RX3141

User's Manual

Revision 1.01
Oct. 21, 2004

Table of Contents

List of Figures

List of Tables

1 Introduction

Congratulations on becoming the owner of RX3141. Your LAN (local area network) will now be able to access the Internet using your high-speed broadband connection such as those with ADSL or cable modem.

This User Manual will show you how to set up the RX3141, and how to customize its configuration to get the most out of this product.

1.1 Features

- LAN: 4-port Gigabit switch, jumbo frame supports up to 9Kbyte.
- WAN: 10/100Base-T Ethernet provides Internet access for all computers on your LAN
- Firewall & NAT (Network Address Translation) functions provide secure Internet access for your LAN
- Automatic network address assignment through DHCP Server
- Services including IP route, DNS and DDNS configuration
- Configuration program accessible via a web browser, such as Microsoft Internet Explorer 6.0 or newer.

1.2 System Requirements

In order to use the RX3141 for Internet access, you must have the following:

- ADSL or cable modem and the corresponding service up and running, with at least one public Internet address assigned to your WAN
- One or more computers each containing an Ethernet 10Base-T or 100Base-T or 1000Base-T network interface card (NIC)
- (Optional) An Ethernet hub/switch, if you want to connect the router to more than four computers on an Ethernet network.
- For system configuration using the web-based GUI: web browser such as Microsoft IE 6.0 or newer.

1.3 Using this Document

1.3.1 Notational conventions

- Acronyms are defined the first time they appear in the text.
- For brevity, RX3141 is sometimes referred to as the "router" or the "gateway".
- The terms *LAN* and *network* are used interchangeably to refer to a group of Ethernet-connected computers at one site.
- Sequence of mouse actions is denoted by the "➔" character. For instance, **Router Setup ➔ Connection** means double click the **Router Setup** menu and then click the **Connection** submenu.

1.3.2 Typographical conventions

- **Boldface** type text is used for items you select from menus and drop-down lists, and text strings you type when prompted by the program.

1.3.3 Special messages

This document uses the following icons to call your attention to specific instructions or explanations.

Note	*Provides clarification or non-essential information on the current topic.*
Definition	*Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.*
WARNING	*Provides messages of high importance, including messages relating to personal safety or system integrity.*

2 Getting to Know RX3141

2.1 Parts List

In addition to this document, RX3141 should come with the following:

- The System unit, RX3141
- AC Adapter
- User Manual
- Compact Disk of Multi-language Quick installation Guide

2.2 Hardware Features

- LAN
  - 4-port Gigabit switch
  - Auto speed negotiation
  - 9KB jumbo frame support
  - 4K MAC address table w/ auto learning and aging
- WAN
  - 10/100M Ethernet
  - Auto MDI/MDIX

2.3 Software Features

2.3.1 NAT Features

RX3141 provides NAT to share a single high-speed Internet connection and to save the cost of multiple connections required for the hosts on the LAN segments connected to it. This feature conceals network address and prevents them from becoming public. It maps unregistered IP address of hosts connected to the LAN with valid ones for Internet access. RX3141 also provides reverse NAT capability, which enables users to host various services such as e-mail servers, web servers, etc. The NAT rules drive the translation mechanism. The following types of NAT are supported by RX3141.

- NAPT (Network Address and Port Translation) – Also called IP Masquerading or ENAT (Enhanced NAT). Maps many internal hosts to only one globally valid IP address. The mapping usually contains a pool of network ports to be used for translation. Every packet is translated with the globally valid IP address; the port number is translated with a free pool from the pool of network ports.
- Reverse NAPT – Also called inbound mapping, port mapping, or virtual server. Any packet coming to the router can be relayed to an internal host based on the protocol, port number and/or IP Address specified in the rule. This is useful when multiple services are hosted on different internal hosts.

2.3.2 Firewall Features

The firewall as implemented in RX3141 provides the following features to protect your network from being attacked and to prevent your network from being used as the springboard for attacks.

- Stateful Packet Inspection
- Packet Filtering (ACL)
- Defense against Denial of Service Attacks
- Log

2.3.2.1 Stateful Packet Inspection

The RX3141 Firewall uses “stateful packet inspection” that extracts state-related information required for the security decision from the packet and maintains this information for evaluating subsequent connection attempts. It has awareness of application and creates dynamic sessions that allow dynamic connections so that no ports need to be opened other than the required ones. This provides a solution which is highly secure and that offers scalability and extensibility.

2.3.2.2 Packet Filtering – ACL (Access Control List)

ACL rule is one of the basic building blocks for network security. Firewall monitors each individual packet, decodes the header information of inbound and outbound traffic and then either blocks the packet from passing or allows it to pass based on the contents of the source address, destination address, source port, destination port, and protocol defined in the ACL rules.

ACL is a very appropriate measure for providing isolation of one subnet from another. It can be used as the first line of defense in the network to block inbound packets of specific types from ever reaching the protected network.

The RX3141 Firewall’s ACL methodology supports:

- Filtering based on destination and source IP address, port number and protocol
- Use of the wild card for composing filter rules
- Filter Rule priorities

2.3.2.3 Defense against DoS Attacks

The RX3141 Firewall has an Attack Defense Engine that protects internal networks from known types of Internet attacks. It provides automatic protection from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. For example, the RX3141 Firewall provides protection from “WinNuke”, a widely used program to remotely crash unprotected Windows systems in the Internet. The RX3141 Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, and Reassembly attacks.

The type of attack protections/detections provided by the RX3141 is listed in Table 2.1.

Table 2.1. DoS Attacks

Type of Attack	**Name of Attacks**
Re-assembly attacks	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt, IP fragmentation overlap
ICMP Attacks	Ping of Death, Smurf, Twinge
Flooders	Logging only for ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	Logging only for TCP SYN Scan Attack packets dropped: TCP XMAS Scan, TCP Null Scan, TCP Stealth Scan
Protection with PF Rules	Echo-Chargen, Ascend Kill
Miscellaneous Attacks	IP Spoofing, LAND, Targa, Winnuke

2.4.1.1 Application Level Gateway (ALG)

Applications such as FTP open connections dynamically based on the respective application parameter. To go through the firewall on the RX3141, packets pertaining to an application, require a corresponding *allow* rule. In the absence of such rules, the packets will be dropped by the RX3141 Firewall. As it is not feasible to create policies for numerous applications dynamically (at the same time without compromising security), intelligence in the form of Application Level Gateways (ALG), is built to parse packets for applications and open dynamic associations. The RX3141 NAT provides a number of ALGs for popular applications such as FTP, and Netmeeting.

2.4.1.2 Log

Events in the network, that could be attempts to affect its security, are recorded in the RX3141 system log file. The log maintains a minimum log details such as, time of packet arrival, description of action taken by Firewall and reason for action.

2.4 Finding Your Way Around

2.4.1 Front Panel

The front panel contains LED indicators that show the status of the unit.

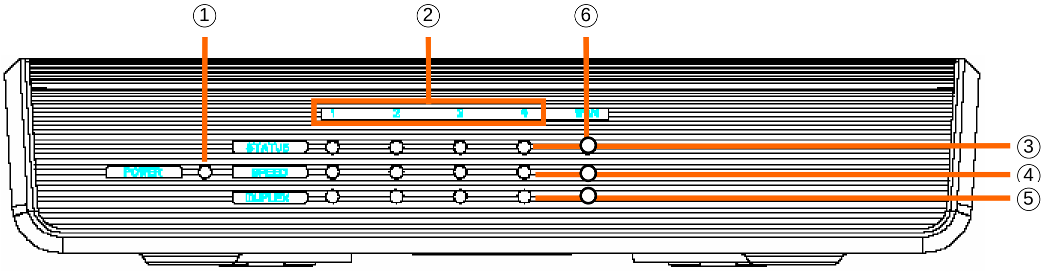


Figure 2.1. Front Panel LEDs

Table 2.2. Front Panel Label and LEDs

	LED Label	Color	Status	Indication
①	**POWER**	Green	ON OFF	RX3141 is powered on RX3141 is powered off
②	**1 – 4**			Identifies the LAN port LEDs. Status of each LAN port is indicated by 3 LEDs: STATUS, SPEED and DUPLEX.
③	STATUS	Green	ON Blinking OFF	Ethernet link is established and active Data is transmitted or received via the connection No Ethernet link
④	SPEED	Green Amber	ON ON OFF	Speed is 1000Mbps Speed is 100Mbps Speed is 10Mbps or no link is established.
⑤	DUPLEX	Amber	ON Blinking OFF	The LAN port is operating in full-duplex mode. The LAN port is operating in half-duplex mode and collision is occurring. The LAN port is operating in half duplex mode and no collision is detected.
⑥	**WAN**			Identifies the WAN port LED
③	STATUS	Green	ON OFF	Ethernet link is established and active. No Ethernet link is established.
④	SPEED	Green	ON Blinking	Speed is 100Mbps Green: Data is transmitted or received via the connection

LED Label	Color	Status	Indication
	Amber	ON Blinking	Speed is 10Mbps Data is transmitted or received via the connection
		OFF	No link is established.
⑤ DUPLEX	Amber	ON	The LAN port is operating in full-duplex mode.
		OFF	The LAN port is operating in half duplex mode and no collision is detected.

2.4.2 Rear Panel

The rear panel contains the ports for the unit's data and power connections.

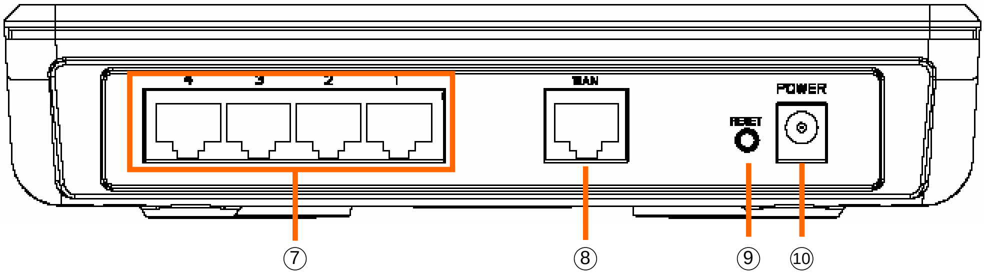
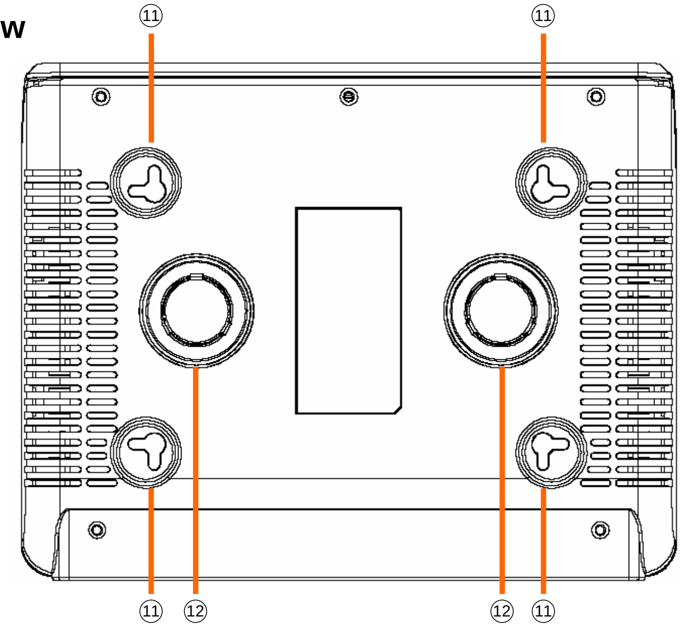


Figure 2.2. Rear Panel Connectors

Table 2.3. Rear Panel Labels and LEDs

Label	Indication
⑦ **1 – 4**	**LAN Ports**: connects to your PC's Ethernet port, or to the uplink port on your LAN's hub/switch, using the Ethernet cable.
⑧ **WAN**	**WAN Port**: connects to your WAN device, such as ADSL or cable modem.
⑨ **RESET**	**Reset Button** 1. Reboots the device 2. Resets the system configuration to the factory defaults if pressed for more than 5 seconds.
⑩ **POWER**	**Power Input Jack**: connects to the supplied AC adapter

2.4.3 Bottom View



⑪ **Wall Mount Slots**: You may use these slots to hang RX3141 on the wall to save space. Depending on your particular requirement by taking into account the location of the power outlet, power cord length, Ethernet cable length and etc., you can hang RX3141 in 4 different orientations: front panel up, rear panel up, left side up or right side up.

⑫ **Magnets**: The magnets allow you to place RX3141 on any metal surface to save space.

2.5 Placement Options

Depending on your environment, you may choose one of the three supported placement options for RX3141 – desktop placement, magnet mount and wall mount.

2.5.1 Desktop Placement

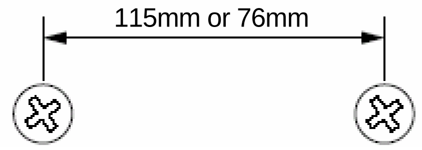
You may place RX3141 on any flat surface. The space-saving design of RX3141 occupies only a small area on your desk.

2.5.2 Magnet Mount Instructions

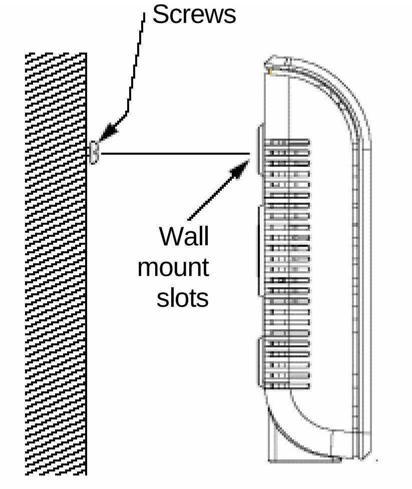
Place RX3141 onto any metal surface that attracts magnet, such as most desktop computer housings, cabinets and etc.

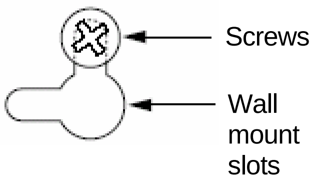
2.5.3 Wall Mount Instructions:

1. Attach two screws on the wall, separated by 115mm if you want the front or rear panel facing upward, 76mm if you want left or right side facing upward. Make sure that the two screws are leveled. Note that there are four wall mount slots and you may choose any adjacent slots for wall mounting.



2. Line up the wall mount slots with the screws and maneuver RX3141 so that both screws are inserted into the wall mount slots as indicated in the following figures.





Maneuver the switch so that both screws are inserted into the wall mount slots.

Line up the wall mount slots w/ both screws.

3 Quick Start Guide

This Quick Start Guide provides basic instructions for connecting the RX3141 to a computer or a network and to the Internet.

- Part 1 provides instructions to set up the hardware.
- Part 2 describes how to configure Internet properties on your computer(s).
- Part 3 shows you how to configure basic settings on the RX3141 to get your LAN connected to the Internet.

After setting up and configuring the device, you can follow the instructions on page 17 to verify that it is working properly.

This Quick Start Guide assumes that you have already established ADSL or cable modem service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

3.1 Part 1 — Connecting the Hardware

In Part 1, you connect the device to an ADSL or a cable modem (which in turn is connected to a phone jack or a cable outlet), the power outlet, and your computer or network.

WARNING

> ***Before you begin, turn the power off for all devices.*** *These include your computer(s), your LAN hub/switch (if applicable), and the RX3141.*

Figure 3.1 illustrates the hardware connections. Please follow the steps that follow for specific instructions.

3.1.1 Step 1. Connect an ADSL or a cable modem.

For the RX3141: Connect one end of the Ethernet cable to the port labeled WAN on the rear panel of the device. Connect the other end to the Ethernet port on the ADSL or cable modem.

3.1.2 Step 2. Connect computers or a Network.

If your LAN has no more than 4 computers, you can use an Ethernet cable to connect computers directly to the built-in switch on the device. Note that you should attach one end of the Ethernet cable to any of the port labeled 1 – 4 on the rear panel of the router and connect the other end to the Ethernet port of a computer.

If your LAN has more than 4 computers, you can attach one end of an Ethernet cable to a hub or a switch (probably an uplink port; please refer to the hub or switch documentations for instructions) and the other to the Ethernet switch port (labeled 1 – 4) on the RX3141.

Note that either the crossover or straight-through Ethernet cable can be used to connect the built-in switch and computers, hubs or switches as the built-in switch is smart enough to make connections with either type of cables.

3.1.3 Step 3. Attach the AC adapter.

Attach the AC adapter to the POWER input jack on the back of the device and plug in the adapter to a wall outlet or a power strip.

3.1.4 Step 4. Power on RX3141, the ADSL or cable modem and power up your computers.

Plug the AC adapter to the power input jack of RX3141. Turn on your ADSL or cable modem. Turn on and boot up your computer(s) and/or any LAN devices such as wireless AP, hubs or switches.

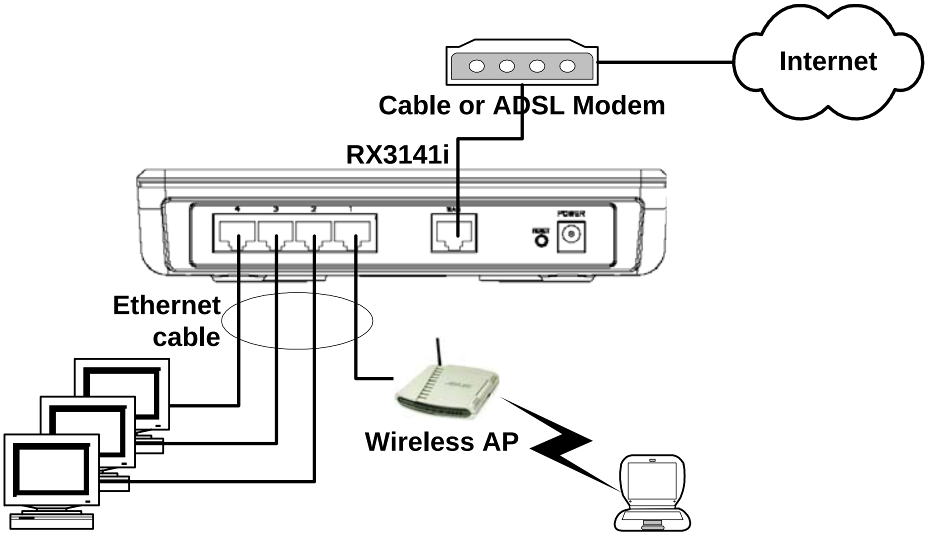


Figure 3.1. Overview of Hardware Connections

You should verify that the LEDs are illuminated as indicated in Table 3.1.

Table 3.1. LED Indicators

This LED:	...should be:
POWER	Solid green to indicate that the device is turned on. If this light is not on, check if the AC adapter is attached to the RX3141 and if it is plugged into a power source.
1 – 4 STATUS LED	Solid green to indicate that the device can communicate with your LAN or flashing when the device is sending or receiving data to/from your LAN computer(s).
WAN	Solid green to indicate that the device has successfully established a connection with your ISP or flashing when the device is sending or receiving data to/from the Internet.

If the LEDs illuminate as expected, the RX3141 is working properly.

3.2 Part 2 — Configuring Your Computers

Part 2 of the Quick Start Guide provides instructions for configuring the network settings on your computers to work with the RX3141.

3.2.1 Before you begin

By default, the RX3141 automatically assigns all required network settings (e.g. IP address, DNS server IP address, default gateway IP address) to your PCs. You need only to configure your PCs to accept the network settings provided by the RX3141.

Note

In some cases, you may want to configure network settings manually to some or all of your computers rather than allow the RX3141 to do so. See "Assigning static IP addresses to your PCs" in page 15 for instructions.

- If you have connected your PC via Ethernet to the RX3141, follow the instructions that correspond to the operating system installed on your PC.

3.2.2 Windows® XP PCs:

1. In the Windows task bar, click the **<Start>** button, and then click **Control Panel**.
2. Double-click the Network Connections icon.
3. In the LAN or High-Speed Internet window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (Often this icon is labeled *Local Area Connection*).

   The Local Area Connection dialog box displays with a list of currently installed network items.
4. Ensure that the check box to the left of the item labeled Internet Protocol TCP/IP is checked, and click **<Properties>** button.
5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
6. Click **<OK>** button twice to confirm your changes, and close the Control Panel.

3.2.3 Windows® 2000 PCs:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the **<Start>** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.

   The Local Area Connection Properties dialog box displays a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click **<Install>** button.

5. In the Select Network Component Type dialog box, select **Protocol**, and then click **<Add>** button.
6. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **<OK>** button.

   You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
7. If prompted, click **<OK>** button to restart your computer with the new settings.

   Next, configure the PCs to accept IP addresses assigned by the RX3141:
8. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
9. In Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.
10. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click **<Properties>** button.
11. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
12. Click **<OK>** button twice to confirm and save your changes, and then close the Control Panel.

3.2.4 Windows® 95, 98, and Me PCs

1. In the Windows task bar, click the **<Start>** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network** icon.

   In the Network dialog box, look for an entry started w/ "**TCP/IP ->**" and the name of your network adapter, and then click **<Properties>** button. You may have to scroll down the list to find this entry. If the list includes such an entry, then the TCP/IP protocol has already been enabled. Skip to step 8.
3. If Internet Protocol (TCP/IP) does not display as an installed component, click **<Add>** button.
4. In the Select Network Component Type dialog box, select **Protocol**, and then click **<Add>** button.
5. Select **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list, box and then click **<OK>** button.

   You may be prompted to install files from your Windows 95, 98 or Me installation CD or other media. Follow the instructions to install the files.
6. If prompted, click **<OK>** button to restart your computer with the new settings.

   Next, configure the PCs to accept IP information assigned by the RX3141:
7. In the Control Panel, double-click the Network icon.
8. In the Network dialog box, select an entry started with "**TCP/IP ->"** and the name of your network adapter, and then click **<Properties>** button.
9. In the TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address automatically**.
10. In the TCP/IP Properties dialog box, click the "**Default Gateway**" tab. Enter 192.168.1.1 (the default LAN port IP address of the RX3141) in the "**New gateway**" address field and click **<Add>** button to add the default gateway entry.
11. Click **<OK>** button twice to confirm and save your changes, and then close the Control Panel.
12. If prompted to restart your computer, click **<OK>** button to do so with the new settings.

3.2.5 Windows® NT 4.0 workstations:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the **<Start>** button, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double click the **Network** icon.
3. In the Network dialog box, click the **Protocols** tab.

   The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP Protocol, then the protocol has already been enabled. Skip to step 9.
4. If TCP/IP does not display as an installed component, click **<Add>** button.
5. In the Select Network Protocol dialog box, select **TCP/IP**, and then click **<OK>** button.

   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
6. Click **<Yes>** button to continue, and then click **<OK>** button if prompted to restart your computer.

   Next, configure the PCs to accept IP addresses assigned by the RX3141:
7. Open the Control Panel window, and then double-click the **Network** icon.
8. In the Network dialog box, click the **Protocols** tab.
9. In the Protocols tab, select **TCP/IP**, and then click **<Properties>** button.
10. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
11. Click **<OK>** button twice to confirm and save your changes, and then close the Control Panel.

3.2.6 Assigning static IP addresses to your PCs

In some cases, you may want to assign IP addresses to some or all of your PCs directly (often called "statically"), rather than allowing the RX3141 to assign them. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN.

However, during the first time configuration of your RX3141, you must assign an IP address in the 192.168.1.0 network for your PC, say 192.168.1.2, in order to establish connection between the RX3141 and your PC as the default LAN IP on RX3141 is pre-configured as 192.168.1.1. Enter 255.255.255.0 for the subnet mask and 192.168.1.1 for the default gateway. These settings may be changed later to reflect your true network environment.

On each PC to which you want to assign static information, follow the instructions on pages 13 through 15 relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server, and default gateway, click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the RX3141's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in the section 5.1.1 to change the LAN port IP address accordingly.

3.3 Part 3 — Quick Configuration of the RX3141

In Part 3, you log into the Configuration Manager on the RX3141 and configure basic settings for your router. Your ISP should provide you with the necessary information to complete this step. Note the intent here is to quickly get the RX3141 up and running, instructions are concise. You may refer to corresponding chapters for more details.

3.3.1 Setting Up the RX3141

Follow these instructions to setup the RX3141:

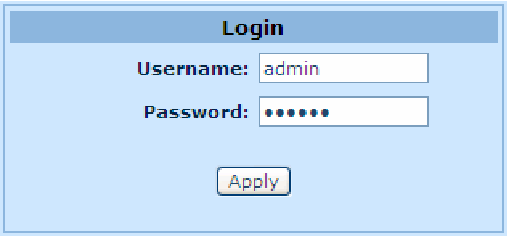
1. Before accessing the Configuration Manager in RX3141, make sure that the HTTP proxy setting is disabled in your browser. In IE, click "**Tools**" ➔ "**Internet Options…**" ➔ "**Connections**" tab ➔ "**LAN settings…**" and then uncheck "**Use proxy server for your LAN …**"

2. On any PC connected to one of the four LAN ports on the RX3141, open your Web browser, and type the following URL in the address/location box, and press **<Enter>**:

   http://192.168.1.1

   This is the predefined IP address for the LAN port on the RX3141.

   A login screen displays, as shown in Figure 3.2.



Login

Username: admin

Password: ••••••

Figure 3.2. Login Screen

   If you have problem connecting to the RX3141, you may want to check if your PC is configured to accept IP address assignment from the RX3141. Another method is to set the IP address of your PC to any IP address in the 192.168.1.0 network, such as 192.168.1.2.

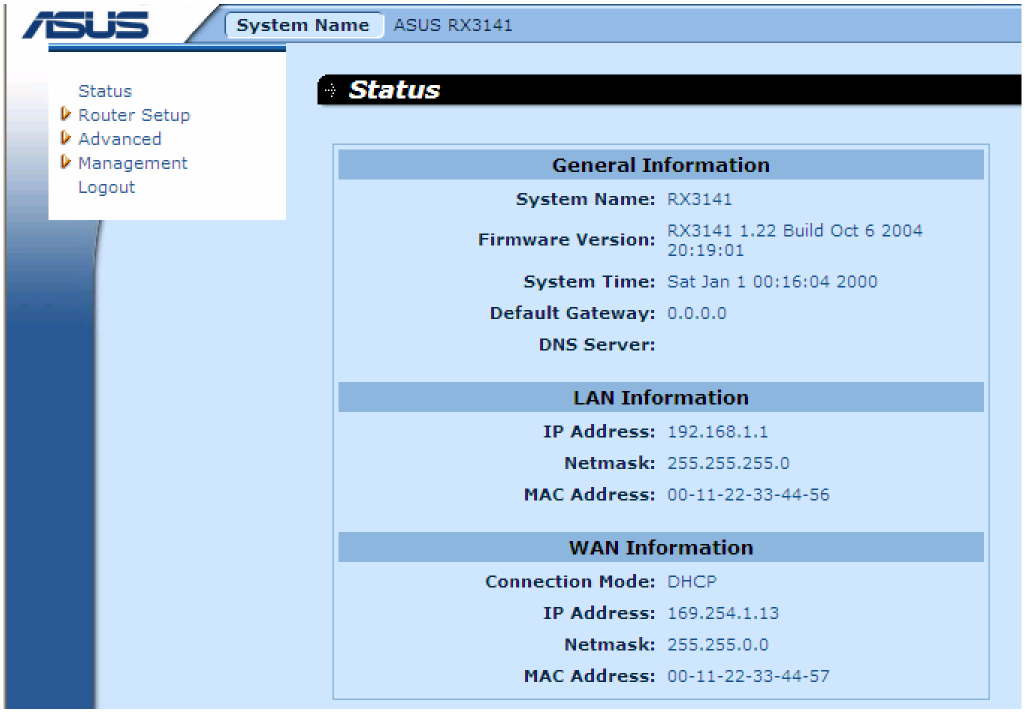
3. Enter your username and password, and then click Apply to enter the Configuration Manager. The first time you log into this program, use these defaults:

Default Username:	admin
Default Password:	admin

Note

> *You can change the password at any time (see section 11.1 Login Password and System-Wide Settings).*

The System Information page displays each time you log into the Configuration Manager (shown in Figure 3.3).



System Name ASUS RX3141

Status

General Information

System Name: RX3141

Firmware Version: RX3141 1.22 Build Oct 6 2004 20:19:01

System Time: Sat Jan 1 00:16:04 2000

Default Gateway: 0.0.0.0

DNS Server:

LAN Information

IP Address: 192.168.1.1

Netmask: 255.255.255.0

MAC Address: 00-11-22-33-44-56

WAN Information

Connection Mode: DHCP

IP Address: 169.254.1.13

Netmask: 255.255.0.0

MAC Address: 00-11-22-33-44-57

Figure 3.3. System Status Page

4. Follow the instructions described in Chapter 5 "Router Connection Setup" to set up the LAN and WAN settings for RX3141.

After completing the basic configuration for RX3141, read the following section to determine if you can access the Internet.

3.3.2 Testing Your Setup

At this point, the RX3141 should enable any computers on your LAN to use the RX3141's ADSL or cable modem connection to access the Internet.

To test the Internet connection, open your web browser, and type the URL of any external website (such as http://www.asus.com). The LED labeled WAN should be blinking rapidly and may appear solid as the device connects to the site. You should also be able to browse the web site through your web browser.

If the LEDs do not illuminate as expected or the web page does not display, see Appendix 13 for troubleshooting suggestions.

3.3.3 Default Router Settings

In addition to handling the DSL connection to your ISP, the RX3141 can provide a variety of services to your network. The device is pre-configured with default settings for use with a typical home or small office network.

Table 3.2 lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration settings, review the settings in Table 3.2 to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

Before you modifying any settings, review Chapter 4 for general information about accessing and using the Configuration Manager program. We strongly recommend that you contact your ISP prior to changing the default configuration.

Table 3.2. Default Settings Summary

Option	Default Setting	Explanation/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.100 through 192.168.1.149	The RX3141 maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in Part 2 of the Quick Start Guide. See section 6.1 for an explanation of the DHCP service.
LAN Port IP Address	Static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the RX3141. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See section 5.1.1 LAN IP Address for instructions.

4 Using the Configuration Manager

The RX3141 includes a preinstalled program called the *Configuration Manager*, which provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You access it through your web browser from any PC connected to the RX3141 via the LAN or the WAN ports.

This chapter describes the general guides for using the Configuration Manager.

4.1 Log into the Configuration Manager

The Configuration Manager program is preinstalled on the RX3141. To access the program, you need the following:

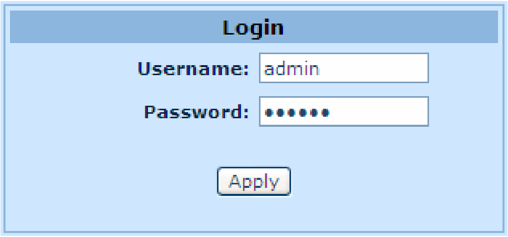
- A computer connected to the LAN or WAN port on the RX3141 as described in the Quick Start Guide chapter.
- A web browser installed on the computer. The program is designed to work best with Microsoft Internet Explorer® 6.0 or later.

You may access the program from any computer connected to the RX3141 via the LAN or WAN ports. However, the instructions provided here are for computers connected via the LAN ports.

1. From a LAN computer, open your web browser, type the following in the web address (or location) box, and press **<Enter>**:

   http://192.168.1.1

   This is the predefined IP address for the LAN port on the RX3141. A login screen displays, as shown in Figure 4.1.



Login

Username: admin

Password: ••••••

Apply

Figure 4.1. Configuration Manager Login Screen

2. Enter your username and password, and then click Apply.

   The first time you log into the program, use these defaults:

Default Username:	admin
Default Password:	admin

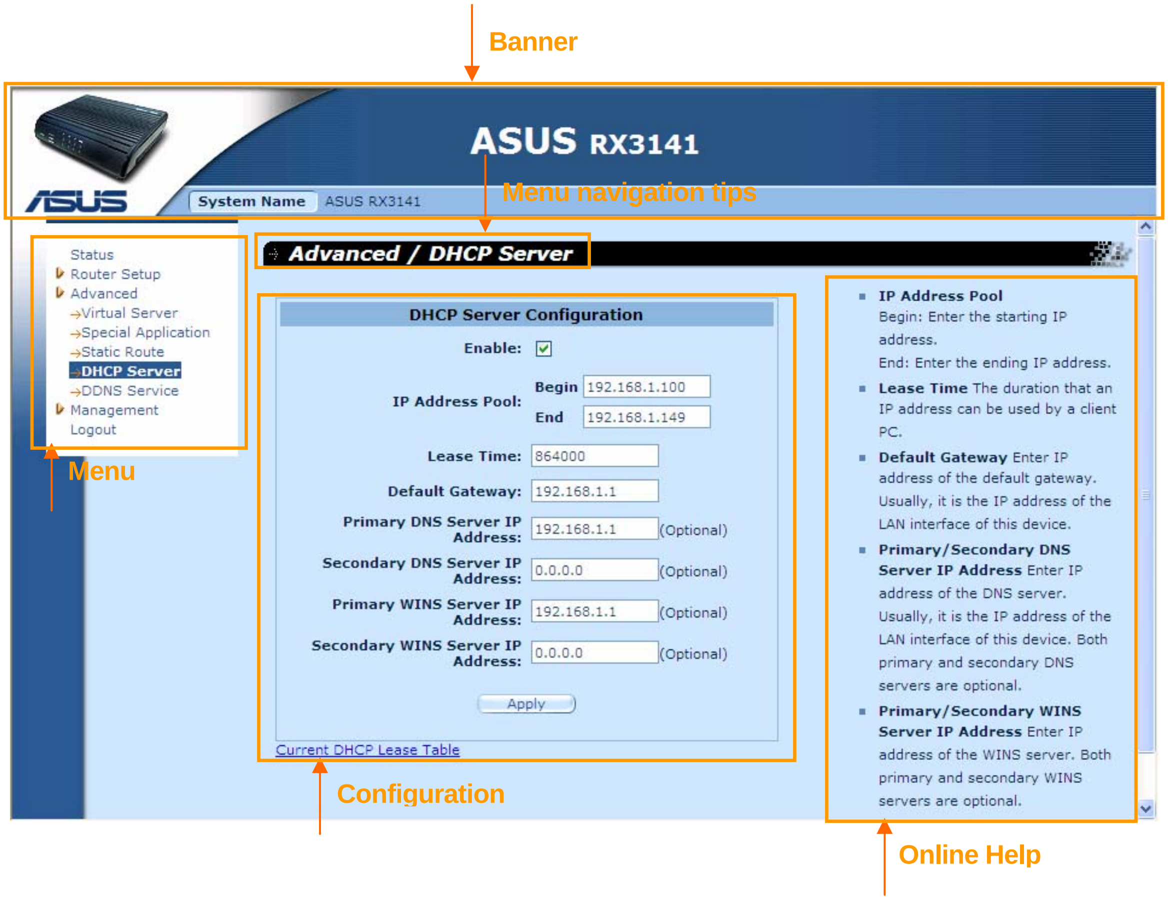
Note

You can change the password at any time (see section 11.1 Login Password and System-Wide Settings).

The System Information page displays every time you log into the Configuration Manager (shown in Figure 4.3 on page 22).

4.2 Functional Layout

Typical Typical Configuration page consists of several elements – banner, menu, menu navigation tips, configuration, and on-line help. You can click on any menu item to expand/contract any menu groups or to access a specific configuration page. The configuration pane is where you interact with the Configuration Manager to configure the settings for RX3141. Menu navigation tips show how the current configuration can be accessed via the menus.



DHCP Server Configuration

Enable: ☑

IP Address Pool: Begin 192.168.1.100 End 192.168.1.149

Lease Time: 864000

Default Gateway: 192.168.1.1

Primary DNS Server IP Address: 192.168.1.1 (Optional)

Secondary DNS Server IP Address: 0.0.0.0 (Optional)

Primary WINS Server IP Address: 192.168.1.1 (Optional)

Secondary WINS Server IP Address: 0.0.0.0 (Optional)

- **IP Address Pool** Begin: Enter the starting IP address. End: Enter the ending IP address.
- **Lease Time** The duration that an IP address can be used by a client PC.
- **Default Gateway** Enter IP address of the default gateway. Usually, it is the IP address of the LAN interface of this device.
- **Primary/Secondary DNS Server IP Address** Enter IP address of the DNS server. Usually, it is the IP address of the LAN interface of this device. Both primary and secondary DNS servers are optional.
- **Primary/Secondary WINS Server IP Address** Enter IP address of the WINS server. Both primary and secondary WINS servers are optional.

Figure 4.2. Typical Configuration Manager Page

4.2.1 Menu Navigation

- To expand a group of related menus: double click the menu or the icon, ▶ .
- To contract a group of related menus: double click the menu or the icon, ▼ .
- To open a specific configuration page, click the menu or the icon, →.

4.2.2 Commonly Used Buttons and Icons

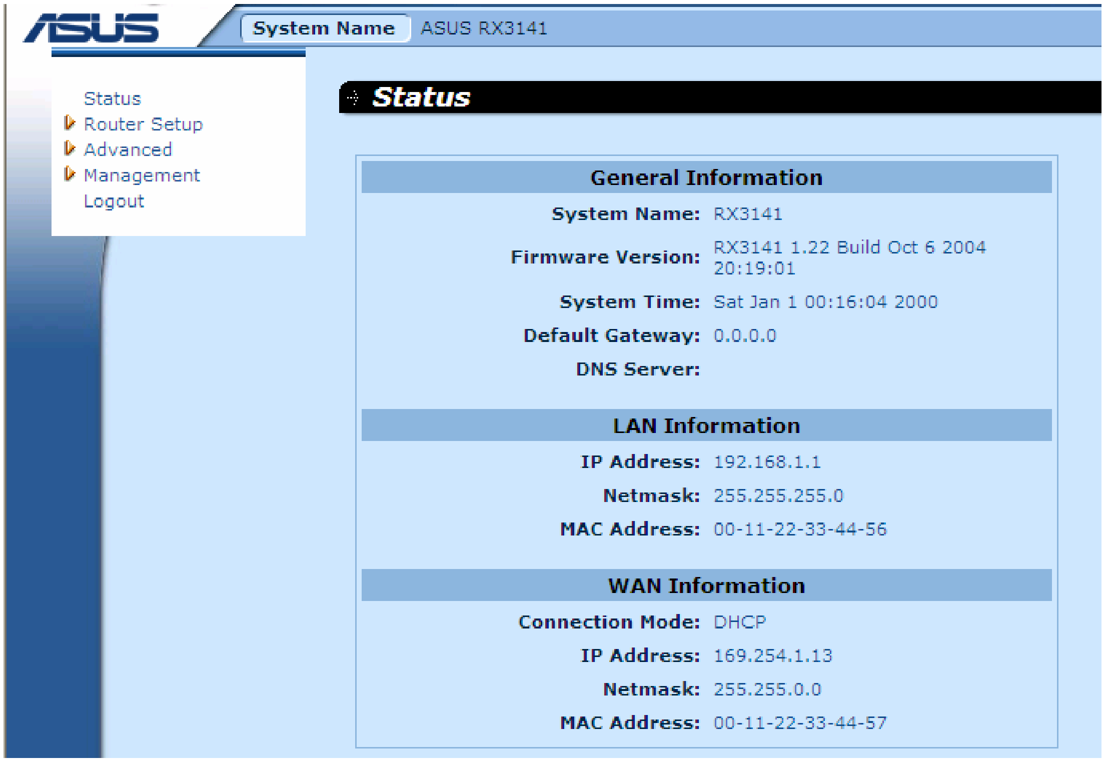
The following buttons or icons are used throughout the application. The following table describes the function for each button or icon.

Table 4.1. Description of Commonly Used Buttons and Icons

Button/Icon	***Function***
Apply	Stores any changes you have made on the current page.
Add	Adds a new configuration to the system, e.g. a static route or a firewall ACL rule and etc.
Modify	Modifies existing configuration in the system, e.g. a static route or a firewall ACL rule and etc.
Reload	Redisplays the current page with updated statistics or settings.
✎	Selects the item for editing.
🗑	**Trash -** Deletes the selected item.
Browse...	**Browse**
Undo	**Undo**
Cancel	**Cancel**
OK	**OK**
Open	**Open**
Save	**Save**
▶	**Folder Off**
▼	**Folder On**
→	**Item**

4.3 Overview of System Configuration

To view the overall system configuration, log into the Configuration Manager, and then click **Status** menu. Figure 4.3 shows sample information available in the System Information page.



General Information	
System Name:	RX3141
Firmware Version:	RX3141 1.22 Build Oct 6 2004 20:19:01
System Time:	Sat Jan 1 00:16:04 2000
Default Gateway:	0.0.0.0
DNS Server:	

LAN Information	
IP Address:	192.168.1.1
Netmask:	255.255.255.0
MAC Address:	00-11-22-33-44-56

WAN Information	
Connection Mode:	DHCP
IP Address:	169.254.1.13
Netmask:	255.255.0.0
MAC Address:	00-11-22-33-44-57

Figure 4.3. System Information Page

5 Router Connection Setup

This chapter describes how to configure the basic settings for your router so that the computers on your LAN can communicate with each other and have access to the Internet. Network setup consists of LAN and WAN configurations.

5.1 LAN Configuration

5.1.1 LAN IP Address

If you are using RX3141 with multiple PCs on your LAN, you must connect your LAN to the Ethernet ports on the built-in Ethernet switch. You must assign a unique IP address to each device residing on your LAN. The LAN IP address that identifies the RX3141 as a node on your network must be in the same subnet as the PCs on your LAN. The default LAN IP address for the RX3141 is 192.168.1.1.

Definition

> *A **network node** can be thought of as any interface where a device connects to the network, such as the RX3141's LAN port and the network interface cards on your PCs. See Appendix 12 for an explanation of subnets.*

You can change the default IP address to reflect the true IP address that you want to use with your network.

5.1.2 LAN Configuration Parameters

Table 5.1 describes the configuration parameters available for LAN IP configuration.

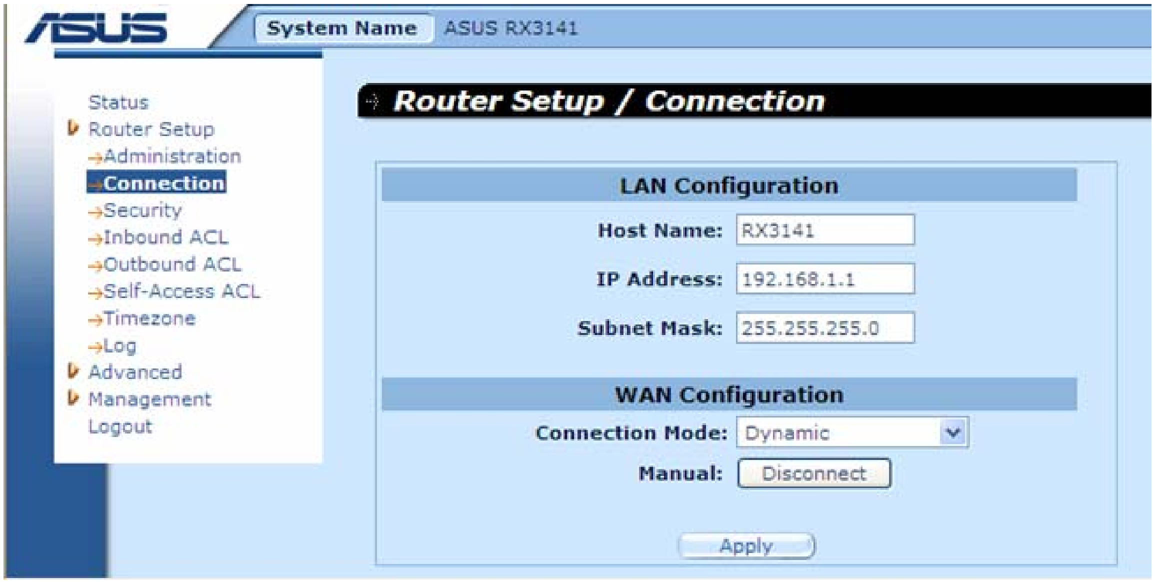
Table 5.1. LAN Configuration Parameters

Setting	Description
Host Name	For identification only.
IP Address	The LAN IP address of the RX3141. This IP address is used by your computers to identify the RX3141's LAN port. Note that the public IP address assigned to you by your ISP **is not** your LAN IP address. The public IP address identifies the WAN port on the RX3141 to the Internet.
Subnet Mask	The LAN subnet mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network. Your device is preconfigured with a default subnet mask of 255.255.255.0.

5.1.3 Configuring the LAN IP Address

Follow these steps to change the default LAN IP address.

1. Log into Configuration Manager, and then double click **Router Setup → Connection** menu. The Router Connection Setup configuration page is then displayed as shown in Figure 5.1.



System Name: ASUS RX3141

Host Name: RX3141

IP Address: 192.168.1.1

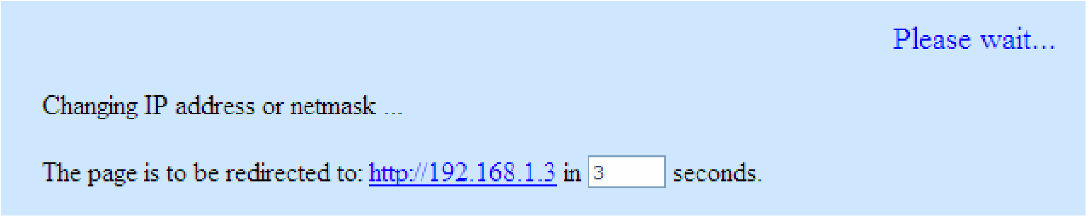
Subnet Mask: 255.255.255.0

Connection Mode: Dynamic

Manual: Disconnect

Figure 5.1. Router Connection Setup Configuration – LAN Configuration

2. (Optional) Enter the host name for RX3141. Note that the host name is used for identification only and is not used for any other purpose.
3. Enter the LAN IP address and subnet mask for the RX3141 in the spaces provided.
4. Proceed to the WAN Configuration section for instructions on setting up the WAN port if you have not yet done so.
5. Click Apply to save the settings. If you are using an Ethernet connection for the current session, and change the IP address, the connection will be terminated.
6. You will see the following message displayed as shown below.



Please wait...

Changing IP address or netmask ...

The page is to be redirected to: http://192.168.1.3 in 3 seconds.

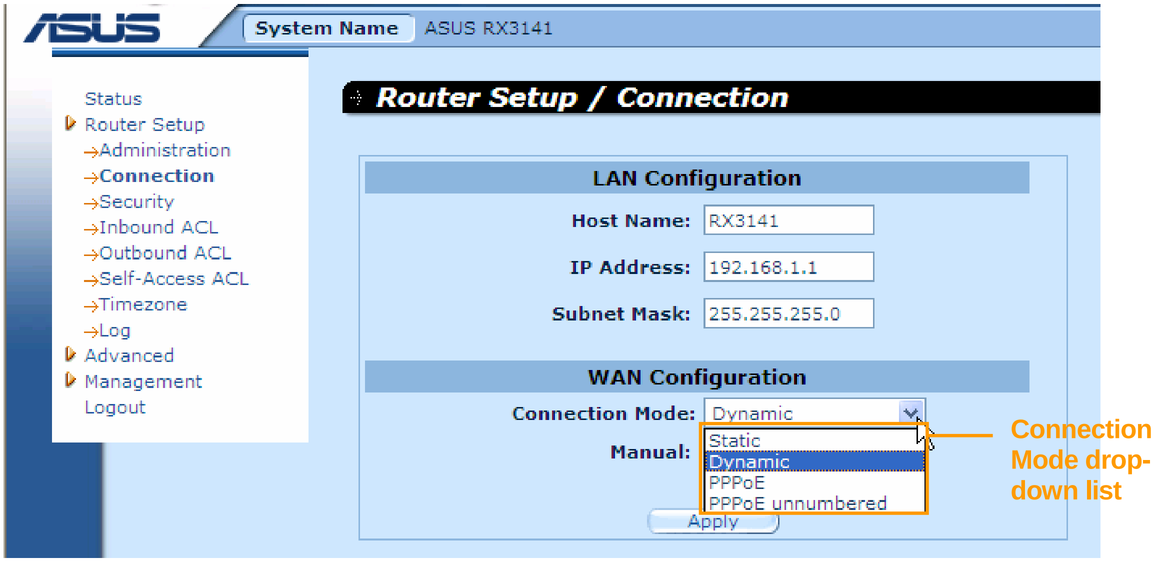
7. You will then be prompted to log back into the Configuration Manager once the timer elapses.

5.2 WAN Configuration

This section describes how to configure WAN settings for the WAN interface on the RX3141 that communicates with your ISP. You'll learn to configure IP address, DHCP and DNS server for your WAN in this section.

5.2.1 WAN Connection Mode

Four modes of WAN connection are supported by the RX3141 – PPPoE (multi-session), PPPoE unnumbered, dynamic IP and static IP. You may select one of the WAN connection modes required by your ISP from the Connection Mode drop-down list in Network Setup Configuration page as shown in Figure 5.2.



System Name ASUS RX3141

Host Name: RX3141

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Connection Mode: Dynamic

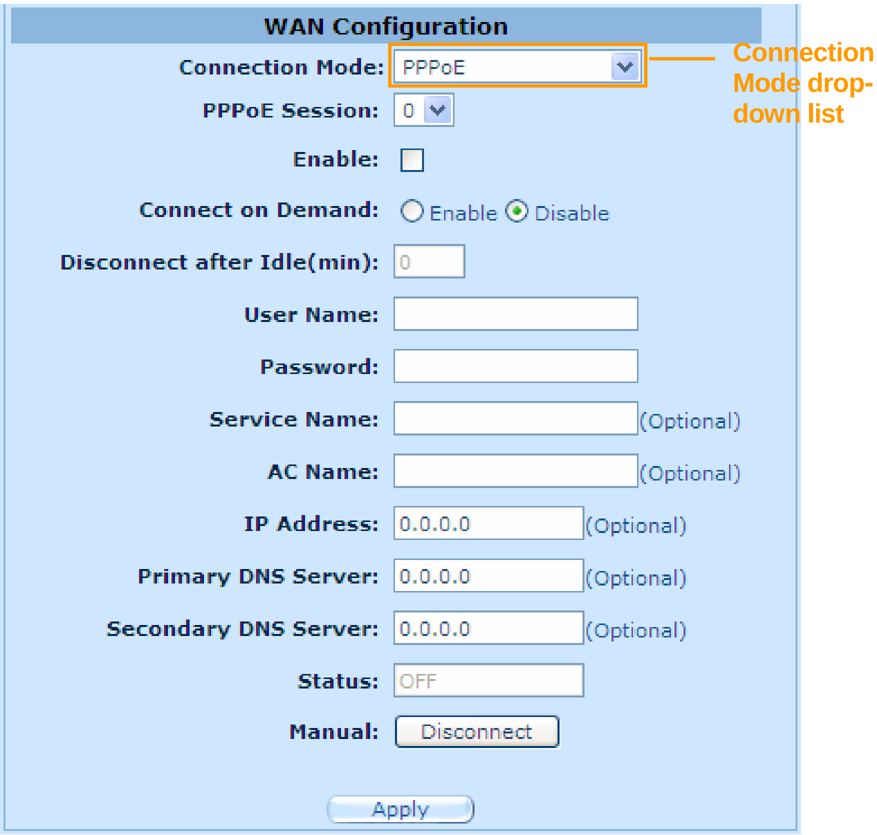
Manual:

Connection Mode drop-down list

Figure 5.2. Network Setup Configuration Page – WAN Configuration

5.2.2 PPPoE

PPPoE connection is most often used by ADSL service providers.



WAN Configuration

Connection Mode: PPPoE

PPPoE Session: 0

Enable: □

Connect on Demand: ○ Enable ● Disable

Disconnect after Idle(min): 0

User Name:

Password:

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0 (Optional)

Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

Status: OFF

Manual: Disconnect

Apply

Connection Mode drop-down list

Figure 5.3. WAN – PPPoE Configuration

5.2.2.1 WAN PPPoE Configuration Parameters

Table 5.2 describes the configuration parameters available for PPPoE connection mode.

Table 5.2. WAN PPPoE Configuration Parameters

Setting	Description
Connection Mode	Select **PPPoE** from the connection mode drop-down list.
PPPoE Session	Select the PPPoE session ID for this PPPoE session. Note that only two simultaneous PPPoE sessions are supported.
Enable	Check or uncheck this box to activate this PPPoE session.
Connection on Demand	Check "**Enable**" or "**Disable**" radio button to enable/disable this option.
Disconnect after Idle (min)	Enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. A value of 0 means no activity time out. Note that SNTP service may interfere with this function if there are activities from the service.
User Name and Password	Enter the username and password you use to log into your ISP. (Note: this is different from the information you used to log into Configuration Manager.)
Service Name	Enter the service name provided by your ISP. Service name is optional but may be required by some ISP.
IP Address	Enter a static IP address here only when your service provider requires a static IP for PPPoE connection. This IP address must be provided by your service provider. Most service providers do not require user to use a static IP for PPPoE connection.
Primary/Secondary DNS Server	IP address of the primary and/or secondary DNS are optional as PPPoE will automatically detect the DNS IP addresses configured at your ISP. However, if there are other DNS servers you would rather use, enter the IP addresses in the spaces provided.
Status	On: PPPoE connection is active. Off: PPPoE connection is inactive. Connecting: RX3141 is trying to connect to your ISP using PPPoE connection mode.
Manual Disconnect/Connect	Click the **Disconnect** or **Connect** button to disconnect or connect to your service provider using the PPPoE connection mode.

5.2.2.2 Configuring PPPoE for WAN

Follow the instructions below to configure PPPoE settings:

1. Open the Router Connection configuration page by double clicking the **Router Setup ➔ Connection** menu.
2. Select **PPPoE** from the WAN Connection Mode drop-down list as shown in Figure 5.3.
3. Select PPPoE session ID from the PPPoE session ID drop-down list. Currently, two sessions are supported.
4. Enter the user name and password provided by your ISP.
5. (Optional) Enter the service name if required by your ISP.
6. Enter appropriate connection settings for "**Disconnect after Idle (min)**" and "**Connect on Demand**".
7. Click Apply to save the settings.

5.2.2.3 Configuring PPPoE Multi-session for WAN

Follow the instructions below to configure PPPoE multi-session settings for the PPPoE multi-session example as shown in Figure 5.4.

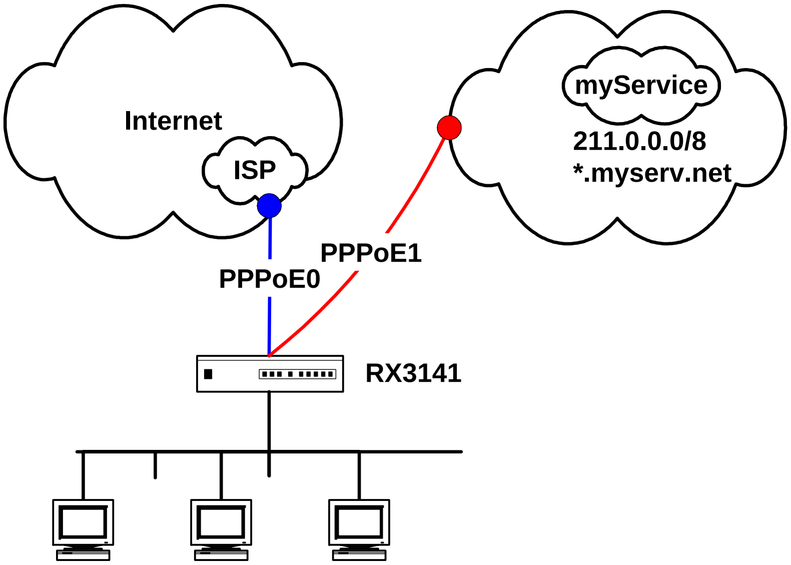
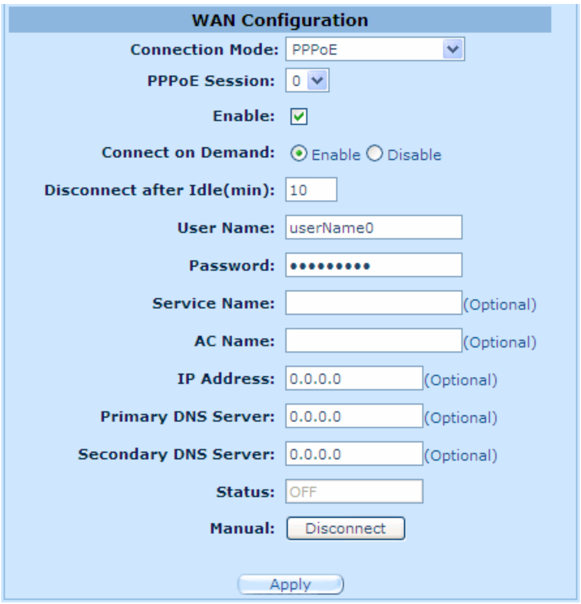


Figure 5.4. WAN – PPPoE Multi-session Example

1. Open the Router Connection configuration page by double clicking the **Router Setup ➔ Connection** menu.
2. Configure PPPoE settings as you normally would for each PPPoE session as described in section 5.2.2.2 "Configuring PPPoE for WAN". Note that maximum of two PPPoE sessions are supported. The following figures show the settings for the two PPPoE sessions.



WAN Configuration

Connection Mode: PPPoE

PPPoE Session: 0

Enable: ☑

Connect on Demand: ● Enable ○ Disable

Disconnect after Idle(min): 10

User Name: userName0

Password: •••••••••

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0 (Optional)

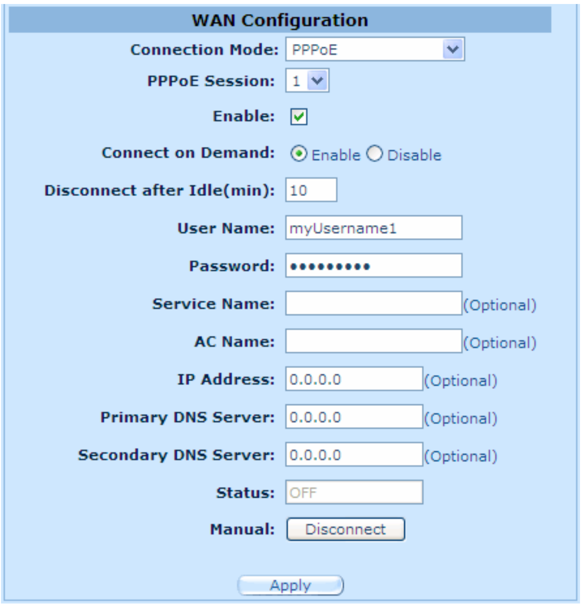
Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

Status: OFF

Manual: Disconnect

Apply



WAN Configuration

Connection Mode: PPPoE

PPPoE Session: 1

Enable: ☑

Connect on Demand: ● Enable ○ Disable

Disconnect after Idle(min): 10

User Name: myUsername1

Password: •••••••••

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0 (Optional)

Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

Status: OFF

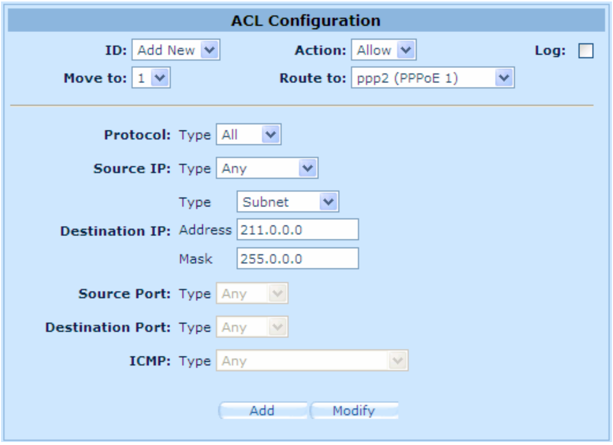
Manual: Disconnect

Apply

Figure 5.5. WAN – PPPoE0 Settings

Figure 5.6. WAN – PPPoE1 Settings

3. Configure firewall outbound ACL rules to forward the designated traffic to each intended PPPoE session. Please refer to section 9.5 "Configuring Outbound ACL Rules" for instructions on setting up ACL rules. Figure 5.7 and Figure 5.8 show the settings for the two outbound ACL rules – one specify the destination network using the network address and subnet mask and the other using the domain name. Only one of the two ACL rules is needed. However, if you intend to use IP address and the domain name to access the myService network, you'll need to configure both rules.



ACL Configuration

ID: Add New Action: Allow Log: □

Move to: 1 Route to: ppp2 (PPPoE 1)

Protocol: Type All

Source IP: Type Any

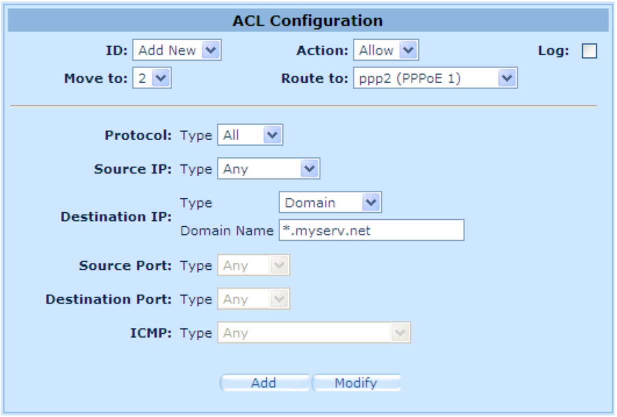
Destination IP: Type Subnet, Address 211.0.0.0, Mask 255.0.0.0

Source Port: Type Any

Destination Port: Type Any

ICMP: Type Any

Add Modify



ACL Configuration

ID: Add New Action: Allow Log: □

Move to: 2 Route to: ppp2 (PPPoE 1)

Protocol: Type All

Source IP: Type Any

Destination IP: Type Domain, Domain Name *.myserv.net

Source Port: Type Any

Destination Port: Type Any

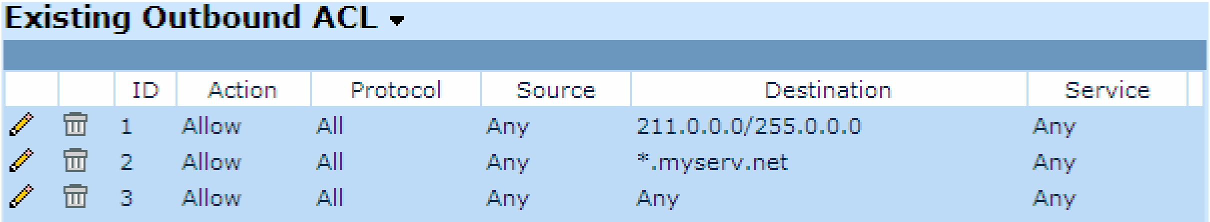
ICMP: Type Any

Add Modify

Figure 5.7. WAN – First ACL Rule Settings (using network address/subnet mask) for Forwarding Packets to PPPOE1 Session

Figure 5.8. WAN – Second ACL Rule Settings (using domain name) for Forwarding Packets to PPPOE1 Session

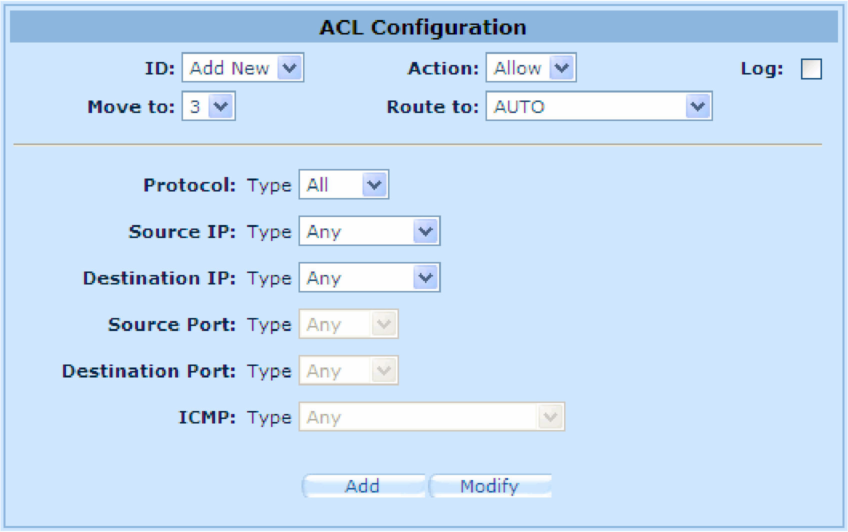
4. Verify that you have all the rules properly configured as indicated in the "Existing Outbound ACL" table as shown in Figure 5.9. Note that the third rule is the default outbound ACL rule that allows all the outbound traffic to go through the firewall. You'll have to configure this rule (see the default outbound ACL settings in Figure 5.10) if you had deleted. The third rule is used to forward all the outbound traffic to PPPoE0 session except those intended for PPPoE1 session.



Existing Outbound ACL

		ID	Action	Protocol	Source	Destination	Service
		1	Allow	All	Any	211.0.0.0/255.0.0.0	Any
		2	Allow	All	Any	*.myserv.net	Any
		3	Allow	All	Any	Any	Any

Figure 5.9. WAN – Outbound ACL Rule Settings for PPPoE Multi-session Example



ACL Configuration

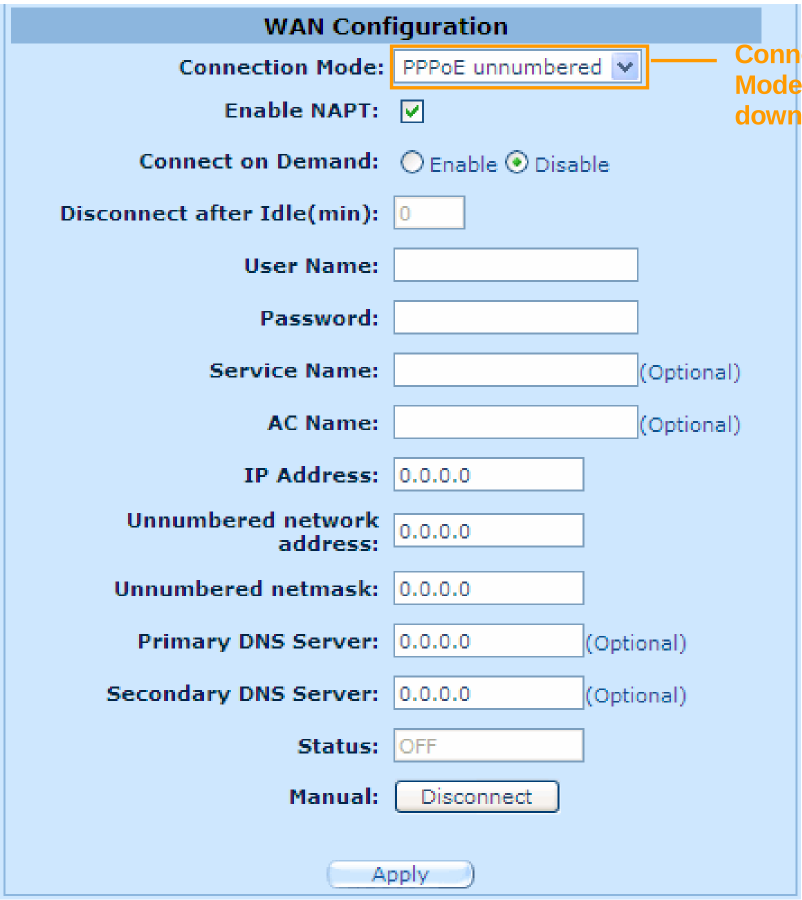
ID: Add New
Action: Allow
Log: □
Move to: 3
Route to: AUTO

Protocol: Type All
Source IP: Type Any
Destination IP: Type Any
Source Port: Type Any
Destination Port: Type Any
ICMP: Type Any

Figure 5.10. WAN – Default Outbound ACL Rule for PPPoE Multi-session Example

5.2.3 PPPoE Unnumbered

Some of the ADSL service providers may offer PPPoE unnumbered service. Choose this connection mode if your ISP provides such service.



WAN Configuration

Connection Mode:	PPPoE unnumbered
Enable NAPT:	☑
Connect on Demand:	○ Enable ● Disable
Disconnect after Idle(min):	0
User Name:	
Password:	
Service Name:	(Optional)
AC Name:	(Optional)
IP Address:	0.0.0.0
Unnumbered network address:	0.0.0.0
Unnumbered netmask:	0.0.0.0
Primary DNS Server:	0.0.0.0 (Optional)
Secondary DNS Server:	0.0.0.0 (Optional)
Status:	OFF
Manual:	Disconnect

Connection Mode drop-down list

Figure 5.11. WAN – PPPoE Unnumbered Configuration

5.2.3.1 WAN PPPoE Unnumbered Configuration Parameters

Table 5.3 describes the configuration parameters available for PPPoE unnumbered connection mode.

Table 5.3. WAN PPPoE Unnumbered Configuration Parameters

Setting	Description
Connection Mode	Select **PPPoE Unnumbered** from the connection mode drop-down list. Traditionally, each network interface must have a unique IP address. However, an unnumbered interface does not have to have a unique IP address. This means that when this option is selected, the WAN and the LAN use the same IP address. Network resources are therefore conserved because fewer network IP addresses are used and routing table is smaller.
Enable NAPT	Check or uncheck this box to enable NAPT for this connection.
Connect on Demand	Check "**Enable**" or "**Disable**" radio button to enable/disable this option.
Disconnect after Idle (min)	Enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. A value of 0 means no activity time out. Note that SNTP service may interfere with this function if there are activities from the service.
IP Address	Enter a static IP address here for the PPPoE unnumbered connection. This IP address must be provided by your service provider.
Unnumbered network address	Enter the network address provided by your ISP.
Unnumbered netmask	Enter the subnet mask provided by your ISP.
User Name and Password	Enter the username and password you use to log into your ISP. (Note: this is different from the information you used to log into Configuration Manager.)
Service Name	Enter the service name provided by your ISP. Service name is optional but may be required by some ISPs.
Status	On: PPPoE unnumbered connection is active. Off: No PPPoE unnumbered connection is inactive. Connecting: RX3141 is trying to connect to your ISP using PPPoE unnumbered connection mode.
Manual Disconnect/Connect	Click the **Disconnect** or **Connect** button to disconnect or connect to your service provider using the PPPoE unnumbered connection mode.

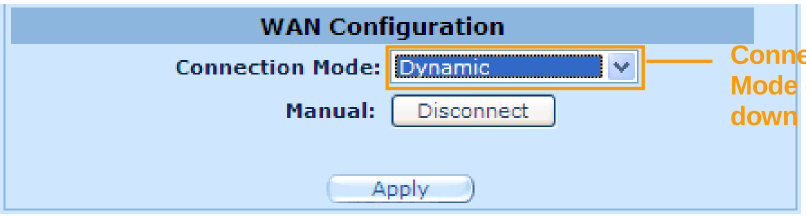
5.2.3.2 Configuring PPPoE Unnumbered for WAN

Follow the instructions below to configure PPPoE unnumbered settings:

1. Open the Router Connection configuration page by double clicking the **Router Setup ➔ Connection** menu.
2. Select **PPPoE Unnumbered** from the WAN Connection Mode drop-down list as shown in Figure 5.11.
3. Enter user name and password provided by your ISP..
4. (Optional) Enter the service name if required by your ISP.
5. Enter appropriate connection settings for "**Disconnect after Idle (min)**" and "**Connect on Demand**".
6. Click Apply to save the settings.

5.2.4 Dynamic IP

Dynamic IP is most often used by the cable modem service providers.



WAN Configuration

Connection Mode: Dynamic

Connection Mode drop-down list

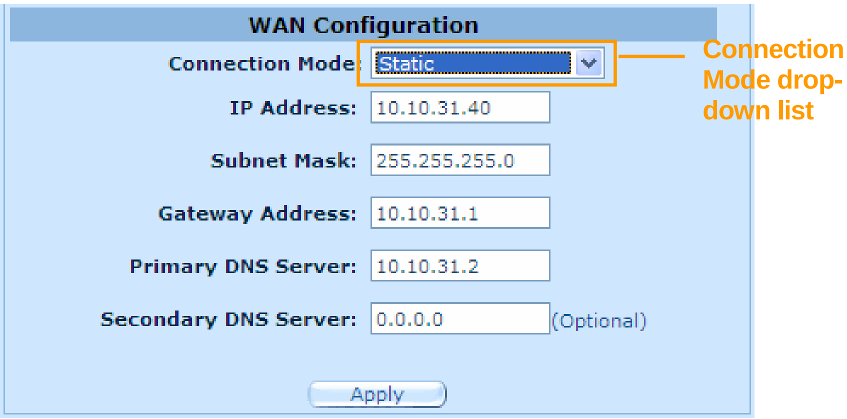
Figure 5.12. WAN – Dynamic IP (DHCP client) Configuration

5.2.4.1 Configuring Dynamic IP for WAN

Follow the instructions below to configure dynamic IP settings:

1. Open the Router Connection configuration page by double clicking the **Router Setup ➔** menu.
2. Select Dynamic from the Connection Mode drop-down list as shown in Figure 5.12. Note that the IP addresses for the primary and/or the secondary DNS servers are automatically assigned by the DHCP server of your ISP.
3. Click Apply to save the settings.

5.2.5 Static IP



WAN Configuration

Connection Mode: Static

IP Address: 10.10.31.40

Subnet Mask: 255.255.255.0

Gateway Address: 10.10.31.1

Primary DNS Server: 10.10.31.2

Secondary DNS Server: 0.0.0.0 (Optional)

Connection Mode drop-down list

Figure 5.13. WAN – Static IP Configuration

5.2.5.1 WAN Static IP Configuration Parameters

Table 5.4 describes the configuration parameters available for static IP connection mode.

Table 5.4. WAN Static IP Configuration Parameters

Setting	Description
Connection Mode	Select **Static** from the connection mode drop-down list.
IP Address	WAN IP address provided by your ISP.
Subnet Mask	WAN subnet mask provided by your ISP. Typically, it is set as 255.255.255.0.
Gateway Address	Gateway IP address provided by your ISP. It must be in the same subnet as the WAN on the RX3141.
Primary/Secondary DNS Server	You must at least enter the IP address of the primary DNS server. Secondary DNS server is optional

5.2.5.2 Configuring Static IP for WAN

Follow the instructions below to configure static IP settings:

1. Open the Router Connection configuration page by double clicking the **Router Setup → Connection** menu.
2. Select Static from the Connection Mode drop-down list as shown in Figure 5.13.
3. Enter WAN IP address in the IP Address field. This information should be provided by your ISP.
4. Enter Subnet Mask for the WAN. This information should be provided by your ISP. Typically, it is 255.255.255.0.
5. Enter gateway address provided by your ISP in the space provided.
6. Enter the IP address of the primary DNS server. This information should be provided by your ISP. Secondary DNS server is optional.
7. Click Apply to save the settings

.

6 DHCP Server Configuration

6.1 DHCP (Dynamic Host Control Protocol)

6.1.1 What is DHCP?

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device — such as the RX3141 — to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a *DHCP server*, and the receiving device is a *DHCP client*.

Note

If you followed the Quick Start Guide instructions, you either configured each LAN PC with an IP address, or you specified that it will receive IP information dynamically (automatically). If you chose to have the information assigned dynamically, then you configured your PCs as DHCP clients that will accept IP addresses assigned from a DCHP server such as the RX3141.

The DHCP server draws from a defined pool of IP addresses and "leases" them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned *dynamically* rather than *statically.* A DHCP client can be assigned a different address from the pool each time it reconnects to the network.

6.1.2 Why use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from the RX3141. Without DHCP, you would have to configure each computer separately with IP address and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.

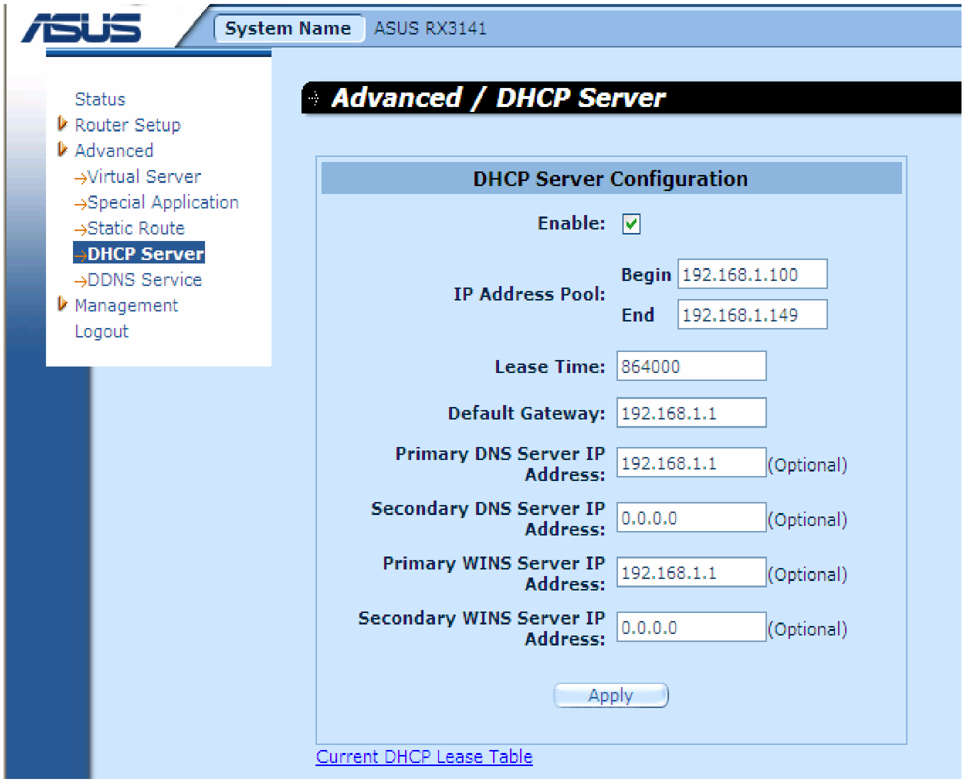
6.1.3 Configuring DHCP Server

Note

The RX3141 is configured as a DHCP server on the LAN side, with a predefined IP address pool of 192.168.1.100 through 192.168.1.149 (subnet mask 255.255.255.0). To change this range of addresses, follow the procedures described in this section.

First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the DHCP Server Configuration page, shown in Figure 6.1, by double clicking **Advanced ➔ DHCP Server** menu.



System Name ASUS RX3141

Advanced / DHCP Server

DHCP Server Configuration

Enable: ☑

IP Address Pool: Begin 192.168.1.100
End 192.168.1.149

Lease Time: 864000

Default Gateway: 192.168.1.1

Primary DNS Server IP Address: 192.168.1.1 (Optional)

Secondary DNS Server IP Address: 0.0.0.0 (Optional)

Primary WINS Server IP Address: 192.168.1.1 (Optional)

Secondary WINS Server IP Address: 0.0.0.0 (Optional)

Figure 6.1. DHCP Server Configuration Page

2. Enter the information for the *IP Address Pool (Begin/End Address*), Sub*net Mask*, *Lease Time* and *Default Gateway IP Address,* fields; others, such as *Primary/Secondary DNS Server IP Address* and *Primary/Secondary WINS Server IP Address* are optional. However, it is recommended that you enter the primary DNS server IP address in the space provided. You may enter the LAN IP or your ISP's DNS IP in the primary DNS Server IP Address field. Table 6.1 describes the DHCP configuration parameters in detail.

Table 6.1. DHCP Configuration Parameters

Field	Description
Enable	Check or uncheck this box to enable or disable DHCP server service for your LAN.
IP Address Pool Begin/End	Specify the lowest and highest addresses in the DHCP address pool.
Lease Time	The amount of time in seconds the assigned address will be used by a device connected on the LAN.
Default Gateway IP Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the device that the DHCP client computers first contacted to communicate with the Internet. Typically, it is the RX3141's LAN port IP address.
Primary/Secondary DNS Server IP Address	The IP address of the *Domain Name System* server to be used by computers that receive IP addresses from this pool. The DNS server translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, the server(s) are located with your ISP. However, you may enter LAN IP address of the RX3141 as it will serve as DNS proxy for the LAN computers and forward the DNS request from the

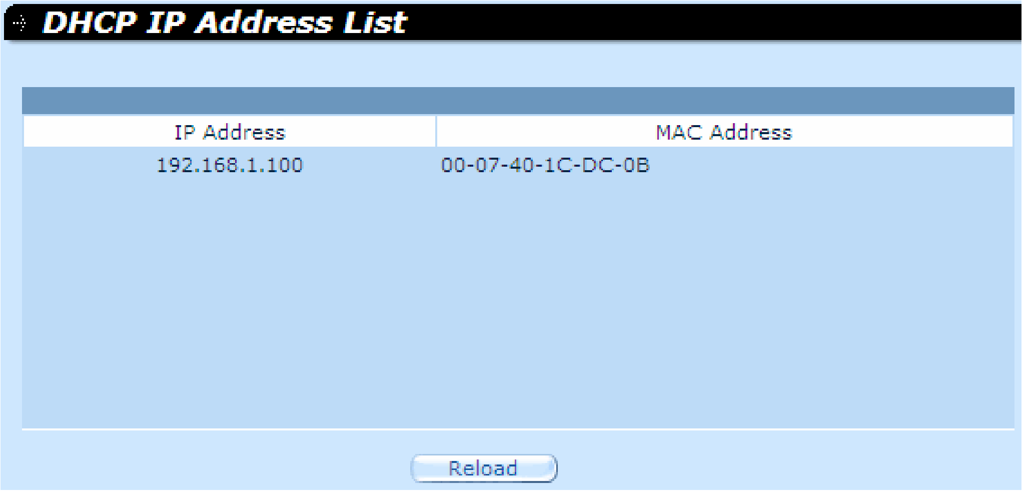
Field	Description
	LAN to DNS servers and relay the results back to the LAN computers. Note that both the primary and secondary DNS servers are optional.
Primary/Secondary WINS Server IP Address (optional)	The IP address of the WINS servers to be used by computers that receive IP addresses from the DHCP IP address pool. You don't need to enter this information unless your network has WINS servers.

3. Click Apply to save the DHCP server configurations.

6.1.4 Viewing Current DHCP Address Assignments

When the RX3141 functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, just open the DHCP Server Configuration page and click on the link "**Current DHCP Lease Table**" located at the bottom of the configuration page. A page displays similar to that shown in Figure 6.2.

The DHCP lease table lists any IP addresses leased and the corresponding MAC addresses.



DHCP IP Address List

IP Address	MAC Address
192.168.1.100	00-07-40-1C-DC-0B

Figure 6.2. DHCP Lease Table

7 Configuring Static Routes

You can use Configuration Manager to define specific routes for your Internet and network data communication. This chapter describes basic routing concepts and provides instructions for creating static routes. Note that most users do not need to define static routes.

7.1 Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to? When you define IP routes, you provide the rules that the RX3141 uses to make these decisions.

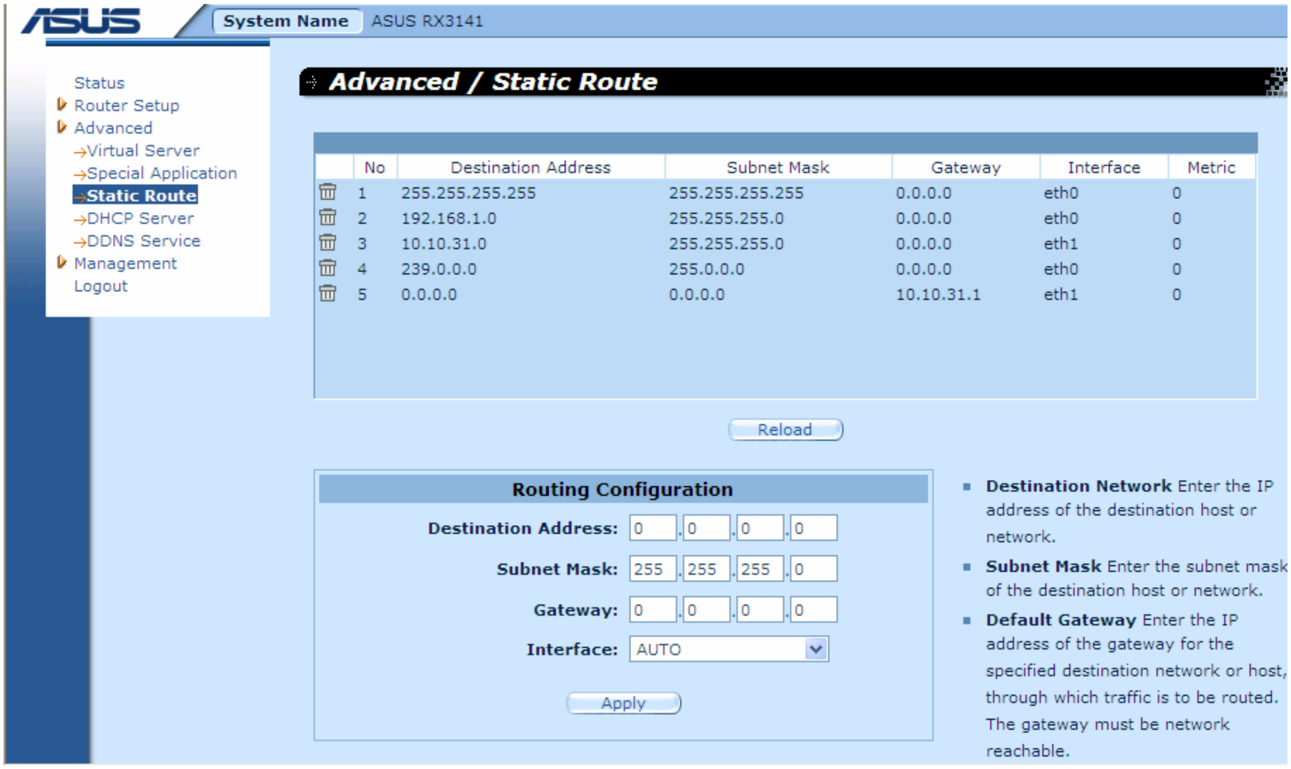
7.1.1 Do I need to define static routes?

Most users do not need to define static routes. On a typical small home or office network, the existing routes that set up the default gateways for your LAN computers and for the RX3141 provide the most appropriate path for all your Internet traffic.

- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the RX3141. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the Quick Start Guide instructions, Part 2.)
- On the RX3141 itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described in section 7.2.2 Adding Static Routes.)

You may need to define static routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

7.2 Static Route



System Name ASUS RX3141

Advanced / Static Route

	No	Destination Address	Subnet Mask	Gateway	Interface	Metric
🗑	1	255.255.255.255	255.255.255.255	0.0.0.0	eth0	0
🗑	2	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
🗑	3	10.10.31.0	255.255.255.0	0.0.0.0	eth1	0
🗑	4	239.0.0.0	255.0.0.0	0.0.0.0	eth0	0
🗑	5	0.0.0.0	0.0.0.0	10.10.31.1	eth1	0

Routing Configuration

Destination Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Interface: AUTO

- **Destination Network** Enter the IP address of the destination host or network.
- **Subnet Mask** Enter the subnet mask of the destination host or network.
- **Default Gateway** Enter the IP address of the gateway for the specified destination network or host, through which traffic is to be routed. The gateway must be network reachable.

Figure 7.1. Routing Configuration Page

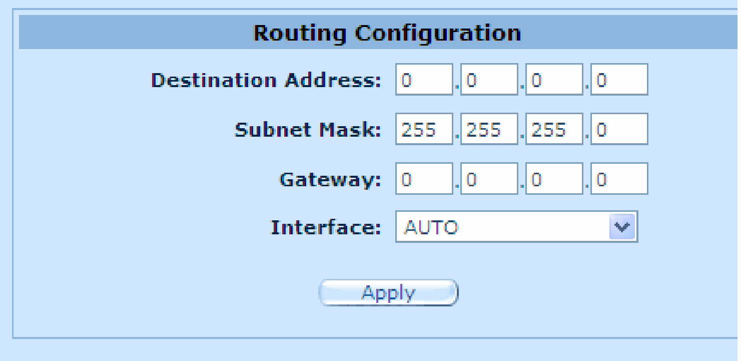
7.2.1 Static Route Configuration Parameters

The following table defines the available configuration parameters for static routing configuration.

Table 7.1. Static Route Configuration Parameters

Field	Description
Destination Address	Specifies the IP address of the destination computer or an entire destination network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway). Note that destination IP must be a network ID. The default route uses a destination IP of 0.0.0.0. Refer to Appendix 12 for an explanation of network ID.
Subnet Mask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix 12, for an explanation of network masks. The default route uses a 0.0.0.0 for subnet mask.
Gateway	Gateway IP address
Interface	Available option include AUTO, Eth0 (LAN), Eth1 (WAN), PPPoE:0 (unnumbered), PPPoE:1 (1st PPPoE session), PPPoE:2 (2nd PPPoE session). These options are selectable from the drop-down list. If AUTO is selected, the router will automatically assign an interface to route the packets based on the gateway IP address.

7.2.2 Adding Static Routes



Routing Configuration

Destination Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Interface: AUTO

Figure 7.2. Static Route Configuration

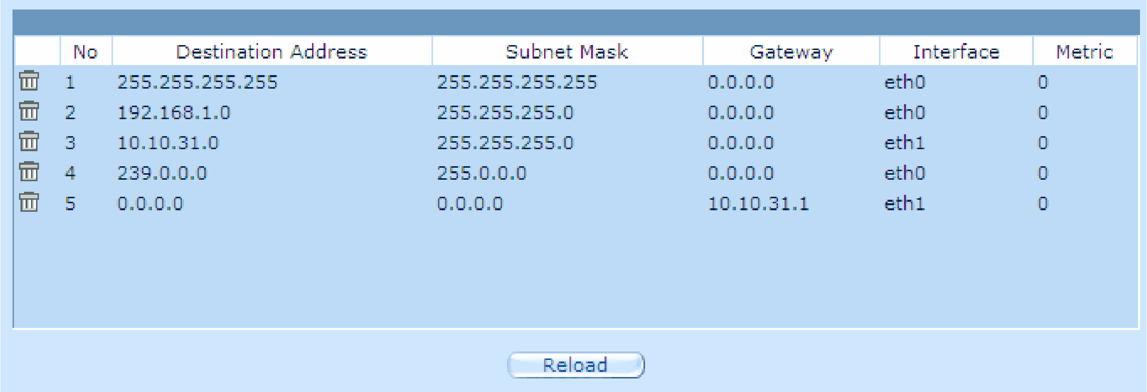
Follow these instructions to add a static route to the routing table.

1. Open the Static Route configuration page by double clicking the **Advanced → Static Route** menu.
2. Enter static routes information such as destination IP address, destination subnet mask, gateway IP address and the interface in the corresponding fields.

   For a description of these fields, refer to Table 7.1. Static Route Configuration Parameters.

   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the **Destination IP Address** and **Subnet Mask** fields.
3. Click Apply to add a new route.

7.2.3 Deleting Static Routes



	No	Destination Address	Subnet Mask	Gateway	Interface	Metric
🗑	1	255.255.255.255	255.255.255.255	0.0.0.0	eth0	0
🗑	2	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
🗑	3	10.10.31.0	255.255.255.0	0.0.0.0	eth1	0
🗑	4	239.0.0.0	255.0.0.0	0.0.0.0	eth0	0
🗑	5	0.0.0.0	0.0.0.0	10.10.31.1	eth1	0

Figure 7.3. Sample Routing Table

Follow these instructions to delete a static route from the routing table.

1. Open the Static Route configuration page by double clicking the **Advanced → Static Route** menu.
2. Click on the 🗑 icon of the route to be deleted in the Routing Table.

WARNING

Do not remove the route for default gateway unless you know what you are doing. Removing the default route will render the Internet unreachable.

7.2.4 Viewing the Static Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these *destination IP addresses*, the table lists the IP address of the first hop the data should take. This table is known as the device's *routing table*.

To view the RX3141's routing table, double click the **Advanced → Static Route** menu. The Routing Table displays at the upper half of the Static Route Configuration page, as shown in Figure 7.1:

The Routing Table displays a row for each existing route containing the IP address of the destination network, subnet mask of destination network and the IP of the gateway that forwards the traffic.

8 Configuring DDNS

Dynamic DNS is a service that allows computers to use the same domain name, even when the IP address changes from time to time (during reboot or when the ISP's DHCP server resets IP leases). RX3141 connects to a Dynamic DNS service provider whenever the WAN IP address changes. It supports setting up the web services such as Web server, FTP server using a domain name instead of the IP address. Dynamic DNS supports the DDNS clients with the following features:

- Update DNS records (addition) when an external interface comes up
- Force DNS update

Only HTTP DDNS client is supported.

HTTP Dynamic DNS Client

HTTP DDNS client uses the mechanism provided by the popular DDNS service providers for updating the DNS records dynamically. In this case, the service provider updates DNS records in the DNS. RX3141 uses HTTP to trigger this update. RX3141 supports HTTP DDNS update with the following service provider:

- www.dyndns.org

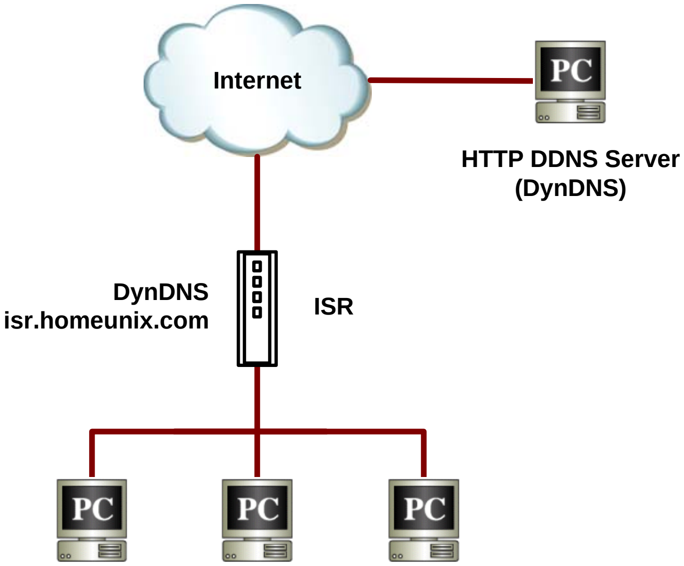


Figure 8.1. Network Diagram for HTTP DDNS

Whenever IP address of the configured DDNS interface changes, DDNS update is sent to the specified DDNS service provider. RX3141 should be configured with the DDNS username and password that are obtained from your DDNS service provider.

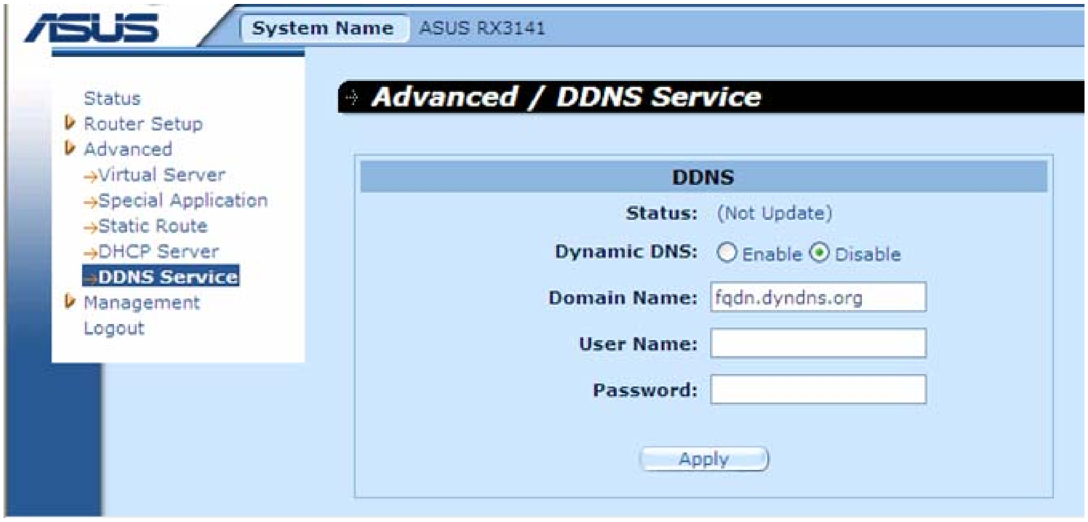
8.1 DDNS Configuration Parameters

Table 8.1 describes the configuration parameters available for DDNS service.

Table 8.1. DDNS Configuration Parameters

Field	Description
Status Shows the state of DDNS.	
Dynamic DNS	
Enable	Click on this radio button to enable the DDNS Service
Disable	Click on this radio button to disable the DDNS Service
Domain Name Enter the registered domain name provided by your ISP into this field. For example, If the host name of your RX3141 is "host1" and the domain name is "yourdomain.com", The fully qualify domain name (FQDN) is "host1.yourdomain.com".	
Username Enter the username provided by your DDNS service provider in this field.	
Password Enter the password provided by your DDNS service provider in this field.	

8.2 Configuring HTTP DDNS Client



System Name ASUS RX3141

Advanced / DDNS Service

DDNS

Status: (Not Update)

Dynamic DNS: ○ Enable ● Disable

Domain Name: fqdn.dyndns.org

User Name:

Password:

Figure 8.2. HTTP DDNS Configuration Page

Follow these instructions to configure the HTTP DDNS:

1. First, you should have already registered a domain name to the DDNS service provider. If you have not done so, please visit www.dyndns.org for more details.
2. Log into the Configuration Manager, and then click **Advanced → DDNS Service** menu to open the DDNS Configuration page.
3. In the DDNS Configuration page, select "Enable" for the Dynamic DNS.
4. Enter the domain name in the Domain Name field.
5. Enter the username and password provided by your DDNS service providers.
6. Click on Apply button to send a DNS update request to your DDNS service provider. Note that DNS update request will also be sent to your DDNS Service provider automatically whenever the WAN port status is changed.

9 Configuring Firewall/NAT Settings

The RX3141 provides built-in firewall/NAT functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN while providing Internet access sharing at the same time. You can also specify how to monitor attempted attacks, and unwanted network access.

This chapter describes how to configure router security settings, and create/modify/delete ACL (Access Control List) rules to control the data passing through your network. You will use firewall configuration pages to:

- Configure router security and DoS settings
- Create, modify, delete and view inbound/outbound/self-access ACL rules.
- View firewall log.

Note: *When you define an ACL rule, you instruct the RX3141 to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the network or Internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.*

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

9.1 Firewall Overview

9.1.1 Stateful Packet Inspection

The stateful packet inspection engine in the RX3141 maintains a state table that is used to keep track of connection states of all the packets passing through the firewall. The firewall will open a “hole” to allow the packet to pass through if the state of the packet that belongs to an already established connection matches the state maintained by the stateful packet inspection engine. Otherwise, the packet will be dropped. This “hole” will be closed when the connection session terminates. No configuration is required for stateful packet inspection; it is enabled by default when the firewall is enabled. Please refer to section 9.2.1 “Basic Router Security Configuration Parameters” to enable or disable firewall service on the RX3141.

9.1.2 DoS (Denial of Service) Protection

Both DoS protection and stateful packet inspection provide first line of defense for your network. No configuration is required for both protections on your network as long as firewall is enabled for the RX3141. By default, the firewall is enabled at the factory. Please refer to section 9.2.1 “Basic Router Security Configuration Parameters” to enable or disable firewall service on the RX3141.

9.1.3 Firewall and Access Control List (ACL)

9.1.3.1 Priority Order of ACL Rule

All ACL rules have a rule ID assigned – the smaller the rule ID, the higher the priority. Firewall monitors the traffic by extracting header information from the packet and then either drops or forwards the packet by looking for a match in the ACL rule table based on the header information. Note that the ACL rule checking starts from the rule with the smallest rule ID until a match is found or all the ACL rules are examined. If no match is found, the packet is dropped; otherwise, the packet is either dropped or forwarded based on the action defined in the matched ACL rule.

9.1.3.2 ACL Rule and Connection State Tracking

The stateful packet inspection engine in the firewall keeps track of the state, or progress, of a network connection. By storing information about each connection in a state table, RX3141 is able to quickly determine if a packet passing through the firewall belongs to an already established connection. If it does, it is passed through the firewall without going through ACL rule evaluation.

For example, an ACL rule allows outbound ICMP packet from 192.168.1.1 to 192.168.2.1. When 192.168.1.1 sends an ICMP echo request (i.e. a ping packet) to 192.168.2.1, 192.168.2.1 will respond with an ICMP echo reply to 192.168.1.1. In the RX3141, you don't need to create another inbound ACL rule because stateful packet inspection engine tracks the connection state and allows the ICMP echo reply to pass through the firewall

9.1.4 Default ACL Rules

The RX3141 supports three types of default access rules:

- Inbound Access Rules: for controlling incoming access to your LAN.
- Outbound Access Rules: for controlling outbound access to external networks for hosts on your LAN.
- Self-Access Rules: for controlling access to the RX3141 itself.

Default Inbound Access Rules

No default inbound access rule is configured. That is, all traffic from external hosts to the internal hosts is denied.

Default Outbound Access Rules

The default outbound access rule allows all the traffic originated from your LAN to be forwarded to the external network using NAT.

Default Self Access Rules

The default self access rules allow http, ping, DNS, DHCP access to the RX3141 router from the LAN.

WARNING

It is not necessary to remove the default ACL rule from the ACL rule table! It is better to create higher priority ACL rules to override the default rule.

9.2 Router Security Settings

9.2.1 Basic Router Security Configuration Parameters

Table 9.1 describes the configuration parameters available for basic router security configuration.

Table 9.1. Basic Router Security Configuration Parameters

Field	Description
Firewall	Check or uncheck this box to enable or disable firewall.
NAT	Check or uncheck this box to enable or disable NAT.
Log Port Probing	Connection attempt to closed ports will be logged if this option is enabled.
Stealth Mode	If enabled, RX3141 will not respond to remote peer's attempt to connect to the closed TCP/UDP ports.

To configure firewall basic settings, follow the instructions below:

1. Open the Router Security configuration page as shown in Figure 9.1 by double clicking on **Router Setup ➔ Security** menu.
2. Check or uncheck individual check box for each security option.
3. Click Apply to save the settings.

9.2.2 DoS Configuration

The RX3141 has an Attack Defense Engine that protects internal networks from Denial of Service (DoS) attacks such as IP spoofing, LAND, Ping of Death, smurf and all re-assembly attacks. It can drop ICMP redirects and IP loose/strict source routing packets. For example, a security device with the RX3141 Firewall provides protection from "WinNuke", a widely used program to remotely crash unprotected Windows systems. For a complete list of DoS protection provided by the RX3141, please see Tables 2.1 and 9.2.

9.2.2.1 DoS Protection Configuration Parameters

Table 9.2 provides explanation for each type of DoS attacks. You may check or uncheck the check box to enable or disable the protection or detection for each type DoS attacks.

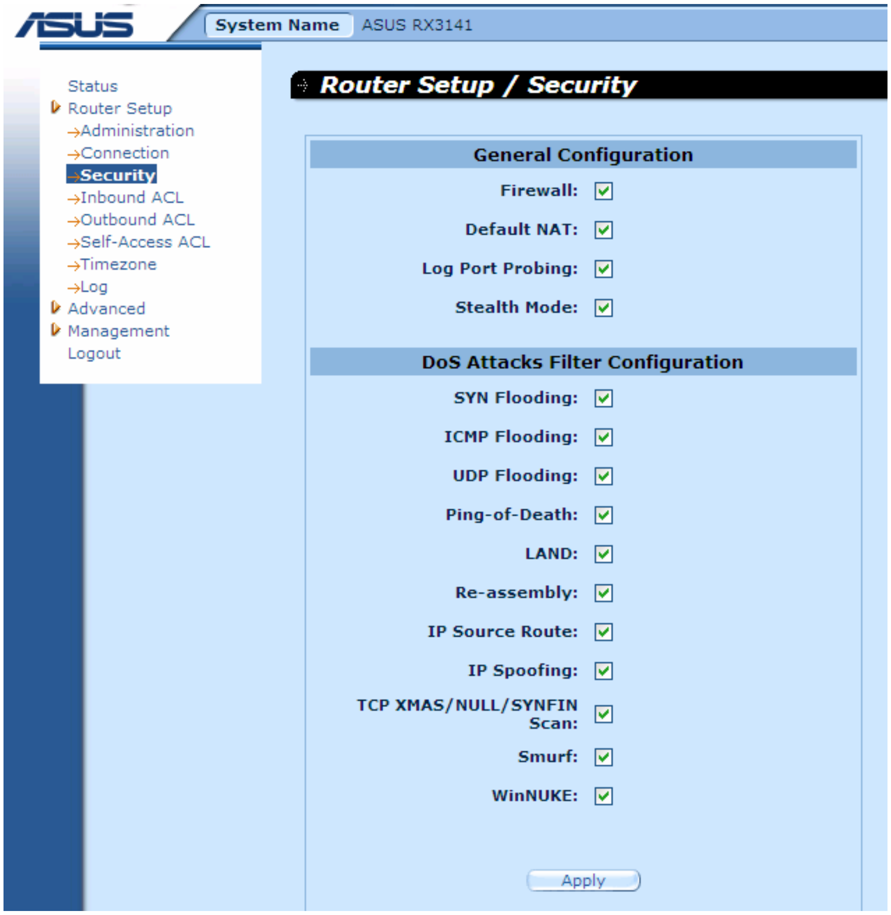
Table 9.2. DoS Attack Definition

Field	Description
IP Source Route	Intruder uses "source routing" in order to break into the target system.
IP Spoofing	Spoofing is the creation of TCP/IP packets using somebody else's IP address. IP spoofing is an integral part of many network attacks that do not need to see responses.
Land	Attacker sends out packets to the system with the same source and destination IP address being that of the target system and causes the target system trying to resolve an infinite series of connections to itself. This can cause the target system to slow down drastically.
Ping of Death	An attacker sends out larger than 64KB packets to cause certain operating system to crash.
Smurf	An attacker issues ICMP echo requests to some broadcast addresses. Each datagram has a spoofed IP source address to be that of a real target-host. Most of the addressed hosts will respond with an ICMP echo reply, but not to the real initiating host, instead all replies carry the IP address of the previously spoofed host as their current destination and cause the victim host or network to slow down drastically.
SYN/ICMP/UDP Flooding	Check or un-check this option to enable or disable the logging for SYN/ICMP/UDP flooding attacks. These attacks involve sending lots of TCP SYN/ICMP/UDP to a host in a very short period of time. RX3141 will not drop the flooding packets to avoid affecting the normal traffic.
TCP XMAS/NULL/FIN Scan	A hacker may be scanning your system by sending these specially formatted packets to see what services are available. Sometimes this is done in preparation for a future attack, or sometimes it is done to see if your system might have a service, which is susceptible to attack. XMAS scan: A TCP packet has been seen with a sequence number of zero and the FIN, URG, and PUSH bits are all set. NULL scan: A TCP packet has been seen with a sequence number of zero and all control bits are set to zero. FIN scan: A hacker is scanning the target system using a "stealth" method. The goal of the hacker is to find out if they can connect to the system without really connecting using the "FIN" scanning. It attempts to close a non-existent connection on the server. Either way, it is an error, but systems sometimes respond with different error results depending upon whether the desired service is available or not.
Teardrop	In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.
WinNUKE	Check or un-check this option to enable or disable protection against Winnuke attacks. Some older versions of the Microsoft Windows OS are vulnerable to this attack. If the computers in the LAN are not updated with recent versions/patches, you are advised to enable this protection by checking this check box.

9.2.2.2 Configuring DoS Settings

To configure DoS settings, follow the instructions below:

1. Open the Router Security configuration page as shown in Figure 9.1 by double clicking on **Router Setup ➔ Security** menu.
2. Check or uncheck individual check box for each type DoS attack.
3. Click Apply to save the settings.



Router Setup / Security

General Configuration

Firewall:	☑
Default NAT:	☑
Log Port Probing:	☑
Stealth Mode:	☑

DoS Attacks Filter Configuration

SYN Flooding:	☑
ICMP Flooding:	☑
UDP Flooding:	☑
Ping-of-Death:	☑
LAND:	☑
Re-assembly:	☑
IP Source Route:	☑
IP Spoofing:	☑
TCP XMAS/NULL/SYNFIN Scan:	☑
Smurf:	☑
WinNUKE:	☑

Figure 9.1. Router Security Configuration Page

9.3 ACL Rule Configuration Parameters

9.3.1 ACL Rule Configuration Parameters

Table 9.3 describes the configuration parameters firewall inbound, outbound and self-access ACL rules.

Table 9.3. ACL Rule Configuration Parameters

Field	Description
ID	
Add New	Click on this option to add a new ACL rule.
Rule Number	Select a rule from the drop-down list, to modify its settings.
Mave This option allows you to set a priority for this rule. The RX3141 Firewall acts on packets based on the priority of the rules. Set a priority by specifying a number for its position in the list of rules:	
1 (First)	This number marks the highest priority.
Other numbers	Select other numbers to indicate the priority you wish to assign to the rule.
Action	
Allow	Select this button to configure the rule as an **allow** rule. This rule when bound to the Firewall will allow matching packets to pass through.
Deny	Select this button to configure the rule as a **deny** rule. This rule when bound to the Firewall will **not allow** matching packets to pass through.
Route to (only for outbound ACL) This field is used for policy routing needed for PPPoE unnumbered or PPPoE multi-session. Available options include AUTO, ppp0 (unnumbered), ppp1 (1st PPPoE session), ppp2 (2nd PPPoE session). These options are selectable from the drop-down list. If AUTO is selected, the router will route the packets based on the information in the routing table.	
Log Select or deselect the check box to enable or disable logging for this ACL rule.	
Protocol This option allows you to select protocol type from a drop-down list. Available settings are All, TCP, UDP, ICMP, IGMP, AH and ESP.	
Source IP This option allows you to set the **source network** to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the source network, such as those on the Internet for the inbound traffic or all the computers in the local network for outbound traffic.
IP Address	This option allows you to specify an IP address on which this rule will be applied.
IP Address	Specify the appropriate network address

Field	Description
Subnet	This option allows you to include all the computers that are connected in an IP subnet. When this option is selected, the following fields become available for entry:
Address	Enter the appropriate IP address.
Mask	Enter the corresponding subnet mask.
Self (for self access rule only)	Indicates the router itself.
Destination IP This option allows you to set the **destination network** to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the local network for inbound traffic or any computer in the Internet for outbound traffic..
IP Address, Subnet	Select any of these options and enter details as described in the **Source IP** section above.
Self (for self access rule only)	Indicates the router itself.
Domain	In order for this option to work, user's PC must use RX3141 as its DNS server. The domain name variable / IP addresses association is cleared after every system restart. Multiple ACL rules can be associated to the same domain name / IP addresses association. ▶ Maximum of 30 domain name variables is supported. ▶ Each domain name variable / IP addresses association is updated only when the LAN client issues the DNS query to RX3141. For example, when entering the address "http://www yahoo.com" on your browser, RX3141 will update the IP address association w/ www.yahoo.com in the internal database referenced by the firewall. ▶ Each domain name variable can be associated up to 256 IP addresses. ▶ Wild card character "*" is allowed in the domain name Its usage is illurstrated in the following examples: 1. www.google.* : match www.google.com and ww.google.net and does not match www.google.com.tw 2. www.google.*.*: match www.google.com.tw, and www.google.com.sg and does not match www.google.com 3. .com.tw : match www.google.com.tw, www.com.tw and does not match com.tw 4. *.com : match google.com and abc.com and does not match www.google.com, com 5. *: match any domain name 6. . (a single dot): match any domain name
Source Port This option allows you to set the source port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an

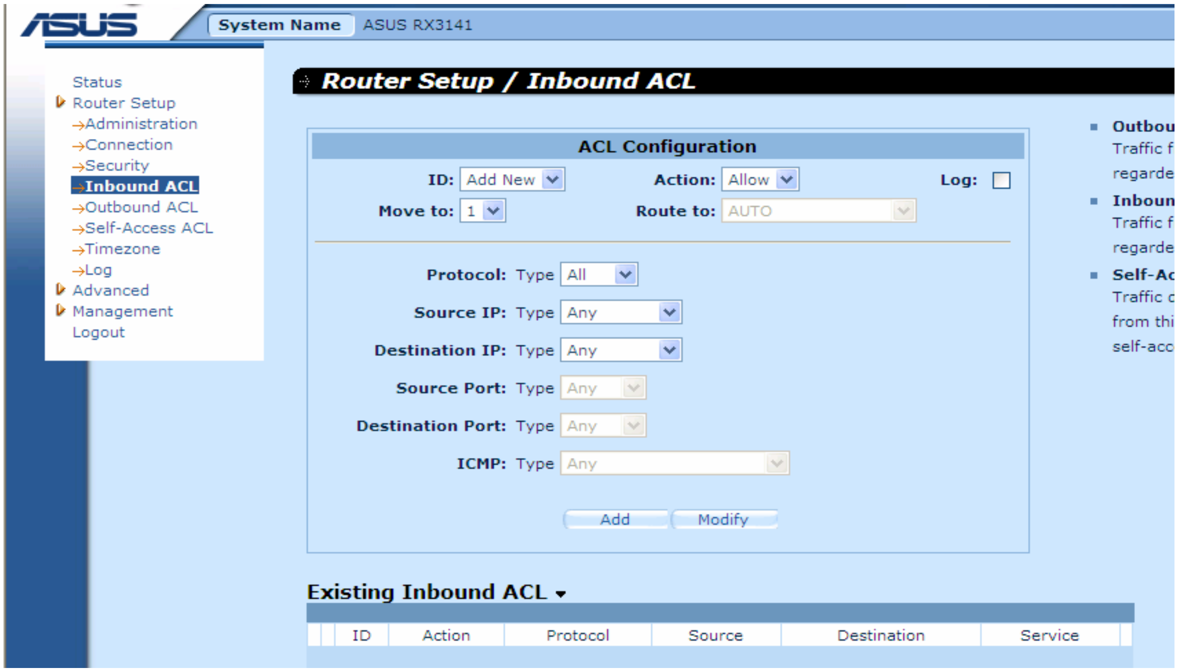
Field	Description
	arbitrary source port number.
Single	This option allows you to apply this rule to an application with a specific source port number.
Port Number	Enter the source port number
Range	Select this option if you want this rule to apply to applications with this port range. The following fields become available for entry when this option is selected.
Start Port	Enter the starting port number of the range
End Port	Enter the ending port number of the range
Destination Port This option allows you to set the destination port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an arbitrary destination port number.
Single, Range	Select any of these and enter details as described in the **Source Port** section above.
ICMP (available only when protocol type is set to ICMP) This option allows you to select the ICMP message type for the ACL rule. The supported ICMP message types are: • Any (default) • 0: Echo reply • 1: Type 1 • 2: Type 2 • 3: Dst unreach: destination unreachable • 4: Src quench: source quench • 5: Redirect • 6: Type 6 • 7: Type 7 • 8: Echo req: • 9: Router advertisement • 10: Router solicitation • 11: Time exceed: time exceeded • 12: Parameter problem • 13: Timestamp request • 14: Timestamp reply • 15: Info request: information request • 16: Info reply: information reply • 17: Addr mask req: address mask request • 18: Addr mask reply: address mask reply	

9.4 Configuring Inbound ACL Rules

By creating ACL rules in Inbound ACL configuration page as shown in Figure 9.2, you can control (allow or deny) incoming access to computers on your LAN.

Options in this configuration page allow you to:

- Add a rule, and set parameters for it
- Modify an existing rule
- Delete an existing rule
- View configured inbound ACL rules



ACL Configuration

ID: Add New | Action: Allow | Log: □

Move to: 1 | Route to: AUTO

Protocol: Type All

Source IP: Type Any

Destination IP: Type Any

Source Port: Type Any

Destination Port: Type Any

ICMP: Type Any

Existing Inbound ACL

ID	Action	Protocol	Source	Destination	Service

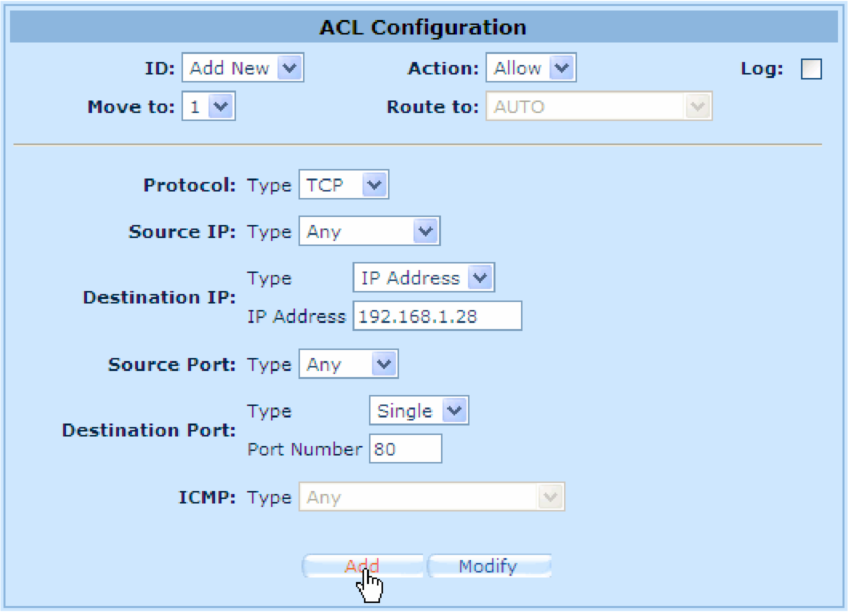
Figure 9.2. Inbound ACL Configuration Page

9.4.1 Add Inbound ACL Rules

To add an inbound ACL rule, follow the instructions below:

1. Open the Inbound ACL Rule configuration page, as shown in Figure 9.2, by double clicking the **Router Setup → Inbound ACL** menu.
2. Select "**Add New**" from the "**ID**" drop-down list.
3. Set desired action (Allow or Deny) from the "**Action**" drop-down list.
4. Make changes to any or all of the following fields: source/destination IP, source/destination port, protocol, ICMP message type and log. Please see Table 9.3 for explanation of these fields.
5. Assign a priority for this rule by selecting a number from the "**Move to**" drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.
6. Click on the Add button to create the new ACL rule. The new ACL rule will then be displayed in the inbound access control list table at the bottom half of the Inbound ACL Configuration page.

Figure 9.3 illustrates how to create a rule to allow inbound HTTP (i.e. web server) service. This rule allows inbound HTTP traffic to be directed to the host w/ IP address 192.168.1.28. Note that the newly added inbound ACL rule is displayed in the Existing Inbound ACL table shown in Figure 9.4.

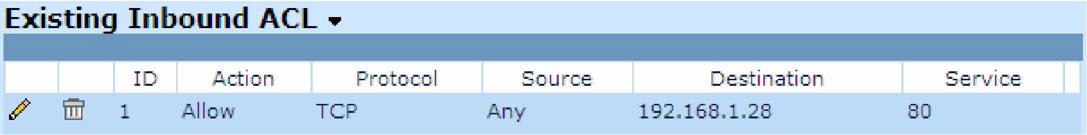


ACL Configuration

ID: Add New | Action: Allow | Log: □
Move to: 1 | Route to: AUTO

Protocol: Type TCP
Source IP: Type Any
Destination IP: Type IP Address; IP Address 192.168.1.28
Source Port: Type Any
Destination Port: Type Single; Port Number 80
ICMP: Type Any

Figure 9.3. Inbound ACL Configuration Example



Existing Inbound ACL ▾

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	TCP	Any	192.168.1.28	80

9.4.2 Figure 9.4. Sample Inbound ACL List TableModify Inbound ACL Rules

To modify an inbound ACL rule, follow the instructions below:

1. Open the Inbound ACL Rule configuration page, as shown in Figure 9.2, by double clicking the **Router Setup ➔ Inbound ACL** menu.
2. Click on the ✎ icon of the rule to be modified in the inbound ACL table or select the rule number from the "**ID**" drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, ICMP message type and log. Please see Table 9.3 for explanation of these fields.
4. Click on the Modify button to modify this ACL rule. The new settings for this ACL rule will then be displayed in the inbound access control list table at the bottom half of the Inbound ACL Configuration page.

9.4.3 Delete Inbound ACL Rules

To delete an inbound ACL rule, open the Inbound ACL Rule configuration page by double clicking the **Router Setup ➔ Inbound ACL** menu and then click on the 🗑 in front of the rule to be deleted.

9.4.4 Display Inbound ACL Rules

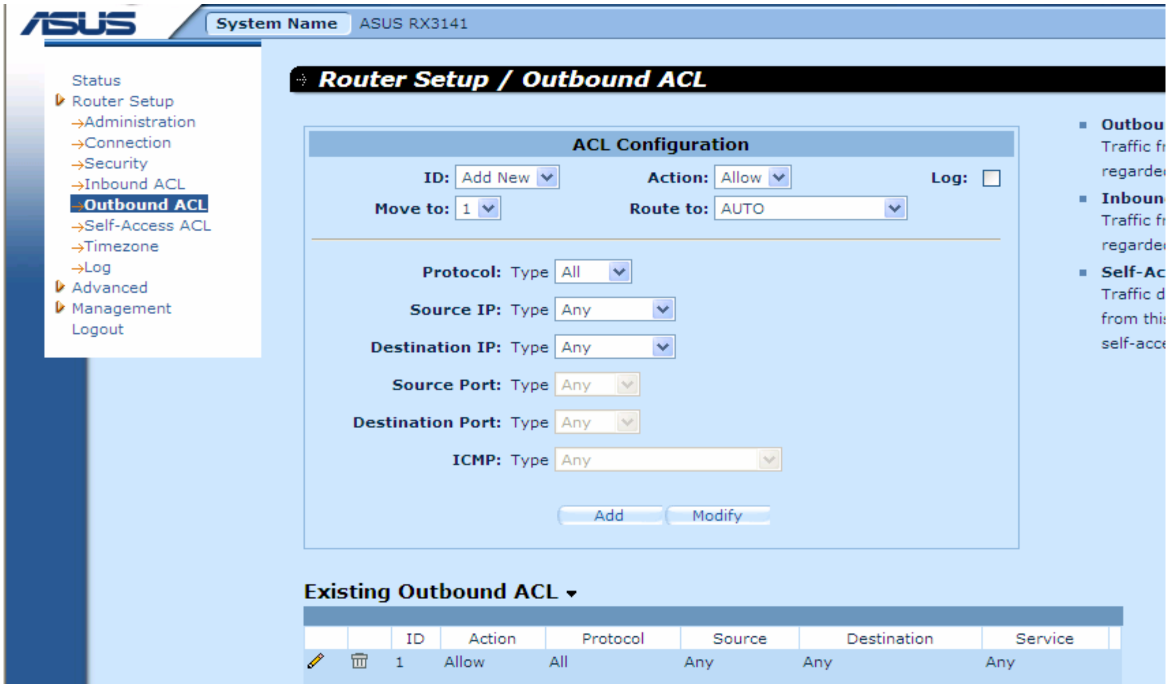
To see existing inbound ACL rules, just open the Inbound ACL Rule configuration page by double clicking the **Router Setup → Inbound ACL** menu. The existing inbound ACL rules are displayed at the bottom of the configuration page.

9.5 Configuring Outbound ACL Rules

By creating ACL rules in outbound ACL configuration page as shown in Figure 9.5, you can control (allow or deny) Internet or external network access for computers on your LAN.

Options in this configuration page allow you to:

- Add a rule, and set parameters for it
- Modify an existing rule
- Delete an existing rule
- View configured outbound ACL rules



Router Setup / Outbound ACL

ACL Configuration

ID: Add New   Action: Allow   Log: □
Move to: 1   Route to: AUTO

Protocol: Type All
Source IP: Type Any
Destination IP: Type Any
Source Port: Type Any
Destination Port: Type Any
ICMP: Type Any

Existing Outbound ACL

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	All	Any	Any	Any

Figure 9.5. Outbound ACL Configuration Page

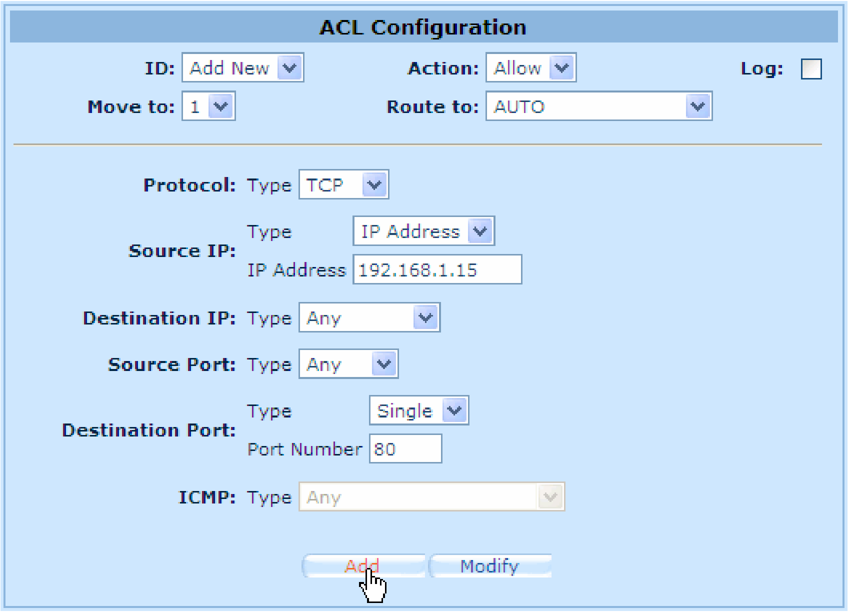
9.5.1 Add an Outbound ACL Rule

To add an outbound ACL rule, follow the instructions below:

1. Open the Outbound ACL Rule configuration page, as shown in Figure 9.5, by double clicking the **Router Setup → Outbound ACL** menu.
2. Select "**Add New**" from the "**ID**" drop-down list.
3. Set desired action (Allow or Deny) from the "**Action**" drop-down list.

4. Assign a priority for this rule by selecting a number from the "**Move to**" drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.
5. Select an interface through which to send the packets. Options available are "AUTO", "ppp0 (unnumbered)", "ppp1 (PPPoE 0)" and "ppp2 (PPPoE 1)". Normally select AUTO for router to determine where to send the traffic for packets matched this ACL rule.
6. Make changes to any or all of the following fields: source/destination IP, source/destination port, protocol, ICMP message type and log. Please see Table 9.3 for explanation of these fields.
7. Click on the Add button to create the new ACL rule. The new ACL rule will then be displayed in the outbound access control list table at the bottom half of the Outbound ACL Configuration page.

Figure 9.6 illustrates how to create a rule to allow outbound HTTP traffic. This rule allows outbound HTTP traffic (destination port 80) to be forwarded to any host on the external network for a host in your LAN w/ IP address 192.168.1.15. Note that the newly added outbound ACL rule is displayed in the Existing Outbound ACL table shown in Figure 9.7.



ACL Configuration

ID: Add New | Action: Allow | Log: □

Move to: 1 | Route to: AUTO

Protocol: Type TCP

Source IP: Type IP Address; IP Address 192.168.1.15

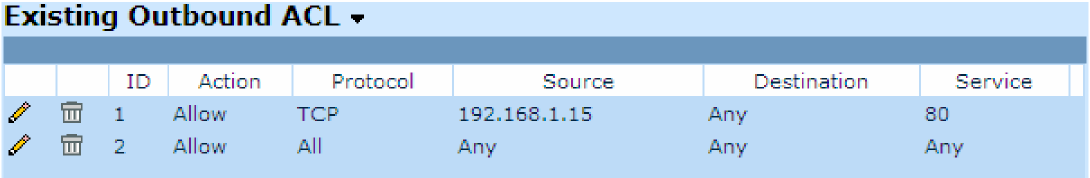
Destination IP: Type Any

Source Port: Type Any

Destination Port: Type Single; Port Number 80

ICMP: Type Any

Figure 9.6. Outbound ACL Configuration Example



Existing Outbound ACL

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	TCP	192.168.1.15	Any	80
✎	🗑	2	Allow	All	Any	Any	Any

Figure 9.7. Sample Outbound ACL List Table

9.5.2 Modify Outbound ACL Rules

To modify an outbound ACL rule, follow the instructions below:

1. Open the Outbound ACL Rule configuration page, as shown in Figure 9.5, by double clicking the **Router Setup → Outbound ACL** menu.

2. Click on the ✎ icon of the rule to be modified in the outbound ACL table or select the rule number from the "**ID**" drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, ICMP message type and log. Please see Table 9.3 for explanation of these fields.
4. Click on the Modify button to modify this ACL rule. The new settings for this ACL rule will then be displayed in the outbound access control list table at the bottom half of the Outbound ACL Configuration page.

9.5.3 Delete Outbound ACL Rules

To delete an outbound ACL rule, just open the Outbound ACL Rule configuration page by double clicking the **Router Setup ➔ Outbound ACL** menu and then click on the 🗑 in front of the rule to be deleted:

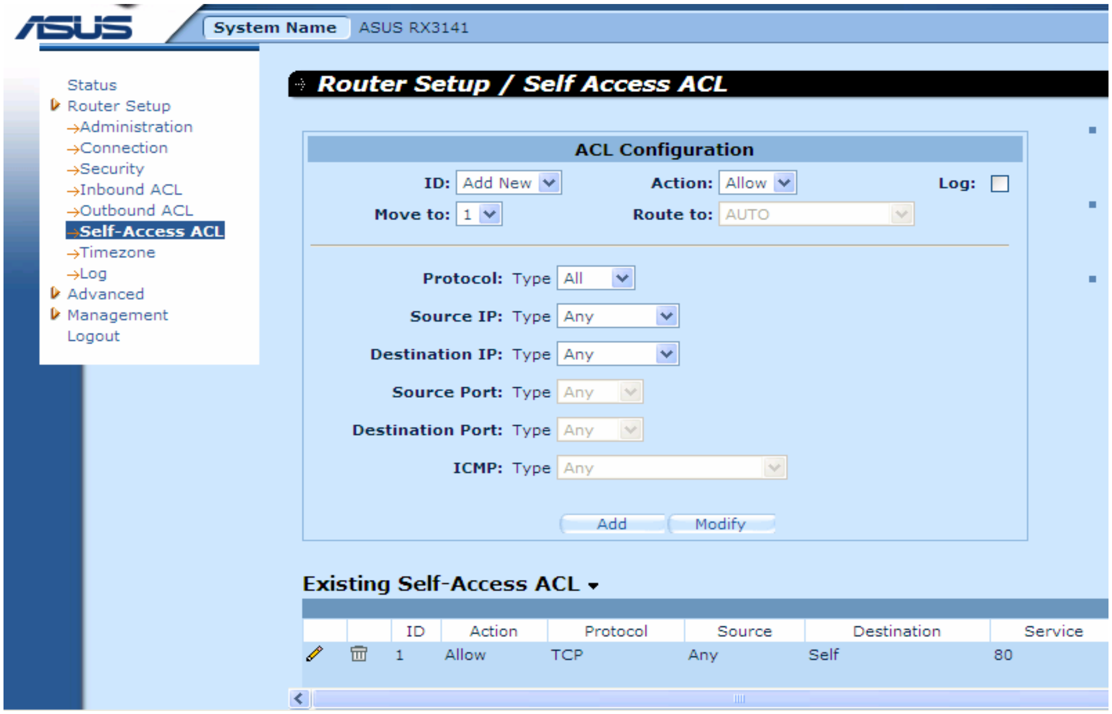
9.5.4 Display Outbound ACL Rules

Open the Outbound ACL Rule configuration page by double clicking the **Router Setup ➔ Outbound ACL** menu.

9.6 Configuring Self-Access ACL Rules – (Router Setup ➔ Self-Access ACL)

Self-Access rules control access to/from the RX3141 itself. You may use Self-Access Rule Configuration page, as illustrated in Figure 9.8, to:

- Add a Self-Access rule
- Modify an existing Self-Access rule
- Delete an existing Self-Access rule
- View existing Self-Access rules



System Name ASUS RX3141

Router Setup / Self Access ACL

ACL Configuration

ID: Add New
Action: Allow
Log: □
Move to: 1
Route to: AUTO

Protocol: Type All
Source IP: Type Any
Destination IP: Type Any
Source Port: Type Any
Destination Port: Type Any
ICMP: Type Any

Existing Self-Access ACL

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	TCP	Any	Self	80

Figure 9.8. Self-Access ACL Configuration Page

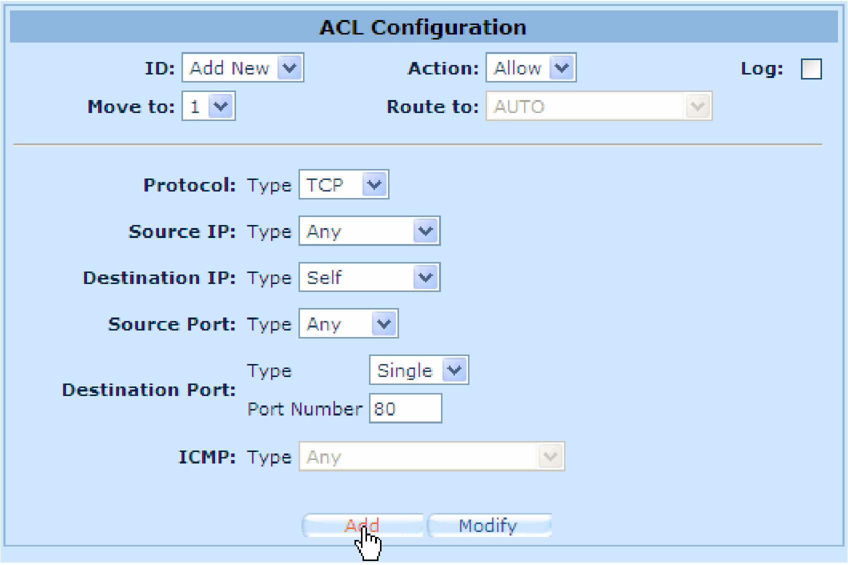
9.6.1 Add a Self-Access Rule

To add a Self-Access rule, follow the instructions below:

1. Open the Self-Access Rule configuration page, as shown in Figure 9.8, by double clicking the **Router Setup ➔ Self Access ACL** menu.
2. Select "**Add New**" from the "**ID**" drop-down list.
3. Set desired action (Allow or Deny) from the "**Action**" drop-down list.
4. Assign a priority for this rule by selecting a number from the "**Move to**" drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.
5. Make desired changes to any or all of the following fields: source/destination IP, source/destination port, protocol, ICMP message type and log. Please see Table 9.3 for explanation of these fields.
6. Click on the Add button to create the new Self-Access rule. The new rule will then be displayed in the Existing Self-Access ACL list table at the bottom half of the Self-Access ACL configuration page.

Example

Figure 9.9 shows a sample self-access ACL configuration to allow TCP port 80 traffic (i.e. HTTP traffic) from any one to RX3141.



ACL Configuration

ID: Add New Action: Allow Log: □

Move to: 1 Route to: AUTO

Protocol: Type TCP

Source IP: Type Any

Destination IP: Type Self

Source Port: Type Any

Destination Port: Type Single
Port Number 80

ICMP: Type Any

Figure 9.9. Self-Access ACL Configuration Example

9.6.2 Modify a Self-Access Rule

To modify a Self-Access rule, follow the instructions below:

1. Open the Self-Access Rule configuration page, as shown in Figure 9.8, by double clicking the **Router Setup ➔ Self Access ACL** menu.
2. Click on the ✏ icon of the Self-Access rule to be modified in the **Existing Self-Access ACL** table or select the Self-Access ACL from the **ID** drop-down list.

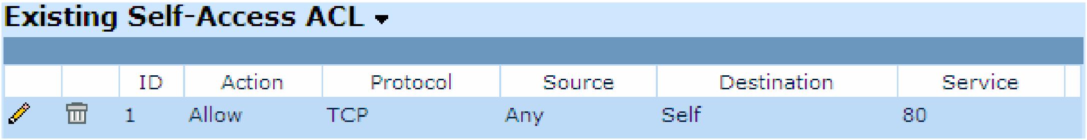
3. Make desired changes to any settings..
4. Click on the Modify button to save the changes. The new settings for this Self-Access rule will then be displayed in the **Existing Self-Access ACL** table located at the bottom half of the Self-Access ACL configuration page.

9.6.3 Delete a Self-Access Rule

To delete a Self-Access rule, open the Self-Access Rule configuration page by double clicking the **Router Setup ➔ Self Access ACL** menu and then click on the 🗑 icon of the rule to be deleted.

9.6.4 View Configured Self-Access Rules

To see existing Self-Access Rules, just open the Self-Access ACL configuration page by double clicking **Router Setup ➔ Self-Access ACL** menu.



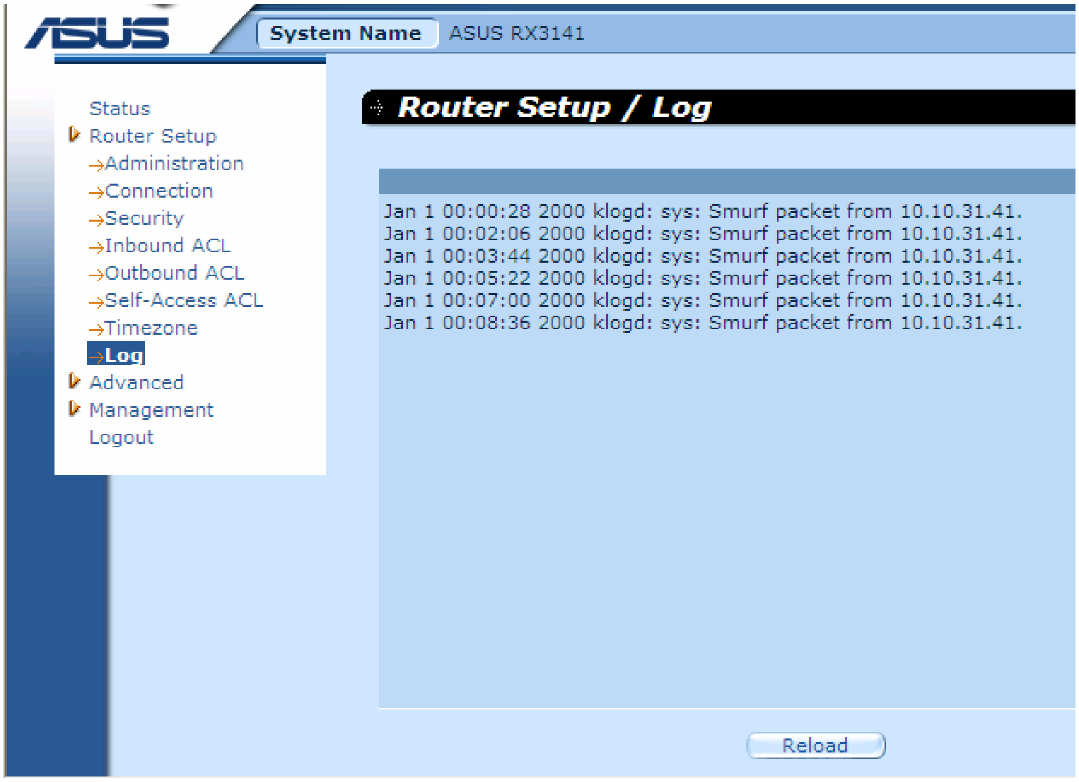
Existing Self-Access ACL ▾

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	TCP	Any	Self	80

Figure 9.10. Existing Self-Access ACL Rules

9.7 Firewall Log – (Router Setup ➔ Log)

You may open the firewall log page by double clicking **Router Setup ➔ Log** menu to see any logged events for any security breaches. Figure 9.11 shows a sample firewall log. You may click on the Reload button at the bottom of the Log page to see the updated log messages.



```
Jan 1 00:00:28 2000 klogd: sys: Smurf packet from 10.10.31.41.
Jan 1 00:02:06 2000 klogd: sys: Smurf packet from 10.10.31.41.
Jan 1 00:03:44 2000 klogd: sys: Smurf packet from 10.10.31.41.
Jan 1 00:05:22 2000 klogd: sys: Smurf packet from 10.10.31.41.
Jan 1 00:07:00 2000 klogd: sys: Smurf packet from 10.10.31.41.
Jan 1 00:08:36 2000 klogd: sys: Smurf packet from 10.10.31.41.
```

Figure 9.11 Sample Firewall Log

9.7.1 Log Format

Two types of log are supported by the RX3141 – system security log and firewall access control log. They are designated by the two keywords, sys and fw respectively. The log format is best explained by examples:**System Security Log Example:**

Jan 1 00:01:22 2000 klogd: sys: TCP XMAS/NULL packet from 192.168.1.100.

Explanation: **Jan 1 00:01:22 2000** indicates the time of the attack; **klogd: sys**, this attack is detected by the system security model; **TCP XMAS/NULL**, the type of attack detected; **192.168.1.100**, source of the attack.

Firewall Access Control Log Example:

Jan 1 00:03:11 2000 klogd: fw: OUTBOUND rule=1 allow icmp from 192.168.1.100 to 211.1.1.1 type=8 code=0 id=512Explanation: **Jan 1 00:03:11 2000** indicates the time of the access; **klogd: fw**, indicates the log is related to firewall access control; **OUTBOUND**, the direction of the traffic; **rule=1**, the rule that matches the IP information of the traffic; **allow**, action taken by the firewall; **icmp**, protocol type of the traffic; **192.168.1.100**, source of the traffic; **211.1.1.1**, destination of the traffic; type=8, ICMP message type; code=0, ICMP message code; id=512, ICMP message ID.

10 Virtual Sever and Special Application

This chapter describes the configuration procedures for:

- Virtual Server
- Special Application

NAT is the technology used to support the above applications.

10.1 NAT Overview

Network Address Translation allows use of a single device, such as the RX3141, to act as an agent between the Internet (public network) and a local (private) network. This means that a NAT IP address can represent an entire group of computers to any entity outside a network. Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. Because of the translation of IP addresses, NAT also conceals true network address from privy eyes and provide a certain degree security to the local network.

10.1.1 NAPT (Network Address and Port Translation) or PAT (Port Address Translation)

Also called IP Masquerading, this feature maps many internal hosts to one globally valid Internet address. The mapping contains a pool of network ports to be used for translation. Every packet is translated with the globally valid Internet address and the port number is translated with an un-used port from the pool of network ports. Figure 10.1 shows that all the hosts on the local network gain access to the Internet by mapping to only one globally valid IP address and different port numbers from a free pool of network ports.

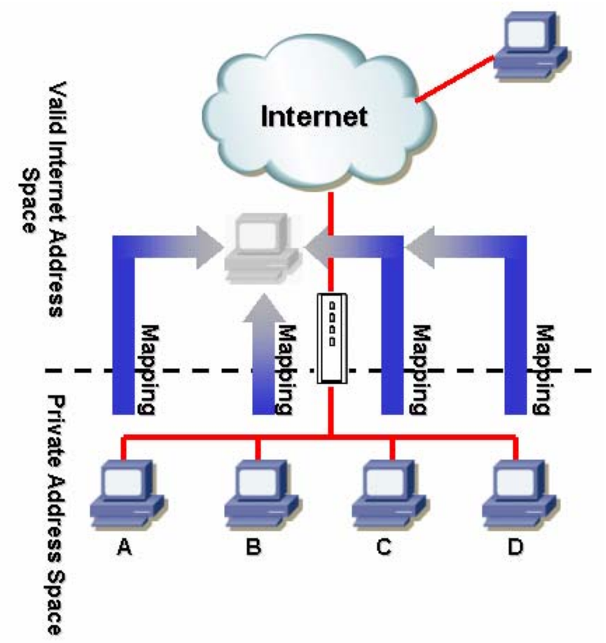


Figure 10.1 NAPT – Map Any Internal PCs to a Single Global IP Address

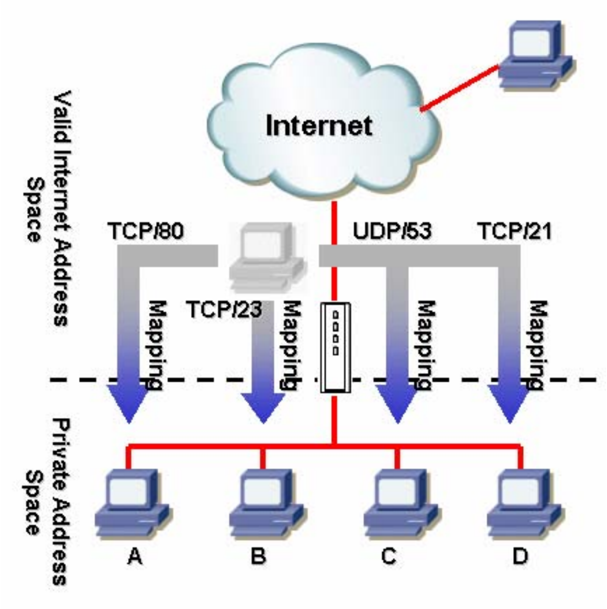


Figure 10.2 Reverse NAPT – Relayed Incoming Packets to the Internal Host Base on the Protocol, Port Number or IP Address

10.1.2 Reverse NAPT / Virtual Server

Reverse NAPT is also called inbound mapping, port mapping, or virtual server. Any packet coming to the RX3141 can be relayed to the internal host based on the protocol, port number and/or IP address specified in the ACL rule. This is useful when multiple services are hosted on different internal hosts. Figure 10.2 shows that web server (TCP/80) is hosted on PC A, telnet server (TCP/23) on PC B, DNS server (UDP/53) on PC C and FTP server (TCP/21) on PC D. This means that the inbound traffic of these four services will be directed to respective host hosting these services.

10.2 Configure Virtual Server

Virtual server allows you to configure up to ten public servers, such as a Web, E-mail, FTP server and etc. accessible by external users of the Internet. Each service is provided by a dedicated server configured with a fixed IP Address. Although the internal service addresses are not directly accessible to the external users, the router is able to identify the service requested by the service port number and redirects the request to the appropriate internal server.

Note

RX3141 supports only one server of any particular type at a time.

10.2.1 Virtual Server Configuration Parameters

Table 10.1 describes the configuration parameters available for virtual server configuration.

Table 10.1. Virtual Server Configuration Parameters

Setting	Description
Enable	Select an application from the list of pre-configured applications. The corresponding protocol and the redirect port range will be automatically selected. Select "Manual Setting" if you want to configure the settings yourself. To activate the policy, make sure the check box is checked. For a list of pre-configured applications, please refer to Table 10.2.
Protocol	This option allows you to select protocol type from a drop-down list. Available settings are All, TCP, UDP, TCP/UDP, and ESP.
Redirect Port Range	Enter the desired port numbers.
To IP Address	Enter the server IP address.

Table 10.2. Port Numbers for Popular Applications

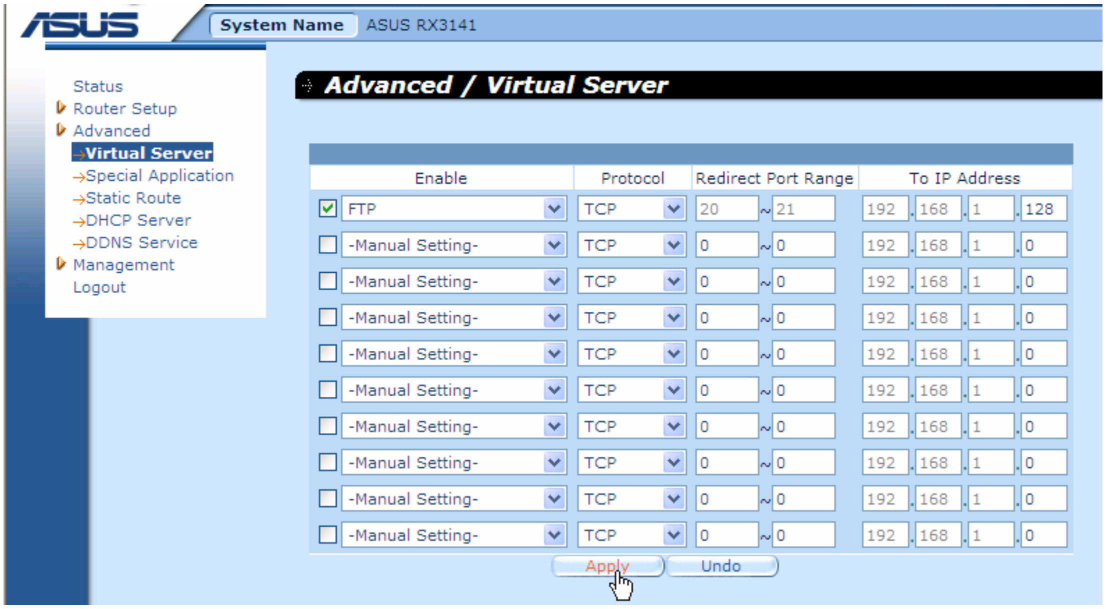
Application	Service Port Numbers
AOE II(Server)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648, 56800,24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(ALG)-21
GOPHER	TCP 70-70
HTTP	TCP 80-80
HTTP8080	TCP 8080-8080
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mIrc	6601-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 49500-49700
Netmeeting File Transfer	TCP 1503-1503

Application	Service Port Numbers
Netmeeting or VOIP	1503-1503, 1720 (ALG)
NEWS	TCP 119-119
PC Anywhere	TCP: 5631
PC Anywhere	TCP: 5631, UDP: 5632
POP3	TCP 110-110
Powwow Chat	13223-13223
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5900

10.2.2 Virtual Server Example

Following describes the procedure to setup a FTP server:

1. Open the Virtual Server configuration page, as shown in Figure 10.3, by double clicking the **Advanced ➔ Virtual Server** menu.
2. Select **FTP** from the Enable drop-down list and the check the check box to activate this policy. Note that the protocol and the redirect port range are automatically selected.
3. Enter the IP address of the FTP server. Note that this IP address is a private IP address.
4. Click Apply to save the settings.



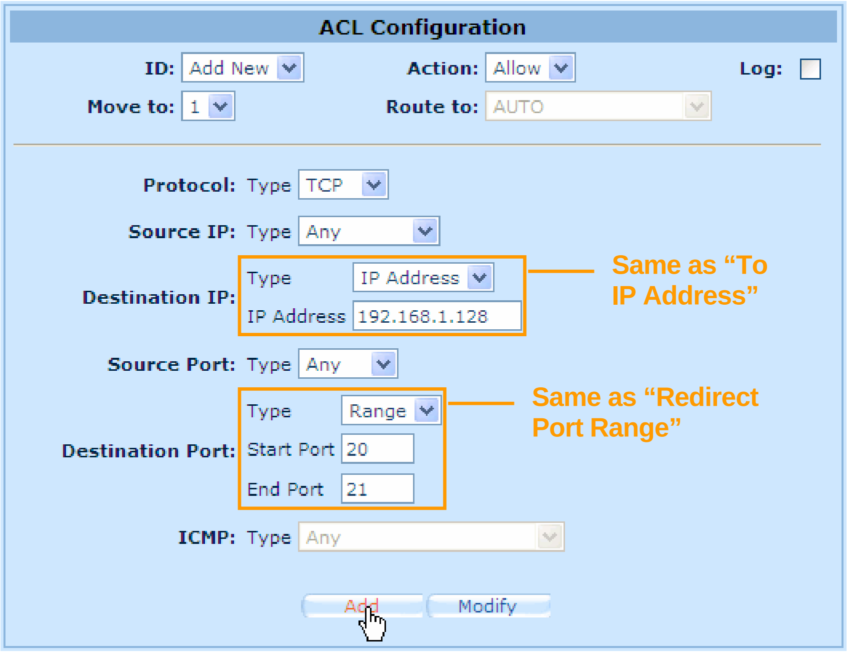
System Name ASUS RX3141

Advanced / Virtual Server

Enable		Protocol	Redirect Port Range	To IP Address
☑	FTP	TCP	20 ~ 21	192 . 168 . 1 . 128
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0
☐	-Manual Setting-	TCP	0 ~ 0	192 . 168 . 1 . 0

Figure 10.3. Virtual Server Example

5. For security concerns, the RX3141 denies all the access requests from the external users unless a proper inbound ACL rule is setup for each virtual server to allow external users to access the internal servers set up in the Virtual Server configuration page. For example, if you want to allow any one in the external network to access the FTP server, define an inbound ACL rule as configured in Figure 10.4. Note that the destination IP address is the IP address entered in the "**To IP Address**" and the destination port is the port numbers entered in the "**Redirect Port Range**" in the Virtual Server configuration page. If you want to restrict access to the FTP server from particular IP addresses, change the settings for the source IP in the inbound ACL rule. For example, if source IP in the inbound ACL rule is configured as 198.175.2.10, the RX3141 will deny all the external access to the FTP server except those from this particular IP address. For detail information about configuring an inbound ACL rule, please refer to the section **9.4 Configuring Inbound ACL Rules**.



ACL Configuration

ID: Add New
Action: Allow
Log: □
Move to: 1
Route to: AUTO

Protocol: Type TCP
Source IP: Type Any
Destination IP: Type IP Address
IP Address 192.168.1.128
Source Port: Type Any
Destination Port: Type Range
Start Port 20
End Port 21
ICMP: Type Any

Same as "To IP Address"

Same as "Redirect Port Range"

Figure 10.4. Virtual Server Example – Inbound ACL RuleConfigure Special Application

Some applications use multiple TCP/UDP ports to transmit data. Due to the NAT operation, these applications cannot work with the router. Special Application setting allows some of these applications to work properly.

Note

Only one PC can use one particular special application at any time.

10.2.3 Special Application Configuration Parameters

Table 10.1 describes the configuration parameters available for Special Application configuration.

Table 10.3. Special Application Configuration Parameters

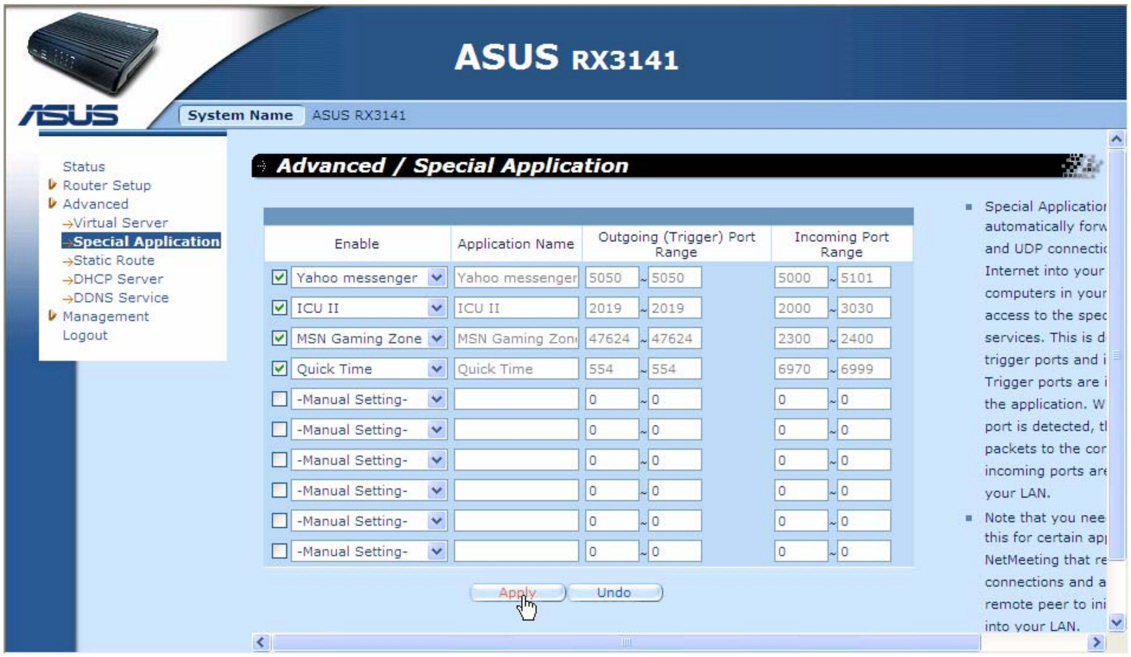
Setting	Description
Enable	Select an application from the list of pre-configured applications. The corresponding protocol and the redirect port range will be automatically selected. Select "Manual Setting" if you want to configure the settings yourself. To activate the policy, make sure the check box is checked.

Setting	Description
Application Name	The name identifying the application.
Outgoing (Trigger) Port Range	The port range this application uses when it sends outbound packets. The outgoing port numbers act as the trigger. When the router detects the outgoing packets with these port numbers, it will allow the corresponding inbound packets with the incoming port numbers specified in the **Incoming Port Range** field to pass through the router. For a list of port numbers used by some popular applications, please refer to Table 10.4.
Incoming Port Range	The port range that the corresponding inbound packet used. For a list of port numbers used by some popular applications, please refer to Table 10.4.

Table 10.4. Port Numbers for Popular Applications

Application	Outgoing Port Number	Incoming Port Range
Battle.net	6112	6112
DialPad	7175	51200,51201,51210
ICU II	2019	2000-2038, 2050-2051, 2069,2085,3010-3030
MSN Gaming Zone	47624	2300-2400,28800-29000
PC to Phone	12053	12120,12122,24150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020

10.2.4 Special Application Example



System Name ASUS RX3141

Advanced / Special Application

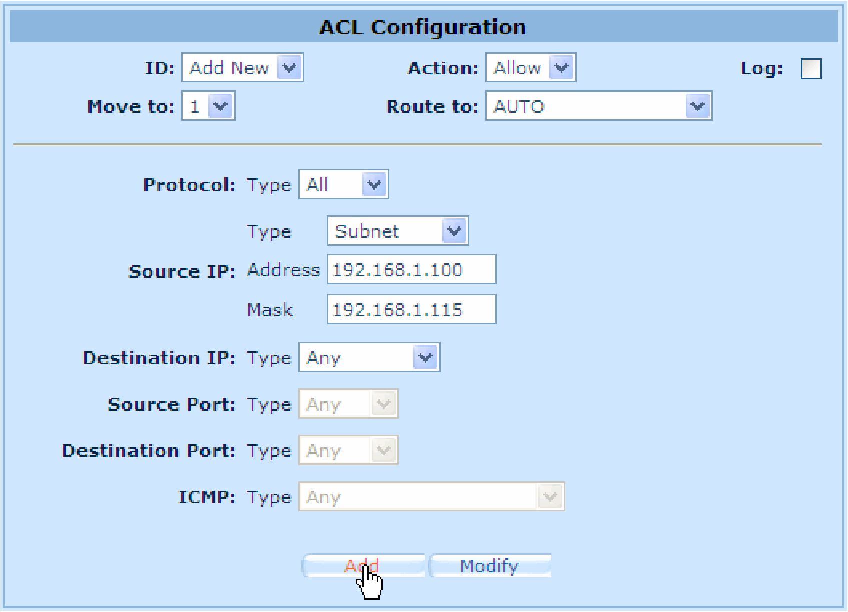
Enable		Application Name	Outgoing (Trigger) Port Range		Incoming Port Range	
☑	Yahoo messenger	Yahoo messenger	5050	~5050	5000	~5101
☑	ICU II	ICU II	2019	~2019	2000	~3030
☑	MSN Gaming Zone	MSN Gaming Zon	47624	~47624	2300	~2400
☑	Quick Time	Quick Time	554	~554	6970	~6999
□	-Manual Setting-		0	~0	0	~0
□	-Manual Setting-		0	~0	0	~0
□	-Manual Setting-		0	~0	0	~0
□	-Manual Setting-		0	~0	0	~0
□	-Manual Setting-		0	~0	0	~0
□	-Manual Setting-		0	~0	0	~0

- Special Applicatio
automatically forw
and UDP connecti
Internet into your
computers in your
access to the spec
services. This is d
trigger ports and i
Trigger ports are i
the application. W
port is detected, t
packets to the cor
incoming ports ar
your LAN.
- Note that you nee
this for certain ap
NetMeeting that re
connections and a
remote peer to ini
into your LAN.

Figure 10.5. Special Application Configuration Page

Following describes the procedure to setup a special application for Quick Time.

1. Open the Special Application configuration page, as shown in Figure 10.5, by double clicking the **Advanced ➔ Special Application** menu.
2. Select **Quick Time** from the Enable drop-down list and the check the check box to activate this policy. Note that the application name, outgoing and incoming port range are automatically selected.
3. Click Apply to save the settings.
4. The RX3141 has a default outbound ACL rule to forward all the outbound traffic to the external networks. This default outbound ACL rule allows any one to use application defined in the Special Application configuration page. If this is what you want, skip this step. However, for security concerns or any other reasons, you may want to restrict the use of these applications to a particular group of users. Then configure an outbound ACL rule to control outbound access as illustrated in Figure 10.6. This example restricts the access to hosts in the IP address range from 192.168.1.110 to 192.168.1.115. Note that you must remove the default firewall outbound ACL rule for the access restriction to work because the default outbound ACL rule allows any one to use any applications setup in the Special Application configuration page. To delete the default outbound ACL rule, just click the 🗑 icon in front of the default ACL rule in the Outbound ACL Rule table located in the Outbound ACL Rule configuration page (as shown in Figure 10.7). For details on configuring an outbound ACL rule, please refer to the section **9.5 Configuring Outbound ACL Rules**.



ACL Configuration

ID: Add New Action: Allow Log: □

Move to: 1 Route to: AUTO

Protocol: Type All

Source IP: Type Subnet
Address 192.168.1.100
Mask 192.168.1.115

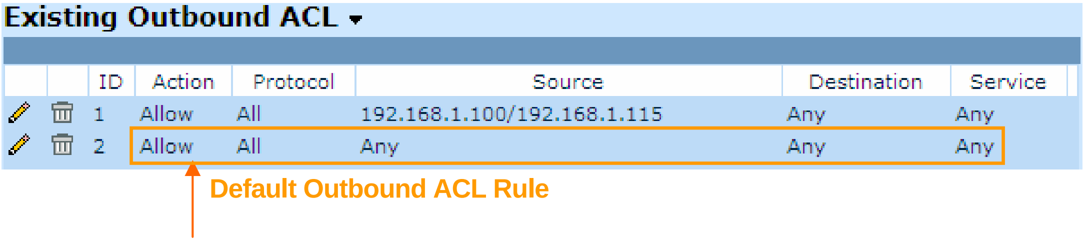
Destination IP: Type Any

Source Port: Type Any

Destination Port: Type Any

ICMP: Type Any

Figure 10.6. Special Application Example – Outbound ACL Rule



Existing Outbound ACL ▾

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	All	192.168.1.100/192.168.1.115	Any	Any
✎	🗑	2	Allow	All	Any	Any	Any

Default Outbound ACL Rule

Figure 10.7. Outbound ACL Rule Table

11 System Management

This chapter describes the following administrative tasks that you can perform using the Configuration Manager:

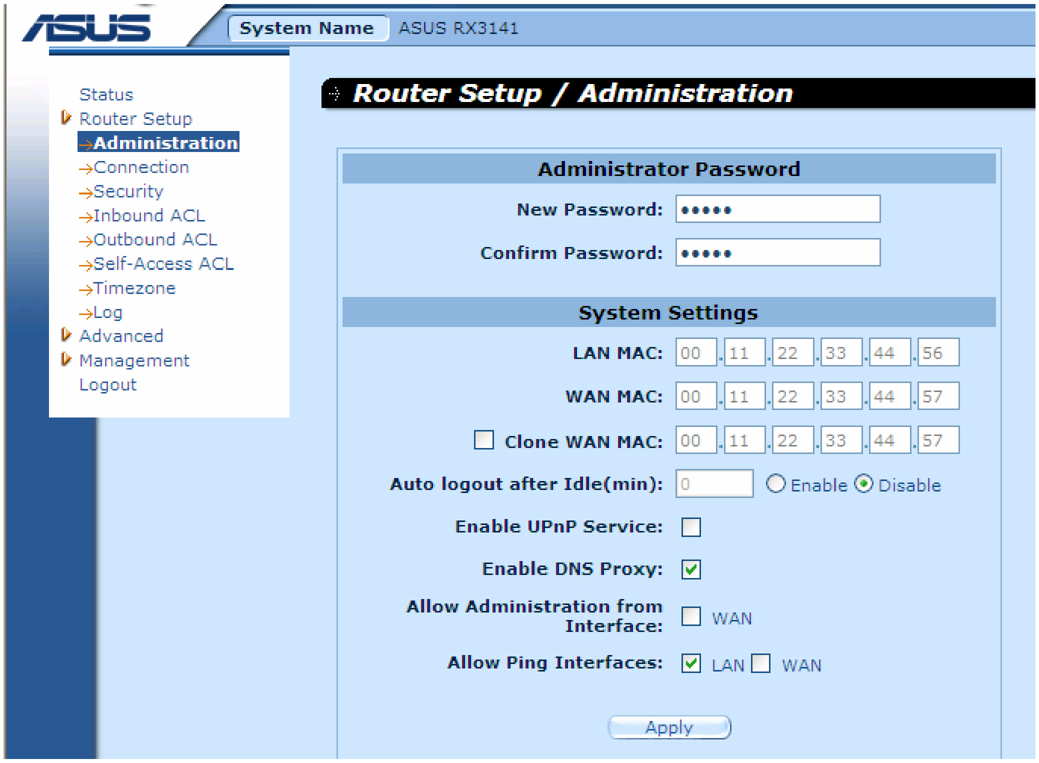
- Modify password and system-wide settings
- View system information
- Modify system date and time
- Reset system configuration
- Reboot system
- Update firmware
- Backup/restore system configuration

11.1 Login Password and System-Wide Settings

The first time you log into the Configuration Manager, you use the default username and password (admin and *admin*).

Note

> *This username and password is only used for logging into the Configuration Manager; it is not the same login password that you use to connect to your ISP.*



Router Setup / Administration

Administrator Password

New Password: •••••

Confirm Password: •••••

System Settings

LAN MAC: 00 . 11 . 22 . 33 . 44 . 56

WAN MAC: 00 . 11 . 22 . 33 . 44 . 57

□ Clone WAN MAC: 00 . 11 . 22 . 33 . 44 . 57

Auto logout after Idle(min): 0 ○ Enable ● Disable

Enable UPnP Service: □

Enable DNS Proxy: ☑

Allow Administration from Interface: □ WAN

Allow Ping Interfaces: ☑ LAN □ WAN

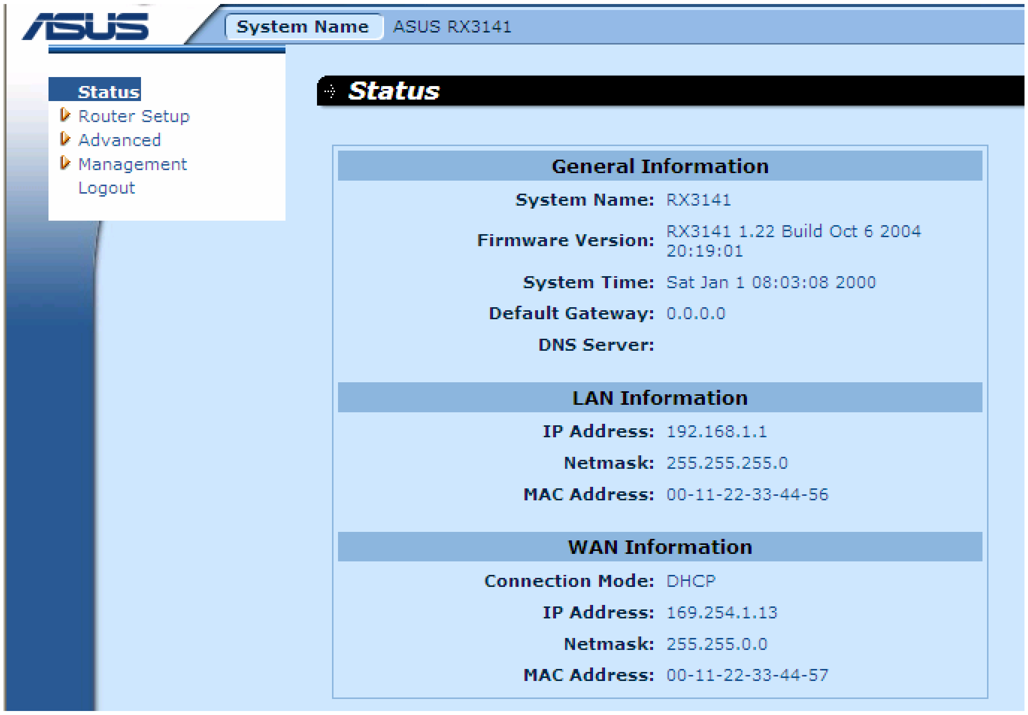
Figure 11.1. System Administration Configuration Page

System Administration configuration page, as shown in Figure 11.1, allows you to change login password and other global settings for RX3141. Follow the steps below to change password and/or system-wide settings:

1. Open the System Administration configuration page, as shown in Figure 11.1, by double clicking the **Router Setup ➔ Administration** menu.
2. Changing login password
    a) Type the new password in the New Password text field and again in the Confirm Password text field. The password can be up to 16 characters long. When logging in, you must type the new password in the same upper and lower case characters that you enter here.
3. Clone the MAC address for WAN
    a) If you had previously registered a specific MAC address with your ISP for Internet access, enter the registered MAC address here; otherwise, keep the default setting – the factory assigned MAC address for the WAN port.
4. Auto logout after idle (min): Click "Enable" radio button and enter in-activity time out period to enable this option; otherwise, click on the "Disable" radio button, or enter 0 in the text field to diable this option. When this option is enabled, you will be automatically disconnected from the router when the idle timer expires during system configuration via your browser. You'll have to log into the RX3141 again if you want to continue system configuration.
5. Enable UPnP service: check or uncheck the check box to enable or disable UpnP service.
6. Enable DNS Proxy: Check or uncheck the check box to enable or disable DNS proxy service.
7. Allow Administration from Interface: check or uncheck the check box to enable or disable remote management via WAN port.
8. Allow Ping Interface: You may check the LAN and/or WAN check box to allow ping to the RX3141 from the LAN or WAN interface. It is recommended that you enable this option for the LAN only.
9. Click on Apply button to save the settings.

11.2 Viewing System Information

System Information page displays whenever you log into RX3141. It contains information for the overall system settings.



General Information

System Name: RX3141

Firmware Version: RX3141 1.22 Build Oct 6 2004 20:19:01

System Time: Sat Jan 1 08:03:08 2000

Default Gateway: 0.0.0.0

DNS Server:

LAN Information

IP Address: 192.168.1.1

Netmask: 255.255.255.0

MAC Address: 00-11-22-33-44-56

WAN Information

Connection Mode: DHCP

IP Address: 169.254.1.13

Netmask: 255.255.0.0

MAC Address: 00-11-22-33-44-57

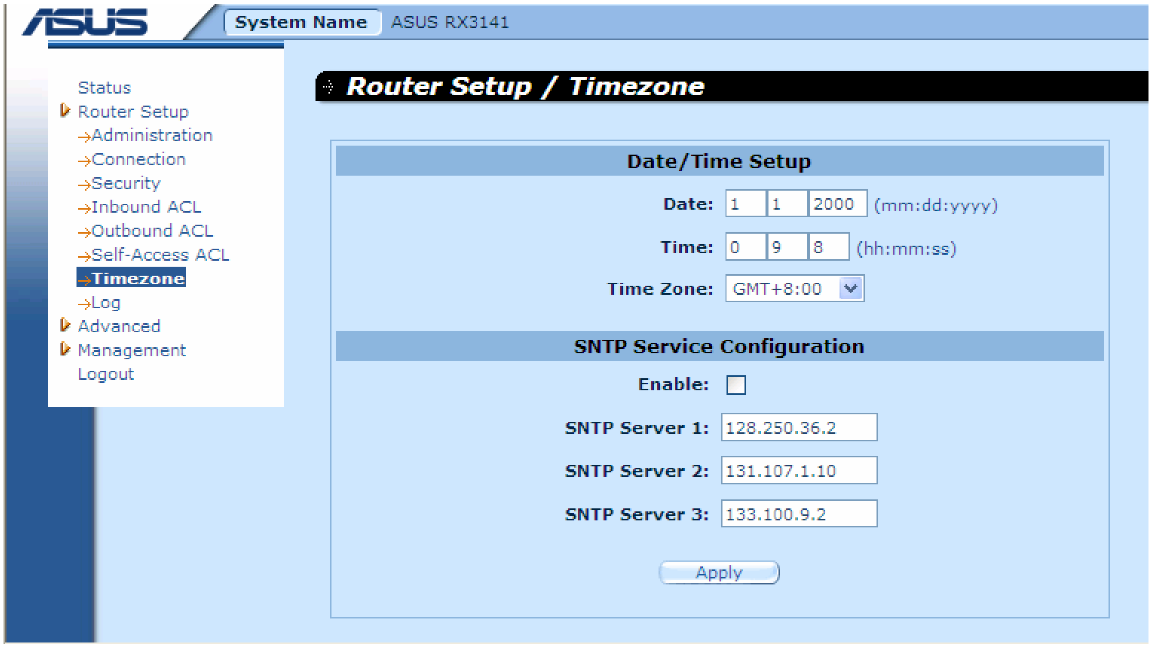
Figure 11.2. System Status Page

11.3 Setup Date and Time

RX3141 keeps a record of the current date and time, which it uses to calculate and report various data. However, there is no real time clock inside RX3141; RX3141 relies on external time servers to maintain correct time. RX3141 allows you to configure up to three external time servers. Make sure that the "**Enable**" check box is checked to activate the SNTP (Simple Network Time Protocol) service for time keeping.

Note

Changing the date and time on RX3141 does not affect the date and time on your PCs.



System Name: ASUS RX3141

Router Setup / Timezone

Date/Time Setup

Date: 1 1 2000 (mm:dd:yyyy)

Time: 0 9 8 (hh:mm:ss)

Time Zone: GMT+8:00

SNTP Service Configuration

Enable: □

SNTP Server 1: 128.250.36.2

SNTP Server 2: 131.107.1.10

SNTP Server 3: 133.100.9.2

Apply

Figure 11.3. Date and Time Configuration Page

The maintain accurate time for the router:

1. Open the Date and Time configuration page, as shown in,Figure 11.3 by double clicking the **Router Setup ➔ Timezone** menu.
2. Select your time zone from the drop-down list.
3. Check the **Enable** check box to activate the SNTP (Simple Network Time Protocol) service.
4. Enter IP addresses for the SNTP servers that will be used to update the system time.
5. Click on Apply button to save the settings.

You can manually enter the correct time, however the time will be reset to the default time, 1/1/2000 00:00:00, after system is rebooted or powered off.

11.3.1 View the System Date and Time

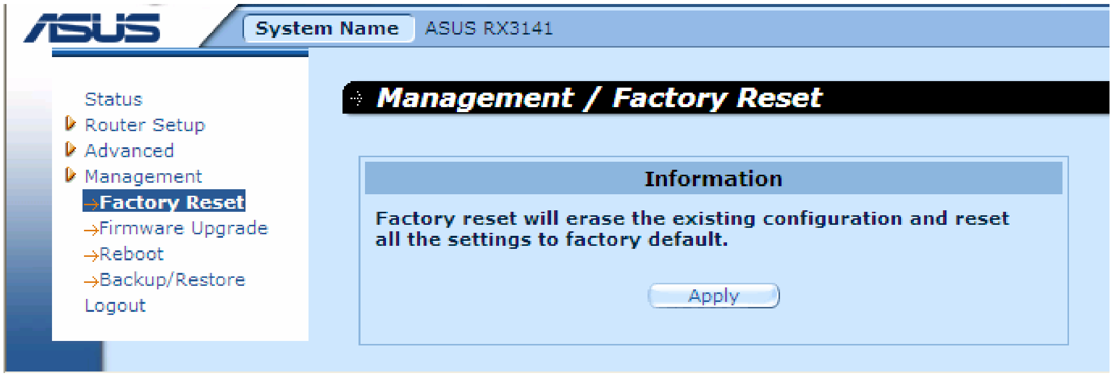
To view the updated system date and time, log into Configuration Manager, click the **Router Setup → Timezone** menu. Note that the system will go back to the default time, 1/1/2000 00:00:00, if SNTP service is not enabled or none of the configured SNTP servers are not accessible after system is rebooted or powered off.

11.4 Reset to Factory Default Settings

11.4.1 Reset to Factory Default Settings using GUI

At times, you may want to revert to the factory default settings to eliminate problems resulted from incorrect system configuration. Follow the steps below to reset system configuration:

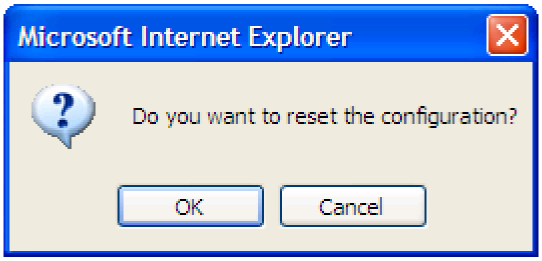
1. Log into Configuration Manager by double clicking the **Management → Factory Reset** menu. The Default Settings Configuration page displays, as shown in Figure 11.4.



Factory reset will erase the existing configuration and reset all the settings to factory default.

Figure 11.4. Factory Reset Page

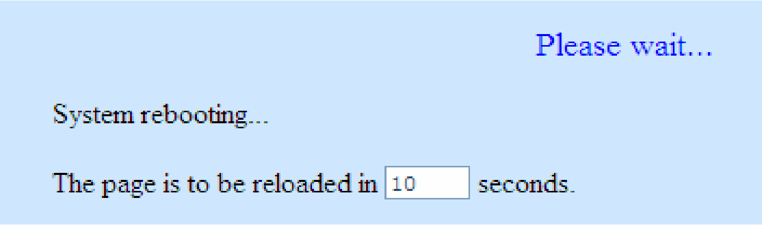
2. Click on Apply button to set the system configuration back to factory default.
3. A dialog window as shown in Figure 11.5 will pop up to ask for confirmation. Click on the OK button to proceed; otherwise, click on the Cancel button to cancel the action.
4.



Do you want to reset the configuration?

Figure 11.5. Factory Reset Confirmation

5. RX3141 will then reboot thereafter to make the factory default configuration in effect. Note a count down timer such as the one shown in Figure 11.6 will display to indicate when the reboot process will be completed.



Please wait…

System rebooting…

The page is to be reloaded in 10 seconds.

Figure 11.6. Factory Reset Count Down Timer

11.4.2 Reset to Factory Default Settings using the Reset Button

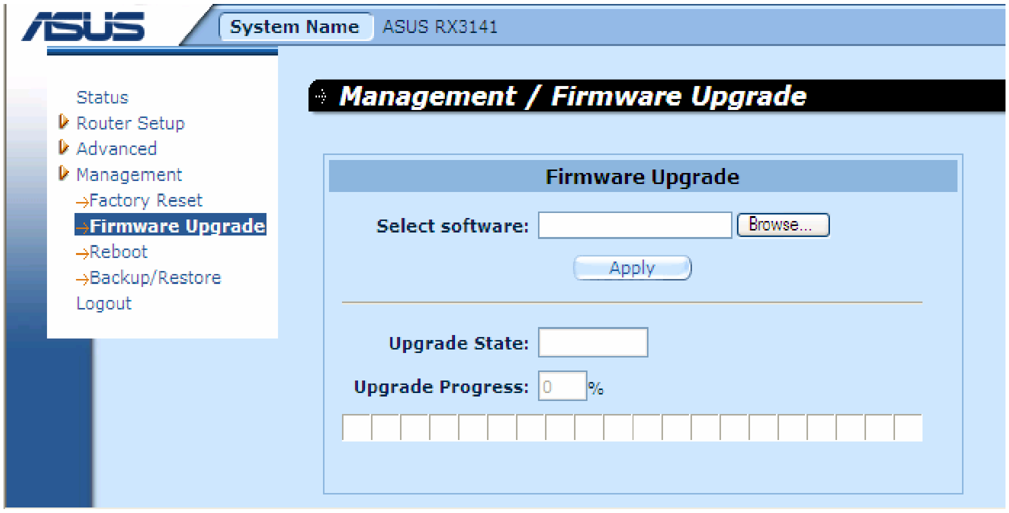
Note

Sometimes, you may find that you have no way to access the RX3141, e.g. you forget your password or the IP address of RX3141. The only way out in this scenario is to reset the system configuration to the factory default by pressing the reset button (located on the rear panel the router) for at least 5 seconds. The system configuration will be reverted back to the factory default settings after RX3141 is rebooted.

11.5 Firmware Upgrade

ASUSTeK may from time to time provide you with an update to the firmware running on the RX3141. All system software is contained in a single file, called an *image*. Configuration Manager provides an easy way to upload the new firmware image. To upgrade the image, follow this procedure:

1. Open the Firmware Upgrade page, as shown in Figure 11.7, by double clicking the **Management ➔ Firmware Upgrade** menu.



System Name ASUS RX3141

Management / Firmware Upgrade

Firmware Upgrade

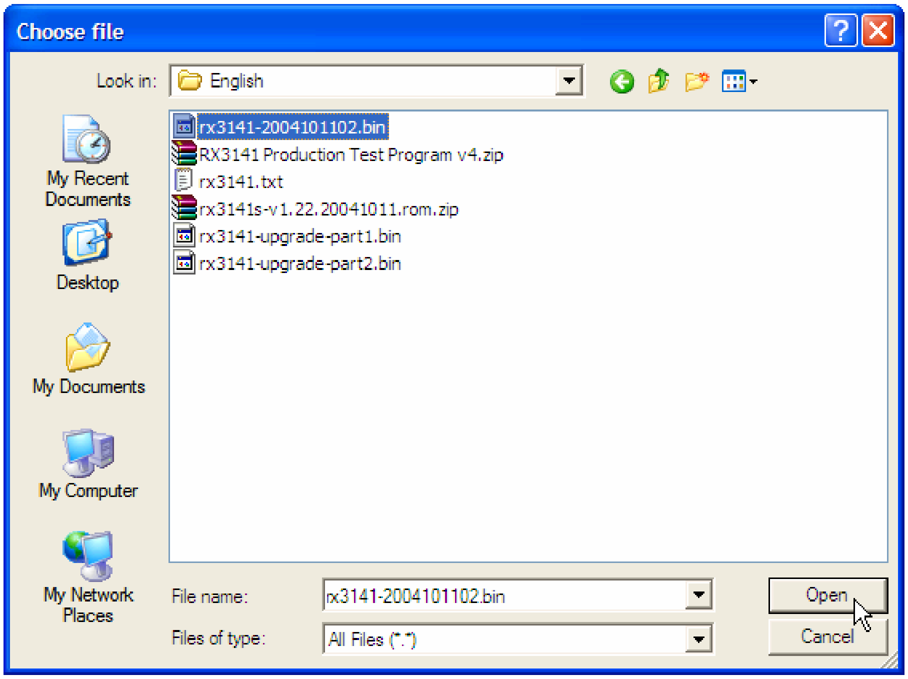
Select software:

Upgrade State:

Upgrade Progress: 0 %

Figure 11.7. Firmware Upgrade Page

2. In the Firmware text box, enter the path and name of the firmware image file. Alternatively, you may click on Browse... button to open a file manager to search for the firmware image on your computer.



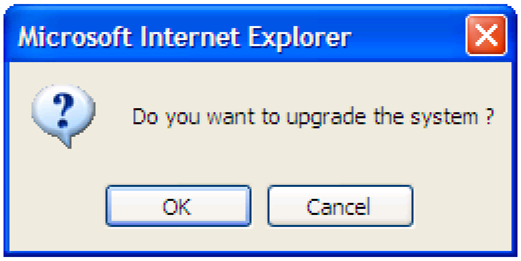
Look in: English

File name: rx3141-2004101102.bin

Files of type: All Files (*.*)

Figure 11.8. File Manager

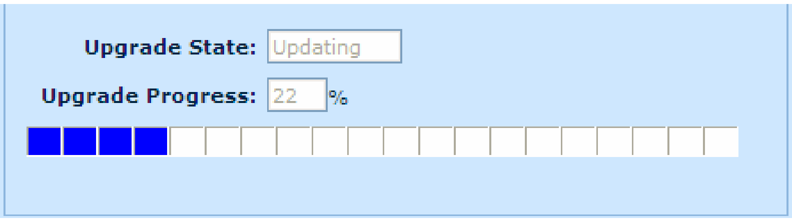
3. Click on Apply button to update the firmware. A dialog window, such as the one below, will pop up to ask for confirmation of the firmware upgrade. Click the OK button to proceed; otherwise, click the Cancel button to cancel the action.



Do you want to upgrade the system ?

Figure 11.9. Firmware Upgrade Confirmation

4. Firmware upgrade status and progress will be shown as illustrated in .

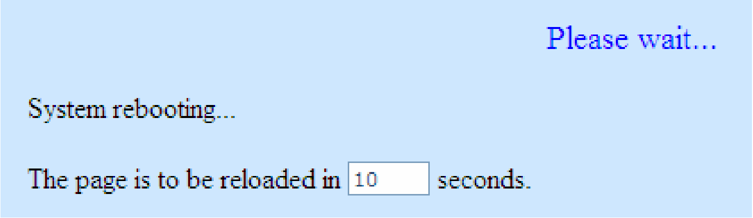


Upgrade State: Updating

Upgrade Progress: 22 %

Figure 11.10. Firmware Upgrade Status

5. A count down timer will display, as shown in Figure 11.11, after the firmware upgrade is completed. You'll be reconnected back to RX3141 when the counter returns to zero. You may need to manually connect back to the RX3141 if you are not connected back to RX3141 automatically.



Please wait...

System rebooting...

The page is to be reloaded in 10 seconds.

Figure 11.11. Firmware Upgrade Count Down Timer

6. When you are reconnected to the RX3141, click **Status** menu to check if the new firmware is properly upgraded. Note that you probably need to clear the cache of your web browser to see the new System Information page. Following is the procedure to clear the browser cache for Microsoft Internet Explorer:

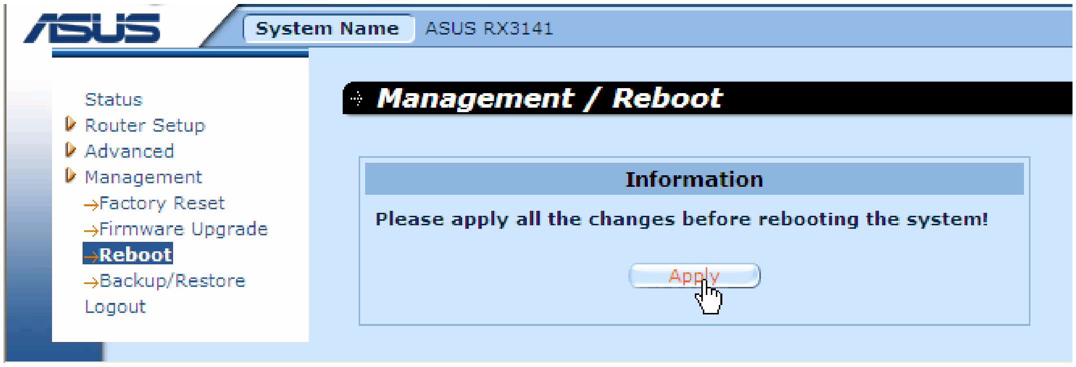
   a) Click on "Tools" menu

   b) Click on "Internet Options…" menu

   c) Click on "Delete Files…" button to clear the browser cache.

11.6 System Reboot

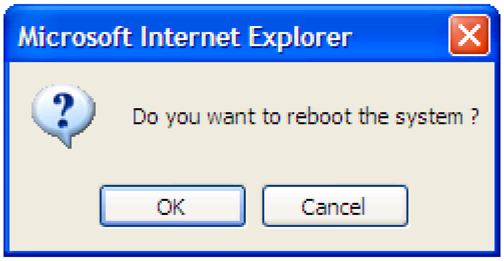
1. Open the System reboot page, as shown in Figure 11.12, by double clicking the **Management → Reboot** menu.
2. Click on the Apply button in the reboot the system.



Please apply all the changes before rebooting the system!

Figure 11.12. System Reboot Page

3. A dialog window will popup, as illustrated in Figure 11.13. Click on the OK button to proceed or click on the Cancel button to cancel.

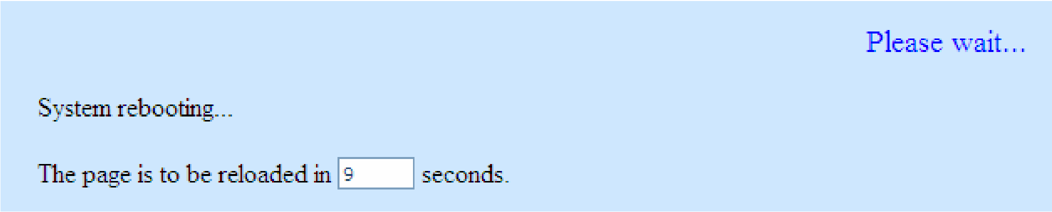


Do you want to reboot the system ?

Figure 11.13. System Reboot Confirmation

Your browser will be reconnected back to the RX3141 when the timer, as illustrated in

4. Figure 11.14, elapses.



Please wait...

System rebooting...

The page is to be reloaded in 9 seconds.

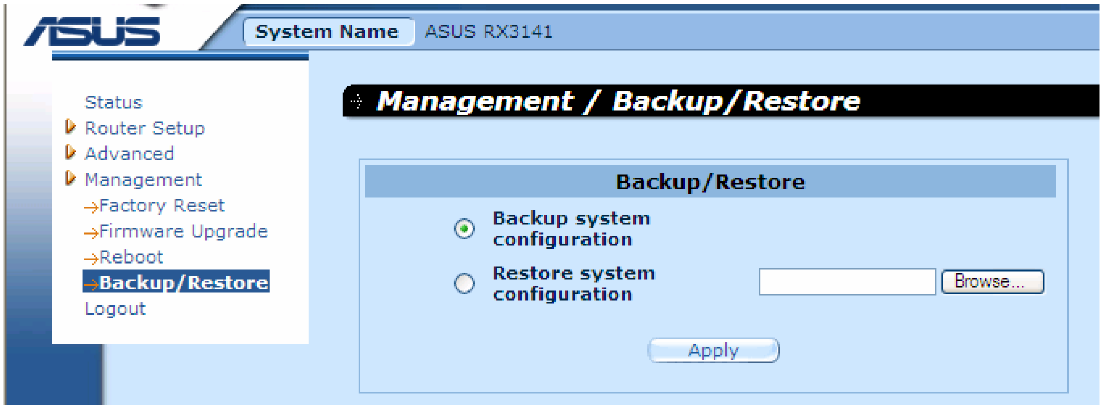
Figure 11.14. System Reboot Countdown Timer

11.7 . System Configuration Management

11.7.1 Backup System Configuration

Follow the steps below to backup system configuration:

1. Open the System Configuration Backup/Restore page, as illustrated in Figure 11.15, by double clicking the Management ➔ Backup/Restore menu.



Management / Backup/Restore

Backup/Restore

● Backup system configuration

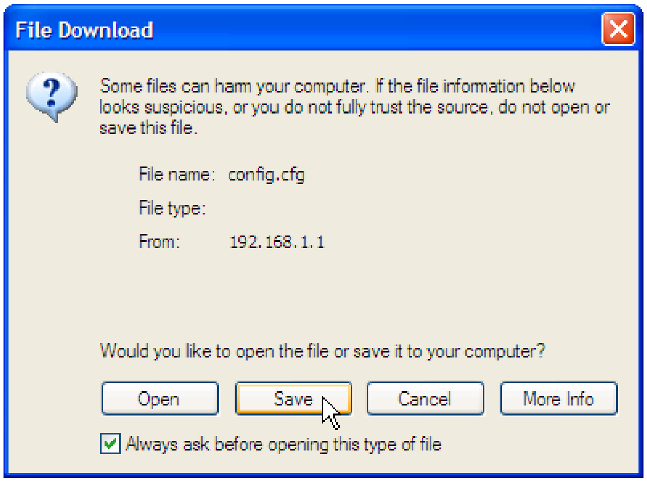
○ Restore system configuration

Figure 11.15. System Configuration Backup Page

2. Click the "**Backup system configuration**" radio button.

3. Click the Apply button to backup the system configuration.

4. If you are using Microsoft Windows, a "**File Download**" dialog window will pop up, click on the Save button as illustrated in Figure 11.16.



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: config.cfg

File type:

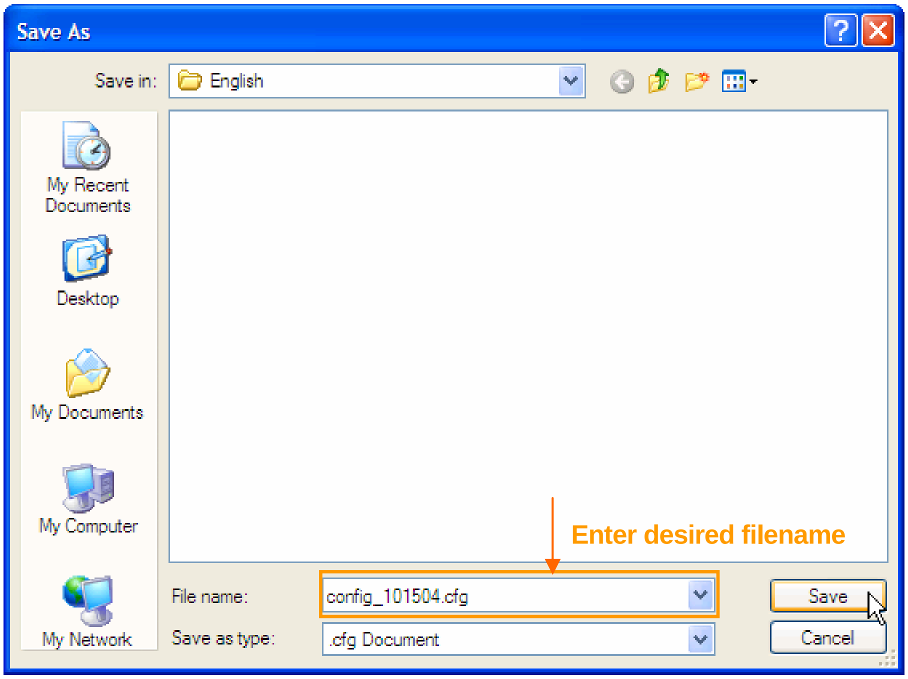
From: 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Figure 11.16. System Configuration Backup Page – File Download Dialog

5. Enter the desired filename for the backup configuration file as illustrated in Figure 11.17and click on the Save button to continue.



Save in: English

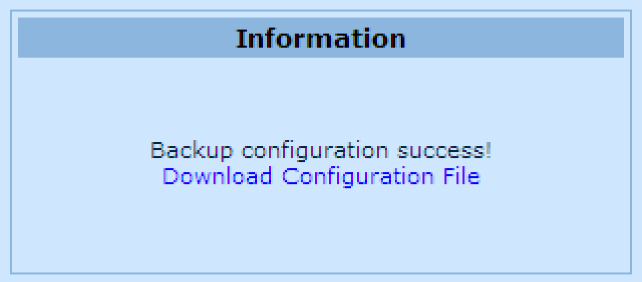
File name: config_101504.cfg

Save as type: .cfg Document

Enter desired filename

Figure 11.17. System Configuration Backup Page – Save As Dialog

6. Finally, a message, as shown in Figure 11.18, will display to let you know whether the system configuration is successfully saved to your computer.



Information

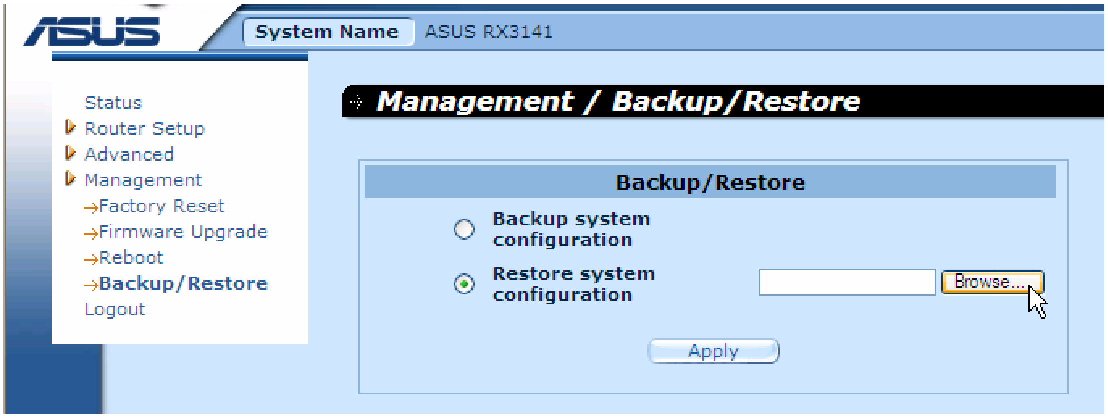
Backup configuration success!
Download Configuration File

Figure 11.18. System Configuration Backup Status

11.7.2 Restore System Configuration

Follow the steps below to backup system configuration:

1. Open the **System Configuration Backup/Restore** configuration page by double clicking the **Management ➔ Backup/Restore** menu.
2. Enter the path and filename of the system configuration file that you want to restore in the text field.



System Name: ASUS RX3141

Management / Backup/Restore

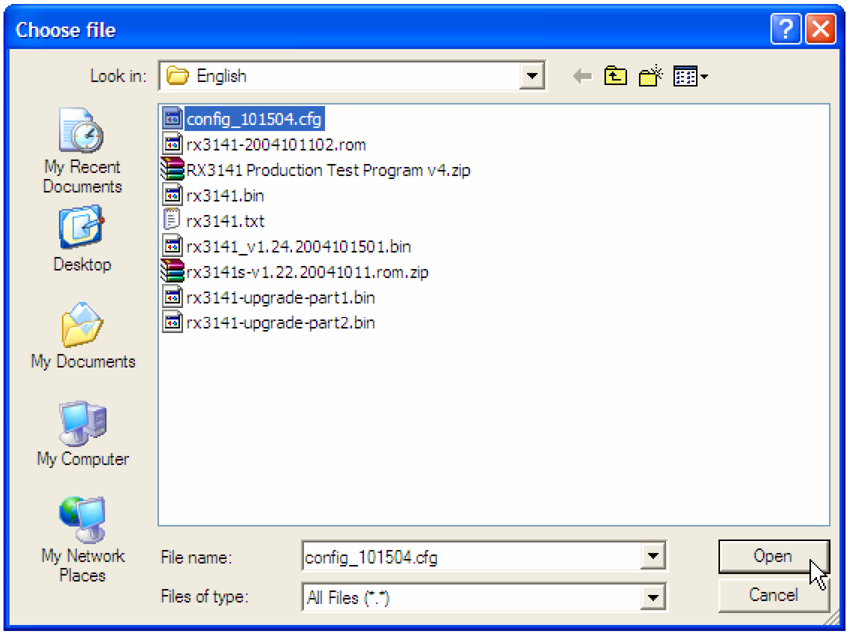
Backup/Restore

○ Backup system configuration

● Restore system configuration

Figure 11.19. System Configuration Restore Page

Alternatively, you may click on the Browse... button to search for the system configuration file on your computer. A window similar to the one shown in Figure 11.20 will pop up for you to select the configuration file to restore. Select the desired configuration file, and then click on the Open button to continue.



Choose file

Look in: English

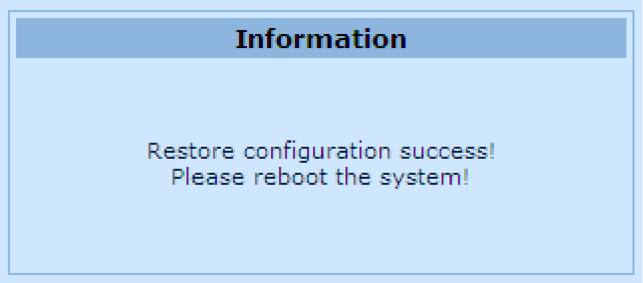
config_101504.cfg
rx3141-2004101102.rom
RX3141 Production Test Program v4.zip
rx3141.bin
rx3141.txt
rx3141_v1.24.2004101501.bin
rx3141s-v1.22.20041011.rom.zip
rx3141-upgrade-part1.bin
rx3141-upgrade-part2.bin

File name: config_101504.cfg

Files of type: All Files (*.*)

Figure 11.20. System Configuration Restore Page – Choose File Dialog

3. Click on Apply button to restore the system configuration.
4. A message will pop up, as illustrated in Figure 11.21, to let you know whether the system configuration is successfully restored. Note that you must reboot the RX3141 to make the new system configuration in effect.



Information

Restore configuration success!
Please reboot the system!

Figure 11.21. System Configuration Restore Status

12 IP Addresses, Network Masks, and Subnets

12.1 IP Addresses

Note

This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes. For details on this subject, see Appendix 12.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

12.1.1 Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- *Network ID*
  Identifies a particular network within the Internet or Intranet
- *Host ID*
  Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section). Table 12.1 shows the structure of an IP address.

Table 12.1. IP Address Structure

	Field1	**Field2**	**Field3**	**Field4**
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

12.2 Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:

field1 = 1-126:	Class A
field1 = 128-191:	Class B
field1 = 192-223:	Class C

  (field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

12.3 Subnet masks

Definition
mask

A mask *looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."*

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

Note

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask*. These masks are:*

Class A:	*255.0.0.0*
Class B:	*255.255.0.0*
Class C:	*255.255.255.0*

These are called default *because they are used when a network is initially configured, at which time it has no subnets.*

13 Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the RX3141, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Problem	Troubleshooting Suggestion
Power LED does not illuminate after product is turned on.	Verify that you are using the AC adapter provided with the device and that it is securely connected to the RX3141 and a wall socket/power strip.
LINK WAN LED does not illuminate after Ethernet cable is attached.	Verify that an Ethernet cable like the one provided is securely connected to the Ethernet port of your ADSL or cable modem and the WAN port of the RX3141. Make sure that your ADSL or cable modem is powered on. Wait 30 seconds to allow the RX3141 to negotiate a connection with your broadband modem.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the RX3141. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (100BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.
Internet Access	
PC cannot access Internet	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the RX3141's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: • Check that the gateway IP address on the computer is your public IP address (see the Quick Start Guide chapter, Part 2 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. • Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. • Verify that a Network Address Translation rule has been defined on the RX3141 to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules. Or, configure the PC to accept an address assigned by another device (see section 3.2 "Part 2 — Configuring Your Computers"). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool

Problem	Troubleshooting Suggestion
PCs cannot display web pages on the Internet.	Verify that the DNS server specified on the PCs is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.
Configuration Manager Program	
You forgot/lost your Configuration Manager user ID or password.	If you have not changed the password from the default, try using "admin" as the user ID and "admin" for the password. Otherwise, you can reset the device to the default configuration by following the instructions provided in section 11.4 "Reset to Factory Default Settings". **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
Cannot access the Configuration Manager program from your browser.	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the RX3141's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer 6.0 or newer. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the RX3141.
Changes to Configuration *Manager are not being retained.*	Be sure to click on Apply button to save any changes.

13.1 Diagnosing Problem using IP Utilities

13.1.1 ping

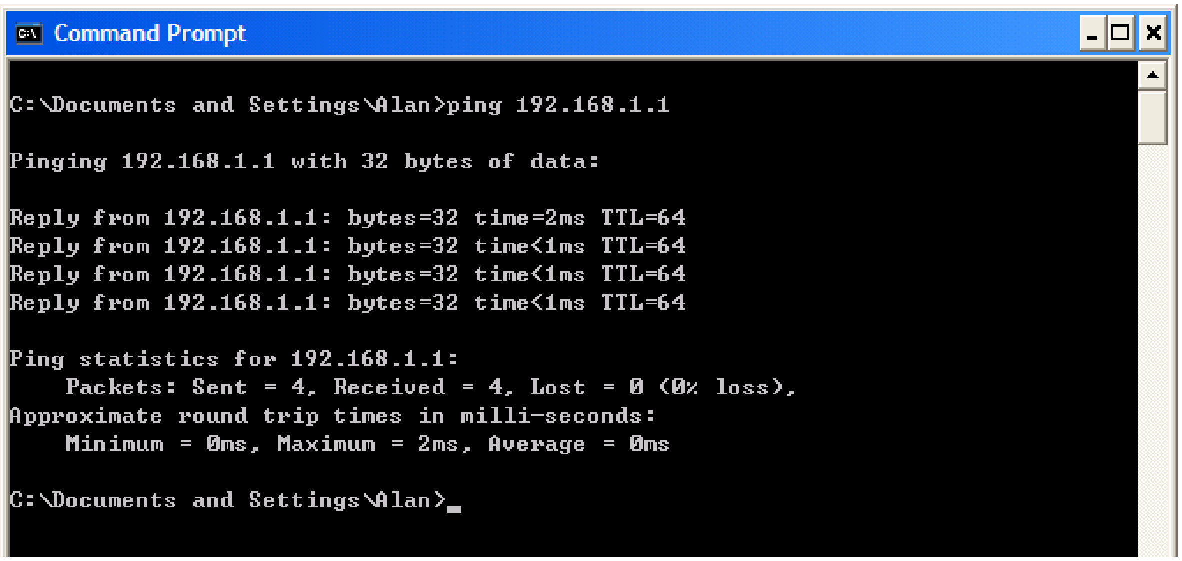
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

```
ping 192.168.1.1
```

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window displays like that shown in Figure 13.1.



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

Pinging 192.168.1.1 with 32 bytes of data:

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

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

C:\Documents and Settings\Alan>_
```

Figure 13.1. Using the ping Utility

If the target computer cannot be located, you will receive the message "Request timed out."

Using the ping command, you can test whether the path to the RX3141 is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

13.1.2 nslookup

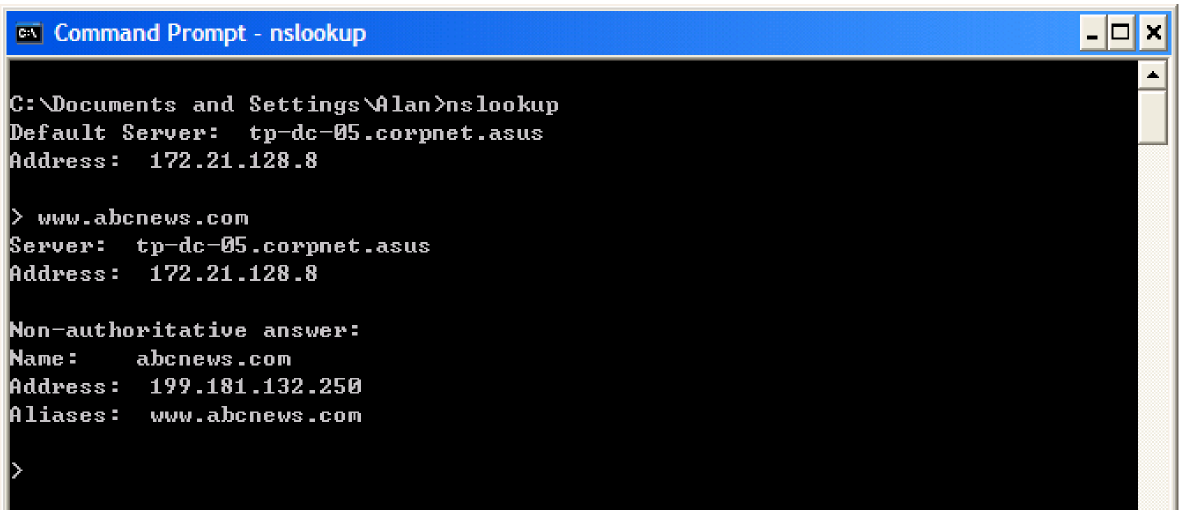
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

nslookup

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address you are interested in, such as www.absnews.com.

The window will display the associate IP address, if known, as shown in Figure 13.2.



```
C:\Documents and Settings\Alan>nslookup
Default Server:  tp-dc-05.corpnet.asus
Address:  172.21.128.8

> www.abcnews.com
Server:  tp-dc-05.corpnet.asus
Address:  172.21.128.8

Non-authoritative answer:
Name:    abcnews.com
Address:  199.181.132.250
Aliases:  www.abcnews.com

>
```

Figure 13.2. Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **<Enter>** at the command prompt.

14 Index