



USER GUIDE



WIRED BARRICADE™ Router

SMCBR14

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2009 by
SMC Networks, Inc.
20 Mason
Irvine, CA 92618

All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement:

SMC Networks, Inc. (.SMC.) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an .Active. SMC product. A product is considered to be .Active. while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an .Active. SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to

returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968.

Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE:

IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER ASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY

FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
20 Mason
Irvine, CA 92618

COMPLIANCES

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.

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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning



This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Package Contents

The following contents should be found in your package:

- One SMCBR14 Cable/DSL Router
- One AC power Adapter for SMCBR14 Cable/DSL Router
- One warranty Card
- One RJ45 Cable
- Quick Installation Guide
- One Resource CD for SMCBR14 Cable/DSL Router, which include This Guide

 **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

CONTENTS

Chapter 1. Introduction	1
1.1 Product Overview	1
1.2 Main Features	1
1.3 Conventions	2
Chapter 2. Hardware Installation	3
2.1 Panel Layout	3
2.1.1 The Front Panel	3
2.1.2 The Rear Panel	3
2.2 System Requirements	4
2.3 Installation Environment Requirements	4
2.4 Connecting the Router	4
Chapter 3. Quick Installation Guide	6
3.1 Configure PC	6
3.2 Login	9
Chapter 4. Configuring the Router	13
4.1 Status	13
4.2 Quick Setup	15
4.3 Network	15
4.3.1 LAN	15
4.3.2 WAN	16
4.3.3 MAC Clone	25
4.4 DHCP	26
4.4.1 DHCP Settings	26
4.4.2 DHCP Clients List	27
4.4.3 Address Reservation	28
4.5 Forwarding	29
4.5.1 Virtual Servers	29
4.5.2 Port Triggering	31
4.5.3 DMZ	33
4.5.4 UPnP	34
4.6 Security	35
4.6.1 Firewall	35
4.6.2 IP Address Filtering	36
4.6.3 Domain Filtering	39
4.6.4 MAC Filtering	41
4.6.5 Advanced Security	42
4.7 Static Routing	44
4.8 IP QoS	45

4.9	IP & MAC Binding	47
4.9.1	Binding Setting	47
4.9.2	ARP List.....	49
4.10	DDNS.....	49
4.10.1	Dyndns DDNS	49
4.10.2	PeanutHull DDNS	50
4.10.3	Comexe DDNS	51
4.11	System Tools	52
4.11.1	Time.....	53
4.11.2	Firmware.....	54
4.11.3	Factory Defaults.....	55
4.11.4	Backup and Restore	56
4.11.5	Reboot	57
4.11.6	Password.....	58
4.11.7	Syslog.....	58
4.11.8	Remote Management	59
4.11.9	Statistics	60
Appendix A: Specifications		62
Appendix B: FAQ.....		63
Appendix C: Glossary.....		67

Chapter 1. Introduction

1.1 Product Overview

Thank you for choosing the SMCBR14 Cable/DSL Router. This router provides dedicated solutions for Small Office/Home Office (SOHO) networks. With your network all connected, your local network can share Internet access, files and fun for multiple PCs through one ISP account.

The SMCBR14 Cable/DSL Router integrates a 4-port switch, firewall, and NAT-router. It provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network on real time. It also supports VPN pass-through for sensitive data secure transmission.

The SMCBR14 Cable/DSL Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun comfortably.

Before installing the router, please look through this guide to get to know about the router's functions.

1.2 Main Features

- Built in 4-port 10/100Mbps switch
- Ethernet connection to a WAN device, such as a Cable modem or DSL modem
- Shares data and Internet access for the network, connecting Internet through PPPoE on demand and disconnecting when idle
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Statistics
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter

- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

1.3 Conventions

The Router or SMCBR14 mentioned in this User guide stands for SMCBR14 Cable/DSL Router without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

Chapter 2. Hardware Installation

2.1 Panel Layout

2.1.1 The Front Panel

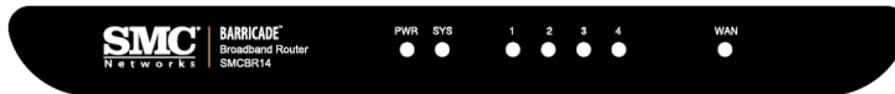


Figure 2-1

The LED indicators displayed on the front panel, the status of these LED indicators represent the device's working circs. For details, please refer to LED Explanation.

LED Explanation:

Name	Action	Description
PWR	Not lit	The router is powered off
	Lit up	The router is powered up
SYS	Not lit	The router works abnormality
	Lit up	
	Flashing	The router works properly
1/2/3/4	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
WAN	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

2.1.2 The Rear Panel



Figure 2-2

The rear panel contains the following features.

- **POWER:** The Power plug is where you will connect the power adapter.

 **Note:**

Please use the power adapter supplied with the SMCBR14 Cable/DSL Router, if you use a different adapter, it may cause damage to the Router.

- **RESET:** Use the button to reset the router's factory defaults. There are two ways to reset the router's factory defaults:
 1. Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.
 2. Use the Factory Default Reset button: Press the Reset button for five seconds and then wait for the router to reboot.

 **Note:**

Ensure the router is powered on before it restarts completely.

- **WAN:** One RJ45 port for connecting the router to a cable, DSL modem or Ethernet
- **4/3/2/1:** Four LAN 10/100Mbps RJ45 ports for connecting the router to the local PCs

2.2 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (It's not necessary if you connect the router to Ethernet)
- Each PC on the LAN needs an Ethernet Adapter and an Ethernet cable with RJ45 connectors
- An operating system supporting the TCP/IP protocol
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

2.3 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard

2.4 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your

broadband service successfully. If there is any problem, please contact with your ISP for help. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

- Step 1:** Locate an optimum location for the Router. The best place is usually near the center of the area in which your PC will be wirelessly connected. The place had better accord with the [Installation Environment Requirements](#).
- Step 2:** Connect the PC(s) and Switch/Hub in your LAN to the LAN Ports on the router, shown in Figure 2-3.
- Step 3:** Connect the DSL/Cable modem to the WAN port on the router, shown in Figure 2-3.
- Step 4:** Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.

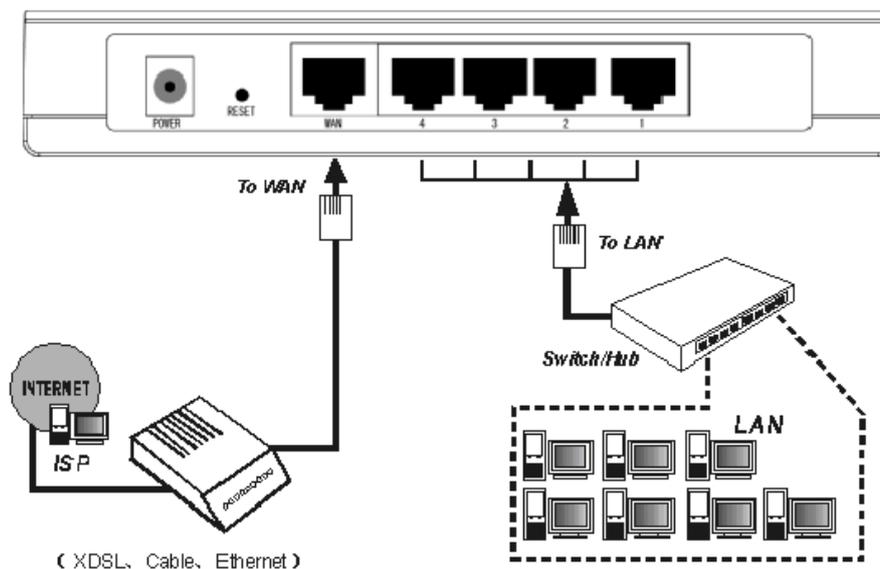


Figure 2-3

Chapter 3. Quick Installation Guide

After connecting the SMC BR14 router to your network, you should configure it. This chapter describes how to configure the PC and the Router to access the Internet immediately after it has been successfully configured (take Windows XP for example).

3.1 Configure PC

Step 1: Click the **Start** menu on your desktop, right click **My Network Places**, and then select **Properties** (shown in Figure 3-1).



Figure 3-1

Step 2: In the next screen, right click **Local Area Connection (LAN)**, and then select **Properties**.

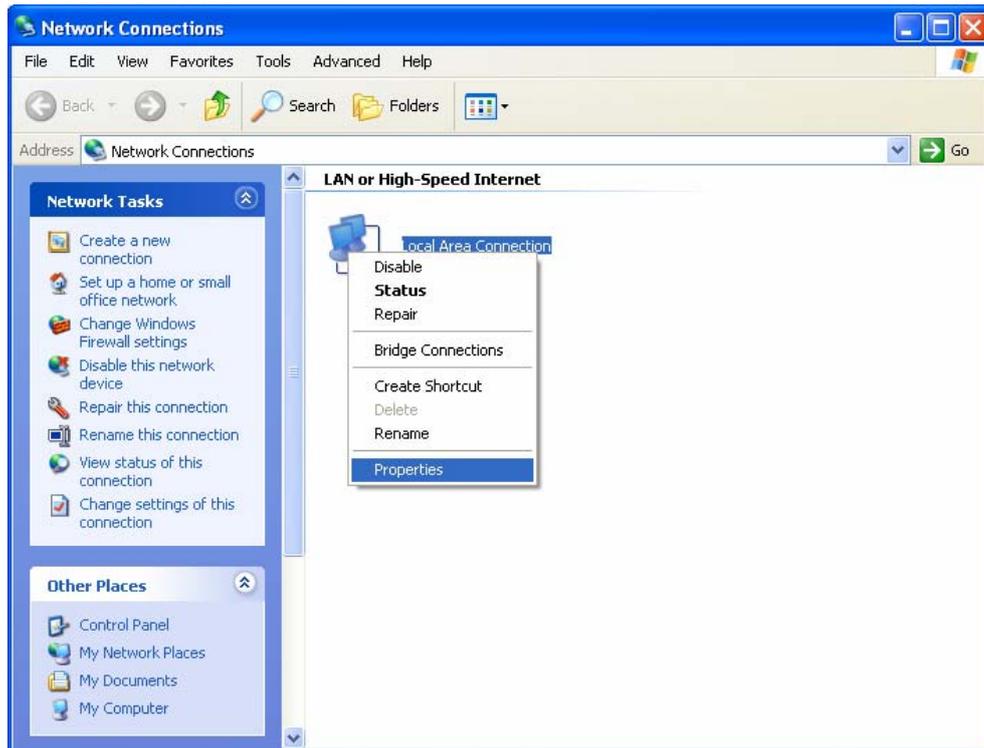


Figure 3-2

Step 3: In the next screen, select **General** tab, highlight Internet Protocol (TCP/IP), and then click the **Properties** button.

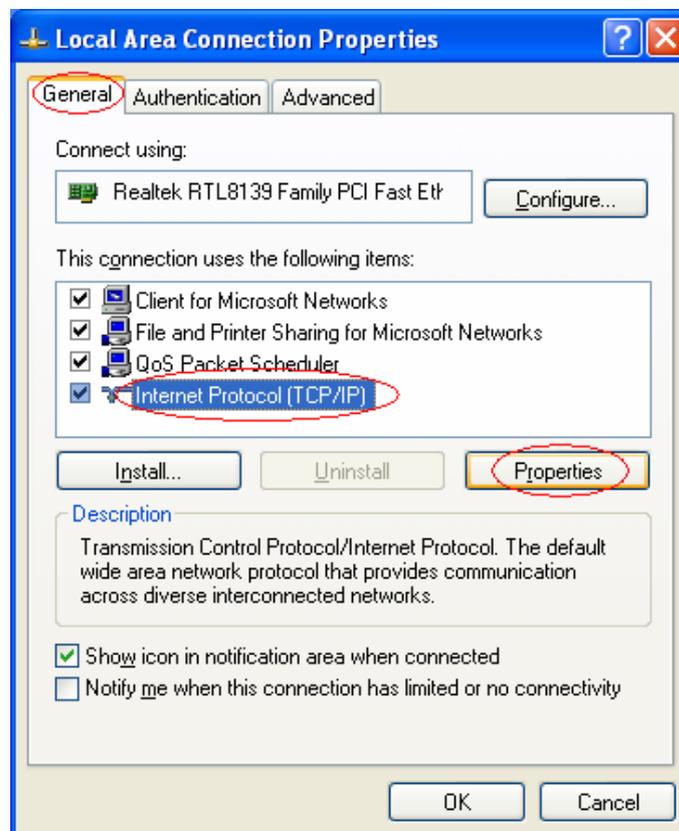


Figure 3-3

Step 4: Configure the IP address as shown in Figure 3-4. After that, click **OK**.

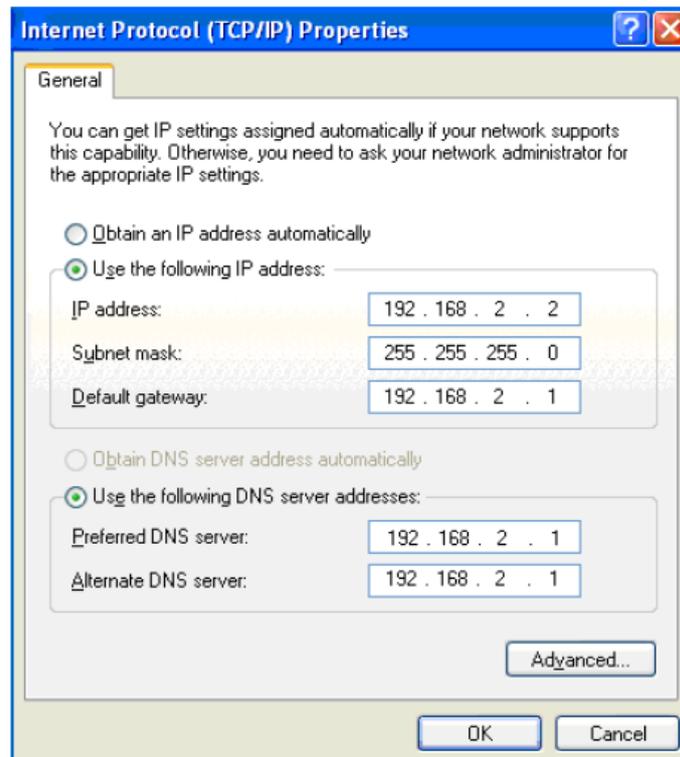


Figure 3-4

Note:

You can configure the PC to get an IP address automatically, select “Obtain an IP address automatically” and “Obtain DNS server address automatically” in the screen above.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd** in the field, and then type *ping 192.168.2.1* on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Router has been established.

```
Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 3-5

If the result displayed is similar to the screen shown below, it means that your PC has not

connected to the Router.

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

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

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3-6

You can check it follow the steps below:

 **Note:**

Is the connection between your PC and the Router correct?

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

Is the TCP/IP configuration for your PC correct?

If the Router's IP address is 192.168.2.1, your PC's IP address must be within the range of 192.168.2.2 ~ 192.168.2.254, the gateway must be 192.168.2.1.

3.2 Login

Once your host PC is properly configured, please proceed as follows to use the Web-based Utility: Start your web browser and type the private IP address of the Router in the URL field: **192.168.2.1**.

Address

After that, you will see the screen shown below, enter the default User Name **admin** and the default Password **smcadmin**, and then click **OK** to access to the **Quick Setup** screen. You can follow the steps below to complete the Quick Setup.



Figure 3-7

 **Note:**

If the above screen (Figure 3-7) does not prompt, it means that your web-browser may be set to a proxy. Choose **Tools menu**→**Internet Options**→**Connections**→**LAN Settings**, in the screen that appears, cancel the **Using Proxy checkbox**, and click **OK** to finish it.

Step 1: Select the **Quick Setup** tab on the left of the main menu and the “Quick Setup” screen will appear. Click the **Next** button.

Quick Setup

The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

Exit

Next

Figure 3-8

Step 2: Select the connection type to connect to the ISP and then click the **Next** button.

Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

- PPPoE
 Dynamic IP
 Static IP

Back

Next

Figure 3-9

 **Note:**

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP, if you are given another way that is not listed here, refer to **Network**→ **WAN** for detailed list.

Step 3: If you choose **PPPoE**, you will see the screen as shown in Figure 3-10, enter the **Username** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

Quick Setup - PPPoE

Account Name:

username

Password:

●●●●●●●●

Back

Next

Figure 3-10

Step 4: If you choose **Dynamic IP** in Figure 3-9, the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

Step 5: If you Choose **Static IP**, you should enter the detailed IP information in Figure 3-11. Click the **Next** button

Quick Setup - Static IP

IP Address:	<input type="text" value="0.0.0.0"/>	
Subnet Mask:	<input type="text" value="0.0.0.0"/>	
Default Gateway:	<input type="text" value="0.0.0.0"/>	(Optional)
Primary DNS:	<input type="text" value="0.0.0.0"/>	(Optional)
Secondary DNS:	<input type="text" value="0.0.0.0"/>	(Optional)

Figure 3-11

Step 6: After that, you will see the next screen. Click **Finish** to complete the quick installation.

Quick Setup - Finish

Congratulations! The router is now connecting you to the Internet. For detail settings, please contact other menus if necessary.

Figure 3-12

Chapter 4. Configuring the Router

This User Guide recommends using the “Quick Installation Guide” for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, you need to read this chapter and configure advanced settings through the Web-based Utility.

After your successful login, you can configure and manage the router. There are main menus on the left of the Web-based Utility. Submenus will be available after you click one of the main menus. On the center of the web-based Utility, you can configure the function. Besides this, you can refer to the help on the right of the Web-based Utility. To apply any settings you have altered on the page, please click the **Save** button.

4.1 Status

Choose “**Status**” menu, you can view the router's current status and configuration as shown in Figure 4-1. All information is read-only.

Router Status

Firmware Version: 3.5.1 Build 070515 Rel.62388na
Hardware Version: SMCBR14 1004225B

LAN

MAC Address: 00-0A-EB-22-13-51
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0

WAN

MAC Address: 00-0A-EB-22-13-52
IP Address: 0.0.0.0 PPPoE
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
DNS Server: 0.0.0.0, 0.0.0.0
Online Time: 0 day(s) 00:00:00

Traffic Statistics

	Received	Sent
Bytes:	0	0
Packets:	0	0

System Up Time: 0 day(s) 07:05:08

Figure 4-1

- **LAN** - This field displays the current settings or information for the LAN, including the “MAC address”, “IP address” and “Subnet Mask”.
- **WAN** - This field displays the parameters applied to the WAN port of the router, including “MAC address”, “IP address”, “Subnet Mask”, “Default Gateway” and so on.

 **Note:**

If PPPoE/L2TP/PPTP is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, a **Connect** button will be shown, you can then establish the connection by clicking the button.

- **Traffic Statistics:** This field displays the router's traffic statistics.
- **System Up Time:** This field displays the time of the router running from the time it is powered on or is reset.

4.2 Quick Setup

Please refer to [Chapter 3"Quick Installation Guide."](#)

4.3 Network

Choose menu “**Network**”, you can see the submenus under the Network menu: **LAN**, **WAN** and **MAC Clone**.



Figure 4-2

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.3.1 LAN

Choose menu “**Network**→**LAN**”, you can configure the IP parameters of the LAN on the screen below.

 A screenshot of a web page titled 'LAN'. The page has a light yellow background. It contains three rows of configuration fields:

- MAC Address:** 00-0A-EB-22-13-51
- IP Address:** 192.168.2.1 (text input field)
- Subnet Mask:** 255.255.255.0 (text input field with a dropdown arrow on the right)

 At the bottom of the form is a 'Save' button.

Figure 4-3

- **MAC Address** - This field displays the physical address of the LAN. The value can't be changed.
- **IP Address** - Enter the IP address for the LAN of the Router, the formal is in dotted-decimal notation (the factory default value is 192.168.2.1).
- **Subnet Mask** - Enter the subnet mask for the LAN of the Router, this address code determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

 **Note:**

- 1) If you change the IP address of the LAN, you must use the new IP address to login to the router.
- 2) If the new LAN IP Address you set is not in the same subnet, the IP Address pool in the DHCP server will not take effect, until they are re-configured. Besides this, the Virtual Server and DMZ Host may change accordingly at the same time, you'd better re-configure it as well.

4.3.2 WAN

Choose menu "**Network**→**WAN**", you can configure the IP parameters of the WAN on the screen below.

The Router provides six connection types for WAN to connect to the Internet, they are "Dynamic IP", "Static IP", "PPPoE", "BigPond Cable", "L2TP", "PPTP". (The default type is "Dynamic IP"). For configuring the WAN, you should select the connection type firstly according your needs.

1. Dynamic IP

If you aren't given any login parameters and IP information, please select **Dynamic IP** (shown in Figure 4-4), then the router will automatically get IP parameters from your ISP. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

WAN

WAN Connection Type:

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Obtaining network parameters...

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Use These DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Get IP with Unicast DHCP (It is usually not required.)

Figure 4-4

- **Host Name** - Enter the host name.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS & Secondary DNS** - If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

 **Note:**

If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get correct DNS server.

- **Get IP with Unicast DHCP:** A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (You don't need select this option generally).

2. Static IP

If you are given a fixed IP (static IP), please select **Static IP** (shown in Figure 4-5), and then fixed IP parameters specified by your ISP.

The screenshot shows the WAN configuration interface. At the top, the title 'WAN' is displayed. Below it, the 'WAN Connection Type' is set to 'Static IP' in a dropdown menu. The following fields are visible:

- IP Address:** 0.0.0.0
- Subnet Mask:** 0.0.0.0
- Default Gateway:** 0.0.0.0 (Optional)
- MTU Size (in bytes):** 1500 (The default is 1500, do not change unless necessary.)
- Primary DNS:** 0.0.0.0 (Optional)
- Secondary DNS:** 0.0.0.0 (Optional)

A 'Save' button is located at the bottom of the form.

Figure 4-5

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP (Optional).
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - Type the DNS address in dotted-decimal notation provided by your ISP (Optional).
- **Secondary DNS** - Type another DNS address in dotted-decimal notation provided by your ISP if provided (Optional).

3. PPPoE

If you are given a user name and a password, please select **PPPoE** (shown in Figure 4-6). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

WAN

WAN Connection Type:

User Name:

Password:

Wan Connection Mode:

Connect on Demand
 Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting
 Period of Time: from : (HH:MM) to : (HH:MM)

Connect Manually
 Max Idle Time: minutes (0 means remain active at all times.)

Figure 4-6

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button.

 **Note:**

- 1) If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
 - 2) Sometimes the connection can not be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.
- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
 - **Time-based Connecting** - You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.

 **Note:**

Only you have set the system time on **System Tools**→**Time** screen, will the **Time-based Connecting** function take effect.

- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically even though you attempt to access the Internet again. You need click the **Connect** button manually to connect immediately, or click the **Disconnect** button manually to disconnect immediately; To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

 **Note:**

- 1) If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.
- 2) Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.

Click the **Advanced** button to set up the advanced option as shown in Figure 4-7.

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

Use IP address specified by ISP

ISP specified IP Address:

Detect Online Interval: Seconds (0 ~ 120 seconds, 0 means not detecting.)

Use the following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Figure 4-7

- **MTU Size-** The default MTU size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address -** If you know that your ISP does not automatically transmit your IP address to the router during login, select **Use IP Address specified by ISP** and enter the IP in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval -** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between the time. If the value is 0, it means the Router does not detect.
- **Primary DNS & Secondary DNS -** If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use the following DNS servers** and enter the address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

4. BigPond Cable

If you are provided **BigPond Cable** for ISP connection, your ISP will provides user name, password, Auth Name and Auth Domain for you. You should select "BigPond Cable" (shown in Figure 4-8).and enter these information correctly.

WAN

WAN Connection Type:	<input type="text" value="BigPond Cable"/>
User Name:	<input type="text" value="username"/>
Password:	<input type="password" value="••••••••"/>
Auth Server:	<input type="text" value="sm-server"/>
Auth Domain:	<input type="text"/>
MTU Size (in bytes):	<input type="text" value="1500"/> (The default is 1500, do not change unless necessary.)
	<input type="radio"/> Connect on Demand Max Idle Time: <input type="text" value="0"/> minutes (0 means remain active at all times.)
	<input checked="" type="radio"/> Connect Automatically
	<input type="radio"/> Connect Manually Max Idle Time: <input type="text" value="0"/> minutes (0 means remain active at all times.)
	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> Disconnected
	<input type="button" value="Save"/>

Figure 4-8

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server & Auth Domain:** Enter the Auth Name and Auth Domain provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

 **Note:**

Please refer to [3 PPPoE](#) for the explanations of **Connect on Demand**, **Connect Automatically**, **Connect Manually**.

5. L2TP

If you are provided **L2TP** for ISP connection, your ISP will provides user name, password and other information for you. Please select “L2TP” and then enter the following parameters (shown in Figure 4-9).

WAN

WAN Connection Type:

User Name:

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0 , 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): (The default is 1460, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Wan Connection Mode:
 Connect on Demand
 Connect Automatically
 Connect Manually

Figure 4-9

- **User Name & Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive
- **Connect & Disconnect** - Click the button, you can handle the on-line connection or disconnection
- **Dynamic IP & Static IP** - Select the type of IP address under your ISP's introduction (We select Dynamic IP for example as shown in Figure 4-9).
- **Server IP Address/Name** - Please type the correct Server IP Address/Name which your ISP provided.
- **MTU Size (in bytes)** - The default value is 1460, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

 **Note:**

Please refer to **3 PPPoE** for the explanations of **Connect on Demand**, **Connect Automatically**, **Connect Manually**.

6. PPTP

If you are provided **PPTP** for ISP connection, your ISP will provides user name, password and other information for you. Please select “L2TP” and then enter the following parameters (shown in Figure 4-10).

WAN

WAN Connection Type:

User Name:

Password:

Connecting...

Dynamic IP Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0 , 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): (The default is 1420, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Wan Connection Mode:

Connect on Demand
 Connect Automatically
 Connect Manually

Figure 4-10

- **User Name & Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive

- **Connect & Disconnect** - Click the button, you can handle the on-line connection or disconnection
- **Dynamic IP & Static IP** - Select the type of IP address under your ISP's introduction (We select Dynamic IP for example as shown in Figure 4-10).
- **Server IP Address/Name** - Please type the correct Server IP Address/Name which your ISP provided.
- **MTU Size (in bytes)** - The default value is 1420, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

 **Note:**

Please refer to [3 PPPoE](#) for the explanations of **Connect on Demand**, **Connect Automatically**, **Connect Manually**.

4.3.3 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below (shown in Figure 4-11).

Some ISPs require that you register the MAC address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. You do not generally need to change anything here.

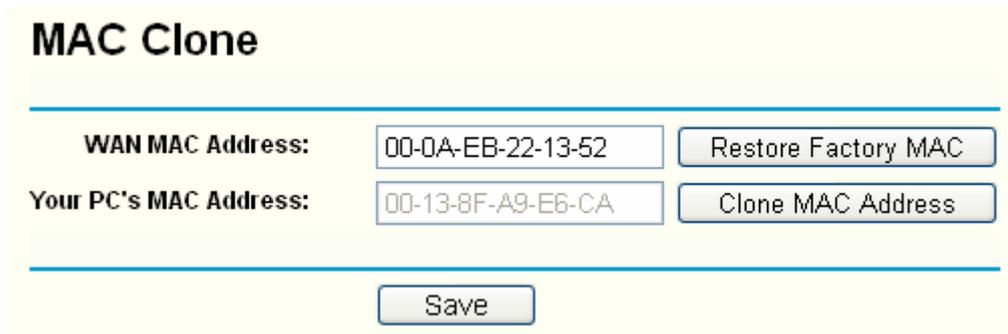


Figure 4-11

- **WAN MAC Address** - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC address is XX-XX-XX-XX-XX-XX (for example: 00-0A-EB-22-13-52).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the "WAN MAC Address" field.

 **Note:**

- 1) Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

- 2) Only the PC(s) on your LAN can use the **MAC Address Clone** feature.
- 3) After you finish the configuration, click the **Save** button, and the router will prompt you to reboot.

4.4 DHCP

Choose menu “**DHCP**”, you can see the submenus under the main menu: **DHCP Settings**, **DHCP Clients List** and **Address Reservation**.

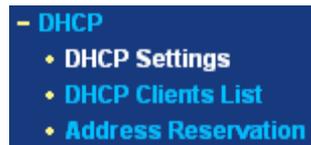


Figure 4-12

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.4.1 DHCP Settings

Choose menu “**DHCP**→**DHCP Settings**”, you can configure the DHCP in the next screen (shown in Figure 4-13).

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

Figure 4-13

- **DHCP Server** - Enable or disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first address in the IP address pool. The default address is 192.168.2.100.
- **End IP Address** - This field specifies the end address in the IP address pool. The default address is 192.168.2.199.
- **Address Lease Time** - This is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time (in minutes), the range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - Suggest to input the IP address of the LAN port of the router, default value is 192.168.2.1. (Optional)
- **Default Domain** - Input the domain name of your network. (Optional)
- **Primary DNS** - Input the DNS IP address provided by your ISP. You can consult your ISP for it. (Optional)
- **Secondary DNS** - Input the IP address of another DNS server if your ISP provides two DNS servers. (Optional)

 **Note:**

To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

4.4.2 DHCP Clients List

Choose menu "**DHCP→DHCP Clients List**", you can view the information about the clients attached to the router in the next screen (shown in Figure 4-14). Click the **Refresh** button to update the information.

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	User	00-13-8F-A9-E6-CA	192.168.2.104	01:59:53

Figure 4-14

- **Client Name** - This field displays the name of the DHCP client
- **MAC Address** - This field displays the MAC address of the DHCP client

- **Assigned IP** - This field displays the IP address that the router has allocated to the DHCP client.
- **Lease Time** - This field displays the time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

4.4.3 Address Reservation

Choose menu “**DHCP → Address Reservation**”, you can view and add reserved addresses for clients via the next screen (shown in Figure 4-15).

If you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

ID	MAC Address	Reserved IP Address	Status	Modify
1	00-13-8F-A9-E6-CA	192.168.2.100	Enabled	Modify Delete

Figure 4-15

- **MAC Address** - This field displays the MAC address of the PC for which you want to reserve IP address.
- **Reserved IP Address** - This field displays the IP address of the router reserved.
- **Status** - This field displays the status of the virtual server entry. **Enabled** means that the entry will take effect, **Disabled** means that the entry will not take effect.

To add/modify a reserved IP address:

Step 1: Click **Add New.../Modify** shown in Figure 4-15, you will see a new screen shown in Figure 4-16.

Step 2: Enter the MAC address, IP address and select Status as shown in the screen below.

Add or Modify a Address Reservation Entry

MAC Address:	<input style="width: 60%;" type="text" value="00-13-8F-A9-E6-CA"/>
Reserved IP Address:	<input style="width: 60%;" type="text" value="192.168.2.100"/>
Status:	<input style="width: 60%;" type="text" value="Enabled"/> ▼

Figure 4-16

Step 3: Click the **Save** button when finished.

Note:

- 1) If you want to add more than one reserved IP, please go to **step 1** to continue.
- 2) The function won't take effect until the router reboots.

Other configurations for the entries as shown in Figure 4-15:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.5 Forwarding

Choose menu “**Forwarding**”, you can see the submenus under the main menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**.



Figure 4-17

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.5.1 Virtual Servers

Choose menu “**Forwarding**→**Virtual Servers**”, you can view and add virtual servers in the next screen (shown in Figure 4-18).

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was configured as a virtual server must have a static or a reserved IP address because its IP address may change when using the DHCP function.

ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.2.100	TCP	Enabled	Modify Delete
2	80	192.168.2.101	ALL	Enabled	Modify Delete

Figure 4-18

- **Service Port** - This field displays the numbers of External Ports. It can be a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address** - This field displays the IP address of the PC running the service application.
- **Protocol** - This field displays the protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status** - This field displays the status of the virtual server entry. **Enabled** means that the entry will take effect, **Disabled** means that the entry will not take effect.

To add/modify a virtual server entry:

Step 1: Click **Add New.../Modify** shown in Figure 4-15, you will see a new screen shown in Figure 4-19.

Step 2: Select the service you want from the “Common Service Port”, then the port and protocol value will be added to the corresponding field automatically, you only need to configure the IP address for the virtual server; If the “Common Service Port” does not contain the service that you want, please configure the Service Port, IP Address and Protocol manually.

Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)
IP Address:
Protocol: ▼
Status: ▼
Common Service Port: ▼

Figure 4-19

Step 3: After that, select **Enabled** to make the entry take effect.

Step 4: Click **Save** button to save the configuration.

Note:

- 1) If you want to add more than one reserved IP, please go to **step 1** to continue.
- 2) It is possible that you configure more than one type of available service on a computer or server, it means the IP addresses for the virtual servers are same.

Other configurations for the entries as shown in Figure 4-19:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

Note:

If you set the virtual server of the service port as 80, you must set the web management port on **Security → Remote Management** screen to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

4.5.2 Port Triggering

Choose menu "**Forwarding → Port Triggering**", you can view and add port triggerings in the next screen (shown in Figure 4-20).

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

Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	6112	ALL	6112	ALL	Enabled	Modify Delete

Figure 4-20

- **Trigger Port** - This displays the port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol** - This displays the protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Incoming Ports** - This displays the port or port range used by the remote system, they are used for responding to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol** - This displays the protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **ALL** (all protocols supported by the router).
- **Status** - This displays the status. **Enabled** means that the rule will take effect, **Disabled** means that the rule will not take effect.

Once configured, the operation for Port Triggering will proceed as follows:

- Step 1:** A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
- Step 2:** The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
- Step 3:** When necessary, the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

To add/modify a port triggering entry:

- Step 1:** Click **Add New.../Modify** shown in Figure 4-20, you will see a new screen shown in Figure 4-21.
- Step 2:** Select the application you want from the "Common Applications", then the Trigger port and Incoming ports will be added to the corresponding field automatically, you only need to configure the Trigger protocol and Incoming Protocol for the entry; If the "Common Applications" does not contain the

applications that you want, please configure these options manually.

Add or Modify a Port Triggering Entry

Trigger Port:	<input type="text" value="6112"/>
Trigger Protocol:	<input type="text" value="ALL"/>
Incoming Ports:	<input type="text" value="6112"/>
Incoming Protocol:	<input type="text" value="ALL"/>
Status:	<input type="text" value="Enabled"/>
Common Applications:	<input type="text" value="Battle.net"/>

Figure 4-21

Step 3: After that, select **Enabled** to make the entry take effect.

Step 4: Click **Save** button to save the configuration.

Note:

- 1) If you want to add more than one reserved IP, please go to **step 1** to continue.
- 2) When the trigger connection is released, the according opening ports will be closed.
- 3) Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
- 4) Incoming Port Range cannot overlap each other.

Other configurations for the entries as shown in Figure 4-21:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.5.3 DMZ

Choose menu "**Forwarding**→**DMZ**", you can view and configure DMZ host in the screen (shown in Figure 4-22).

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host

forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Figure 4-22

To assign a computer or server to be a DMZ server:

Step 1: Click the **Enable** radio button

Step 2: Enter the local host IP address in the **DMZ Host IP Address** field

Step 3: Click the **Save** button.

Note:

After you set the DMZ host, the firewall related to the host will not take effect.

4.5.4 UPnP

Choose menu “**Forwarding**→**UPnP**”, you can view the information about UPnP in the screen (shown in Figure 4-23). You can click **Refresh** to update the Current UPnP Settings List before viewing the information.

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

UPnP

Current UPnP Status: **Enabled**

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	ftp	21	TCP	21	192.168.2.102	Enabled

Figure 4-23

- **Current UPnP Status** - If you want to use the Router’s UPnP function, please click **Enable** button. If you don’t want use the function, please click **Disable** button.

Allowing the function may cause a risk to security, this feature is disabled by default.

- **App Description** - This displays the description provided by the application in the UPnP request.
- **External Port** - This displays the external port, which the router opened for the application.
- **Protocol** - This displays the protocol for the application.
- **Internal Port** - This displays the Internal port, which the router opened for local host.
- **IP Address** - The UPnP device that is currently accessing the router.
- **Status** - This displays the status. **Enabled** means that the port is still active, **Disabled** means that the port is inactive.

4.6 Security

Choose menu “**Security**”, you can see the submenus under the main menu: **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Filtering** and **Advanced Security**.



Figure 4-24

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.6.1 Firewall

Choose menu “**Security**→**Firewall**”, you can control the general firewall switch in the next screen (shown in Figure 4-25). The default setting for the switch is off, and the IP Address Filtering, DNS Filtering and MAC Filtering are disabled, their settings are ineffective in this situation.

Firewall

Enable Firewall (the general firewall switch)

Enable IP Address Filtering
 Default IP Address Filtering Rules:

Allow the packets not specified by any filtering rules to pass through the router

Deny the packets not specified by any filtering rules to pass through the router

Enable Domain Filtering

Enable MAC Address Filtering
 Default MAC Address Filtering Rules:

Allow these PCs with enabled rules to access the Internet

Deny these PCs with enabled rules to access the Internet

Figure 4-25

- **Enable Firewall** - Enable the general firewall switch or not.
- **Enable IP Address Filtering** - Enable the IP Address Filtering or not. There are two default filtering rules, please select the rule for your need.
- **Enable Domain Filtering** - Enable the Domain Filtering or not. There are two default filtering rules, please select the rule for your need.
- **Enable MAC Address Filtering** - Enable MAC Address Filtering or not. There are two default filtering rules, please select the rule for your need.

4.6.2 IP Address Filtering

Choose menu “**Security**→**IP Address Filtering**”, you can configure the IP Address filtering rule in the next screen (shown in Figure 4-26). The IP Address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses.

IP Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: **Enabled**

Enable IP Address Filtering: **Enabled**

Default Filtering Rules: **Allow** the packets not specified by any filtering rules to pass through the router

ID	Effective time	LAN IP	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	1800-2200	192.168.2.7	-	25	ALL	Deny	Enabled	Modify Delete
2	1800-2200	192.168.2.7	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.2.8-192.168.2.12	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

ID to ID

Figure 4-26

- **Effective Time** - This is the time or the range of time for the entry to take effect. For example, 1800 - 2200, it means that the entry will take effect from 18:00 to 22:00.
- **LAN IP** - This is the LAN IP address or the range of LAN IP addresses in dotted-decimal notation format. For example, 192.168.2.20 - 192.168.2.30. Keep the field blank, which means all LAN IP addresses are controlled by the rule.
- **WAN IP** - This is the WAN IP address or the range of WAN IP addresses in dotted-decimal notation format. For example, 202.96.134.210 – 202.96.134.230. Keep the field blank, which means all WAN IP addresses are controlled by the rule.
- **WAN Port** - This is the WAN Port or the range of WAN Ports. For example, 25 – 110. Keep the field blank, which means all WAN Ports are controlled by the rule.
- **Protocol** - This indicates which protocol is used, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Action** - This field displays the action that the Router takes to deal with the traffic. **Allow** means that the Router allows the traffic through the Router, **Deny** means that the Router rejects the traffic through the router.
- **Status** - This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.

To add/modify an IP Address filtering entry:

For example: If you desire to block E-mail received and sent by the IP address 192.168.2.7 on your local network during the time of 1800 to 2200; And wish to make the PCs with IP addresses 192.168.2.8 to 192.168.2.12 unable to visit the website of IP address 202.96.134.12 all the day, while other PCs have no limit. You can configure the rules as follows.

Step 1: Enable the “Firewall” and “IP Address Filtering” on the Firewall screen (show in Figure 4-25), and then, you should select the Default IP Address Filtering Rule

"Allow the packets not specified by any filtering rules to pass through the router".

Step 2: Click **Add New.../Modify** shown in Figure 4-26, you will see a new screen shown in Figure 4-27.

Step 3: Enter the "Effective time" that the rule will take effect as shown in Figure 4-27.

Step 4: Enter the "LAN IP Address", "WAN IP Address" and "WAN Port" in the corresponding field as shown in Figure 4-27.

Step 5: Select the "Protocol", "Action" and "Status" for the rule as shown in the next screen.

Add or Modify an IP Address Filtering Entry

Effective time: 1800 - 2200

LAN IP Address: 192.168.2.7 -

WAN IP Address: -

WAN Port: 25 -

Protocol: ALL

Action: Deny

Status: Enabled

Save Return

Figure 4-27

Step 6: Click the **Save** button to save this entry.

Step 7: Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	Effective time	LAN IP	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	1800-2200	192.168.2.7	-	25	ALL	Deny	Enabled	Modify Delete
2	1800-2200	192.168.2.7	-	110	ALL	Deny	Enabled	Modify Delete
3	0000 2400	192.168.2.8	192.168.2.12	202.96.134.12	ALL	Deny	Enabled	Modify Delete

Figure 4-28

Note:

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-25).

Other configurations for the entries as shown in Figure 4-26:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.6.3 Domain Filtering

Choose menu “**Security**→**Domain Filtering**”, you can configure the Domain filtering rule in the next screen (shown in Figure 4-29). The Domain Filtering feature allows you to control access to certain websites on the Internet by specifying their domains or key words.

Domain Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: **Enabled**

Enable Domain Filtering: **Enabled**

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

Figure 4-29

- **Effective Time** - This is the time or the range of time for the entry to take effect. For example, 0800 - 2400, it means that the entry will take effect from 08:00 to 20:00.
- **Domain Name** - This is the domain or key word as desired. Leaving the field blank means all websites on the Internet are prohibited from accessing.
- **Status** - This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add or modify a Domain Filtering entry:

For example: if you want to block the PCs on your LAN from accessing websites www.xxyy.com.cn, www.aabbcc.com and websites with end of .net on the Internet, while no limit for other websites, you can configure as follows.

- Step 1:** Enable the “Firewall” and “Domain Filtering” on the Firewall screen (show in Figure 4-25).
- Step 2:** Click **Add New.../Modify** shown in Figure 4-29, you will see a new screen shown in Figure 4-30.
- Step 3:** Enter the “Effective time” that the rule will take effect, enter the “Domain Name” as shown in Figure 4-30.
- Step 4:** Select the “Status” for the rule as shown in the next screen.

Add or Modify a Domain Filtering entry

Effective time	-	<input type="text" value="0000"/>	<input type="text" value="2400"/>
Domain Name:	<input type="text" value="www.xxyy.com.cn"/>		
Status:	<input type="text" value="Enabled"/> ▼		

Figure 4-30

- Step 5:** Finally, click **Save** to make the rule take effect.
- Step 6:** Go to **Step 2** to complete the other rules continually.
- After you finish the configurations, you will see the rules in the table below:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

Figure 4-31

 **Note:**

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-25).

Other configurations for the entries as shown in Figure 4-26:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.6.4 MAC Filtering

Choose menu “**Security**→**MAC Address Filtering**”, you can configure the MAC Address filtering rule in the next screen (shown in Figure 4-32). The MAC Address Filtering feature allows you to control access to the Internet by users on your local network based on their MAC addresses.

MAC Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: Enabled

Enable MAC Address Filtering: Enabled

Default Filtering Rules: Deny these PCs with enabled rules to access the Internet

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

Add New...
Enable All
Disable All
Delete All

Previous
Next

Figure 4-32

- **MAC Address** - This is the PC'S MAC address which is controlled by the rule, its format of is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
- **Description** - This is the description about the PC, Fox example: John's PC.
- **Status** - This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add or modify a Domain Filtering entry:

Fox example: If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, you can configure as follows.

Step 1: Enable the “Firewall” and “MAC Address Filtering” on the Firewall screen (show in Figure 4-25). And then specify the Default MAC Address Filtering Rule "Deny these PCs with enabled rules to access the Internet".

Step 2: Click **Add New.../Modify** shown in Figure 4-32, you will see a new screen shown in Figure 4-33.

Step 3: Enter the appropriate MAC address and descriptions, then select the status as shown in Figure 4-33.

Add or Modify a MAC Address Filtering Entry

MAC Address:
Description:
Status:

Figure 4-33

Step 4: Finally, click **Save** to make the rule take effect.

Step 5: Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

Figure 4-34

Note:

Before adding a MAC Address Filtering entry, you should enable the Firewall and the MAC Address Filtering function first (shown in Figure 4-25).

Other configurations for the entries as shown in Figure 4-26:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.6.5 Advanced Security

Choose menu "**Security**→**Advanced Security**", you can configure the functions below to protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN (shown in Figure 4-35).

Advanced Security

Packets Statistics Interval (5 ~ 60): Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): Packets/s

Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): Packets/s

Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): Packets/s

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Figure 4-35

- **Packets Statistic Interval (5 ~ 60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The “Packets Statistic interval” value indicates the time section of the packets statistic.
- **DoS Protection** - Enable or disable the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering** - Enable or disable the “ICMP-FLOOD Attack Filtering”.
- **ICMP-FLOOD Packets Threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 and 3600 packets/s. When the current number of ICMP-FLOOD packets is beyond the permitted value, the Router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering** - Enable or disable the “UDP-FLOOD Filtering”.
- **UDP-FLOOD Packets Threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets/s. When the current number of UPD-FLOOD Packets is beyond the permitted value, the router will start up the blocking function

immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or disable the “TCP-SYN-FLOOD Attack Filtering”.
- **TCP-SYN-FLOOD Packets Threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets/s. When the current number of **TCP-SYN-FLOOD** Packets is beyond the permitted value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port** - Enable or disable “ignore ping packet from WAN port”. The default is disabled. If enabled, the ping packet from the Internet can not access the router.
- **Forbid Ping Packet from LAN Port** - Enable or disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port can not access the router. (Defends against some viruses)

Click the **Save** button to save the settings.

Click the **Blocked DoS Host List** button to view the blocked hosts.

4.7 Static Routing

Choose menu “**static route**”, you can configure the static route in the next screen (shown in Figure 4-36). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Static Routing

ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
1	202.96.134.210	255.255.255.0	192.168.2.2	Enabled	Modify Delete

Figure 4-36

- **Destination IP Address** - The “Destination IP Address” is the address of the network or host that you want to assign to a static route.
- **Subnet Mask** - The “Subnet Mask” determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Default Gateway** - This is the IP address of the gateway device that allows for contact between the router and the network or host.
- **Status** - This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add/modify a static routing entry:

Step 1: Click **Add New.../Modify** shown in Figure 4-36, you will see a new screen shown in Figure 4-37.

Step 2: Enter the appropriate Destination IP Address, Subnet Mask and Default Gateway, and then select the status.

Add or Modify a Static Route Entry

Destination IP Address:	<input type="text" value="202.96.134.210"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.2.2"/>
Status:	<input type="text" value="Enabled"/> ▼

Figure 4-37

Step 3: Click **Save** to make the entry take effect.

Note:

If you want to add more than one static route, please go to **step 1** to continue.

Other configurations for the entries as shown in Figure 4-26:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.8 IP QoS

Choose menu "**IP QoS**", you can configure the IP QoS function in the next screen (shown in Figure 4-38).

IP QoS

Enable IP QoS

Choose BandWidth Type:

Bandwidth Apply: Kbps

ID	IP Range	Mode	Bandwidth	Description	Enable	Delete
1	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
2	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
3	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
4	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
5	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
6	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
7	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete
8	192.168.2 <input type="text"/> - 192.168.2 <input type="text"/>	Minimum Bandw <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Delete

Figure 4-38

- **Enable IP QoS** - Open or close the function of IP QoS.
- **Choose BandWidth Type** - Network connection type.
- **Bandwidth Apply** - Bandwidth you get. If you are not clear about that, please contact with your ISP for help.
- **IP Range** - IP range of this entry.
- **Mode** - There are 2 types of mode: Minimum Bandwidth Guarantee and Maximum Bandwidth Limit.
- **Bandwidth** - Bandwidth you supply to this entry.
- **Description** - Description of this entry.
- **Enable** - Enable this entry.

Click the **Delete** button to delete single entry.

Click the **Delete All** button to delete all entries.

Click the **Save** button to save all configuration.

Note:

- 1) The conversion relation of bandwidth: 1Mbps=1000Kbps.
- 2) Please choose the Network Connection Type and set the bandwidth according to your Network. If you are not clear about that, please contact with your ISP for help.
- 3) IP address range for different entries could not have intersection with each other.
- 4) After the configuration, click "Save" button for the change to take effect.

4.9 IP & MAC Binding

Choose menu “**IP & MAC Binding**”, you can see the submenus under the main menu: **Binding Setting, ARP List**.



Figure 4-39

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.9.1 Binding Setting

Choose menu “**IP & MAC Binding**→**Binding Setting**”, you can view and add IP & MAC binding entries in the next screen (shown in Figure 4-40).

 A screenshot of the 'IP & MAC Binding Setting' configuration page. At the top, there is a title 'IP & MAC Binding Setting'. Below the title, there is a section for 'ARP Binding:' with two radio buttons: 'Disable' (unselected) and 'Enable' (selected). To the right of these buttons is a 'Save' button. Below this is a table with the following columns: 'ID', 'MAC Address', 'IP Address', 'Bind', and 'Modify'. The table contains one row with ID '1', MAC Address '00-13-8F-A9-E6-CA', IP Address '192.168.2.100', and a checked 'Bind' box. The 'Modify' column contains links for 'Edit' and 'Delete'. Below the table are four buttons: 'Add New...', 'Enable All', 'Delete All', and 'Find'. At the bottom, there are 'Previous' and 'Next' buttons, and a 'Page 1' dropdown menu.

Figure 4-40

- **MAC Address** - This field displays the MAC address of the controlled computer in the LAN.
- **IP Address** - This field displays the assigned IP address of the controlled computer in the LAN.
- **Bind** - Select Whether enable the arp binding or not. Only bind the MAC address and IP address can the function take effect.

To add/modify an IP & MAC binding entry:

Step 1: Click **Add New.../Modify** shown in Figure 4-40, you will see a new screen shown in Figure 4-41.

Step 2: Enter the MAC Address and IP Address in the corresponding field.

IP & MAC Binding Setting

Bind:

MAC Address:

IP Address:

Figure 4-41

Step 3: Bind the MAC and IP address, then click **Save** button to save the configuration.

To find a specific IP & MAC binding entry:

Step 1: Click **Find** shown in Figure 4-40, you will see a new screen shown in Figure 4-42.

Step 2: Enter the specific MAC Address or IP Address in the corresponding field.

Find IP & MAC Binding Entry

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind	Link
1	00-13-8F-A9-E6-CA	192.168.2.100	<input checked="" type="checkbox"/>	Turn to this page

Figure 4-42

Step 3: Click **Find** button, then you will see the entry with the specific MAC address or IP address.

Step 4: Click **Return** to return the previous screen.

 **Note:**

You can click “Turn to this page” to edit the entry in the corresponding screen.

Other configurations for the entries as shown in Figure 4-40:

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.9.2 ARP List

Choose menu “**IP & MAC Binding**→**ARP List**”, you can view the ARP list in the next screen (shown in Figure 4-43). This screen displays the ARP list, it shows all the existing IP & MAC Binding entries.

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also.

ID	MAC Address	IP Address	Status	Configure
1	00-13-8F-A9-E6-CA	192.168.2.100	Bound	<input type="button" value="Load"/> <input type="button" value="Delete"/>

Figure 4-43

Click **Load** to load the specific item to the IP & MAC Binding list (shown in Figure 4-40).

Click **Delete** to load the specific item to the IP & MAC Binding list.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list (shown in Figure 4-40).

Click the **Refresh** button to refresh all items.

Note:

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before.

4.10 DDNS

Choose menu “**Dynamic DNS**”, you can configure DDNS function.

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

4.10.1 Dyndns DDNS

If your dynamic DNS Service Provider is www.dyndns.org, you can configure in the next

screen (shown in Figure 4-44).

DDNS

Service Provider: DynDNS (www.dyndns.org) [Go to register...](#)

User Name:

Password:

Domain Name:

Enable DDNS

Connection Status: DDNS not launching !

Figure 4-44

- **Connection Status** - The status of the DDNS service is displayed here.

To set up for DynDNS DDNS, follow these instructions:

Step 1: Type the “User Name” and “Password” for your DDNS account.

Step 2: Enter the domain name your dynamic DNS service provider offer.

Step 3: Enable DDNS, and click **Save** to save the current configuration.

Click **Login** to login the DDNS service.

Click **Logout** to logout the DDNS service.

4.10.2 PeanutHull DDNS

If your dynamic DNS Service Provider is www.oray.net, you can configure in the next screen (shown in Figure 4-45).

DDNS

Service Provider: PeanutHull (www.oray.net)

User Name:

Password:

Enable DDNS

Connection Status: Disconnected !

Service Type: ---

Domain Name: ---

Figure 4-45

To set up for PeanutHull DDNS, follow these instructions:

Step 1: Type the User Name and Password for your DDNS account.

Step 2: Enable DDNS, and click **Save** to save the current configuration.

Click the **Login** button to login to the DDNS service.

Click **Logout** to logout of the DDNS service.

4.10.3 Comexe DDNS

If your dynamic DNS Service Provider is www.comexe.cn, you can configure in the next screen (shown in Figure 4-46).

DDNS

Service Provider: Comexe (www.comexe.cn)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: Disconnected !

Figure 4-46

To set up for Comexe DDNS, follow these instructions:

Step 1: Enter the domain name your dynamic DNS service provider offer.

Step 2: Type the “User Name” and “Password” for your DDNS account.

Step 3: Enable DDNS, and click **Save** to save the current configuration.

Click **Login** to login the DDNS service.

Click **Logout** to logout the DDNS service.

4.11 System Tools

Choose menu “**System Tools**”, you can see the submenus under the main menu: **Time**, **Firmware**, **Factory Defaults**, **Backup and Restore**, **Reboot**, **Password**, **Log**, **Remote Management** and **Statistics**.

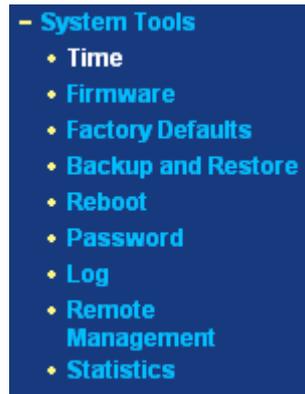


Figure 4-47

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.11.1 Time

Choose menu “**System Tools**→**Time**”, you can configure the time on the screen (shown in Figure 4-48).

Time Settings

Time zone: (GMT+08:00) Taipei

Date: 5 21 2007 (MM/DD/YY)

Time: 17 40 57 (HH/MM/SS)

Using Daylight Saving Time:

DST begin : 0 0 0 (MM/DD/HH)

DST end: 0 0 0 (MM/DD/HH)

Preferable NTP Server: 0.0.0.0 0.0.0.0

(Get GMT when connected to Internet)

Figure 4-48

- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.
- **Using Daylight Saving Time** - Select this option if you want use Daylight Saving Time (DST), and configure the DST begin time and end time below.

- **Preferable NTP Server** - Enter the address for the NTP Server, then the Router will get the time from the Preferable NTP Server firstly. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To configure the system manually:

Step 1: Select your local time zone.

Step 2: Enter date and time in the right blanks.

Step 3: Select Using Daylight Saving Time if you need, and configure the begin time and end time for the function.

Step 4: Click Save to save the configuration.

To configure the system automatically:

Step 1: Select your local time zone.

Step 2: Enter the IP address for Preferable NTP Server, then the Router will get the time from the Preferable NTP Server firstly.

Step 3: Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

Note:

- 1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, or else, the time limited on these functions will not take effect.
- 2) The time will be lost if the router is turned off.
- 3) The router will obtain GMT time automatically from Internet if it has already connected to the Internet.

4.11.2 Firmware

Choose menu “**System Tools** → **Firmware**”, you can update the latest version of firmware for the Router on the screen (shown in Figure 4-49).

Firmware

File:

Firmware Version: 3.5.1 Build 070515 Rel.62388na

Hardware Version: SMCBR14 1004225B

Figure 4-49

- **Firmware Version** - This displays the current firmware version.

- **Hardware Version** - This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

To upgrade the router's firmware, follow these instructions below:

Step 1: Download a more recent firmware upgrade file from the SMC website (www.smcnetworks.com.tw)

Step 2: Type the path and file name of the update file into the "File" field. Or click the **Browse** button to locate the update file.

Step 3: Click the **Upgrade** button.

Note:

- 5) New firmware versions are posted at www.smcnetworks.com.tw and can be downloaded for free. If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use.
- 6) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.
- 7) Do not turn off the router or press the Reset button while the firmware is being upgraded.
- 8) The router will reboot after the upgrading has been finished.

4.11.3 Factory Defaults

Choose menu "**System Tools**→**Factory Defaults**", you can restore the configurations of the Router to factory defaults on the screen (shown in Figure 4-50).

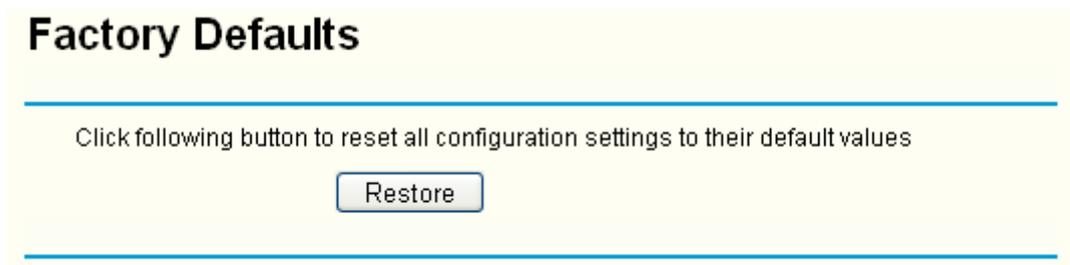


Figure 4-50

Click the **Restore** button to reset all configuration settings to their default values.

Note:

- 1) The default **User Name** is admin.
- 2) The default **Password** is smcadmin.
- 3) The default **IP Address** is 192.168.2.1.
- 4) The default **Subnet Mask** is 255.255.255.0.
- 5) All settings you have saved will be lost when the default settings are restored.

4.11.4 Backup and Restore

Choose menu “**System Tools**→**Backup and Restore**”, you can save the current configuration of the Router as a backup file and restore the configuration via a backup file (shown in Figure 4-51).

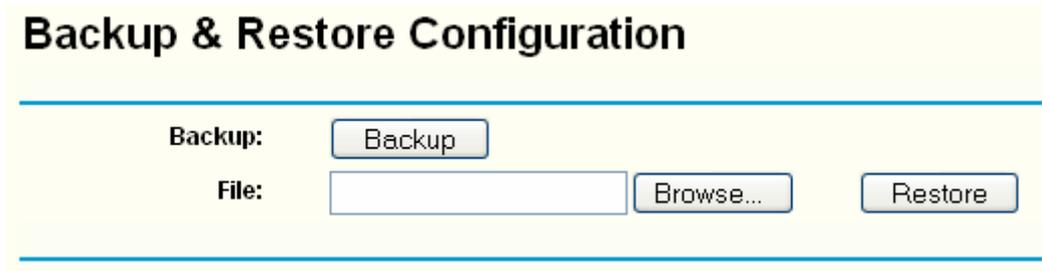


Figure 4-51

To back up the Router's current settings:

Step 1: Click the **Backup** button (shown in Figure 4-51), click **Save** button in the next screen (shown in Figure 4-52) to proceed.

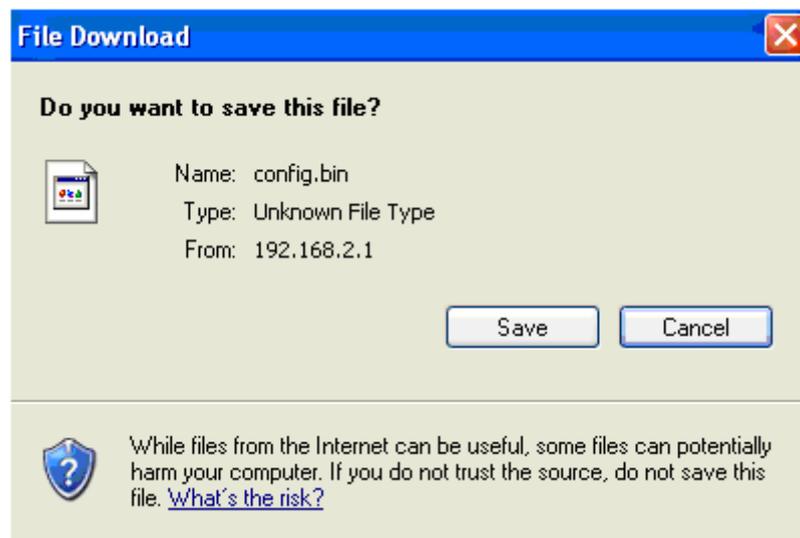


Figure 4-52

Step 2: Save the file as the appointed file (shown in Figure 4-53).

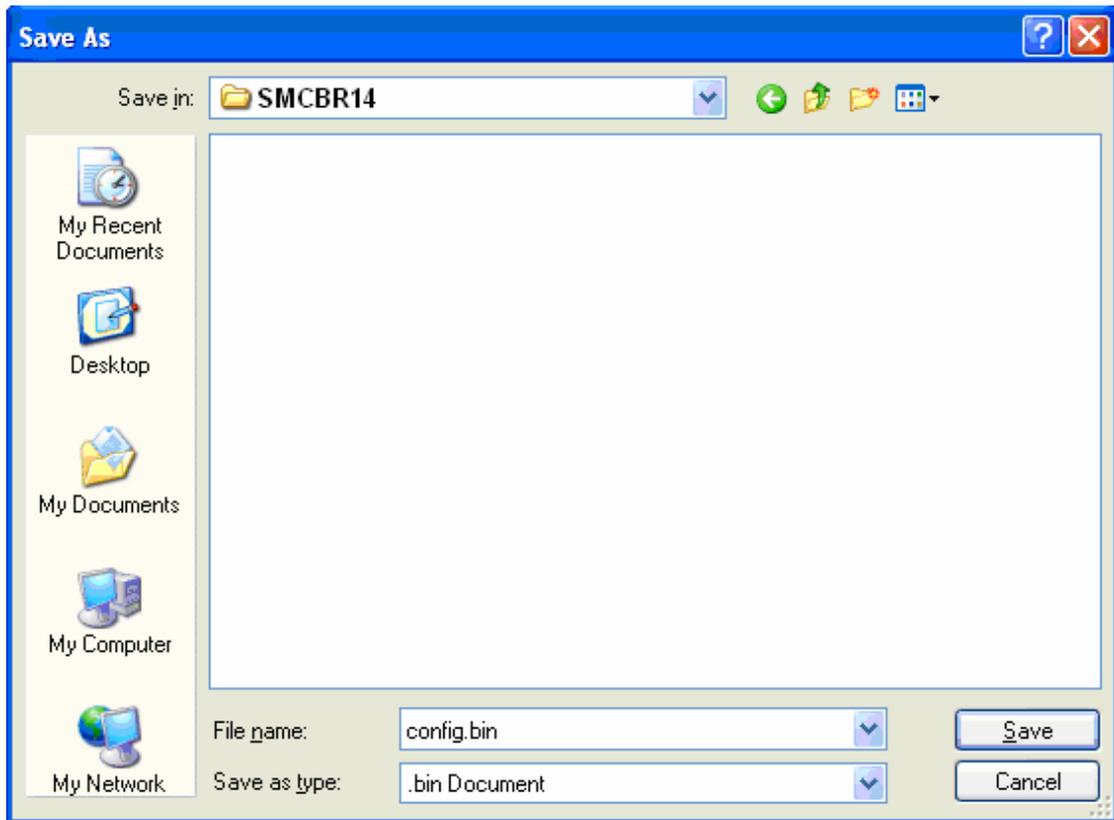


Figure 4-53

To restore the Router's settings:

Step 1: Click the **Browse** button to locate the update file for the device, or enter the exact path to the Setting file in the text box.

Step 2: Click the **Restore** button to complete.

4.11.5 Reboot

Choose menu "**System Tools**→**Reboot**", click the **Reboot** button to reboot the router via the next screen.

Reboot

Click this button to reboot the router.

Reboot

Figure 4-54

Note:

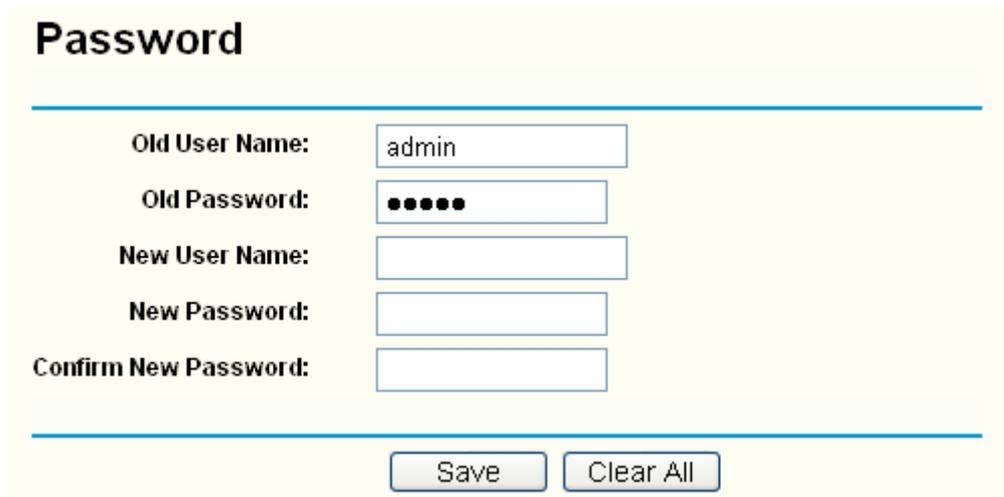
Some settings of the router will take effect only after rebooting, which include:

- 1) Change LAN IP Address. (System will reboot automatically)
- 2) MAC Clone (system will reboot automatically)

- 3) DHCP service function.
- 4) Static address assignment of DHCP server.
- 5) Web Service Port of the router.
- 6) Upgrade the firmware of the router (system will reboot automatically).
- 7) Restore the router's settings to factory default (system will reboot automatically).

4.11.6 Password

Choose menu “**System Tools**→**Password**”, you can change the factory default user name and password of the router in the next screen (shown in Figure 4-55). After configuration, click the **Save** button.



The screenshot shows a web form titled "Password" with a light yellow background. It contains five input fields: "Old User Name" (containing "admin"), "Old Password" (containing six black dots), "New User Name" (empty), "New Password" (empty), and "Confirm New Password" (empty). At the bottom, there are two buttons: "Save" and "Clear All".

Figure 4-55

 **Note:**

- 1) It is strongly recommended that you change the factory default user name and password of the router. All users who try to access the router's web-based utility will be prompted for the router's user name and password.
- 2) The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.
- 3) You can click the **Clear All** button to clear all the configurations.

4.11.7 Syslog

Choose menu “**System Tools**→**Syslog**”, you can view the logs of the Router.

System Log

Index	Log Content
1	0000:System: Router initialization succeeded. Time = 2007-05-22 8:47:29 1510s H-Ver = SMCBBR14 1004225B : S-Ver = 3.5.1 Build 070515 Rel.62388na L = 192.168.1.253 : M = 255.255.255.0 W1 = PPPoE : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0 Free=5024, Busy=1, Bind=0, Inv=0/0, Bc=0/3, Dns=0, cl=256, fc=0/0, sq=0/0

Figure 4-56

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear All** button to clear all the logs.

4.11.8 Remote Management

Choose menu “**System Tools→Remote Management**”, you can configure the Remote Management function on this screen (shown in Figure 4-57). This feature allows you to manage your Router from a remote location via the Internet.

Remote Management

Web Management Port:

Remote Management IP Address:

Figure 4-57

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router’s default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when

accessing your router from the Internet. The default IP address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP address to another IP address as desired.

Note:

- 1) To access the router, you will type your router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number you use is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web-based utility.
- 2) Be sure to change the router's default password to a very secure password.

4.11.9 Statistics

Choose menu “**System Tools**→**Statistics**”, you can view the statistics of the Router. This screen (shown in Figure 4-58) displays the network traffic of each PC on LAN, including total traffic and current traffic of the last “Packets Statistic interval” seconds.

Statistics

Current Statistics Status: Enabled Disable

Packets Statistics Interval(5-60): 10 Seconds

Auto-refresh Refresh

Sorted Rules: Sorted by IP Address Reset All Delete All

IP Address/ MAC Address	Total		Current				Modify	
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx		SYN Tx
192.168.2.100 00-13-8F-A9-E6-CA	29	4038	1	197	0/0	0/0	0/0	Reset Delete

Figure 4-58

- **Current Statistics Status** - Enable or Disable the statistics function. The default status is disabled. Click the **Enable** button to use the function. Click the **Disable** button to disable the function.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules** - Select the rule for displaying the traffic information.

- **Statistics Table** - This table displays the statistics information about the traffic.

IP Address		The IP address whose statistics information are displayed
Total	Packets	The total amount of packets received and transmitted by the router
	Bytes	The total amount of bytes received and transmitted by the router
Current	Packets	The total amount of packets received and transmitted in the last "Packets Statistic interval" seconds
	Bytes	The total amount of bytes received and transmitted in the last "Packets Statistic interval" seconds
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last "Packets Statistic interval" seconds
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last "Packets Statistic interval" seconds
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last "Packets Statistic interval" seconds

 **Note:**

- 1) If the **Current Statistics Status** function is disabled, the DoS protection in **Advanced Security** will be ineffective.
- 2) Select the **Auto-refresh**, then the traffic information will be refreshed automatically during the Packets Statistics Interval. Click the **Refresh** button to refresh the information in the table immediately.

Appendix A: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation WAN RJ45 port. Four 10/100M Auto-Negotiation LAN RJ45 ports (Auto MDI/MDIX)
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Physical and Environment	
Working Temperature	0°C~40°C (32°F~104°F)
Working Humidity	10% - 90% RH, Non-condensing

Appendix B: FAQ

1. How do I configure the router to access Internet by ADSL users?

Step 1: First, configure the ADSL modem in RFC1483 bridge model.

Step 2: Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.

Step 3: Login to the router, click the menu **Network**→**WAN** on the left of your browser. On the WAN screen, select “PPPoE” for the type of WAN connection. Then enter the user name and password in the corresponding field, and finish it by clicking **Connect**.

WAN

The screenshot shows the WAN configuration interface. At the top, there is a section titled "WAN Connection Type:" with a dropdown menu set to "PPPoE". Below this, there are two input fields: "User Name:" containing the text "username" and "Password:" which is filled with a series of black dots to mask the characters.

Figure B-1

Step 4: If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “connect Manually” or “Time-based Connecting” for Internet connection mode. Type an appropriate number for “Max Idle Time” or “Period of Time” to avoid wasting paid time. Otherwise, you can select “Connect Automatically” for Internet connection mode.

The screenshot shows the "Wan Connection Mode:" configuration section. It features four radio button options: "Connect on Demand" (selected), "Connect Automatically", "Time-based Connecting", and "Connect Manually". Under "Connect on Demand", there is a "Max Idle Time:" field set to "15" minutes. Under "Time-based Connecting", there is a "Period of Time:" field with sub-fields for "from" (0), "to" (23), and "59" (HH:MM). Below these options are "Connect" and "Disconnect" buttons. At the bottom of the page, there are "Save" and "Advanced" buttons.

Figure B-2

Note:

- 1) Sometimes the connection can not be disconnected although you specify a time to Max Idle Time, because some applications still visit the Internet continually in

the background.

- 2) If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

Step 1: Login to the router, click the menu **Network**→**WAN** on the left of your browser, On the WAN screen, select "Dynamic IP" for "WAN Connection Type", and finish it by clicking **Save**.

Step 2: Some ISPs require that you register the MAC address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the menu **Network**→**MAC Clone**. On the MAC Clone screen, if your PC's MAC address is a proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will be filled in the "WAN MAC Address" field; Or else, enter the specific MAC address into the "WAN MAC Address" field manually. Then click the **Save** button. It will take effect after rebooting.

Figure B-3

3. I want to use Netmeeting, what do I need to do?

If you start Netmeeting as a sponsor, you don't need to do anything with the router.

If you start as a responder, you need configure Virtual Server or DMZ Host as follows:

Method one: Use Virtual Server

Login to the router, click the menu **Forwarding**→**Virtual Servers**. On the Virtual Server screen, add a Virtual Server rule as shown in the next screen: configure 1720 as the "Service Port" and enter your IP address (assuming 192.168.2.102 for an example), then click select the status **Enabled** and click **Save**.

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.2.100	TCP	Enabled	Modify Delete
2	80	192.168.2.101	ALL	Enabled	Modify Delete
3	1720	192.168.2.102	ALL	Enabled	Modify Delete

Figure B-4

Note:

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

Method two: Use DMZ Host

Login to the router, click the menu **Forwarding**→**DMZ**. On the DMZ screen, select “Enable”, and enter your IP address into the “DMZ Host IP Address” field (using 192.168.2.102 as an example), then to click the **Save** button.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Figure B-5

4. I want to build a WEB Server on the LAN, what should I do?

Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference. And then add a WEB Server on your LAN. You can follow the steps below to proceed.

Step 1: To change the WEB management port number: Login to the router, click the menu **Security**→**Remote Management**. On the Remote Management screen, enter a port number except 80 (such as 88) into the “Web Management Port” field. Click **Save** and the router will reboot.

Remote Management

Web Management Port:	<input type="text" value="88"/>
Remote Management IP Address:	<input type="text" value="255.255.255.255"/>
<input type="button" value="Save"/>	

Figure B-6

Note:

- 1) If the above configuration takes effect, for LAN administrators, you should enter <http://192.168.2.1:88> (the router's LAN IP address: Web Management Port) in the address field of the web browser to access the Router.

Address

- 2) For remote access to the router, you should enter the address for example: <http://61.45.120.20:88> (presume the WAN IP address of the router is 61.45.120.20) to access the Router.

Step 2: To add a WEB Server: Login to the router, click the menu **Forwarding**→**Virtual Servers** on the left of your browser, On the Virtual Server screen, add a Virtual Server rule as shown in the next screen: configure “80” as the “Service Port”, and enter your IP address (assuming 192.168.2.188 for an example), remember to “Enable” and “Save”.

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.2.100	TCP	Enabled	Modify Delete
2	80	192.168.2.101	ALL	Enabled	Modify Delete
3	1720	192.168.2.102	ALL	Enabled	Modify Delete

Figure B-7

Appendix C: Glossary

- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name Server)** - An Internet Server that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.



TECHNICAL SUPPORT

From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: (800) SMC-4-YOU / (949) 679-8000
Fax: (949) 679-1481

English: Technical Support information available at www.smc.com

English(For Asia Pacific): Technical Support information available at www.smc-asia.com

Deutsch: Technischer Support und weitere Information unter www.smc.com

Español: En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

Français: Informations Support Technique sur www.smc.com

Português: Informações sobre Suporte Técnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgängligt på www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym są dostępne na www.smc.com

Čeština: Technická podpora je dostupná na www.smc.com

Magyar: Műszaki támogatás információ elérhető -on www.smc.com

简体中文: 技术支持讯息可通过www.smc-prc.com查询

繁體中文: 產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smc-asia.com을 참고하시기 바랍니다

INTERNET

E-mail address: techsupport@smc.com

Driver updates

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web

<http://www.smc.com/>



SMC BR14