support the same WEP encryption bit size and have the same key.

b. Encrypt Type - WPA, WPA2 & WPA2 Mixed

The WPA and WPA2 encrypt each frame transmitted from the radio using the pre-shared key (PSK) which entered from this panel or a key got dynamically through 802.1x.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

SSID:	<input type="text" value="11N_Broadband_Router"/>
Channel Number:	<input type="text" value="11"/>
Encryption:	<input type="text" value="WPA"/>
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>
Pre-Shared Key:	<input type="text"/>
	<input type="button" value="Cancel"/> <input type="button" value="Back"/> <input type="button" value="Finished"/>

WPA (TKIP) and WPA2 (TKIP): Allow the access from WPA clients simultaneously and the encryption keys are given from PSK respectively.

Pre-Shared Key Format: The keys can be entered in ASCII, 8~63 ASCII characters, for example, "0123456789ABCD...." or Hex, 64 bytes hexadecimal digits (0~9, a~f, and A~F). Select the item from drop-down list you wish to use and enter your **Pre-Shared Key**.

After checking each above and choose the suitable item by demand, click **Finished** to proceed.

5.2.4 Basic Setup Complete

The Basic Setup has been completed successfully when you see this screen.



Change setting successfully!

System is configuring, after 86 seconds....

The system will be rebooted automatically and go to the product's diagram homepage. You may connect to Internet via wired or wireless at this moment according to above settings.

Chapter 6 Advanced Configuration

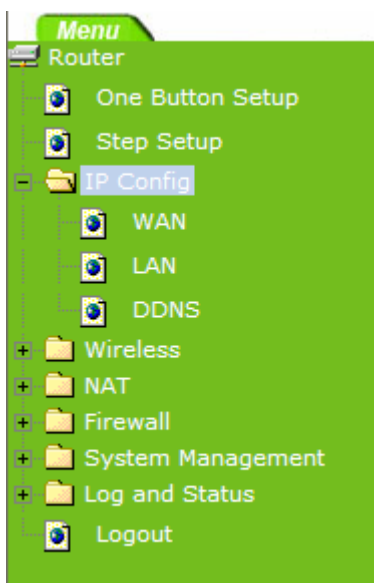
6.1 IP Configuration

This function allows you to add routing rules into 11n Broadband Router. It is useful if you connect several computers behind 11n Broadband Router to share the same connection to Internet.

6.1.1 WAN

Select **WAN** under the **IP Config** menu. 11n Broadband Router supports 3 interfaces and 4 access types. Follow the instructions below for each to set up accordingly.

Choose your WAN Interface and WAN type, and click **Next**, its associated settings will show up.



6.1.1.1 WAN Interface– Ethernet Port

If you are using an Ethernet cable to connect the Internet, please select **Ethernet port**.

6.1.1.2 WAN Interface– Wireless

If you are connecting the internet via wireless, please select **Wireless** and its associated settings will show up underneath at the same time.

You can see a list of available Wireless networks. Select you preferred one to connect and the Encryption type form the drop-down list.

Chapter 7

7.1.1.1 WAN Access Type – Static IP

If you applied for a **Static IP** connection type from ISP, please follow the steps to set up your WAN connection.

1. IP Address

Input your IP Address supplied by ISP. If you don't know, please check with your ISP.

2. Subnet Mask

Input Subnet Mask, normally it is **255.255.255.0**.

3. Default Gateway

Input ISP Default Gateway Address. If you don't know, please check with your ISP.

4. MTU Size

MTU stands for Maximum Transmission Unit. For Static IP connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed by Ethernet at the network layer is 1500 byte

5. DNS

If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.

6. Clone MAC Address

Copy the MAC address from the device you had registered to your ISP if your ISP asks for

the specific MAC Address.

7. Enable IGMP Proxy

The **Internet Group Management Protocol (IGMP)** is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.

8. Enable Ping Access on WAN

Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.

9. Enable Web Server Access on WAN

This option is to enable Web Server Access function on WAN.

10. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on Reset to clear all the input data.

7.1.1.2 WAN Access Type –Dynamic IP

If your WAN access type is **Dynamic IP**, please complete the settings as following instructions.

1. Host Name

The host name is optional; but if your ISP requires you to input a specific host name, please put it in, for example, 11n Broadband Router applied from ISP. Generally, Cable Modem will provide the hostname information.

2. MTU Size

MTU stands for Maximum Transmission Unit. For Static IP connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number is 1492 byte

3. DNS

If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.

4. Clone MAC Address

Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.

5. Enable IGMP Proxy

The **Internet Group Management Protocol (IGMP)** is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.

6. Enable Ping Access on WAN

Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.

7. Enable Web Server Access on WAN

This option is to enable Web Server Access function on WAN.

8. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

7.1.1.3 WAN Access Type –PPPoE

If you applied for a **PPPoE** connection type from ISP, please follow the steps to set up your WAN connection.

1. User Name

Input your user name supplied by ISP. If you don't know, please check with your ISP.

2. Password

Input your Password supplied by ISP.

3. Service Name

Input the service name supplied by ISP.

4. Connection Type

It has three types: **Continuous**, **Connect on Demand**, and **Manual**.

5. Idle Time

It is the time of inactivity before disconnecting your PPPoE session. Enter an Idle Time (in minutes) to define a maximum period of time for which the Internet connect is maintained during inactivity. If the connection is inactive for longer than the defined Idle Time, then the connection will be dropped. Either set this to zero or enable Auto-reconnect to disable this feature.

6. MTU Size

MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed by Ethernet at the network layer is 1492 byte

7. DNS

If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.

8. Clone MAC Address

Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.

9. Enable IGMP Proxy

The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.

10. Enable Ping Access on WAN

Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.

11. Enable Web Server Access on WAN

This option is to enable **Web Server Access** function on WAN.

12. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

7.1.1.4 WAN Access Type – PPTP

If you have applied for a **PPTP** connection type from ISP, please follow the steps to set up your WAN connection.\

1. IP Address

Input your IP Address supplied by ISP. If you don't know, please check with your ISP.

2. Subnet Mask

Input Subnet Mask, normally it is **255.255.255.0**.

3. Server IP Address

Input your Server IP Address supplied by ISP. If you don't know, please check with your ISP.

4. User Name

Input the PPTP Account supplied by ISP, for example. If you don't know, please check with your ISP.

5. Password

Input the Password supplied by ISP.

6. MTU Size

MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed is 1460 byte

7. Request MPPE Encryption

Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol

(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.

8. DNS

If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.

9. Clone MAC Address

Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.

10. Enable IGMP Proxy

The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.

11. Enable Ping Access on WAN

Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.

12. Enable Web Server Access on WAN

This option is to enable Web Server Access function on WAN.

13. Apply Changes & Reset

Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

Chapter 8

8.1.1 LAN Interface Setup

Use this page to set up the local IP address and subnet mask for your router. Please select **LAN Interface Setup** under the **IP Config** menu and follow the instructions below to enter the LAN setting page to configure the settings you want.

LAN Interface Setup

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

Device Name:	<input type="text" value="11N_Broadband_Rou"/>
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.1.1"/>
DHCP:	<input type="text" value="Server"/>
DHCP Client Range:	<input type="text" value="192.168.1.150"/> - <input type="text" value="192.168.1.250"/> <input type="button" value="Show Client"/>
Static DHCP:	<input type="text" value="Disabled"/> <input type="button" value="Set Static DHCP"/>
802.1d Spanning Tree:	<input type="text" value="Disabled"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

1. IP Address

The default value of LAN IP address is **192.168.1.1** for this router.

2. Subnet Mask

Input Subnet Mask, normally it is **255.255.255.0**.

3. Default Gateway

Input ISP Default Gateway Address. If you don't know, please check with your ISP.

4. DHCP

Enable or disable DHCP services. The DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer if enabled.

5. DHCP Client Range

Define the DHCP client range and then the DHCP server will assign an IP to the requesting computer from this range. The **Show Client** will display every assigned IP address, MAC address, and expired time. The default range is 192.168.1.100 - 192.168.1.200.

6. 802.1d Spanning Tree

IEEE 802.1d Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

7. Clone MAC Address

Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.

8. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

8.1.2 Dynamic DNS Setting

Dynamic DNS allows you to make an assumed name as a dynamic IP address to a static hostname. Please configure the dynamic DNS below. Please select DDNS under the IP Config menu, and follow the instructions below to enter the DDNS setting page to configure the settings you want.

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider : << DynDNS >>

Domain Name :

User Name/Email:

Password/Key:

Note:

For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)

For DynDNS, you can create your DynDNS account [here](#)

1. Enable / Disable DDNS

Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.

2. Service Provider

Choose correct Service Provider from drop-down list, here including DynDNS, TZO, Changelp, Eurodns, OVH, NO-IP, ODS, Regfish embedded in 11n Broadband Router.

3. Domain Name

This field represents the host name you register to Dynamic-DNS service and expect to export to the world.

4. User Name /Email

User name is used as an identity to login Dynamic-DNS service.

5. Password /Key

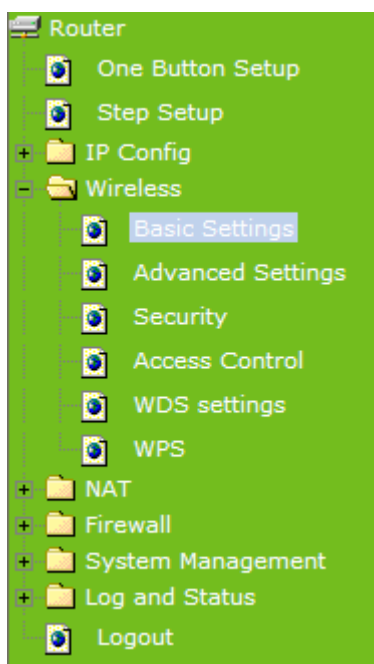
Password is applied to login Dynamic-DNS service.

6. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clear the setting on this page.

8.2 Wireless Setup

11n Broadband Router enables fastest 300 Mbps IEEE802.11g wireless transmissions and keeps compatibility with existing IEEE 802.11n devices. 11n Broadband Router complies with IEEE 802.11b/g standard. Please select **Wireless** under the main menu.



8.2.1 Wireless Basic Settings

Follow the instructions to configure the **Wireless** settings.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▼

Mode: AP ▼

Network Type: Infrastructure ▼

SSID: 11N_Broadband_Router

Channel Width: 40MHz ▼

Control Sideband: Upper ▼

Channel Number: 11 ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface: ESSID_11N_Broadband_Router

1. Disable Wireless LAN Interface

Select **Disable Wireless LAN Interface** to turn off the wireless function.

2. Band

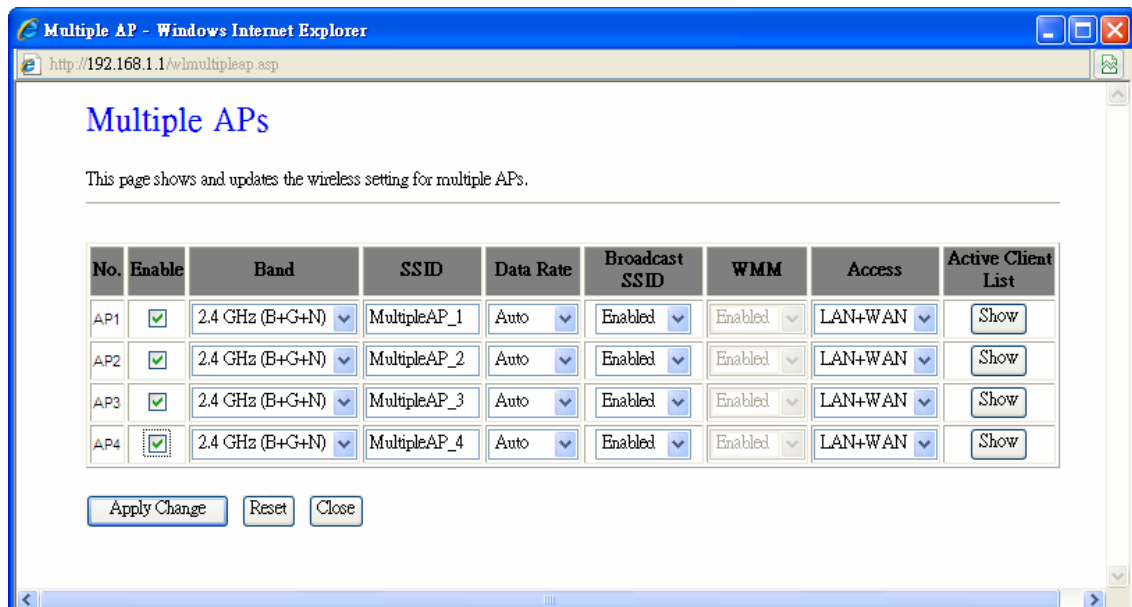
This field indicates the 802.11x interface mode. For example, “**2.4GHz(G)**” prevents the 802.11b clients from accessing the router. “**2.4GHz(B+G)**” allows both 802.11b and 802.11g clients to access the router. There are 6 options, 2.4 GHz (B/G/N/B+G/G+N/B+G+N) from the drop down list.

3. Mode

Select **AP**, **WDS**, or **AP+WDS** to allow or disallow the wireless operation.

► **Multiple APs**

Click Multiple APs to set up 4 different SSIDs to deploy a shared WLAN. Users can add or limit the properties for each SSID, increasing the flexibility and efficiency of the network.



- (1) **Enable:** check it for enable or not.
- (2) **Band:** select the frequency from the drop down list.
- (3) **SSID:** please enter different SSID in each class.
- (4) **Data Rate:** please select the data transmission rate.
- (5) **Access:** defined the access type.
 - a. **LAN+WAN:** the client can access to the Internet and connect to 11N Broadband Router’s GUI to setup.
 - b. **WAN:** the client can only access to the Internet.
- (6) **Active Client List:** display the properties of the client which is connecting successfully.
- (7) **Apply Changes:** Please click **Apply Changes** to initiate or click **Reset** to cancel.

4. Network Type :

Please select “**Infrastructure**” or “**Ad hoc.**” The default is “**Infrastructure.**” The selection is disabled when wireless mode is selected to AP.

5. SSID :

Please input your wireless network name. Default is "11N_Broadband_Router".

6. Channel Width

Please select "20MHZ" or "40MHZ" channel width to change the transmission channels.

7. ControlSideband

Setting the Sideband "Upper" or "lower."

8. Channel Number

Please select your wireless network channel. There are Auto, 2~11.

9. Broadcast SSID

Enable or disable the SSID broadcast function. Disable this feature can provide more security of your WLAN.

10. Data Rate

Rate at which data can be communicated (bps); auto, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M or 54M to be selected from the drop-down list.

11. Associated Clients

Check the WiFi ISP connectors and the connecting status.

12. Enable Mac Clone (Single Ethernet Client)

Copy the MAC Address for identity of some ISPs.

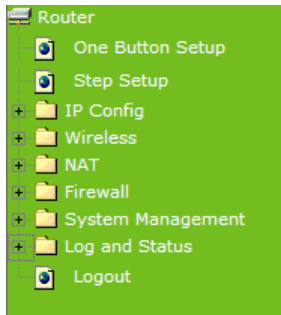
13. Enable Universal Repeater Mode (Acting as AP and Client simultaneously)

Enable **Universal Repeater Mode**, 11n Broadband Router will act as a wireless AP and AP client at the same time, and able to link to another AP.. It uses AP client function to connect to a Root AP (any AP) and uses AP function to service all wireless stations within its coverage. All the stations within the coverage of 11n Broadband Router can be bridged to the Root AP. It can help user to extend the coverage of wireless network.

▶ How to Enable URM (Universal Repeater Mode)

User could enable URM in wireless basic setting page as shown in following figures.

Step 1. Get back to menu "Network Config" and write down the SSID, channel and security.



Encryption	Disabled
MAC	00:e0:4c:81:96:b2
Associated Clients	0
WirelessRepeater Interface Configuration	
Mode	Infrastructure Client
ESSID	ESSID_11N_Broadband_Router
Encryption	Disabled
MAC Address	00:00:00:00:00:00
State	Scanning
LAN Configuration	

Step 2. Setting the same SSID, channel and security you got from “Network Config” and Click on **Apply Changes** to save the setting

Channel Number: 9

Broadcast SSID: Disabled

WMM: Disabled

Data Rate: Auto

Associated Clients: Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface: ESSID_11N_Broadband_Router

Note: If you want to change the setting for Mode and SSID, you must go to EasyConfig page to disable EasyConfig first.

Apply Changes **Reset**

Note: The DHCP server should be disabled under menu “**LAN Interface Setup**” and then the URM could be enabled.

Step 3. Check the AP connectors and the Wireless connecting status.

14. SSID of Extended Interface

When mode is set to “AP” and Universal Repeater Mode is enabled, user should input SSID of another AP (the upper level device) in the field of **SSID of Extended Interface**.

15. Apply Changes & Reset

Click on “**Apply Changes**” to save the setting data. Or you may click on “**Reset**” to clear all the input data.

Chapter 9

9.1.1 Wireless Advanced Settings

Please follow the instructions to configure the **Wireless** settings.

1. Fragment Threshold

To identify the maximum length of packet, the overflow packet length will be fragmented. The allowed range is 256-2364, and default length is 2346 bytes.

2. RTS Threshold

This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.

3. Beacon Interval

Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.

4. Preamble Type

The preamble (also called “a header”) is a section of data at the head of a packet that contains information that wireless devices need when they send and receive packets. Short preambles improve throughput performance, but some wireless devices require long preambles. Select the suitable preamble as short or long preamble.

5. IAPP

Inter Access Point Protocol. Allow seamless roaming between Access Points in your wireless network. Coupled with superior RF performance

6. Protection

Select to enable the wireless protection or not.

7. Aggregation

Data aggregation can reduce the amount of data routed through the network, and increasing throughput.

8. Short GI

Enabling the Short Guard Interval increases the wireless transmission.

9. Apply Changes & Reset

Click on “Apply Changes” to save the setting data. Or you may click on “Reset” to clear all the input data.

9.1.2 Wireless Security Setup

4 encryption types can be selected here, please follow the instructions below for each.

Wireless Security Setup

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

Select SSID:

Encryption:
802.1x Authentication:

1. Encryption – WEP

Enabling WEP can protect your data from eavesdroppers. If you do not need this feature, select “None” to skip the following setting. 11n Broadband Router supports both 64-bit and 128-bit encryption using the Wired Equivalent Privacy (WEP) algorithm. Select the type of encryption you want to use (64 or 128 bit) and configure one to four WEP Keys. The “1280bit” method is more secure than the “64-bit”.

Wireless Security Setup

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

Select SSID:

Encryption:

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length:

Key Format:

Encryption Key:

2.

► Use 802.1x Authentication

Enable 802.1x Authentication so that a wireless node must be authenticated before it can gain access to other LAN resources.

Key Length: For 64bits WEP key, either 5 ASCII characters or 10 hexadecimal digits leading by 0x can be entered. For 128bits WEP key, either 13 ASCII characters or 26 hexadecimal digits leading by 0x can be entered.

Note: 128 bits WEP is most secure, but has more encryption/decryption overhead. Note that all wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Select the item from drop-down list you wish to use.

Encryption Key: At most four keys can be set. A WEP key is either 10 or 26 hexadecimal digits (0~9, a~f, and A~F) based on whether you select 64 bit or 128 bit in the WEP drop-down list.

3. Encryption – WPA (WPA, WPA2 & WPA Mixed)

The WPA, WPA2 & WPA Mixed encrypt each frame transmitted from the radio using the pre-shared key (PSK) which entered from this panel or a key got dynamically through 802.1x.

Wireless Security Setup

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

Select SSID:

Encryption:

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

RADIUS Server IP Address:

RADIUS Server Port:

RADIUS Server Password:

► WPA Authentication Mode

Enterprise (RADIUS): Please input the port, IP address, and password of authentication RADIUS Server.

Personal (Pre-Shared Key): Pre-Shared Key type is coding in ASCII, and the length is between 8 to 63 characters. If the coding is in Hex, the key length is 64 characters.

4. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

9.1.3 Wireless Access Control

With the MAC address, you may allow or disallow the access to your AP.

Wireless Access Control

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

Wireless Access Control Mode:

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		

1. Wireless Access Control Mode

“**Allowed Listed**” means only the MAC address listed on the allowed list can access to your wireless network.

“**Deny Listed**” means the listed MAC Address are not allowed to link to your wireless network.

“**Disable**” for function disuse.

2. MAC Address

Please input the allowed or denied MAC address, for example, 001122334455.

3. Comment

You may input the comments for the set MAC Address.

4. Apply Changes & Reset

Click on “Apply Change” to save the setting data. Or you may click on “Reset” to clear all the input data.

5. Current Access Control List

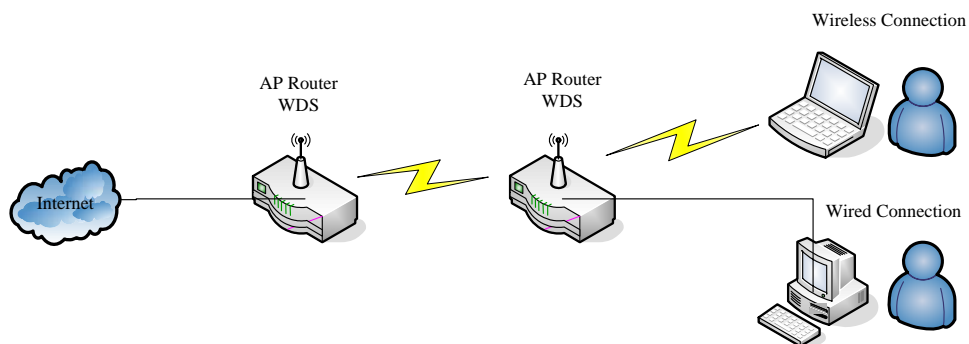
In this list, all the MAC info you input will be displayed.

6. Delete Selected and Delete All

Click on “**Delete Selected**” to erase the selected MAC address. Click on “**Delete All**” to erase all the entered MAC Address.

9.1.4 WDS Settings

WDS (Wireless Distribution System) is a Wireless Access Point mode that enables wireless bridging in which only WDS APs communicate with each other (without allowing for wireless clients or stations to access them), and/or wireless repeating in which APs communicate both with each other and with wireless stations (at the expense of half the throughput).



Please follow the instructions to setup WDS connections.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

Data Rate:

Comment:

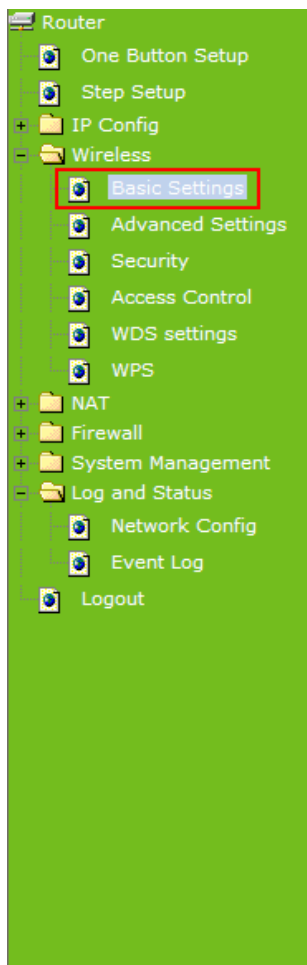
Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Step 1. Check the MAC address and Channel number of the device you want to setup WDS with 11n Broadband Router.

WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11N_Broadband_Router
Channel Number	11
Encryption	Disabled
MAC Address	00:0e:68:ff:05:ae
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:0e:68:ff:05:ae

Step 2. Get back to the menu “Wireless Basic Settings” of 11n Broadband Router. Select **AP+WDS** mode, and then select the Channel Number. Click **Apply Changes** to save the setting data.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▼

Mode: AP+WDS ▼ Multiple AP

Network Type: Infrastructure ▼

SSID: 11N_Broadband_Router

Channel Width: 40MHz ▼

Control Sideband: Upper ▼

Channel Number: 11 ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients: Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface: ESSID_11N_Broadband_Router

Apply Change Reset

Step 3. Enter the WDS Settings page, select Enable WDS, and then input the MAC address of the paired device. Click Apply Changes to save the setting data.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Step 4. When the time counts down to 0, you will see the MAC address of the paired device displaying on **Current WDS AP List**.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:0e:68:ff:05:c8	Auto		<input type="checkbox"/>

Step 5. Head back to LAN Interface, disable DHCP option, and then click Apply Changes to save the setting data.

LAN Interface Setup

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

Device Name:	<input type="text" value="11N_Broadband_Rou"/>
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	Server <input type="button" value="v"/>
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
Static DHCP:	Disabled <input type="button" value="v"/> <input type="button" value="Set Static DHCP"/>
802.1d Spanning Tree:	Disabled <input type="button" value="v"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

Step 6. Doing the same way to setup the MAC address in the paired device. Launch the UT to the menu “**WDS settings**” of the paired device, and input router’s MAC address. Click **Apply Changes** to save the setting data.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address: → Input the MAC address here.

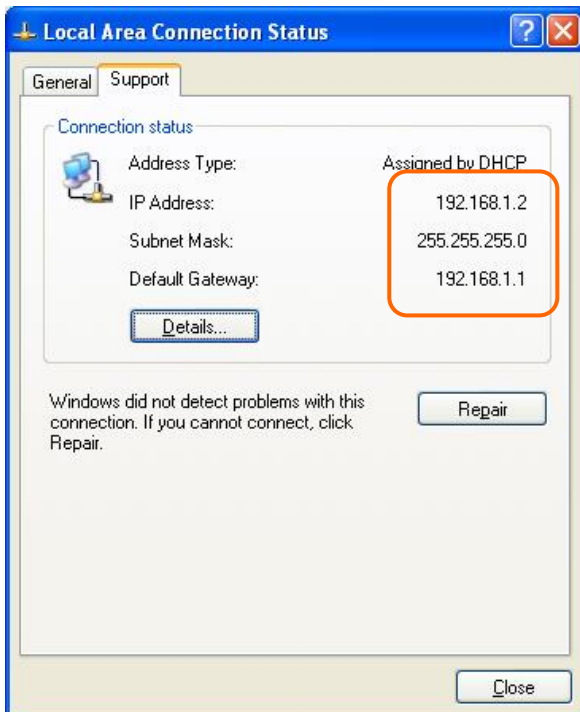
Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Step 7. After initiating the paired device, please check Local Area Connections. Click Supports to check out the IP address which is assigned by the paired device.



Step 8. You can input <http://192.168.9.9> in IE browser to enter the GUI page of the paired device and make sure the connection.



Chapter 10

10.1.1 WPS

Wi-Fi Protected Setup (WPS) is an easy way to establish a secured wireless network between 11n Broadband Router and wireless card. Users do not need to manually entering a creative, yet predictable security key on both Wi-Fi devices to prevent unwanted access to their wireless network. With WPS, it can automatically configure a wireless network with a network name (SSID) and strong WPA data encryption and authentication.

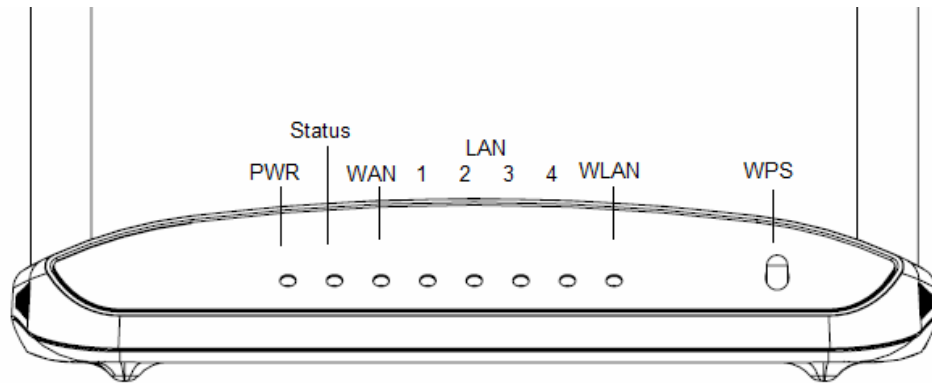
WPS can be enabled by 2 methods:

1. **PBC (Push button configuration) Method**, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.
2. **PIN (Personal Identification Number) Method**, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

Please follow instructions below to enable the WPS function.

- ▶ **Start PBC:**

- (1.) Press the **WPS button** from 11n Broadband Router or click **Start PBC** from menu “Wi-Fi Protected Setup”, and waiting for the WPS wireless card setting.



OR

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number: 18864540

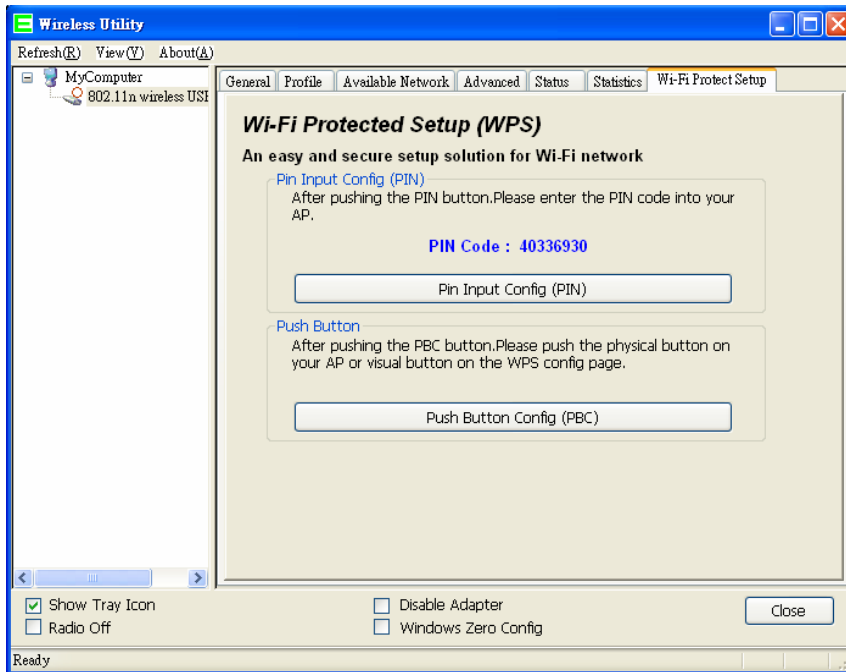
Push Button Configuration:

Current Key Info:

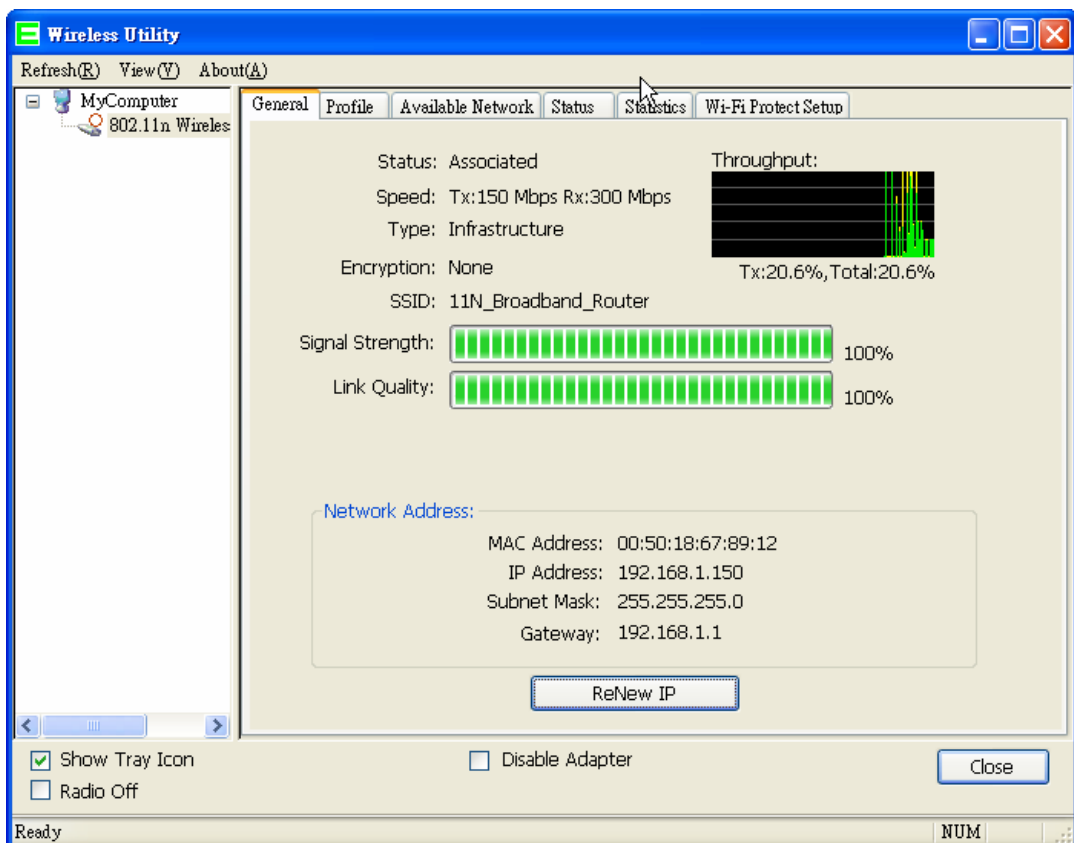
Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

- (2.) Open the “Wireless Utility” of your wireless card, and click its “PBC” button, to start auto pairing.

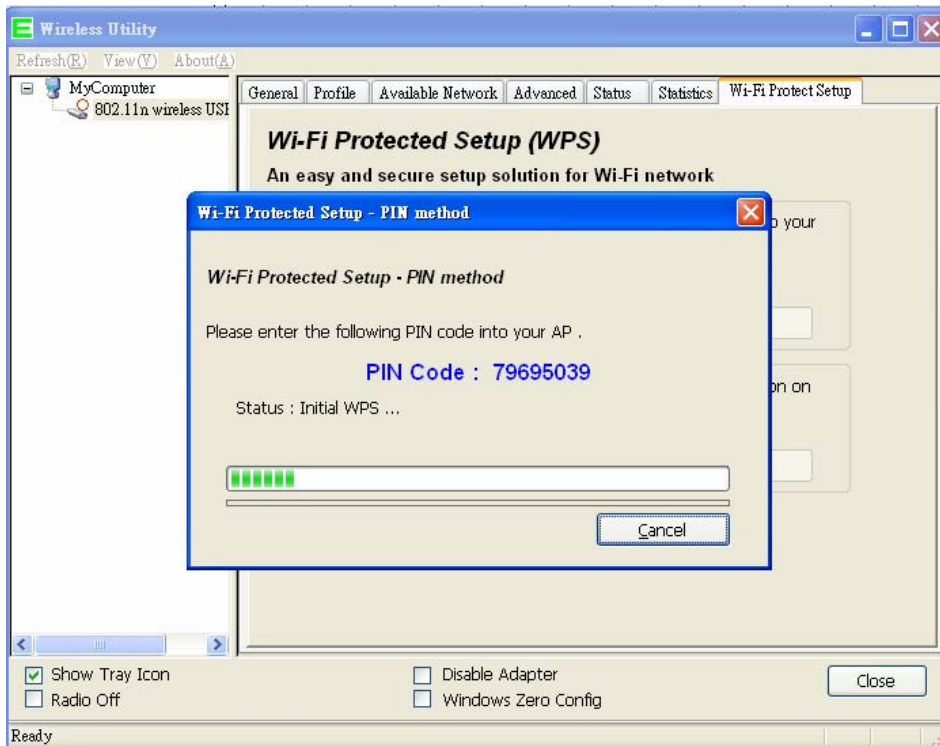


- (3.) While scanning is successful, the information of the wireless card appears in the windows below.



► **Start PIN:**

- (1.) Open the “Wireless Utility” of your wireless card. Follow its PIN instruction to get a new PIN number. Write it down.



- (2.) Open menu “Wi-Fi Protected Setup” of 11n Broadband Router, input the PIN number from the wireless card then click **Start PIN**.

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number: 18864540

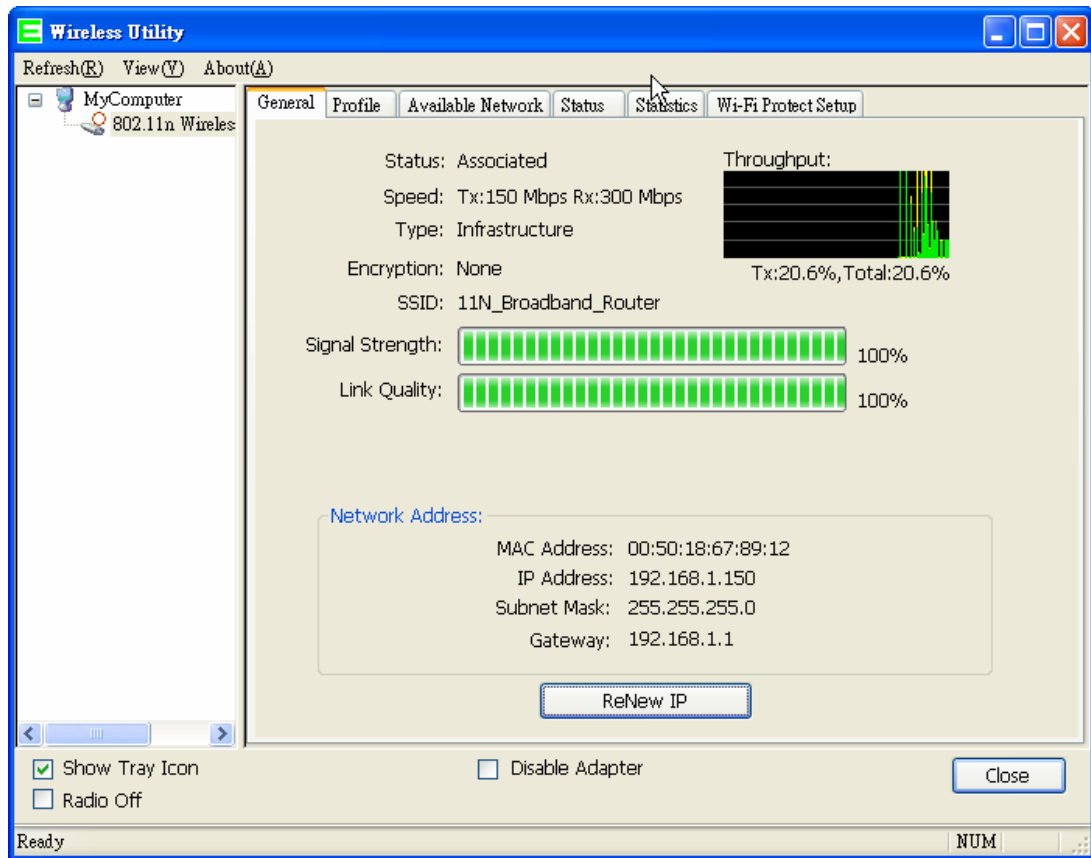
Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number: **Enter the PIN Code you got from the wireless card.**

- (3.) Back to “Wireless Utility” and press the “Start PIN” button to complete the auto-pairing process.

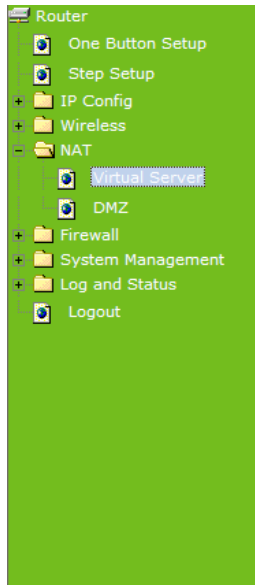


10.2 NAT

NAT is a method of mapping one or more IP addresses and/or services ports into different specified services, where NAT stands for Network Address Translation. It allows the internal IP addresses of many computers on a Local Area Network (LAN) to be translated to one public address, saving users' cost. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. For convenience, we called a router having the NAT facility as a NAT-enabled router.

10.2.1 Visual Server

To offer services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server. Then, add the IP address and network protocol type, port number, and name of the service in the following list. Based on the list, the gateway will forward service request from outside users to the corresponding local server.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

Address : Protocol: Both ▾

Public Port Range: - Private Port Range: -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Public Port Range	Private Port Range	Comment	Select
------------------	----------	-------------------	--------------------	---------	--------

1. Enable Port Forwarding

Enable Port Forwarding to allow an external user to reach a port within a private LAN.

2. IP Address

Specify the private IP address of the internal host offering the service.

3. Protocol

Specify the transport layer protocol (TCP or UDP).

4. Port Range

Enter the Start and End ports in the range you'd like to forward. If you're just forwarding 1 port, set them both equal. For example 80-80 or 20-22.

5. Comment

You can add comments for this port forwarding rule.

6. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

7. Current Port Forwarding Table

It will display all port forwarding regulation you made.

8. Delete Selected & Delete All

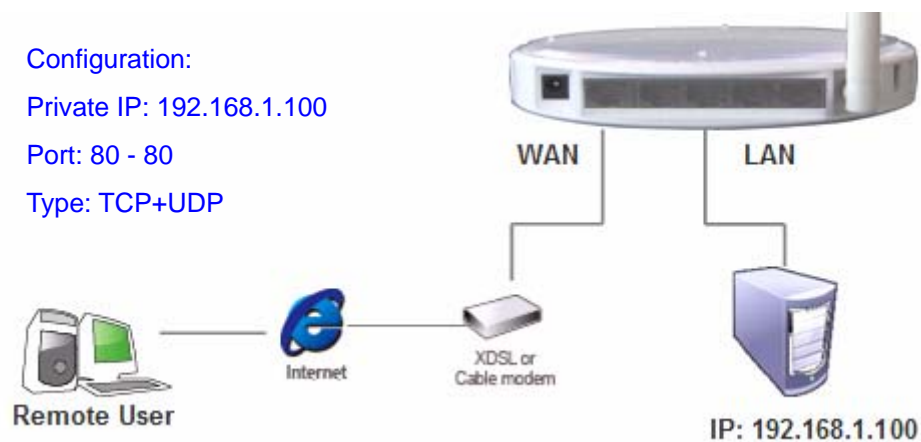
Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

9. Reset

You can click **Reset** to cancel.

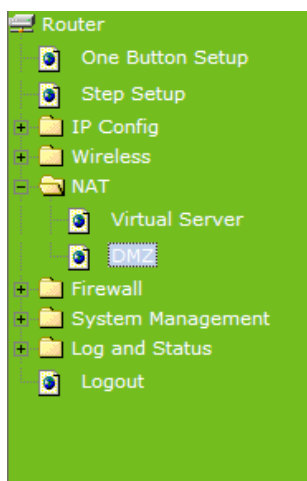
▶ Port Forwarding

The following figure shows the ip forwarding configuration of your web on a local area network. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.



10.2.2 Visual DMZ

Virtual DMZ allows you to expose one computer to Internet, so that all inbound packets will be redirected to the computer you set. It is useful while you run some applications that use uncertain incoming ports. Please use it carefully.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ

DMZ Host IP Address:

1. Enable DMZ

Check **Enable** to apply Virtual DMZ for the Router.

2. DMZ Host IP Address

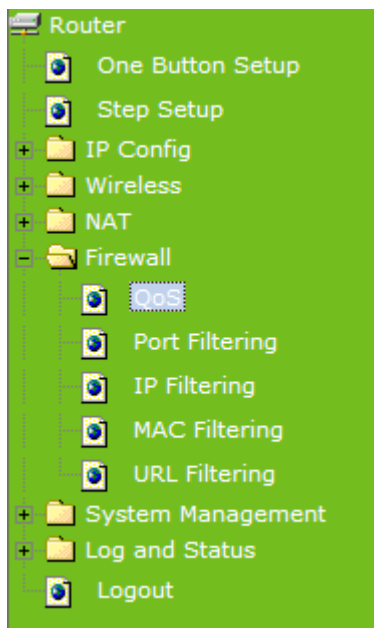
This field stands for the destination IP address that you like to redirect the matched packet to.

3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

10.3 Firewall

The Firewall function helps to protect your local network against attacks from outside. It also provides a way of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.



10.3.1 QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous

Transfer Mode (ATM), Ethernet and 802.1x networks, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN and service provider networks. This chapter provides each setting of QoS.

QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps):

Automatic Downlink Speed

Manual Downlink Speed (Kbps):

QoS Rule Advanced Settings:

Address TypeA: IP MAC

Local IP Address: -

Port: - (1 ~ 65535)

Protocol:

Mode:

Bandwidth (Kbps):

Uplink Bandwidth (Kbps)

Downlink Bandwidth (Kbps)

Comment:

Current QoS Rules Table:

Local IP Address	Port	Protocol	MAC Address	Mode	Uplink Bandwidth (Kbps)	Downlink Bandwidth (Kbps)	Comment	Select

1. Enable QoS

One checkbox appears to activate the QoS control function or not. Click it to force the router

to perform QoS control over traffic flows.

2. Automatic Uplink Speed

Click the checkbox to manage uplink speed automatically.

3. Manual Uplink Speed

Input the number of uplink speed.

4. Automatic Downlink Speed

Click the checkbox to manage downlink speed automatically.

5. Manual Downlink Speed

Input the number of downlink speed.

6. Address TypeA

Select IP or MAC to manage QoS.

7. Mode

Select the type of bandwidth mode.

8. Uplink Bandwidth

Please enter the port number of uplink bandwidth.

9. Downlink Bandwidth

Please enter the port number of downlink bandwidth.

10. Comment

You can add comments for this regulation.

11. Apply Changes

Click on **Apply Changes** to save the setting or **Reset** to clear all the input data.

10.3.2 Port Filtering

This function allows users to filter and manage specific ports; to limit the use of certain applications to transmit through a specific port. Port filtering helps users to improve the security of your network.

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
------------	----------	---------	--------

1. Enable Port Filtering

Check **Enable Port Filtering** to start the service.

2. Port Range

Enter the Start and End ports in the range you'd like them to be filtered.

3. Protocol

Please select the protocol type of the port.

4. Comment

You can add comments for this Port Filtering rule.

5. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6. Current Filter Table

It will display all ports that are filtering now.

7. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

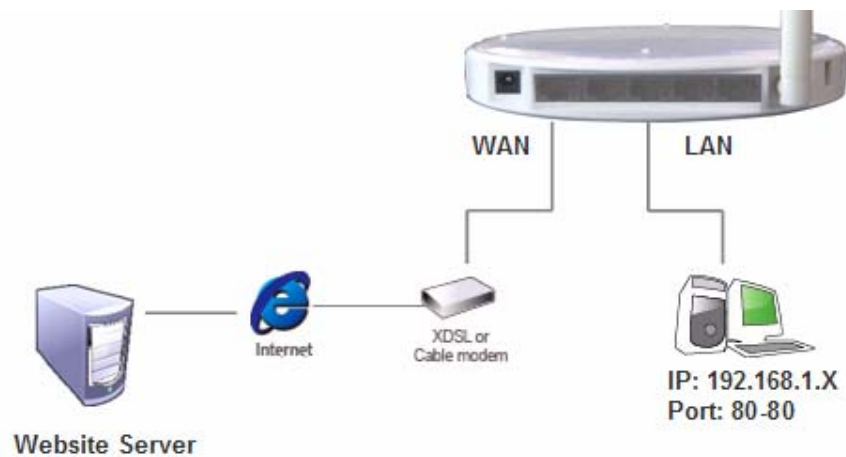
8. Reset

You can click **Reset** to cancel.

► Port Filtering

The following figure shows a user limits some applications to use the 80 port.

**All clients inside the local area network can't open the 80 port through this router.*



10.3.3 IP Filtering

Use IP Filter to deny LAN IP addresses from accessing the Internet. You can deny specific port numbers or all ports for the specific IP address.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address: Protocol: Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
------------------	----------	---------	--------

1. Enable IP Filtering

Check enable or disable to apply IP Filter function.

2. Local IP Address

Please enter the IP address that needs to be filtered.

3. Protocol

Please select the protocol type of the IP address.

4. Comment

You can add comments for this regulation.

5. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6. Current Filter Table

It will display all IP addresses that are filtering now.

7. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

8. Reset

You can click **Reset** to cancel.

10.3.4 MAC Filtering

Use MAC filters to deny LAN computers by their MAC addresses from accessing the Internet. You can manually add a MAC address that is currently connected to 11n Broadband Router.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address: Comment:

Apply Change

Reset

Current Filter Table:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

1. Enable MAC Filtering

Check enable or disable to apply MAC Filter function.

2. MAC Address

Enter the MAC address manually that you want to filter.

3. Comment

You can add comments for this MAC Filtering rule.

4. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5. Current Filter Table

It will display all MAC addresses that are filtering now.

6. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

7. Reset

You can click **Reset** to cancel.

10.3.5 URL Filtering

Keyword based URL (Uniform Resource Locator) filtering allows you to define one or more keywords that should not appear in URL's. Any URL containing one or more of these keywords will be blocked. This is a policy independent feature i.e. it cannot be associated to ACL rules. This feature can be independently enabled / disabled, but works only if firewall is enabled.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL Filtering

URL Address:

Apply Change

Reset

Current Filter Table:

URL Address	Select
-------------	--------

Delete Selected

Delete All

Reset

1. Enable URL Filtering

Check enable or disable to apply URL filter function.

2. URL Address

Enter the URL address into this blank to apply filter blocking, example: "www.yahoo.com."

3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4. Current Filter table

Shows all filtered URL information.

5. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this

table.

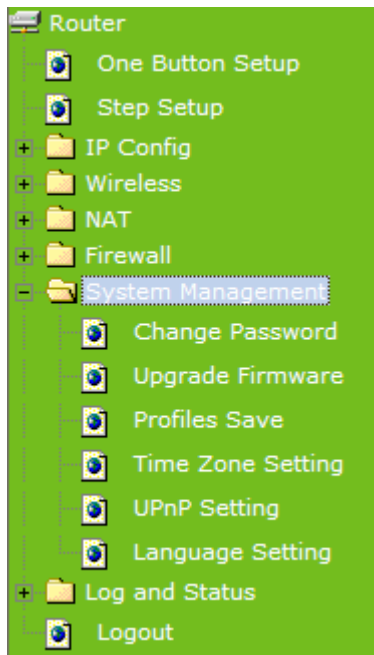
6. Reset

You can click **Reset** to cancel.

Note: URL Filtering cannot work when the Visual Server is enabled. Please disable Visual Server before activate filter.

10.4 System Management

11n Broadband Router provides system management including password changing, upgrade firmware, time setting, user's account setting and other detail settings. Following is detail explanation for each.



10.4.1 Change Password

Administrator can set or change their password in this section.

Change Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name: admin
New Password:
Confirmed Password:

1. New Password

Enter the new password you want to change.

2. New Password (Confirm)

Enter the new password again for confirming.

3. Apply & Cancel

Click **Apply** to continue or **Cancel** to clear the settings on this page.

10.4.2 Upgrade Firmware

There is certain risk while upgrading firmware. Upgrading firmware is not recommended unless the significant faulty is found. You can upgrade the firmware of 11n Broadband Router on this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click **Upgrade Firmware** to proceed.

Firmware Upgrade

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

1. Update Firmware

Click on **Browse...** button to search your local hard drive and locate the firmware to be used for update.

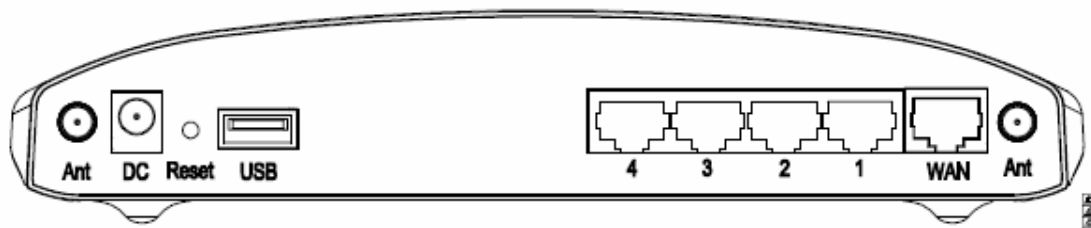
2. Upload & Reset:

Click **Upload** to upgrade the firmware or **Reset** to restore to factory default Settings

Note: 1. To prevent the firmware upgrading interrupted by other wireless signals and caused failure. We recommend using wired connection to do the upgrading.
2. The upgrade firmware will not remove your previous settings.

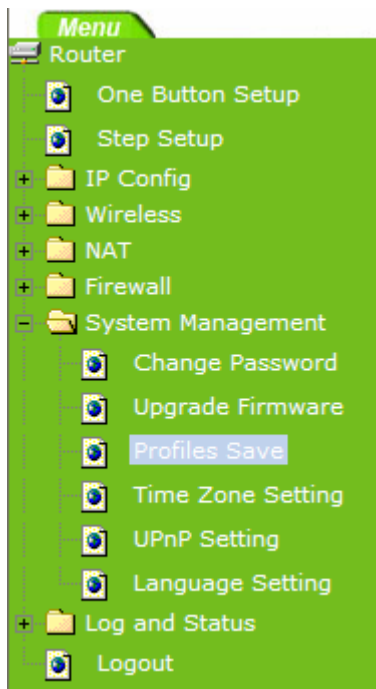
■ Reset button:

On the back of this router, there is a reset button. If you can not login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 10 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



10.4.3 Profiles Save

To back up the current configuration setting or load the backup data, also you can restore 11n Broadband Router to default setting by this function.



1. Save Settings To File

Click on **Save** button for saving the configuration setting into assigned location.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

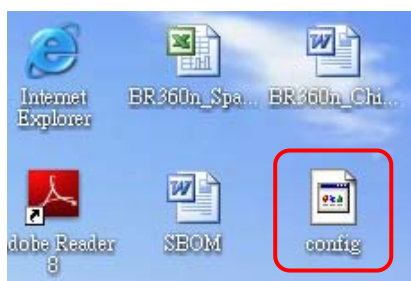
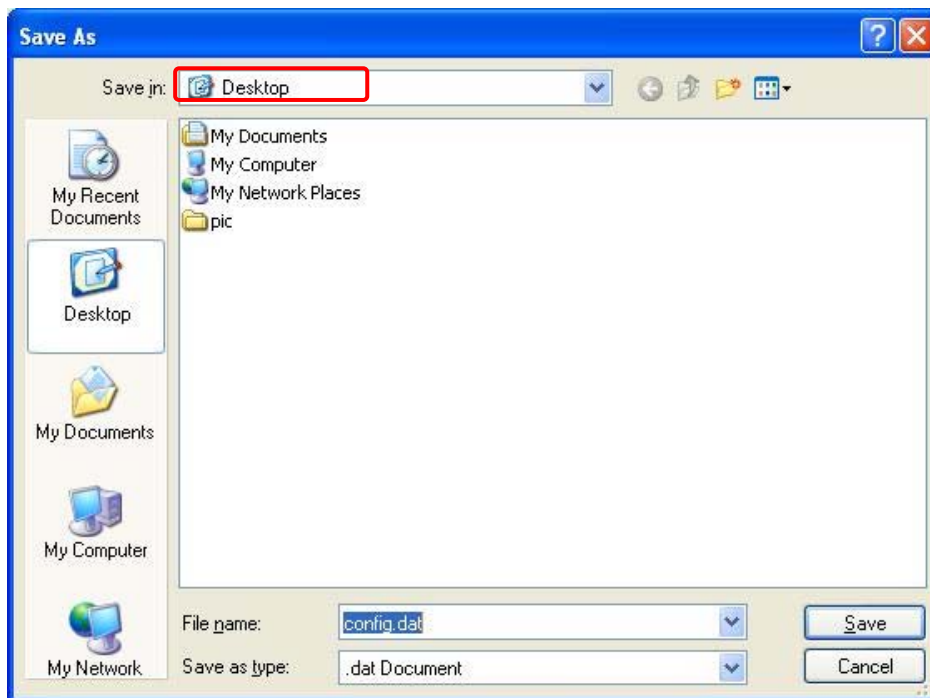
Load Settings from File:

Reset Settings to Default:

A pop window will show up and ask to save **config.dat** file. please select the location (Figure 2), for example: the desktop (Figure 3).



Please select the location, for example: the desktop.



2. Load Settings From File

Click on "**Browse...**" button for searching the saving configuration from hard drive, and then

click on Upload button to load all the settings into the router.

Save/Reload Settings

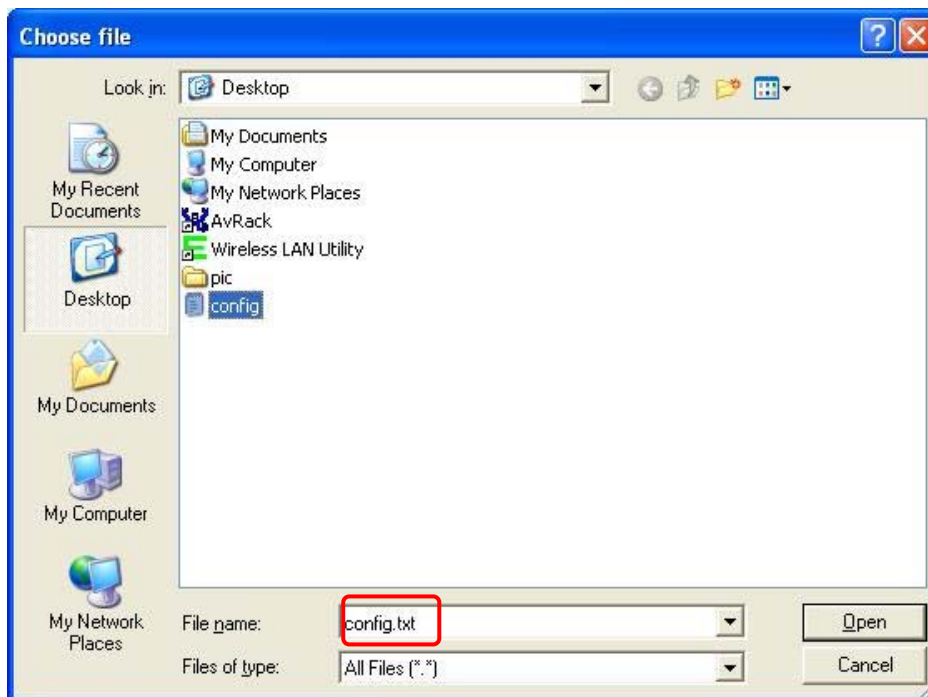
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Select the **config.dat** file.



Click **Upload** to retrieve.

Save/Reload Settings

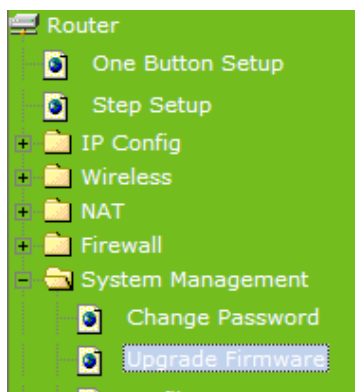
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

When you see the screen below, the updating is completed. Please click **OK** to return to the main menu.



Update Successfully!

OK

3. Reset Setting to Default

After you have tried other methods for troubleshooting your network, you may choose to restore 11n Broadband Router to the factory default settings.

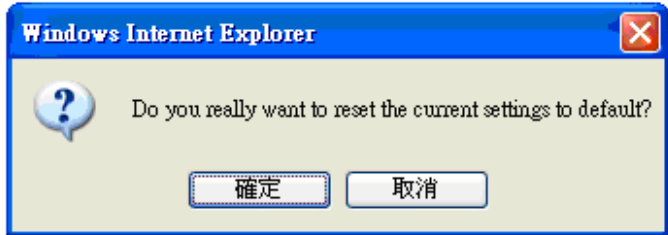
Profiles Save

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

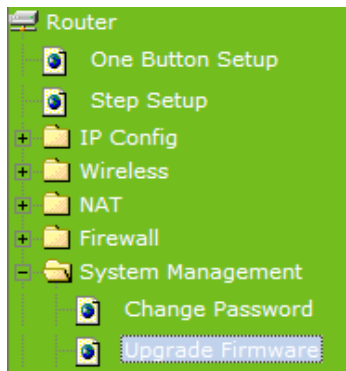
Save Settings to File:

Load Settings from File:

Reset Settings to Default:



When you see the screen below, the resetting is completed. Please click **OK** and return to the main menu.



Reload Setting Successfully!

10.4.4 Time Zone Setting

The System time is the time used by 11n Broadband Router for scheduling services. You can manually set the time or connect to a NTP (Network Time Protocol) server. If a NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

Time Zone Setting

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

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server : (Manual IP Setting)

1. Current Time

Users can input the time manually.

2. Time Zone Select

Select your time zone location from the drop-down list.

3. Enable NTP client update

Check to enable NTP client update.

4. Automatically Adjust Daylight Saving

If you are in daylight saving time area, please enable this item.

5. NTP server

Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.

6. Apply Changes & Reset & Refresh

Please click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data. Or you may click on **Refresh** to update the system time on the screen.

7. NTP Server Type & Default NTP Server

Choose “**General Time Server**” and select the NTP Server from the drop-down list or choose “Customized Time Server” and enter the server by manual.

10.4.5 UPnP Setting

UPnP (Univsersal Plug and Play) allows users to connect their UPnP-enabled broadband router, printer server and other devices right to the network with zero-configuration, meaning easier setup for installing the device on the network. The automatic discovery feature enables the device to obtain an IP address, present and describe itself to other devices and PCs on the network without having to install drivers, but to configure and use those devices.

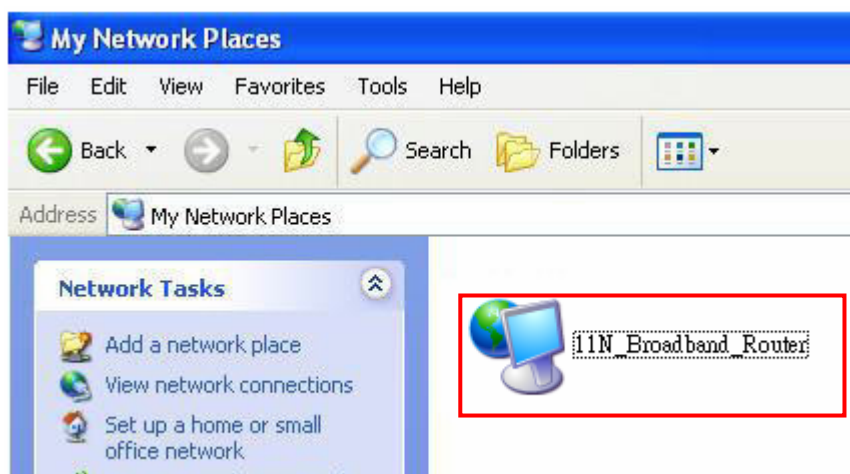
UPnP Setting

In this page,you can turn on or turn off the UPNP feature of your router.

Enable/Disable UPNP: Enabled Disabled

1. Enable/Disable UPnP

Enabling UPNP, click **My Network Places**, and user can open the web GUI by just clicking on the **Internet Gateway Device** icon.



10.4.6 Language Setting

11n Broadband Router provides a user friendly interface in 12 languages. You can create your own language interface by following steps.

Step 1. Select Language: Select your preferred language from the drop down list, for example, Deutsch, and then click **Apply Changes**.

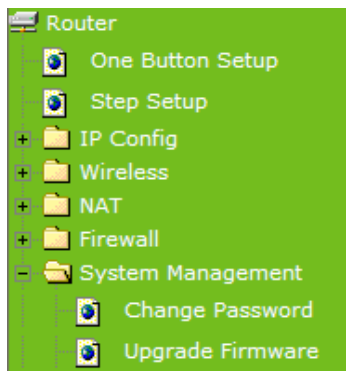
Language Setting

This page allows you setup the GUI language.

Select language:

English	▼	Apply Change
English		
繁體中文		
简体中文		
日本語		
Русский		
Deutsch		
Français		
العربية		
Español		
Português		
한국어		
Italiano		

Step 2. When you see the screen with message in your selected language, the Language setup is completed.

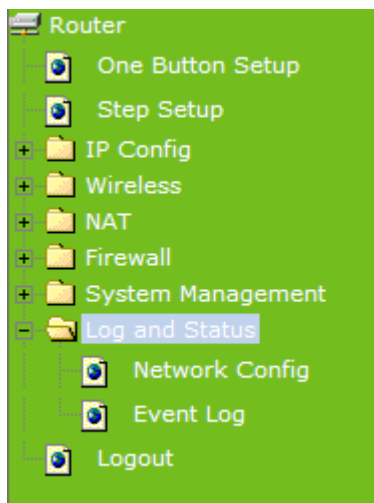


성공의 변화 조정!
체계는 체계가 이전 페이지에 돌려보낼 30 초 후에, 형성하고 있다.

Note: In order to prevent the incomplete translation, you can press "CTRL+F5" to force reload of the page.

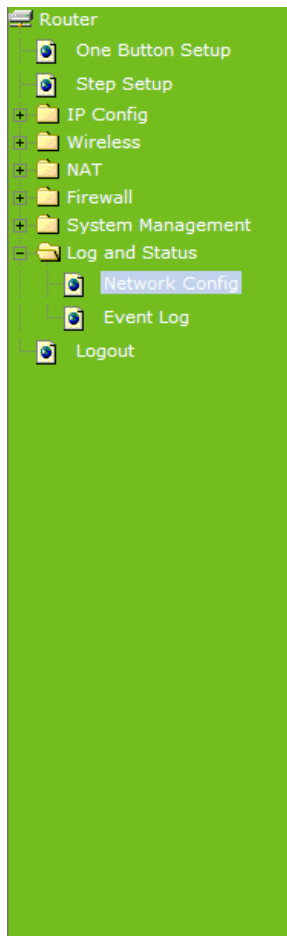
10.5 Log & Status

11n Broadband Router provides the log list and connection status for user to check.



10.5.1 Network Config

Network Configuration shows the firmware version and the connection status of LAN, WAN and Wireless.



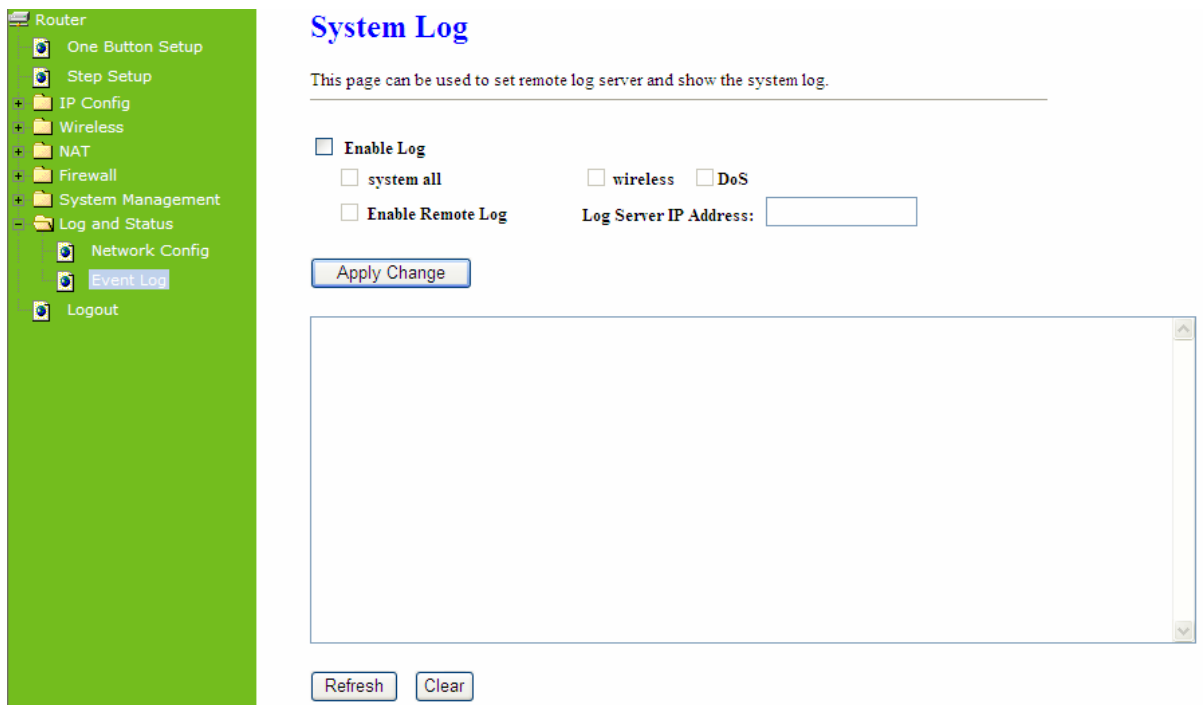
Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:3h:6m:42s
Firmware Version	Ver0.0.6
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	11N_Broadband_Router
Channel Number	11
Encryption	Disabled
MAC Address	00:0e:68:ff:05:ae
Associated Clients	1
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:0e:68:ff:05:ae
WAN Configuration	
Attain IP Protocol	3.5G Disconnected
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:0e:68:ff:05:af

10.5.2 Event Log

11n Broadband Router provides system logs for review.



1. Enable Log

Select Enable Log to record the system log

2. system all, wireless & DoS

Select **Wireless**, **DoS** or **system all** to record

3. Enable Remote Log

You may choose to enable the remote event log or not.

4. Log Server IP Address

Please input the log server IP Address.

5. Apply Changes & Refresh & Clear

Click on **Apply Changes** to save the setting data. Click on **Refresh** to renew the system time, or on **Clear** to clear all the record.

- After clicking **Apply Changes** to record the event log, it will be shown as the example below.

Enable Log

system all **wireless** **DoS**

Enable Remote Log **Log Server IP Address:**

```

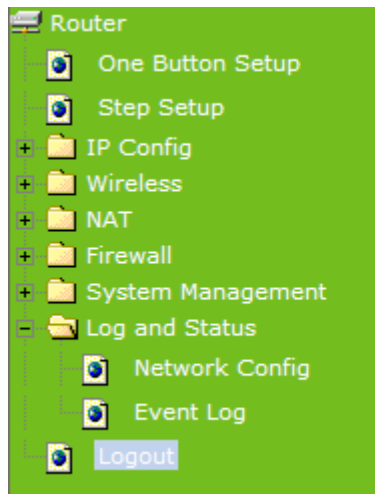
conntrack
Oday 00:00:17 PPTP netfilter connection tracking: registered
Oday 00:00:17 PPTP netfilter NAT helper: registered
Oday 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
Oday 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
Oday 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
Oday 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
Oday 00:00:17 Freeing unused kernel memory: 64k freed
Oday 00:00:17 mount /proc file system ok!
Oday 00:00:17 mount /var file system ok!
Oday 00:00:17 device eth0 entered promiscuous mode
Oday 00:00:17 device wlan0 entered promiscuous mode
Oday 00:00:17 TPT: unreasonable target TSSI 0
Oday 00:00:17 br0: port 2(wlan0) entering listening state
Oday 00:00:17 br0: port 1(eth0) entering listening state
Oday 00:00:17 br0: port 2(wlan0) entering listening state

```


Chapter 11

11.1 Logout

Click **Logout** on the bottom menu to exit and go back to GUI login home page.



Logout

This page is used to logout.

Do you want to logout ?

Chapter 12

Chapter 13

Chapter 14

Chapter 15 DDNS Service Application

DDNS is a service changes the dynamic IP to the static IP. The settings of DDNS can solve the problem of being given the different IP by router every time. After setting the Router, your host name would correspond to your dynamic IP. Moreover, via the host name application, it could be easier for you to use FTP, Webcam and Printer remotely.

Dynamic DNS allows you to make an assumed name as a dynamic IP address to a static host name. Please configure the dynamic DNS below. Please select **Dynamic DNS** under the **IP Config** folder, and follow the instructions below to enter the **Dynamic DNS** page to configure the settings you want.

If you don't have a DDNS account, please follow the steps to complete your DDNS with Dynamic IP settings.

Step 1. First access the Internet and fill <http://www.dyndns.com/> into the address field of your web browser, then click **Create Account**.

The screenshot shows the DynDNS.com website interface. At the top left is the DynDNS.com logo. To the right are input fields for 'User:' and 'Pass:', a 'Login' button, and links for 'Lost Password?' and 'Create Account' (the latter is highlighted with a red box). Below this is a yellow navigation bar with 'About', 'Services', 'Account', 'Support', and 'News'. The main content area features a 'DNSCog beta!' logo, a 'New Diagnostics Tool Now Available' button, a list of system checks (all marked 'Pass'), a 'New to DynDNS.com?' banner, and sections for 'DNS Services' and 'MailHop Services'. A search bar is located at the bottom right, and a news snippet is visible at the bottom left.

Step 2. Fill in the form as required, and then click on **Create Account** button.

Create Your DynDNS Account

Please complete the form to create your free DynDNS Account.

User Information	
Username:	<input type="text"/>
E-mail Address:	<input type="text"/> Instructions to activate your account will be sent to the e-mail address provided.
Confirm E-mail Address:	<input type="text"/>
Password:	<input type="text"/> Your password needs to be more than 5 characters and cannot be the same as your username. Do not choose a password that is a common word, or can otherwise be easily guessed.
Confirm Password:	<input type="text"/>

About You (optional)

Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!

How did you hear about us:	<input type="text" value="---"/>	We do not sell your account information to anyone, including your e-mail address.
Details:	<input type="text"/>	

Terms of Service

Please read the acceptable use policy (AUP) and accept it prior to creating your account. Also acknowledge that you may only have one (1) free account, and that creation of multiple free accounts will result in the deletion of all of your accounts.

Policy Last Modified: February 6, 2006

1. ACKNOWLEDGMENT AND ACCEPTANCE OF TERMS OF SERVICE

All services provided by Dynamic Network Services, Inc. ("DynDNS") are provided to you (the "Member") under the Terms and Conditions set forth in this Acceptable Use Policy ("AUP") and any other operating rules and policies set forth by DynDNS. The AUP comprises the entire agreement between the Member and DynDNS and supersedes all prior agreements between the parties regarding the subject matter contained herein. BY COMPLETING THE REGISTRATION PROCESS AND CLICKING THE "Accept" BUTTON, YOU ARE INDICATING YOUR AGREEMENT TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THE AUP.

2. DESCRIPTION OF SERVICE

I agree to the AUP:	<input checked="" type="checkbox"/>
I will only create one (1) free account:	<input checked="" type="checkbox"/>

- Mailing Lists (optional)

DynDNS maintains a number of mailing lists designed to keep our users informed about product announcements, client development, our company newsletter, and our system status. Please use the checkboxes below to alter your subscription preference. Your subscription preference may be changed at any time through the [account settings](#) page.

newsletters:	<input type="checkbox"/>
press-releases:	<input type="checkbox"/>
system-status:	<input type="checkbox"/>

- Next Step

After you click "Create Account", we will create your account and send you an e-mail to the address you provided. Please follow the instructions in that e-mail to confirm your account. You will need to confirm your account within 48 hours or we will automatically delete your account. (This helps prevent unwanted robots on our systems)

[Create Account](#)

Step 3. When you got this account created message, close it, and check your mailbox. You would get a mail from DynDNS website.

The screenshot shows the DynDNS website interface. At the top left is the DynDNS logo. To the right are input fields for 'User:' and 'Pass:' with a 'Login' button. Below these are links for 'Lost Password?' and 'Create Account'. A navigation bar contains 'About', 'Services', 'Account', 'Support', and 'News'. On the left is a 'My Account' sidebar with links for 'Create Account', 'Login', and 'Lost Password?'. Below the sidebar is a search box with a 'Search' button. The main content area has a grey header 'Account Created' followed by text: 'Your account, TYatLab, has been created. Directions for activating your account have been sent to your e-mail address: clairbleu_ty@hotmail.com. To complete registration, please follow the directions you receive within 48 hours. You should receive the confirmation e-mail within a few minutes. Please make certain that your spam filtering allows messages from support@dyndns.com to be delivered. If you have not received this e-mail within an hour or so, request a [password reset](#). Following the instructions in the password reset e-mail will also confirm your new account. Thanks for using DynDNS!'.

Step 4. Click on the indicated address within your mail to confirm.

Your DynDNS Account 'TYatLab' has been created. You need to visit the confirmation address below within 48 hours to complete the account creation process:

https://www.dyndns.com/account/confirm/Z3OpStScjR_Ypn82CNMyZQ

Our basic service offerings are free, but they are supported by our paid services. See <http://www.dyndns.com/services/> for a full listing of all of our available services.

If you did not sign up for this account, this will be the only communication you will receive. All non-confirmed accounts are automatically deleted after 48 hours, and no addresses are kept on file. We apologize for any inconvenience this correspondence may have caused, and we assure you that it was only sent at the request of someone visiting our site requesting an account.

Sincerely,
The DynDNS Team

Step 5. Click on **login**.




Account Confirmed

The account TYatLab has been confirmed. You can now [login](#) and start using your account.

Be informed of new services, changes to services, and important system maintenance/status notifications by subscribing to our [mailing lists](#). Once there, you may subscribe to the Announce list by checking the appropriate box and clicking the "Save Settings" button.

Step 6. Click **My Services** after logging in.

Account Summary for TYatLab

My Services	Billing	Account Settings
 View, modify, purchase, and delete your services.	 Update your billing information, complete a purchase, and view invoices.	 Update your e-mail address, set preferences, and delete your account.
My Zones	View Shopping Cart	Change E-mail Address
Add Zone Services	Active Services	Change Password
My Hosts	Order History	Change Username
Add Host Services	Billing Profile and Vouchers	Contact Manager
Account Upgrades	Renew Services	Mailing Lists

Step 7. Click **Add New Hostname**.

Account Level Services

Paid Account (?)	No	Technical Support
Account Upgrades (?)	No	View - Add
DNS Service Level Agreement (?)	None	Add DNS Service Level Agreement
Premier Support Option (?)	None Available	Add Premier Support Cases

Zone Level Services

[Add Zone Services](#)

No zone level service items registered: [Add Zone Services](#).

Hostnames

[Add New Hostname](#)

No Hostname services registered.

Step 8. Put in your favorite hostname and service type, and then click **Create Host** after finished.

Hostname: . webhop.net ▼
Wildcard: Yes, alias "*.hostname.domain" to same settings.
Service Type: Host with IP address
 WebHop Redirect
 Offline Hostname ?

IP Address:
[Use auto detected IP address](#)
 TTL value is 60 seconds. [Edit TTL](#).

Mail Routing: Yes, let me configure Email routing.

Create Host

Step 9. Your hostname has been created when you see the following page.

[Add New Hostname](#) - [Host Update](#)

Host Services

Hostname [amigo.webhop.net](#) created.

Hostname	Service	Details	Last Updated
amigo.webhop.net	host	210.68.117.196	Nov. 19, 2007 4:08 AM

Chapter 16

Chapter 17 Q & A

17.1 Installation

1. Q: Where is the XDSL Router installed on the network?

A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. Q: Why does the throughput seem slow?

A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the network does not exceed 10 broadcast messages per second.
- Verify network topology and configuration.

17.2 LED

1. Why doesn't 11n Broadband Router power up?

A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. The Internet browser still cannot find or connect to 11n Broadband Router after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.

A: In case 11n Broadband Router is inaccessible, you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 10 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. Why does 11n Broadband Router shut down unexpectedly?

A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

17.3 IP Address

1. Q: What is the default IP address of the router for LAN port?

A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. Q: I don't know my WAN IP.

A: There are two ways to know.

Way 1: Check with your Internet Service Provider.

Way 2: Check the setting screen of 11n Broadband Router. Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. How can I check whether I have static WAN IP Address?

A: Consult your ISP to confirm the information, or check Network Configuration in 11n Broadband Router's Main Menu.

4. Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?

A: Yes, the Router mode allows for customization of your public IPs and Domain.

17.4 OS Setting

1. Why can't my computer work online after connecting to 11n Broadband Router?

A: It's possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start > Settings > Network and Dial-up Connections >** double click on **Internet Protocol(TCP/IP) >** select **obtain IP address automatically >** Click on **OK** button. Then, open Internet browser for testing. If you still can't go online, please test something else below.

- Verify network configuration by ensuring that there are no duplicate IP addresses.
- Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
 1. Check that the cables and connectors or use another LAN cable.

2. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being

displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

3. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

17.5 11n Broadband Router Setup

1. Q: Why does 11n Broadband Router's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in 11n Broadband Router's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: Why can't my USB devices and LAN ports work properly after setting the DHCP?

A: There are two rules over here.

Rule1: After connecting USB devices, please reboot your Router.

Rule2: Before finishing the DHCP setup, please don't connect any computer to LAN ports, because the conflict of having the same IP may occur and cause some computers a lot of trouble.

※Notice: Make sure that you always click on the Apply button after configuring each setting. And in order to let other LAN ports work properly, please reboot your PC.

3. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via 11n Broadband Router. Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server** under the **IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

4. Q: How do I upgrade the firmware of 11n Broadband Router?

A: Periodically, a new Flash Code is available for 11n Broadband Router on your product supplier's website. Ideally, you should update 11n Broadband Router's Flash Code using **Upgrade Firmware** on the **System Management** menu of 11n Broadband Router Settings.

5. Q: My **11N Broadband Router** cannot connect to the ISP?

A: There are three possible solutions.

1. Check the Cable/XDSL modem is power on.
2. Check the Cable/XDSL link light is on to verify a good physical connection.
3. Check the WAN port LED to verify if the Cable/XDSL modem is connected to the router:

If your ISP Login method is following, please make sure the username and password are correct or not.

If your ISP is using dynamic IP addressing (DHCP) then the DHCP protocol does not have the authentication feature. Some Cable service providers often use the following to determine user's identification.

6. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

7. Q: **11n Broadband Router** couldn't save the setting after click on **Apply** button?

A: 11n Broadband Router will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboot** under **System Management** directory.

17.6 Wireless LAN

1. Q: Why couldn't my wireless notebook work on-line after checking?

A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. Q: My PC can't locate the Wireless Access Point.

A: Check the following:

- Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. Q: Wireless connection speed is very slow.

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. Q: Some applications do not run properly when using the Wireless Router.

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. Q: I can't connect to the Wireless Router to configure it.

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. Q: The WinXP wireless interface couldn't communicate the WEP with 11n Broadband Router's wireless interface.

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of 11n Broadband Router is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and 11n Broadband Router would be communicated.

17.7 Support

1. Q: What is the maximum number of IP addresses that the XDSL Router will support?

A: The Router will support to 253 IP addresses with NAT mode.

5. Q: Is the Router cross-platform compatible?

A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

17.8 Others

1. Q: Why can't I receive corrupted FTP downloads?

A: If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

2. Q: Why does the router dial out for PPPoE mode very often?

A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

3. Q: What can I do if there is already a DHCP server in LAN?

A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.

17.9 USB Device

1. Q: How many USB devices can be connected to the Product?

A: 11n Broadband Router supports maximum of 1 USB ports.

Chapter 18

Chapter 19

Chapter 20 Appendices

20.1 Operating Systems

1. Microsoft : Windows 2000, XP, Vista 32bit and the following related versions.
2. Apple : Mac OS X 10.4.7, Leopard and the following related versions.
3. Linux : Redhat 9, Fedora 6 & 7, Ubuntu 7.04 and the following related versions.

20.2 Browsers

1. Internet Explorer ver. 6 and 7 and the following related versions.
2. FireFox ver. 2.0.0.11 and the following related versions.3.
3. Safari ver. 3.04 and the following related versions.

20.3 Communications Regulation Information

Should any consumers need to learn more information, services and supports, please contact the supplier of your product directly.

Chapter 21