

# **802.11n Wireless Broadband Router**

**User's Manual**

## FCC Certifications



### Federal Communication Commission Interference 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 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.

This 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this 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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## CE Mark Warning



This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

#### Trademarks:

All trade names and trademarks are the properties of their respective companies.  
Copyright © 2007, All Rights Reserved.

---

## Table of Contents

---

UNPACKING INFORMATION .....	5
INTRODUCTION TO WIRELESS ROUTER .....	5
General Description .....	5
Key Features .....	6
The Front Panel .....	7
The Rear Panel .....	8
Power Connection .....	8
Restore Default Button .....	8
Placement (Optional) .....	8
INSTALLING AND USING WIRELESS ROUTER .....	9
Connecting this Router to your network .....	9
Configuring the IP address of your computer .....	9
MANAGEMENT .....	11
Starting the WEB-Based Management Interface .....	11
The Graphic User Interface .....	12
Network Setting .....	13
WAN Interface Setup .....	13
LAN Interface Setup .....	17
QoS Settings .....	19
Wireless Settings .....	21
Basic Settings .....	21
Advanced Settings .....	22
Security Settings .....	24
Access Control .....	27
WDS Settings .....	29
WPS Settings .....	31
NAT Settings .....	33
NAT Settings .....	33
Virtual Server .....	34
Virtual DMZ .....	36
Firewall Settings .....	37
IP Filter .....	37
Port Filter .....	39
MAC Filter .....	41
Layer7 Filter .....	42
Website Filter .....	43
Services Settings .....	44

DDNS Settings .....	44
UPnP Settings .....	45
System Log Settings.....	46
Date/Time Settings .....	47
Management.....	48
Admin Account.....	48
Ping Test.....	49
Config .....	50
Firmware Upgrade.....	50
Information.....	51
System Information.....	51
Packet Statistics .....	52
Routing Table.....	52
System Log .....	53
Logout.....	53
Logout .....	53
Reboot.....	53
PRODUCT SPECIFICATIONS.....	54

## Unpacking Information

---

Thank you for purchasing the product. Before you start, please check all the contents of this package.

The product package should include the following:

1. One Wireless Router
2. One power adapter
3. One User Manual (CD)
4. Three antennae

## Introduction To Wireless Router

---

### **General Description**

The IEEE802.11n Wireless Router is compatible with IEEE802.11n standard, which supports data rate up to 300 Mbps in 2.4 GHz band, which is also compatible with IEEE 802.11b/g wireless devices. The router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in 4-port switch and wireless AP, LAN users can share files, printers, or playing network games all at a blazing speed.

To provide a secure wireless network, this router supports wireless data encryption with 64/128-bit WEP, WPA and WPA2. Network Address Translation (NAT) Firewall is also support to shield your communications and network from hackers and wireless eavesdroppers.

The Wireless Router built-in with 4-port 10/100Mbps Fast Ethernet Switch is the latest generation of Wireless router product for Home/Office and SOHO users. This full-feature and self-contained compact Wireless Router will be fully for broadband access in both of LAN and Wireless environment. This device has been specifically designed to provide LAN and Wireless users the most cost-effective method with multiple accesses to the Internet at the cost of a single public IP address ( IP Sharing ) and enjoy the true Plug-and-Play installation. Moreover, the built-in 4-port 10/100Mbps switch lets users plug the network cable into the device without buying additional switch.

This device is also an Access Point. It has a built-in wireless LAN. Users can connect to Internet using wireless network interfaces anywhere within the range of its radio transmission. It's ideal for SOHO users who require instant and convenient access to Internet without the restriction of connecting cables.

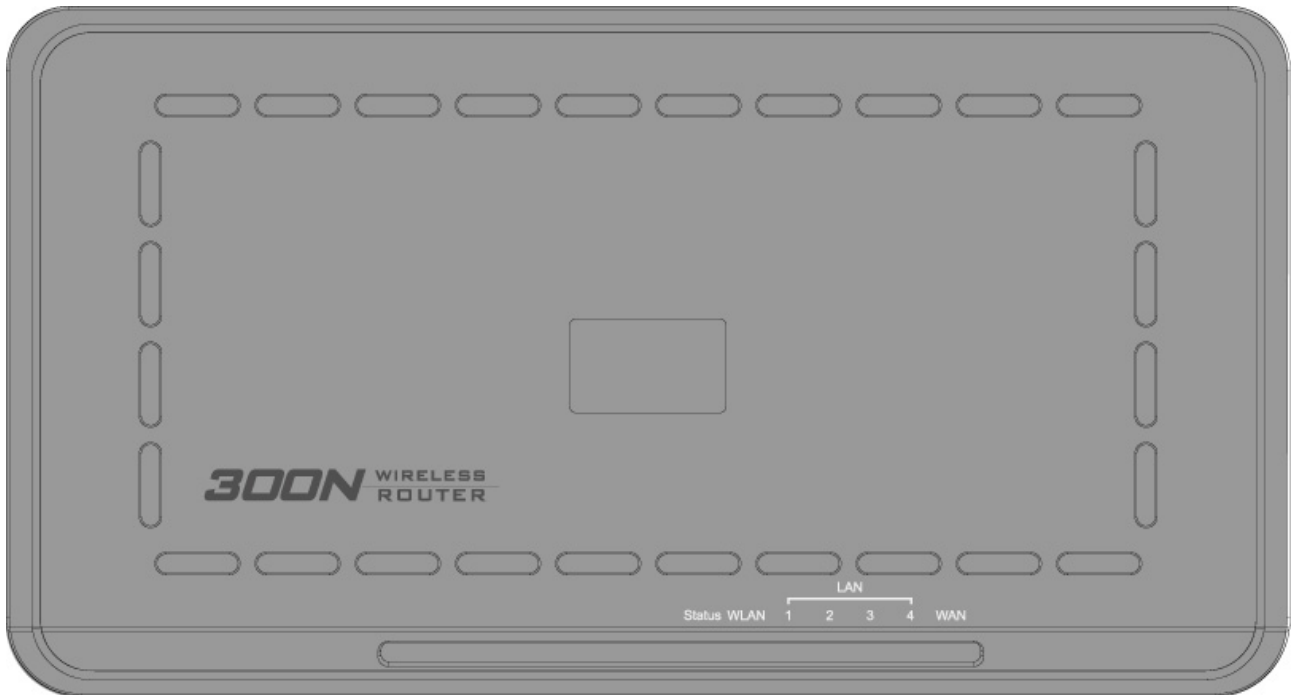
## **Key Features**

The switch provides the following key features:

- Compatible with IEEE 802.11n, 802.11b/g wireless standards
- Provides three 802.11n/b/g wireless Reverse SMA antennae
- High speed transfer data rate up to 300Mbps
- Supports wireless data encryption with 64/128-bit WEP, WPA and WPA2
- Supports authentication for wireless connectivity based on ESSID
- Supports Multiple BSSID.
- Provides MAC access control and hidden SSID function
- WDS supported with WEP, TKIP and AES encryption
- Channel: USA 11, Europe 13
- Supports NAT IP Sharing
- Supports WAN connection type-Static IP, PPPoE, DHCP client
- Firewall; Virtual DMZ; DNS relay; UPnP IGD; LLTD
- Provides DHCP server and client
- Supports ALG for FTP, NetMeeting, DDNS (DynDNS, TZO)
- Supports QoS:WMM
- Supports firmware upgrade function via Web
- Supports system log
- Certifications: FCC Class B, CE Mark, VCCI Class B

## **The Front Panel**

The front panel of the Wireless Router:

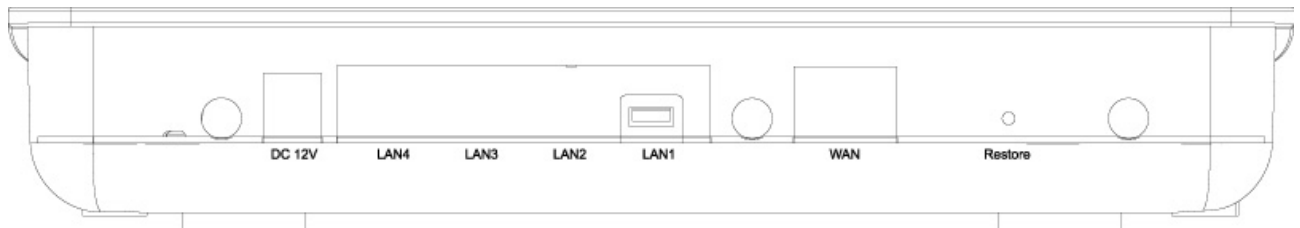


### **LED Definitions**

- **Status LED**  
The LED will be dark for a few seconds when the system is started. After that, the LED will blink periodically to show the Wireless Router is working normally. If the LED stays green/dark that means the system failed, you need to contact your agent or try to reboot the system.
- **WLAN LED**  
When Wireless AP is ready for data transmitting and receiving, it is steady green.
- **LAN LEDs**  
Every port has an Act/Link LED. Steady green (link state) indicates that the port has good linkage to its associated devices. Flashing green indicates that the port is receiving or transmitting data between its associated devices.
- **WAN LED**  
The LED stays light (green) means the WAN port has good linkage to its associated devices.  
The LED will blink green when there is traffic transverse the port.

## **The Rear Panel**

The rear panel of the Wireless Router is shown below.



### **Power Connection**

Plug the circle end of the power adapter firmly into the rear panel of the Wireless Router, and the other end put into an electric service outlet then the system is ready.

### **Restore Default Button**

1. Push the button for more than 5 seconds and then release it, the system will return to factory default setting. In the meantime, system rewrites flash to default value and Status LED halts for a while. Approximately 60 seconds later, the Status LED blinks green periodically, now the whole system parameters have returned to factory default value. If the process has been interrupted by any reason (power off...), the system will fail. Before performing the process, ensure a safe operating environment please!
2. To reboot the Router, press the button for 2-5 seconds and then release it, and all the setting won't be erased. Wait for the Router to complete the reboot, and then you can start to use it.

---

**Warning :** Incomplete factory setting recovery procedure will cause the Wireless Router malfunction ! If you are unfortunately in this situation, do not try to repair it by yourself. Consult your local distributor for help!

---

### **Placement (Optional)**

There are three ways to place the Router. The first way is to place the Router vertically on a surface. The second way is to attach it to a magnetic surface. The third way is to attach it to the wall. If you select a wall-mount option, please follow the steps below:

1. Select a location with access for cables and a power outlet.
2. Unplug the unit. Place it upside down on a flat surface and mark the two holes for anchors.
3. Installing the Wall mount anchor into the wall with tools such as drill or hammer.
4. Insert the screws in each hole of the stand parts.
5. Attaches the unit to the anchors on the wall.



## Installing And Using Wireless Router

---

This Chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. We suggest you go over the whole chapter and then do more advanced operation.

### ***Connecting this Router to your network***

---

Steps to build up the network:

- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.
- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer's Ethernet card to an 10/100Mbps Ethernet port on the back of the Wireless Router.
- Plug-in the power adapter to the Router and the other side to the wall outlet.

### ***Configuring the IP address of your computer***

---

In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to be compatible with the device. The router supports DHCP server and it is enabled as default. Users that configure your IP address as “**Obtain an IP address automatically**” may skip the following IP configuration instruction.

#### **Note:**

1. The default network setting of the device:  

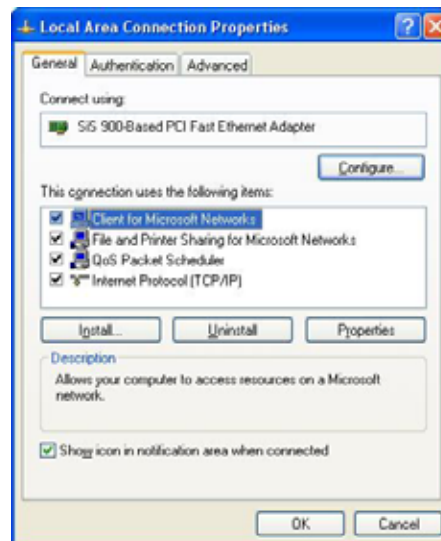
<b>IP address:</b>	192.168.1.1
<b>Subnet Mask:</b>	255.255.255.0
<b>DHCP Server:</b>	enabled
2. In the following TCP/IP configuration guide, the IP address “192.168.1.2 ” is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose “192.168.1.1” for the IP address (192.168.1.1) has been set as the default IP for this device.
3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

## Procedures to configure IP addresses for your computer

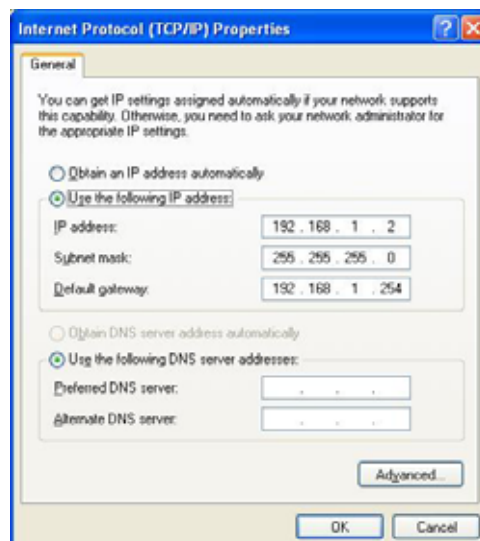
1. If you are in Classic Start menu view, click **Start > Settings > Control Panel > Network Connections**. If you are in Start menu view, click **Start > Control Panel > Network Connections**.
2. Double click **Local Area Connection**.



3. Choose **Internet Protocol (TCP/IP)** and click **Properties**.



4. You may choose “Obtain an IP address automatically”(recommend) to get IP address automatically or choose “Use the following IP address” to specify IP addresses manually. Please click the **OK** button after your configuration.



## Management

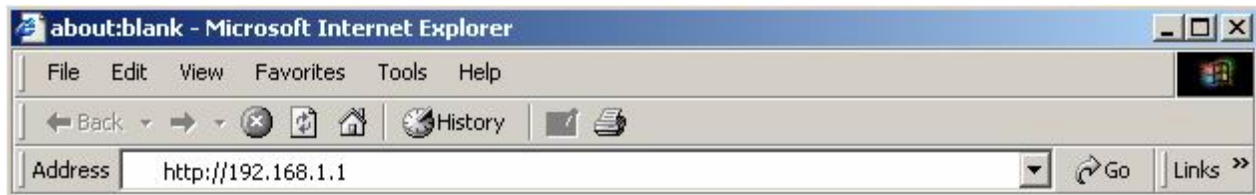
---

### ***Starting the WEB-Based Management Interface***

---

The device uses WEB as the management interface. You can use a browser to access the management interface easily. Please follow the steps listed below.

1. Double click the Internet WEB browser icon on your desktop screen (Netscape Communicator 4.0 and Internet Explorer 3.0 or update version)
2. Type 192.168.1.1 into the URL WEB address location and press Enter.



3. The Login Name and Password Required window appears.
  - Select **Administrator** in the Login Name drop list (default value).
  - Enter **admin** in the Password location (default value).
  - Click **Login** button.

### Login my 802.11n Wireless Router Management Center



Please keyin current password to login. If you are not administrator, please using guest account to login.

Login Name :

Password :

## The Graphic User Interface

After the password authorization, the Information page shows up as the home page of the Graphic User interface. You may click on each folder on left column of each page to get access to each configuration page.

**Note:** Please note that you should click the **Save Settings** button to apply your configuration to this device. You can also restore the default settings by clicking the **Reset Settings** button.

The screenshot displays the web interface of a 'Draft 802.11n Broadband Router'. The interface has a dark header with the title and a tagline. On the left is a sidebar menu with expandable folders. The main content area is divided into four sections, each with a title bar and a list of configuration parameters.

**Header:** Draft 802.11n Broadband Router  
Best Wireless and Networking Solution

**Left Sidebar Menu:**

- [INFORMATION]
- Network Settings
- Wireless Settings
- NAT Settings
- Firewall Settings
- Services Settings
- Management
- Information
- Logout

**SYSTEM INFORMATION**

- SYSTEM NAME : W443
- Firmware Version : Version 0.5 (20070830es)
- Host Name : Wireless.11n.Router
- System Time : 2007-08-30 10:17:37
- Uptime : 41 min

**WAN INTERFACE INFORMATION**

- MAC Address : 00:46:12:34:A0:11
- IP Assign Type : DHCP
- DHCP Client : Active
- DHCP Establish Time : Thu Aug 30 09:54:02 2007
- DHCP Lease Expire Time : Fri Aug 31 09:54:02 2007
- DHCP Server : 192.168.100.254
- IP Address : 192.168.100.63
- Subnet Mask : 255.255.255.0
- MTU Size : 1500
- Default Gateway : 192.168.100.254
- Primary DNS : 192.168.100.13
- Secondary DNS : 192.168.100.254

**LAN INTERFACE INFORMATION**

- MAC Address : 00:08:54:E2:49:04
- IP Address : 192.168.1.1
- Subnet Mask : 255.255.255.0
- DHCP Server : Active

**WLAN INTERFACE INFORMATION**

- Mode : 802.11b/g/n Mixed
- MAC Address : 00:08:54:E2:49:04
- SSID : Wireless
- Channel : 1
- Authentication : WPA Encryption(Personal)

## Network Setting

### WAN Interface Setup

This page allows users to configure those parameters for connecting to Internet. You may select the WAN Access Type from the “My Connection type” column and configure parameters for each mode.

**802.11n Draft 2.0 Broadband Router**  
Best Wireless and Networking Solution

[INFORMATION]

Network Settings

WAN Settings

LAN Settings

QoS Settings

Wireless Settings

NAT Settings

Firewall Settings

Services Settings

Management

Information

Logout

WAN INTERFACE SETTINGS

Using this section to set the type of Internet connection, you can use the connection type as follow : static IP address; DHCP; PPPoE. If you don't sure your Internet connection type, please contact your ISP Provider.

Save Settings

Reset Settings

INTERNET CONNECTION TYPE

MY Connection type :

☒ Static IP ☐ DHCP ☐ PPPoE

IP Address :

10.10.13.195

Subnet Mask :

255.255.0.0

Default Gateway :

10.10.10.254

Primary DNS Server :

168.95.1.1

2nd DNS Server :

168.95.192.1

Static IP MTU :

1500

bytes

Host Name :

Wireless

11n.Router

Ping from WAN :

☒


WAN Ethernet MAC :

☒ Original MAC (00:46:12:34:A0:11 )

☐ Manual Setting 00:00:27:88:81:18

[Clone MAC Address form your Computer]

## Static IP Mode

INTERNET CONNECTION TYPE	
MY Connection type :	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP Address :	<input type="text" value="10.10.13.195"/>
Subnet Mask :	<input type="text" value="255.255.0.0"/> 
Default Gateway :	<input type="text" value="10.10.10.254"/>
Primary DNS Server :	<input type="text" value="168.95.1.1"/>
2nd DNS Server :	<input type="text" value="168.95.192.1"/>
Static IP MTU :	<input type="text" value="1500"/> bytes
Host Name :	<input type="text" value="Wireless"/> . <input type="text" value="11n.Router"/>
Ping from WAN :	<input checked="" type="checkbox"/>
WAN Ethernet MAC :	<input checked="" type="radio"/> Original MAC (00:46:12:34:A0:11 ) <input type="radio"/> Manual Setting <input type="text" value="00:00:27:88:81:18"/> <a href="#">[Clone MAC Address form your Computer]</a>

Items	Information
IP Address, Subnet Mask and Default Gateway	Fill in the IP address, Subnet Mask and Default Gateway that provided by your Internet Service Provider (ISP).
Primary and 2 <sup>nd</sup> DNS server	To specify the Domain Name Server (DNS). Enter the DNS provided by your ISP in 1 <sup>st</sup> and 2 <sup>nd</sup> server.
Static IP MTU	To enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter the MTU number in the blank to set the limitation (default 1500bytes).
Host Name	Name of this device.
Ping from WAN	Mark the checkbox to enable others detecting this device from WAN, and clear the checkbox to disable.
WAN Ethernet MAC	Select to use the following MAC as the MAC while serving Internet: Original MAC: the MAC of the device. Manual Settings: the MAC of your computer. Click on the words in the bracket to clone your computer MAC in the blank. You can also change the MAC numbers if you need.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## DHCP Client Mode

INTERNET CONNECTION TYPE	
MY Connection type :	<input type="radio"/> Static IP <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE
Set DNS server :	<input type="radio"/> Manually <input checked="" type="radio"/> Automatically
DHCP MTU :	<input type="text" value="1500"/> bytes
Host Name :	<input type="text" value="Wireless"/> . <input type="text" value="11n.Router"/>
Ping from WAN :	<input checked="" type="checkbox"/>
WAN Ethernet MAC :	<input checked="" type="radio"/> Original MAC (00:46:12:34:A0:11 ) <input type="radio"/> Manual Setting <input type="text" value="00:00:27:88:81:18"/> <a href="#">[Clone MAC Address form your Computer]</a>

Items	Information
Set DNS server	If your DNS provide by ISP is dynamic, choose "Automatically", if not choose "Manually" and enter the DNS provided by your ISP in DNS 1, 2.
DHCP MTU	To enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation (default 1500bytes).
Host Name	Name of this device.
Ping from WAN	Mark the checkbox to enable others detecting this device from WAN, and clear the checkbox to disable.
WAN Ethernet MAC	Select to use the following MAC as the MAC while serving Internet: Original MAC: the MAC of the device. Manual Settings: the MAC of your computer. Click on the words in the bracket to clone your computer MAC in the blank. You can also change the MAC numbers if you need.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## PPPoE Mode

INTERNET CONNECTION TYPE	
MY Connection type :	<input type="radio"/> Static IP <input type="radio"/> DHCP <input checked="" type="radio"/> PPPoE
PPPoE Username :	<input type="text" value="USERNAME"/>
PPPoE Password :	<input type="password" value="••••••••"/>
Set DNS server :	<input type="radio"/> Manually <input checked="" type="radio"/> Automatically
PPPoE MTU :	<input type="text" value="1492"/> bytes
Host Name :	<input type="text" value="Wireless"/> . <input type="text" value="11n.Router"/>
Ping from WAN :	<input checked="" type="checkbox"/>
WAN Ethernet MAC :	<input checked="" type="radio"/> Original MAC (00:46:12:34:A0:11 ) <input type="radio"/> Manual Setting <input type="text" value="00:00:27:88:81:18"/> <a href="#">[Clone MAC Address form your Computer]</a>

Items	Information
PPPoE Username and Password	Fill in the User Name and Password that provided by your ISP. The default username/password is USERNAME/PASSWORD.
Set DNS server	If your DNS provide by ISP is dynamic, choose "Automatically", if not, choose "Manually" and enter the DNS provided by your ISP in DNS 1, 2.
PPPoE MTU	To enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance. Enter your MTU number in the text-box to set the limitation (default 1492 bytes).
Host Name	Name of this device.
Ping form WAN	Mark the checkbox to enable others detecting this device from WAN, and clear the checkbox to disable.
WAN Ethernet MAC	Select to use the following MAC as the MAC while serving Internet: Original MAC: the MAC of the device. Manual Settings: the MAC of your computer. Click on the words in the bracket to clone your computer MAC in the blank. You can also change the MAC numbers if you need.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.



## LAN Interface Setup

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment.

### LAN INTERFACE SETTINGS

Using this section to setting the parameter for LAN. You can use build-in DHCP server for assign IP to the computers on LAN, this function can reduce setting time.

Save Settings

Reset Settings

### ROUTER SETTINGS

The IP Address field is the IP Address that you use to access the Web-based management center. If you change the IP Address here, you may need to reconnect current IP address again.

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DNS Proxy : ☒ Enable

### DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on LAN.

Enable DHCP Server : ☒

DHCP IP Range : 192.168.1.100 to 192.168.1.150

DHCP Lease Time : 86400 seconds (60.864000)

### DHCP CLIENT LIST

Type	Hostname	MAC	IP	Description	Expire Time
Reserved	hollings-78ccff	00:0a:e4:c2:58:1e	192.168.1.100		Fri Jan 2 08:38:02 1970

## Router Settings

Items	Information
<b>IP Address</b>	The IP of your Router LAN port (default 192.168.1.1).
<b>Subnet Mask</b>	Subnet Mask of you LAN (default 255.255.255.0).
<b>DNS Proxy</b>	DNS proxy takes DNS queries from the local network and forwards them to an Internet DNS. Mark the checkbox to enable DNS Proxy function or clear to disable.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## DHCP Server Settings

Items	Information
<b>Enable DHCP Server</b>	To give your LAN Client an IP, you have to enable DHCP server. If not, manual setting up your client IP is necessary when you want to use the router as your client's default gateway.
<b>DHCP IP Range</b>	Specify the DHCP Client IP address range default (100~150).
<b>DHCP Lease Time</b>	The time for the device to recycle and give out DHCP IP (default 86400).

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## DHCP Client List

The information of type, hostname, MAC, IP, description and expire time of the DHCP clients that have connected with this device.

## QoS Settings

The QoS (Quality of Service) Settings page provides different priority to different users or data flows.

**BANDWIDTH QoS CONTROL**

**Bandwidth Control** enables you to specify the maximum line bandwidth that a particular transfer operation can use, so that it can be carried out in the background, at a low priority, without interfering with interactive users or other network applications. **Bandwidth Control** provides for dynamic load control, ensuring that at any given moment, the particular transfer does not exceed the limit set on its use of the line's bandwidth.

Enable QoS Bandwidth : ☒

**TOTAL BANDWIDTH SETTINGS**

Upload Bandwidth  (Kbps)

Download Bandwidth  (Kbps)

**BANDWIDTH QoS SETTINGS**

Enable this Rule : ☐

Type :  ▼



LAN IP Adress :

Priority :  ▼

Bandwidth : Min:  Max:  (Kbps)

Comment :

Action :

QoS SETTINGS RULE LIST						
Enable	Priority	IP Address	Bandwidth	Comment	Action	
 	Medium	192.168.1.45	1024kbps~10240kbps	Mary	<input type="button" value="Delete"/>	

## Total Bandwidth Settings

You can setup the total upload/ download bandwidth manually (default 102400).

## Bandwidth QoS Settings

Items	Information
<b>Enable this Rule</b>	Mark to enable the configuration, and clear to disable.
<b>Type</b>	Select the type of download or upload.
<b>LAN IP Address</b>	Fill in the IP address that you wish to control.
<b>Priority</b>	Select the transmission priority of low, medium, high, or highest.
<b>Bandwidth</b>	Fill in the minimum and maximum bandwidth.
<b>Comment</b>	Give a definition to the LAN IP Address.
<b>Action</b>	After configuring the above settings, click <b>Add</b> to add a new list in the following MAC Access Control List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Bandwidth QoS Settings

Lists the Bandwidth QoS Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Wireless Settings

### Basic Settings

You can set up the configuration of your Wireless and monitor the Wireless Clients associate with your AP.

**WIRELESS BASIC SETTINGS**

Using this section to setup your wireless interface on your router. You can change SSID, Channel and Wireless protocol for your enviroment. Please note that changes settings on this section may also need to be duplicated on your Wireless Client.

Save Settings

Reset Settings

**WIRELESS SETTINGS**

Enable Wireless :

☒

Wireless Mode :

802.11b/g/n Mixed

Country:

USA(FCC)

Wireless Channel :

2.412GHz (channel 1)

SSID :

Wireless-11n-Router

Items	Information
Enable Wireless	Mark the checkbox to enable Wireless interface or uncheck to disable.
Wireless Mode	To select a band for this device to match 802.11b/g/n mixed, 802.11b/g mixed, 802.11b, 802.11g, or 802.11n.
Country	Select the region you live.
Wireless Channel	Select a channel for the wireless network of this device.
SSID	Service set identifier for the name of the wireless network.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Advanced Settings

---

You can set advanced wireless LAN parameters of this router. We recommend not changing these parameters unless you know what changes will be there on this router.

### WIRELESS ADVANCE SETTINGS

Please ensure you are system administrator and understand every parameters. The parameters of this section will effect the performance of wireless network. Be careful!

**Note:** Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.

Save Settings

Reset Settings

### GENERAL WIRELESS ADVANCE SETTINGS

Hide SSID : ☐

Beacon Period :  ms (20~1023)

DTIM Period :  beacon (1~255)

RTS Threshold :  bytes (0~2347)

Fragment Threshold :  bytes (256~2346)

Tx Power :  ▼

b/g Protection :  ▼

Support WMM : ☐

### 802.11n WIRELESS ADVANCE SETTINGS

HT Operation Mode :  ▼

HT Channel Bandwidth :  ▼

HT Guard Interval :  ▼

Enable HT TX  
Aggregate MSDU : ☐

## General Wireless Advance Settings

Items	Information
<b>Hide SSID</b>	Mark to disable SSID from broadcasting. As default, this device broadcasts its SSID to allow every wireless station located within the coverage of this wireless router to discover this wireless router easily.
<b>Beacon Period</b>	The period of time a beacon is broadcasted (default 100ms).
<b>DTIM Period</b>	The beacon of a Delivery Traffic Indication Message is broadcasted (default 1 beacon).
<b>RTS Threshold</b>	If the packet size is smaller than the Request To Send threshold, the wireless router will not send this packet by using the RTS/CTS mechanism (default 2347 bytes).
<b>Fragment Threshold</b>	Specifies the maximum size of packet during the data transition. A higher value brings a better performance (default 2346 bytes).
<b>Tx Power</b>	Select the Transmission Power of very weak, weak, medium, and strong according to your demand.
<b>b/g Protection</b>	Allows the adapters search for 802.11b/g singles only. Select "Auto" to turns it on or off automatically, select "Always On" to support protection or select "Always Off" to disable this function.
<b>Support WMM</b>	To enable/disable Wi-Fi Multimedia function.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## 802.11n Wireless advance Settings

Items	Information
<b>HT Operation Mode</b>	Select the mixed or green field mode as the Hyper Throughput operation mode.
<b>HT Channel Bandwidth</b>	Select the 40Mhz or 20Mhz as the channel bandwidth.
<b>HT Guard Interval</b>	Select 400ns or 800ns as the interval time.
<b>Enable HT TX Aggregate MSDU</b>	Mark to enable Hyper Throughput TX Aggregate MAC Service Data Unit, and clear to disable.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Security Settings

---

The Security function protects your wireless network from invasion. We provide WEP and WPA encryption to secure your wireless network. As default, the authentication is configured as safe mode. Please select None/WEP/WPA (Personal) in the drop list. If you select none, any data will be transmitted without encryption and any station can access the router.

### WIRELESS SECURITY SETTINGS

Use this section to configure the wireless settings for your Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Save SettingsReset Settings

### WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WEP and WPA-Personal. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.

**Authentication Mode**

### NO SECURITY PROTECTION (PUBLIC NETWORK)

**No security protection, everybody can connect to this router anytime. Be careful! This means your network is public, some hackers can hack your computer easily!**



## WEP Configuration

WEP AUTHENTICATION	
This section allows you setup the WEP key value. You could select ASCII or Hex as the format of input value.	
Authentication :	<input type="text" value="Open"/>
Default Key ID :	<input type="text" value="1"/>
WEP Key1 :	<input type="text" value="ASCII (5 or 13 chars)"/> <input type="text" value="....."/>
WEP Key2 :	<input type="text" value="ASCII (5 or 13 chars)"/> <input type="text" value="....."/>
WEP Key3 :	<input type="text" value="ASCII (5 or 13 chars)"/> <input type="text" value="....."/>
WEP Key4 :	<input type="text" value="ASCII (5 or 13 chars)"/> <input type="text" value="....."/>

Items	Information
Authentication	Open: Wireless AP can associate with this wireless router without WEP encryption. Shared Key: Wireless AP can associate with this wireless router only with WEP encryption.
Default Key ID	Select to use the WEP key value of 1,2,3 or 4 as in the following settings.
WEP Key 1, 2, 3 and 4	Select ASCII or Hex to setup the key value (default 012345).

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## WPA Configuration

WPA AUTHENTICATION (PERSONAL)	
WPA Mode :	Auto (WPA or WPA2) ▼
WPA Encryption :	TKIP/AES ▼
Pre-Shared Key :	Pass Phrase (8..32bytes) ▼ <div> <div>••••••••</div> <div></div> </div>
WPA ReKey Method	Disabled ▼
WPA ReKey Interval	0 (0..67108864, default:0)
Pairwise Master Key Cache Interval	10 ▼ minutes (default:10)
Pre-Authentication Support	<input type="checkbox"/> Enable

Items	Information
WPA Mode	Select the option in the drop list to enable modes of auto, WPA only, or WPA2 only.
WPA Encryption	Select TKIP / AES, TKIP or AES as WPA encryption.
Pre-Shared Key	Select the key format of Pass Phrase or Hex. Enter the Pre-Shared Key according to the key format you select (default 01234567).
WPA ReKey Method	To enable/disable WPA rekey method by time or by packet.
WPA ReKey Interval	Enter the numbers to setup the WPA rekey interval.
Pairwise Master Key Cache Interval	Select 1, 5, 10, 20, 30, 60, or 120 minuets as the cache interval time.
Pre-Authentication Support	Mark this checkbox to enable pre-authentication function, and clear to disable.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Access Control

To restrict the Number of Access authentication of Stations, set up the control list in this page. You may select "Allow Listed" to allow those allowed MAC addresses or select "Deny Listed" to ban those MAC addresses from accessing to this device.

WIRELESS MAC ACCESS CONTROL	
If you choose 'Allowed Listed', only those dients 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.	
MAC Access Policy :	<div>Deny Listed</div> (default: disabled)

MAC ACCESS CONTROL SETTINGS	
Enable this Rule :	<input type="checkbox"/>
MAC Address :	<input type="text"/>
Description :	<input type="text"/>
Action :	<div>Change</div> <div>Add</div>

MAC ACCESS CONTROL LIST			
Enable	Client MAC	Description	Action
	00:13:02:4C:DC:95	NB	<div>Delete</div>

CURRECT ASSOCIATED CLIENT LIST	
MAC address	Description
00:13:02:4C:DC:9A	

## MAC Access Control Settings

Items	Information
<b>Enable this Rule</b>	Mark to enable the configuration, and clear to disable.
<b>MAC Address</b>	Fill in the MAC address that you wish to control.
<b>Description</b>	Give a definition to the MAC Address.
<b>Action</b>	After configuring the above settings, click <b>Add</b> to add a new list in the following MAC Access Control List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## MAC Access Control List

Lists the MAC Access Control Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Current Associated Client List

Lists the current associated client connected to this device. Click on the list to add it into the MAC Access Control List then to do more configurations on it.

## WDS Settings

Wireless Distribution System allows the router to communicate with other APs wirelessly. To make it work, you must ensure that these APs and the Router are in the same Channel and add these APs MAC Address and Comment values into the WDS list.

**WIRELESS DISTRIBUTION SYSTEM (WDS)**

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.

Save Changes

Reset Changes

**WDS SETTINGS**

**WDS Mode :**  (default:disabled)

### AP+WDS (AP Repeater)

**WDS SETTINGS**

Turn on Wds function, the peer Wds APs are according to the mac address listed in WDS MAC List field below.

**WDS Mode :**

(default:disabled)

**WDS Encryption Type :**

**WPA Encryption Key :**

(8..32bytes )

**WDS Partner 1 MAC :**

**WDS Partner 2 MAC :**

**WDS Partner 3 MAC :**

**WDS Partner 4 MAC :**

## WDS (AP Bridge)

WDS SETTINGS	
Turn on Wds function, the peer Wds APs are according to the mac address listed in WDS MAC List field below. In this mode, AP will not send beacon out and will not deal with probe request packets, therefore STA will not possible to connect with it.	
<b>WDS Mode :</b>	WDS (AP Bridge) (default:disabled)
<b>WDS Encryption Type :</b>	WPA/AES
<b>WPA Encryption Key :</b>	(8..32bytes )
<b>WDS Partner 1 MAC :</b>	
<b>WDS Partner 2 MAC :</b>	
<b>WDS Partner 3 MAC :</b>	
<b>WDS Partner 4 MAC :</b>	

## Auto (AP Bridge)

WDS SETTINGS	
Turn on Wds function, and auto learning from WDS packet. But have to note that that there at least has one AP have to fill WDS list.	
<b>WDS Mode :</b>	Auto (AP Bridge) (default:disabled)
<b>WDS Encryption Type :</b>	WEP
[Wireless Security setting Page] You must setup WEP encryption in wireless security page.	

Items	Information
<b>WDS Mode</b>	Select the option in the drop list to enable AP+WDS (AP Repeater), WDS (AP Bridge) or Auto (AP Bridge) as WDS mode.
<b>WDS Encryption Type</b>	Select the option in the drop list to enable WEP, WPA/TKIP, and WPA/AES encryption types. If you select None, any data will be transmitted without encryption and any station can access the router.
<b>WPA Encryption Key</b>	For encryption type of WPA/TKIP and WPA/AES, you have to fill in the WPA encryption key. Please use Pass Phrase (8~32bytes) key format.
<b>WDS Partner 1~4 MAC</b>	For encryption type of WPA/TKIP and WPA/AES, you have to fill in the WDS AP MAC. You can fill up to 4 sets of WDS AP MAC lists.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## WPS Settings

---

WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

**WPS (WiFi PROTECTED SETUP)**  
  
WiFi Protected Setup was designed to ease setup of security enabled WiFi networks in the home and small office environment. It supports methods that are familiar to most consumers to configure a network and enable security, like pushing a button or entering a PIN. The new system, which will be incorporated in Windows Vista, will work with computers, gateways peripherals, and consumer electronics.  
  
**WiFi Protected Setup :** ☒ Enable (default:disabled)

**WPS CONNECTION SETTINGS**  
  
**WPS Config Method** PIN - Personal Identification Number   
**Add Enrollee PIN Code**

**WPS INFORMATION**  
  
**WPS Configured :** N/A  
**WPS Status :** N/A  
**SSID :** Wireless-11n-Router  
**Auth Mode :** Open  
**WPAPSK :** 01234567

## WPS Connection Settings

Items	Information
<b>WPS Config Method</b>	PIN method (Personal Identification Number): read the PIN from either a sticker on the new STA or a display. PBC method (Push Button Communication): in which the user simply has to push a button, either an actual or virtual one, on both the AP and the new STA. (Users can simply click on the <b>Build WPS Connection</b> button in the GUI after selecting this mode.)
<b>Add Enrollee PIN Code</b>	Users have to fill in the PIN code to enrollee device if selecting PIN mode as the WPS Config method. And click on <b>Build WPS Connection</b> button to execute.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## WPS Information

Shows the information of WPA configured, status, SSID, authentication mode, and pre-shared key. Click on **Refresh** button to refresh the information.



## NAT Settings

### NAT Settings

NAT (Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass through a Router or firewall. NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT (NETWORK ADDRESS TRANSLATION)	
Using this section to set the advance NAT settings. You can building VPN passthrough here. Virtual DMZ and virtual server is used to provide Internet services without sacrificing unauthorized access to its local private network. Such as Web (HTTP ) servers, FTP servers, SMTP (e-mail) servers and DNS servers.	
<div>Save Settings</div> <div>Reset Settings</div>	

NAT & ALG SETTINGS	
Enable NAT :	<input checked="" type="checkbox"/>
IPSec Pass Through :	<input checked="" type="checkbox"/>
PPTP Pass Through :	<input checked="" type="checkbox"/>
L2TP Pass Through :	<input checked="" type="checkbox"/>
Non-standard FTP port :	<input type="text"/>

ALG (Application Layer Gateway Service) SETTINGS	
SIP ALG :	<input type="checkbox"/>
NetMeeting ALG :	<input type="checkbox"/>
Window Messenger File Transfer ALG :	<input type="checkbox"/>
StarCraft/Battle.net ALG :	<input type="checkbox"/>

### NAT & ALG Settings

Click on the checkbox to enable NAT function, IPSec (IP Security), PPTP (point-to-point tunneling protocol), and L2TP (layer 2 tunneling protocol) pass through on Virtual Private Network (VPN), or clear to disable. Fill in the port number in the Non-standard FTP port blank if you need.

### ALG Settings

Click on the checkbox to enable SIP (session initiation protocol), NetMeeting, Window Messenger File Transfer, and StarCraft/Battle.net ALG.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Virtual Server

After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

VIRTUAL SERVER	
<p>This page can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network.</p> <p>Depending on the requested service (TCP/UDP port number), we redirects the external service request to the appropriate server within the LAN network.</p>	
Enable Virtual Server <input checked="" type="checkbox"/>	

VIRTUAL SERVER SETTINGS	
Enable this Rule :	<input type="checkbox"/>
Application Select :	Custom <input type="button" value="v"/>
WAN Port :	<input type="text"/>
Protocol :	Both <input type="button" value="v"/>
LAN Server IP :	<input type="text"/>
LAN PORT:	<input type="text"/>
Action :	<input type="button" value="Change"/> <input type="button" value="Add"/>

VIRTUAL SERVER MAPPING LIST					
Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input checked="" type="checkbox"/>	21	Both	192.168.1.25	21	<input type="button" value="Delete"/>

## Virtual Server Settings

Items	Information
<b>Enable this Rule</b>	Mark to enable the configuration, and clear to disable.
<b>Application Select</b>	Select an application for your demand.
<b>WAN Port</b>	Fill in the port number of WAN.
<b>Protocol</b>	Select the protocol type of TCP, UDP or Both.
<b>LAN Server IP</b>	Fill in the IP of your LAN Server.
<b>LAN Port</b>	Fill in the port number of LAN.
<b>Action</b>	After configure the above settings, click <b>Add</b> to add a new list in the following IP Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Virtual Server Mapping List

Lists the Virtual Server Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Virtual DMZ

---

The virtual DMZ (Demilitarized Zone) is used to enable protocols, which need to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click **Save Settings** to enact the setting.

**VIRTUAL DEMILITARIZED ZONE (Virtual DMZ)**

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

Save Settings

Reset Settings

**VIRTUAL DMZ SETTINGS**

Enable Virtual DMZ : ☒

Virtual DMZ IP Address :

## Firewall Settings

### IP Filter

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

IP FILTER
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 Filter <input checked="" type="checkbox"/>

IP FILTER SETTINGS
Enable this Rule : <input type="checkbox"/>
IP Address : <input type="text"/>
Protocol : Both <input type="button" value="v"/>
Filter Mode : Always <input type="button" value="v"/>
Date Define : All <input type="button" value="v"/>
Time Define : 00:00 <input type="button" value="v"/> ~ 00:00 <input type="button" value="v"/>
Action : <input type="button" value="Change"/> <input type="button" value="Add"/>

IP FILTER RULE LIST						
Enable	IP Address	Protocol	Mode	Day	Time	Action
<input checked="" type="checkbox"/>	192.168.1.10	Both	By Schedule	Mon-Fri	10:00~22:00	<input type="button" value="Delete"/>

## IP Filter Settings

Items	Information
<b>Enable this Rule</b>	Mark to enable the configuration, and clear to disable.
<b>IP Address</b>	Fill in the IP address that you wish to filter.
<b>Protocol</b>	Select the protocol type of TCP, UDP or Both.
<b>Filter Mode</b>	Select the filter mode of Always or by Schedule.
<b>Date Define Time Define</b>	For filter mode of by Schedule, you have to define the filter date and time.
<b>Action</b>	After configure the above settings, click <b>Add</b> to add a new list in the following IP Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## IP Filter Rule List

Lists the IP Filter Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Port Filter

The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filtering restricts certain type of data packets from your LAN to Internet through the router. After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

PORT FILTER
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.
<b>Enable Port Filter</b> <input checked="" type="checkbox"/>

PORT FILTER SETTINGS
<b>Enable this Rule :</b> <input type="checkbox"/>
<b>Application Select :</b> Custom <input type="button" value="v"/>
<b>Port Range :</b> <input type="text"/> ~ <input type="text"/>
<b>Protocol :</b> Both <input type="button" value="v"/>
<b>Filter Mode :</b> Always <input type="button" value="v"/>
<b>Date Define :</b> All <input type="button" value="v"/>
<b>Time Define :</b> 00:00 <input type="button" value="v"/> ~ 00:00 <input type="button" value="v"/>
<b>Action :</b> <input type="button" value="Change"/> <input type="button" value="Add"/>

PORT FILTER RULE LIST						
Enable	Port	Protocol	Mode	Date	Time	Action
	20~21	Both	Always	All	00:00~00:00	<input type="button" value="Delete"/>

## Port Filter Settings

Items	Information
<b>Enable this Rule</b>	Mark to enable the configuration, and clear to disable.
<b>Application Select</b>	Select an application for your demand.
<b>Port Range</b>	Fill in the port range that you wish to filter. The valid numbers are 1~65535.
<b>Protocol</b>	Select the protocol type of TCP, UDP or Both.
<b>Filter Mode</b>	Select the filter mode of Always or by Schedule.
<b>Date Define Time Define</b>	For filter mode of by Schedule, you have to define the filter date and time.
<b>Action</b>	After configure the above settings, click <b>Add</b> to add a new list in the following IP Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Port Filter Rule List

Lists the Port Filter Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.



## MAC Filter

The Wireless Router could filter the outgoing packets for security or management consideration. You can set up the filter against the MAC addresses to block specific internal users from accessing the Internet. After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

MAC FILTER
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 Filter <input checked="" type="checkbox"/>

MAC FILTER SETTINGS
Enable this Rule : <input type="checkbox"/>
MAC Address : <input type="text"/>
Filter Mode : <input type="text" value="Always"/>
Date Define : <input type="text" value="All"/>
Time Define : <input type="text" value="00:00"/> ~ <input type="text" value="00:00"/>
Action : <input type="button" value="Change"/> <input type="button" value="Add"/>

MAC FILTER RULE LIST					
Enable	MAC Address	Mode	Day	Time	Action
	00:00:27:88:C1:18	By Schedule	Mon	08:00~10:00	<input type="button" value="Delete"/>

### MAC Filter Settings

Items	Information
Enable this Rule	Mark to enable the configuration, and clear to disable.
MAC Address	Fill in the MAC address that you wish to filter.
Filter Mode	Select the filter mode of Always or by Schedule.
Date Define	For filter mode of by Schedule, you have to define the filter date and time.
Time Define	
Action	After configure the above settings, click <b>Add</b> to add a new list in the following IP Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

### MAC Filter Rule List

Lists the MAC Filter Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Layer7 Filter

The layer7 filtering restricts certain type of data packets from your LAN to Internet through the router. You can setup the filter against the IP address to block specific internal users from accessing protocols that you have designated. After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

LAYER7 FILTER (APPLICATION LAYER FILTER)
Entries in this table are used to restrict certain types of several application from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable Layer7 Filter <input checked="" type="checkbox"/>

LAYER7 FILTER SETTINGS
Enable this Rule : <input type="checkbox"/>
IP Address : <input type="text"/> (0.0.0.0 means no limit)
Layer7 Protocol : <input type="text" value="AIM - AOL instant message"/>
Action : <input type="button" value="Change"/> <input type="button" value="Add"/>

LAYER7 FILTER RULE LIST			
Enable	IP Address	Application	Action
	0.0.0.0	msnmessenger	<input type="button" value="Delete"/>

### Layer7 Filter Settings

Items	Information
Enable this Rule	Mark to enable the configuration, and clear to disable.
IP Address	Fill in the IP address that you wish to filter.
Layer7 Protocol	Select a layer 7 protocol for your demand.
Action	After configure the above settings, click <b>Add</b> to add a new list in the following IP Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

### Layer7 Filter Rule List

Lists the Layer7 Filter Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Website Filter

The Website Filter allows users to prevent certain website from accessing by users in LAN. This filter will block those websites that contain certain keywords. After marking or clearing the enable checkbox, it takes 5 seconds for this device to refresh the page.

WEBSITE FILTER
Web Site filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below. (EX: google; www.google.com or 72.14.203.99)
Enable WebSite Filter <input checked="" type="checkbox"/>

WEBSITE FILTER SETTINGS
Enable this Rule : <input type="checkbox"/>
Client IP Address : <input type="text"/> (0.0.0.0 means no limit)
URL or Key Word : <input type="text"/>
Action : <input type="button" value="Change"/> <input type="button" value="Add"/>

WEBSITE FILTER RULE LIST			
Enable	Client IP	WebSite String	Action
<input checked="" type="checkbox"/>	72.14.203.99	google	<input type="button" value="Delete"/>

### Website Filter Settings

Items	Information
Enable this Rule	Mark to enable the configuration, and clear to disable.
Client IP Address	Fill in the local IP address that you want to restrain it from serving the filtering websites.
URL or Key Word	Fill in the name or keywords of the website to block.
Action	After configure the above settings, click <b>Add</b> to add a new list in the following Website Filter Rule List. The <b>Change</b> button can be used to change the configuration.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

### Website Filter Rule List

Lists the Website Filter Settings you have added before. Click on the list to change configuration, or the **Delete** button to delete the list.

## Services Settings

### DDNS Settings

DDNS (Dynamic Domain Name Server) service allows users to connect to this device via a fixed and easy-to-remember hostname.

**DDNS (DYNAMIC DOMAIN NAME SERVICES)**

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.

[Save Settings](#) [Reset Settings](#)

**DDNS SETTINGS**

Enable DDNS : ☒

Service Provider :

Domain Name :

User Name/Email :

Password/Key :

Confirmed Password :

Items	Information
<b>Enable DDNS</b>	Mark to enable the configuration, and clear to disable.
<b>Service Provider</b>	The website that provides DDNS service. Please select DynDns.org, No-IP.com or TZO from the drop list.
<b>Domain Name</b>	The hostname that you have applied for the device.
<b>User Name/Email</b>	DDNS login account. For DynDNS users, please fill in your user name; for No-IP and TZO users, please fill in your email address (default USER).
<b>Password/Key</b>	The password of your DDNS service account (default PASSWORD).
<b>Confirmed Password</b>	Retype the password to confirm.

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## UPnP Settings

---

The UPnP (Universal Plug and Play) service allows devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments. This page allows user to monitor the information of UPnP clients. Mark or clear the checkbox to enable or disable UPnP IGD, and then click **Save Settings** to enact your settings.

**UPnP IGD (UPnP INTERNET GATEWAY DEVICES)**  
  
UPnP is architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home.  
  

Save Settings    Reset Settings

**UPnP SETTINGS**  
  
Enable UPnP IGD : ☒ (default:disabled)

UPnP MAPPING						
Remote Host	External Port	Internal Client	Internal Port	Protocol	Duration	Description
	8888	192.168.1.2	8888	TCP	0	ES IPcam
	2121	192.168.1.2	2121	UDP	0	ES BT DL

Refresh

## System Log Settings

The System Log Settings page shows the information of the current activities on the router.

**SYSTEM LOG**

This page can be used to set local and remote log server.

[Save Changes](#) [Reset Changes](#)

**SYSTEM LOG SETTINGS**

**System Log** ☒ Enable

**Log Status** Cleanup when reboot ▾

**Log Message Size** 4 ▾ (Kbytes)

**Remote Log** ☒ Enable

**Remote Log Server Address**

**Remote Log Server Port**  (Standard : 514)

**Log to Remote and Local** ☐ Enable

[[Local System Log](#)] You can check your local system log here.

Items	Information
<b>System Log</b>	Mark to enable the configuration, and clear to disable.
<b>Log Status</b>	Select "cleanup when reboot" or "save log message" as the log type.
<b>Log Message Size</b>	Select the log message size of 4, 8, or 32 Kbytes.
<b>Remote Log</b>	Mark to enable the following configuration, and clear to disable.
<b>Remote Log Server Address</b>	Fill in the sever address for remote log.
<b>Remote Log Server Port</b>	Fill in the sever port for remote log.
<b>Log to Remote and Local</b>	To enable/disable log to remote and local

\* Please click on the **Save Settings** button or the **Reset Settings** button on the above table to save/reset the configurations.

## Date/Time Settings

This page allows users to configure the date and time of the router. To specify manually, select the date and time from the drop list and click the **Save Settings** button. To synchronize time from a timeserver, please enter the update interval hour numbers, select an NTP server from the drop list or manually enter a private NTP server and then click the **Save Settings** button. Mark the Daylight Saving checkbox if you want to apply it on system time.

**NTP CLIENT (NETWORK TIME PROTOCOL)**

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

### Manual Time Setting

**DATE & TIME SETTINGS**

SYNC TIME : ☒ Manual Time Setting ☐ NTP Time Server

Time Zone : (GMT+08:00) Beijing, Singapore, Taipei ▾

Daylight Saving : ☐

System Date : Year 2005 ▾ Mon 01 ▾ Day 01 ▾

System Time : Hour 09 ▾ Min 29 ▾ Sec 48 ▾

### NTP Time Server

**DATE & TIME SETTINGS**

SYNC TIME : ☐ Manual Time Setting ☒ NTP Time Server

Time Zone : (GMT+08:00) Beijing, Singapore, Taipei ▾

Daylight Saving : ☐

Update Interval : 24  hours

General NTP Server : None ▾

Private NTP Server :

## Management

### Admin Account

The admin account is the account for accessing this configuration interface. In this page, you can reset the password of the admin account and setup a designated IP to remote control this device.

**REMOTE ADMINISTRATION**  
Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.  
  
**Remote Control** ☒ Enable  
**HTTP port for remote**  (default:8080)  
**Remote Control IP**  (0.0.0.0 means no limit)

Admin Accounts			
Access Level	Password	Confirm Password	Action
<input type="text" value="admin"/> ▼	<input type="text"/>	<input type="text"/>	<input type="button" value="Change"/>

### Remote Administration

Items	Information
Remote Control	Mark this checkbox to allow remote PC accessing the configuration interface of this router.
HTTP port for remote	The HTTP port for accessing this management interface (default 8080).
Remote Control IP	The permitted IP for accessing. The default IP 0.0.0.0 allows all IP addresses form accessing.
Update button	Click on this button to update your setting.

### Admin Accounts

Items	Information
Access Level	Select an access level of admin or guest.
Password	The new password for the admin account.
Confirm Password	Fill in the new password again.
Action	Click <b>Change</b> button to apply the new password.



## Ping Test

---

The Ping Test page allows the administrator to test the connecting status of Internet. Fill in the IP then click on the **Ping Test** button to view the result information.

**PING TEST (PACKET INTERNET GROPER TEST)**

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping and click **Ping**.

Destination host name/IP address :

**PING TESTING RESULT**

```
PING 192.168.1.15 (192.168.1.15): 56 data bytes 84 bytes from
192.168.1.15: icmp_seq=0 ttl=128 time=0.8 ms 84 bytes from
192.168.1.15: icmp_seq=1 ttl=128 time=0.8 ms 84 bytes from
192.168.1.15: icmp_seq=2 ttl=128 time=0.8 ms --- 192.168.1.15
ping statistics --- 3 packets transmitted, 3 packets received, 0%
packet loss round-trip min/avg/max = 0.8/0.8/0.8 ms
```

---

---

---

---

## Information

---

### System Information

---

This information page shows the current settings of this device. You could check if the parameters match your configuration.

SYSTEM INFORMATION
<b>SYSTEM NAME :</b> W443 <b>Firmware Version :</b> Version 0.7 (20070905es) <b>Host Name :</b> Wireless.11n.Router <b>System Time :</b> 2007-09-05 13:10:26 <b>Uptime :</b> 1:03
WAN INTERFACE INFORMATION
<b>MAC Address :</b> 00:46:12:34:A0:11 <b>IP Assign Type :</b> Static IP <b>IP Address :</b> 10.10.13.195 <b>Subnet Mask :</b> 255.255.0.0 <b>MTU Size :</b> 1500 <b>Default Gateway :</b> 10.10.10.254 <b>Primary DNS :</b> 168.95.1.1 <b>Secondary DNS :</b> 168.95.192.1
LAN INTERFACE INFORMATION
<b>MAC Address :</b> 00:0C:43:28:60:00 <b>IP Address :</b> 192.168.1.1 <b>Subnet Mask :</b> 255.255.255.0 <b>DHCP Server :</b> Active
WLAN INTERFACE INFORMATION
<b>Mode :</b> 802.11b/g/n Mixed <b>MAC Address :</b> 00:0C:43:28:60:00 <b>SSID :</b> Wireless-11n-Router <b>Channel :</b> 1 <b>Ahthentication :</b> WEP Encryption
WDS INFORMATION
<b>Mode :</b> AP+WDS (AP Repeater) <b>Encryption Type :</b> None <b>WDS List :</b> 00:46:12:34:A0:11

## Packet Statistics

---

This page allows users to get information of data transferring condition, and monitor the status and performance of this router including interface, receiving/sending packets, and receiving/sending errors.

PACKET STATISTIC				
Some information of netstat will to be show here. You are able to view the amount of receive and send packets that passes through the network interfaces. The traffic counter will reset when the device is rebooted.				
Interface	Recv Pkts	Send Pkts	Recv Errs	Send Errs
br0	218	191	0	0
eth0	0	53	0	0
eth1	218	180	0	0
lo	47	47	0	0
ra0	1382	180	0	0
wds0	0	0	0	0

## Routing Table

---

This page shows the routing table in this router. Users can get connecting information including destination, gateway, net mask, flags, metric, ref, use and interface.

ROUTING TABLE							
A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.							
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
10.10.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
0.0.0.0	10.10.10.254	0.0.0.0	UG	0	0	0	eth0

## System Log

---

This page shows the system log information. Click the **Refresh** button to refresh the list.

SYSTEM LOG
The page can show the local system log here.
<input type="button" value="Refresh"/>

SYSTEM LOG MESSAGES LIST	
Time	Info
Jan 1 08:28:18	started: BusyBox v1.01 (2007.07.10-05:55+0000)

## Logout

---

### Logout

Click the **Logout** button to log out the admin account from this system

LOGOUT ROUTER
Logout the management system!
<input type="button" value="Logout"/>

### Reboot

---

Click the **Reboot** button to restart this system. This may cost 1 minute to restart the system. Please wait upon restarting.

REBOOT ROUTER
Reboot the router, you must wait about 1 minute for reboot.
<input type="button" value="Reboot"/>

## Product Specifications

---

<b>Standard</b>	IEEE 802.11n draft 2.0, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
<b>Interface</b>	LAN: 4 port 10/100Mbps Ethernet, RJ-45 WAN: One RJ-45 port 3* wireless antennae
<b>Antenna</b>	Antenna gain: 2dB Antenna type: Dipole Antenna connector type: Reverse SMA
<b>WAN Connection</b>	Ethernet 10/100 Mbps
<b>Cable Connections</b>	RJ-45 (10BASE-T): Category 3,4,5 UTP RJ-45 (100BASE-TX): Category 5 UTP
<b>Transmission Mode</b>	Auto-Negotiation (Full-duplex, Half-duplex)
<b>LED indications</b>	1*Status, 1*WAN, 4*LAN, 1*WLAN
<b>Security</b>	64/128-bit WEP, WPA, WPA2
<b>Network Data Rate</b>	802.11b: 1,2,5.5, and 11Mbps 802.11g: 6,9,12,18,24,36,48 and 54Mbps 802.11n: up to 300Mbps
<b>Receiver Sensitivity</b>	802.11b-91dBm, 802.11g-78dBm, 802.11n -69dBm
<b>Transmit Power</b>	802.11b 19dBm, 802.11g 16dBm, 802.11n 20MHz and 802.11n 40MHz 16dBm
<b>Channel</b>	USA 11, Europe 13
<b>Range Coverage</b>	Indoor 35~100 meters Outdoor 100~300 meters.
<b>Emission</b>	FCC CLASS B, CE FCC Part 15.247 for US (2.412~2.462MHz) ETS 300 328 for Europe (2.400~2483.5MHz) DGT LP0002 for Taiwan (2.412~2.462MHz)
<b>Operating Temperature</b>	0° ~ 40°C (32° ~ 104°F)
<b>Operating Humidity</b>	10% - 90% RH non-condensing
<b>Power Supply</b>	External Power Adapter, 12VDC/ 1A