



VPN ADSL Router

SL6000/SL6300

User's Manual

Copyright Information

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK COMPUTER INC. (“ASUS”).

ASUS PROVIDES THIS MANUAL “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners’ benefit, without intent to infringe.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Copyright © 2003 ASUSTeK COMPUTER INC. All Rights Reserved.

Product Name:	ASUS VPN ADSL Router (SL6000/SL6300)
Manual Revision:	1 E1428
Release Date:	October 2003

Copyright Information

ASUSTeK COMPUTER INC. (Asia-Pacific)

Address: 150 Li-Te Road, Peitou, Taipei, Taiwan 112
General Tel: +886-2-2894-3447
General Fax: +886-2-2894-3449
Web Site: www.asus.com.tw

Technical Support

Networking (Tel): +886-2-2890-7902 (English)
MB/Others (Tel): +886-2-2890-7121 (English)
Notebook (Tel): +886-2-2890-7122 (English)
Desktop/Server (Tel): +886-2-2890-7123 (English)
Support Fax: +886-2-2890-7698

ASUS COMPUTER INTERNATIONAL (America)

Address: 44370 Nobel Drive, Fremont, CA 94538, USA
General Fax: +1-502-933-8713
General Email: tmd1@asus.com
Web Site: usa.asus.com

Technical Support

Support Fax: +1-502-933-8713
General Support: +1-502-995-0883
Notebook Support: +1-510-739-3777 x5110
Support Email: tsd@asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address: Harkortstr. 25, 40880 Ratingen, BRD, Germany
General Email: sales@asuscom.de (for marketing requests only)
General Fax: +49-2102-9599-31
Web Site: www.asuscom.de

Technical Support

Components: +49-2102-9599-0
Notebook PC: +49-2102-9599-10
Support Fax: +49-2102-9599-11
Support Email: www.asuscom.de/support (for online support)

ASUSTeK COMPUTER (Middle East and North Africa)

Address: P.O. Box 64133, Dubai, U.A.E.
General Tel: +9714-283-1774
General Fax: +9714-283-1775
Web Site: www.ASUSarabia.com

Table of Contents

1. Introduction	9
1.1 Features	9
1.2 System Requirements	9
1.3 Using this Document	10
1.4 Getting Support	10
2. Getting to Know SL6000/SL6300	11
2.1 Parts List	11
2.2 Front Panel	11
2.3 Rear Panel	12
3. Quick Start Guide	13
3.1 Connecting the Hardware	13
3.1.1 Connect the ADSL line	13
3.1.2 Connect the computers or a LAN	14
3.1.3 Attach the power adapter	14
3.1.4 Turn on the SL6000/SL6300 and your computers	14
3.2 Configuring Your Computers	15
3.2.1 Before you begin	15
3.2.2 Windows® XP PCs:	15
3.2.3 Windows® 2000 PCs:	16
3.2.4 Windows® Me PCs	17
3.2.5 Windows® 95, 98 PCs:	18
3.2.6 Windows® NT 4.0 workstations:	19
3.2.7 Assigning static Internet information to your PCs	20
3.3 Quick Configuration of SL6000/SL6300	20
3.3.1 Buttons Used in Setup Wizard	21
3.3.2 Setting Up the SL6000/SL6300	21
3.3.3 Testing Your Setup	31
3.3.4 Default Router Settings	31
4. Starting the Configuration Manager	31
4.1 Log into Configuration Manager	31
4.2 Functional Layout	32
4.2.1 Setup Menu Navigation Tips	32
4.2.2 Commonly Used Buttons and Icons	32
4.3 The Home Page of Configuration Manager	34

Table of Contents

5. System Information	35
6. Configuring LAN Settings	36
6.1 LAN IP Address	36
6.1.1 LAN IP Configuration Parameters	36
6.1.2 Configuring the LAN IP Address	36
6.2 DHCP (Dynamic Host Configuration Protocol)	38
6.2.1 What is DHCP?	38
6.2.2 Why use DHCP?	39
6.2.3 Configuring DHCP Server	39
6.2.4 Viewing Current DHCP Address Assignments	40
6.3 DNS	40
6.3.1 About DNS	40
6.3.2 Assigning DNS Addresses	42
6.3.3 Configuring DNS Relay	42
6.4 Viewing LAN Statistics	43
7. Configuring WAN/ADSL Settings	44
7.1 ADSL Connection	44
7.2 WAN Configuration	45
7.2.1 MPoA Bridged and PPPoE Relay:	45
7.2.2 MPoA Routed:	45
7.2.3 IPoA Routed:	45
7.2.4 PPPoA Routed and PPPoE Routed:	46
7.3 Viewing WAN/ADSL Statistics	47
8. Configuring Routes	48
8.1 Overview of IP Routes	48
8.1.1 Do I need to define IP routes?	48
8.2 DNS Relay Configuration	49
8.3 Static Routing	49
8.3.1 Static Route Configuration Parameters	49
8.3.2 Adding Static Routes	50
8.3.3 Modifying Static Routes	50
8.3.4 Deleting Static Routes	51
8.3.5 Viewing the Static Routing Table	51

Table of Contents

9. Configuring Firewall/NAT Settings	52
9.1 DoS Protection and Stateful Packet Inspection	52
9.2 Default ACL Rules	53
9.3 Configuring Inbound ACL Rules	53
9.3.2 Add Inbound ACL Rules	60
9.3.3 Modify Inbound ACL Rules	61
9.3.4 Delete Inbound ACL Rules	61
9.3.5 Display Inbound ACL Rules	61
9.4 Configuring Outbound ACL Rules	62
9.4.2 Add an Outbound ACL Rule	68
9.4.3 Modify Outbound ACL Rules	69
9.4.4 Delete Outbound ACL Rules	69
9.4.5 Display Outbound ACL Rules	69
9.5 Configuring Group ACL Rules	70
9.5.1 Add/Delete a User Group	70
9.6 Configuring Self Access Rules	72
9.6.1 Add a Self Access Rule	72
9.6.2 View Self Access Summary	72
9.6.3 Delete Self Access Rule	72
9.7 Configuring Service List	73
9.7.1 Options in Service Configuration Page	74
9.7.2 Add a Service	74
9.7.3 Modify a Service	74
9.7.4 Delete a Service	75
9.7.5 View Configured Services	75
9.8 DoS (Denial of Service)	76
9.8.1 SYN Flooding Attack Check	76
9.8.2 Winnuke Attack Check	76
9.8.3 MIME Flood Attack Check	76
9.8.4 Maximum IP Fragment Count	77

Table of Contents

9.9 Policy List	78
9.9.1 Application Filter	78
9.9.2 NAT Pool	81
9.9.3 IP Pool	82
9.9.4 Firewall User	84
9.9.5 Time Range	86
9.10 Firewall Statistics	88
10.2 Establish VPN Connection Using Automatic Keying	91
10.2.1 VPN Tunnel Configuration Parameters for Automatic Keying	91
10.2.2 Add a Rule for VPN Connection Using Preshared Key	95
10.2.3 Modify VPN Rules	96
10.2.4 Delete VPN Rules	97
10.2.5 Display VPN Rules	97
10.3 Establish VPN Connection Using Manual Keys	97
10.3.1 VPN Tunnel Configuration Parameters - Manual Key	99
10.3.2 Add a Rule for VPN Connection Using Manual Key	101
10.3.3 Modify VPN Rules	102
10.3.4 Delete VPN Rules	103
10.3.5 Display VPN Rules	103
10.4 VPN Statistics	103
11. System Log	106
12. System Management	107
12.1 Global Setting Configuration	107
12.2 User Account Management	109
12.3 Modify System Information	109
12.4 Setup Time Zone	109
12.4.1 Change/View the System Time Zone	110
12.5 System Configuration Management	111
12.5.1 Reset System Configuration to Default	111
12.5.2 Backup System Configuration	111
12.5.3 Restore System Configuration	112
12.6 Upgrade Firmware	113

Table of Contents

13. System Reset	114
14. Logout Configuration Manager	115
A. IP Addresses, Network Masks, & Subnets	116
A.1 IP Addresses	116
A.1.1 Structure of an IP address	116
A.1.2 Network classes	117
A.2 Subnet masks	118
B. Troubleshooting	119
B.1 Recall default configuration by “RESET” button	122
B.2 Diagnosing Problem using IP Utilities	125
B.2.1 ping	125
B.2.2 nslookup	126
C. Glossary	127

1. Introduction

Congratulations on becoming the owner of the SL6000/SL6300 VPN ADSL Router. Your LAN (local area network) will now be able to access the Internet via SL6000/SL6300's ADSL connection.

This User Manual will show you how to set up the SL6000/SL6300 VPN ADSL Router, and how to customize its configuration to get the most out of this product.

1.1 Features

- Built-in ADSL modem in SL6000 (G.992.1 Annex A) / SL6300 (G.992.1 Annex B), which offers up to 8Mbps/800Kbps internet surf speed for Downstream/Upstream, respectively.
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- NAT (Network Address Translation), Firewall, and IPSec VPN functions to provide secure Internet access for your LAN
- Automatic network address assignment through DHCP Server
- Services including IP route and DNS configuration, RIP, and IP performance monitoring
- Configuration program accessible via a web browser, such as Microsoft Internet Explorer. Note that Netscape is not supported.

1.2 System Requirements

In order to use the SL6000/SL6300 VPN ADSL Router for Internet access, you must have the following:

- ADSL service subscription from your ISP.
- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC).
- (Optional) An Ethernet hub/switch, if you are connecting the device to more than four computers on an Ethernet network.
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.5 or later

Chapter 1

1.3 Using this Document

1.3.1 Notational conventions

- Acronyms are defined the first time they appear in text and in the glossary (Appendix C).
- For brevity, the SL6000/SL6300 is referred to as “the router.”
- The terms LAN and network are used interchangeably to refer to a group of Ethernet-connected computers at one site.

1.3.2 Typographical conventions

- Italics are used to identify terms that are defined in the glossary (Appendix C).
- 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.



Notes: Provides clarification or nonessential 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.

1.4 Getting Support

See the contact information on first few pages of this manual.

2. Getting to Know SL6000/SL6300

2.1 Parts List

In addition to this document, your SL6000/SL6300 should come with the following:

- SL6000/SL6300 VPN ADSL Router
- Power adapter
- Ethernet cable (RJ-45) “straight-through” type)
- Phone cable (RJ-11)

2.2 Front Panel

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

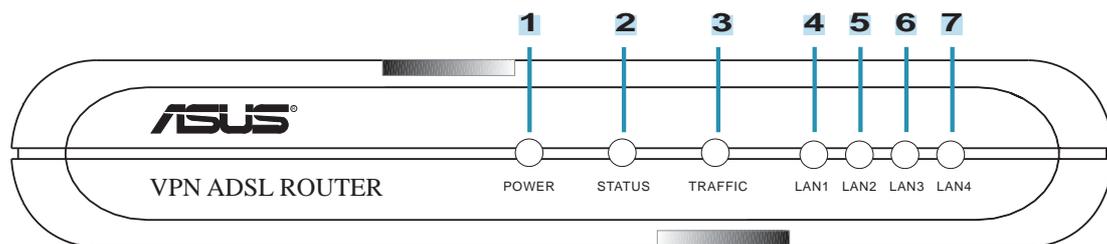


Figure 2.2 Front Panel LEDs

Table 2.1 Front Panel Label and LEDs

Label	Color	Function
POWER	green	On: Unit is powered on Off: Unit is powered off
STATUS	green	On: ADSL link is established and active Flashing: Trying to create an ADSL connection Off: No ADSL link
TRAFFIC	green	Flashing: ADSL data transfer
LAN1-4	green	On: LAN link is established Flashing: Data transfer at LAN connection(s) Off: No LAN link

Chapter 2

2.3 Rear Panel

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

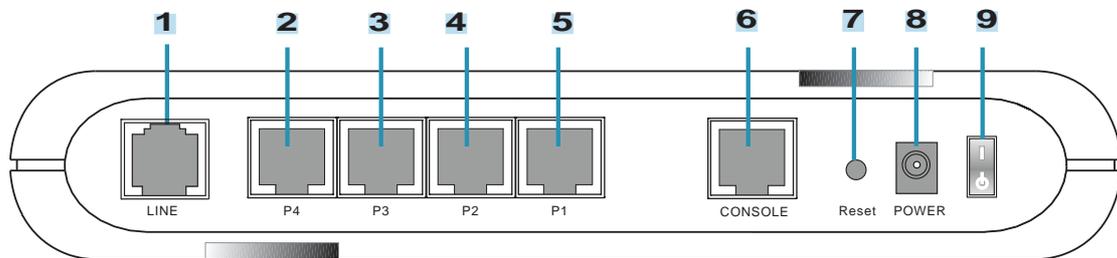


Figure 2.3 Rear Panel Connections

Table 2.2 Rear Panel Labels and Switch/Connectors

1. LINE
Connects to your ADSL line. This is a standard RJ-11 telephone jack on your wall but routed through an ADSL system by your phone company and may have an optional splitter to allow telephone use on the same line.
2. P1 - P4
Connects to your PC's Ethernet port, or to the uplink port on your LAN's hub/switch, using the provided RJ-45 crossover cable.
3. Console
RJ-45 port for advanced console management. An additional RS232 to RJ45 cable is required.
4. Reset
Resets the device.
5. Power
Connects to the supplied power adapter.
6. On/Off
Power switch to turn the unit ON and OFF.

3. Quick Start Guide

This Quick Start Guide provides basic instructions for connecting the SL6000/SL6300 to a computer or a LAN and to the Internet via ADSL.

- 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 SL6000/SL6300 to get your LAN connected to the Internet.

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

This Quick Start Guide assumes that you have already subscribe ADSL 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 Connecting the Hardware

In 3.1, you should connect the device to an ADSL line, 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 SL6000/SL6300.

For hardware connections, please follow the steps that follow for specific instructions.

3.1.1 Connect the ADSL line

For SL6000/SL6300: Connect your ADSL line to the port labeled ADSL on the rear panel of the device. Connect the other end of the line to the wall phone jack or to the POTS splitter (Optional).

3.1.2 Connect the computers or a LAN

If your LAN has no more than 4 computers, you can use 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 LAN1 - LAN4 on the rear panel of the device and connect the other end to the Ethernet port of a computer.

If you LAN has more than 4 computers, you can attach one end of a 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 LAN1 - LAN4) on the SL6000/SL6300.

Note that both 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 Attach the power adapter

Connect the AC power adapter to the POWER connector on the back of the device and plug in the adapter to a wall outlet or a power strip.

3.1.4 Turn on the SL6000/SL6300 and your computers

Press the Power switch on the rear panel of SL6000/SL6300 to the ON position. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches. You should verify that its LEDs are illuminated as shown 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 power adapter is attached to SL6000/SL6300 and if it is plugged into a power source.
LAN1 - LAN4	Solid green to indicate that the device can communicate with your LAN or flashing when the device is sending or receiving data from your LAN computer(s).
ADSL	Solid green to indicate that the device has successfully established a connection to your ADSL line.

If the LEDs illuminate as expected, SL6000/SL6300 hardware is working properly.

3.2 Configuring Your Computers

3.2.1 Before you begin

By default, the SL6000/SL6300 automatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information when it is assigned.



Note: In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the SL6000/SL6300 to do so. See “Assigning static Internet information to your PCs” for instructions.

If you have connected your PC of LAN via Ethernet to the SL6000 / SL6300, 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**.
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** 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 with 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**.
5. In the Select Network Component Type dialog box, select Protocol, and then click **Add**.
6. Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click **OK**.

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** to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the SL6000 / SL6300:
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**.
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** twice to confirm and save your changes, and then close the Control Panel.

3.2.4 Windows® 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 and Dial-up Connections** icon.
3. In the Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.

The Network Properties dialog box displays with 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 11.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
5. In the Select Network Component Type dialog box, select Protocol, and then click **Add**.
6. Select **Microsoft** in the Manufacturers box.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.

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

8. If prompted, click **OK** to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the SL6000 / SL6300:
9. In the Control Panel, double-click the Network and Dial-up Connections icon.
10. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
11. In the Network Properties dialog box, select **TCP/IP**, and then click **Properties**.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled **Server assigned name server address**.
13. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

3.2.5 Windows® 95, 98 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 icon.

The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

3. If TCP/IP does not display as an installed component, click **Add**.

The Select Network Component Type dialog box displays.

4. Select **Protocol**, and then click **Add**.

The Select Network Protocol dialog box displays.

5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.

6. Click **[OK]** to return to the Network dialog box, and then click **[OK]** again.

You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

7. Click **[OK]** to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the SL6000 / SL6300:

8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click **[Properties]**.

If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

10. In the TCP/IP Properties dialog box, click the **IP Address** tab.
11. Click the radio button labeled **Obtain an IP address automatically**.
12. Click the DNS Configuration tab, and then click the radio button labeled **Obtain an IP address automatically**.
13. Click **[OK]** twice to confirm and save your changes.

You will be prompted to restart Windows.

14. Click **[Yes]**.

3.2.6 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, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click **[Add]**.
5. In the Select Network Protocol dialog box, select TCP/IP, and then click **[OK]**.

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]** to continue, and then click **[OK]** if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the SL6000 / SL6300:
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]**.
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]** twice to confirm and save your changes, and then close the Control Panel.

3.2.7 Assigning static Internet information to your PCs

In some cases, you may want to assign Internet information to some or all of your PCs directly (often called “statically”), rather than allowing the SL6000/SL6300 to assign it. 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.

Before you begin, contact your ISP if you do not already have the following information:

- The IP address and subnet mask to be assigned to each PC to which you will be assigning static IP information.
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the SL6000/SL6300. By default, the LAN port is assigned this IP address: 192.168.1.1. (You can change this number, or another number can be assigned by your ISP. See Chapter 6 for more information.)
- The IP address of your ISP’s Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions on previous pages 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 SL6000/SL6300’s LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Chapter 6 to change the LAN port IP address accordingly.

3.3 Quick Configuration of SL6000/SL6300

In this section, you log into the Configuration Manager on the SL6000/SL6300 and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step. Note the intent here is to quickly get SL6000/SL6300 up and running, instructions are concise. You may refer to corresponding chapters for more details.

3.3.1 Buttons Used in Setup Wizard

The SL6000/SL6300 provides a pre-installed software program called Configuration Manager that enables you to configure SL6000/SL6300 via your Web browser. The settings that you are most likely to need to change before using the device are grouped onto sequence of Configuration pages guided by Setup Wizard. The following table shows the buttons that you'll encounter in Setup Wizard.

[Next]
Click this button to proceed to the next configuration page. If there are no changes required in the current configuration page, you can click this button to proceed to the next configuration page.
[Back]
Click this button to go back to the previous configuration page.

3.3.2 Setting Up the SL6000/SL6300

Follow these instructions to setup SL6000/SL6300:

1. At any PC connected to one of the four LAN ports on the SL6000/SL6300, 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 SL6000/SL6300. A login screen displays, as shown in Figure 3.2



Figure 3.2 Login Screen

Chapter 3

If you have problem connecting to SL6000/SL6300, you may want to check if your PC is configured to accept IP address assignment from SL6000/SL6300. 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 but excluding 192.168.1.1 and 192.168.1.255.

2. Enter your user name and password, and then click **[OK]** to enter the Configuration Manager. The first time you log into this program, use these defaults:

Default User Name: **admin**

Default Password: **admin**



Note: You can change the password at any time (see section 12.2 User Account Management).

The Setup Wizard home page displays each time you log into the Configuration Manager (shown in Figure 3.3).



Figure 3.3 Setup Wizard Home Page

3. Click on the **[Next]** button to enter the password configuration page as shown in Figure 3.4. Change the password in the spaces provided if desired. Otherwise, proceed to the next configuration page by clicking on the **[Next]** button.

When changing passwords, make sure you enter the existing login password in the Login Password field, make any changes for the passwords and click the **[Apply]** button to save the changes.

You might get online help from the Setup Wizard by click the **[Help]** button and get Figure 3.5.



User Account Configuration	
Login Password	<input type="text"/>
Supervisor's Password	New Password <input type="text"/>
	Confirm New Password <input type="text"/>
User's Password	New Password <input type="text"/>
	Confirm New Password <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 3.4 Setup Wizard Password Configuration Page

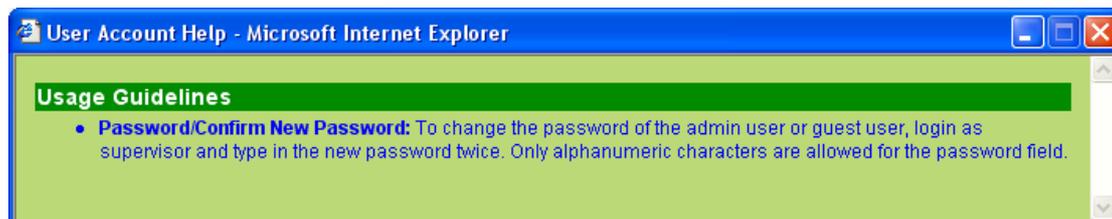


Figure 3.5 Setup Wizard Password Help Page

Chapter 3

- Now we are at the System Information setup page; enter the requested information in the spaces provided and click the **[Apply]** button to save the changes. Otherwise, proceed to the next configuration page by clicking on the **[Next]** button.

System Information Configuration		
System Name	<input type="text" value="SL6000"/>	(Optional)
System Location	<input type="text" value="TAIPEI"/>	(Optional)
System Contact	<input type="text" value="ASUS TAIWAN"/>	(Optional)
<input type="button" value="Apply"/>		

Figure 3.6 Setup Wizard System Identity Configuration Page

- Set the time zone for SL6000/SL6300 by selecting your time zone from the Time Zone drop-down list (shown in Figure 3.7 Time Zone Configuration). Click **[Apply]** to save the settings and then click on the **[Next]** button to go to the next configuration page.

Time Zone Configuration			
Date	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1970"/> (mm:dd:yyyy)
Time	<input type="text" value="15"/>	<input type="text" value="32"/>	<input type="text" value="21"/> (hh:mm:ss)
Location Time	<input type="text" value="GMT"/>		
SNTP Service Configuration			
SNTP Server 1	<input type="text" value="207.46.248.43"/>		
SNTP Server 2	<input type="text" value="192.43.244.18"/>		
SNTP Server 3	<input type="text" value="131.107.1.10"/>		
SNTP Server 4	<input type="text" value="129.6.15.28"/>		
SNTP Server 5	<input type="text" value="129.6.15.29"/>		
Update Interval	<input type="text" value="1"/>	(Hours)	
<input type="button" value="Apply"/>			<input type="button" value="Help"/>

Figure 3.7 Time Zone Configuration

There is no real time clock inside SL6000/SL6300. The system date and time are maintained by external network time server via SNTP (Simple Network Time Protocol). There are five predefined SNTP servers, so you don't need to set the date and time here.

You might get online help from the Setup Wizard by click the **[Help]** button and get Figure 3.8.

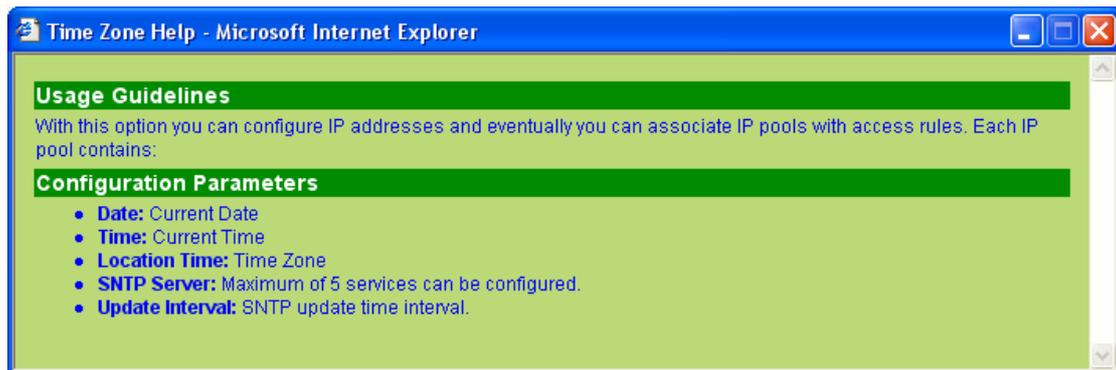


Figure 3.8 Time Zone Help

- It is recommended that you keep the default LAN IP settings at this point until after you have completed the rest of the configurations and confirm that your Internet connection is working. Click on the **[Next]** button to proceed to the next configuration page.

Ethernet IP Configuration	
Mode	<input type="radio"/> Bridge <input checked="" type="radio"/> Router
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Ethernet IP Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Figure 3.9 Setup Wizard LAN IP Configuration Page

Chapter 3

- It is recommended that you keep the default settings for DHCP server until after you have completed the rest of the configurations and confirm that your Internet connection is working. Click on the [Next] button to proceed to the next configuration page.

DHCP Server Configuration

IP Address Pool	Begin <input type="text" value="192.168.1.10"/>
	End <input type="text" value="192.168.1.108"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Lease Time	<input type="text" value="00:23:59"/> (dd:hh:mm)
Default Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS Server	<input type="text" value="192.168.1.1"/> (Optional)
Secondary DNS Server	<input type="text"/> (Optional)
Primary WINS Server	<input type="text" value="192.168.1.1"/> (Optional)
Secondary WINS Server	<input type="text"/> (Optional)

DHCP Configuration

IP Address Pool	192.168.1.10 ~ 192.168.1.108
Lease Time	00:23:59 (dd:hh:mm)
Default Gateway	192.168.1.1
Primary DNS Server	192.168.1.1
Secondary DNS Server	
Primary WINS Server	192.168.1.1
Secondary WINS Server	

DHCP Server Assignments

MAC Address	Assigned IP Address	IP Address Expires On
00:e0:18:00:e1:3b	192.168.1.25	15:12:57 1/2/1970
00:e0:18:75:c0:2a	192.168.1.24	3:19:32 1/2/1970
00:e0:18:2e:17:23	192.168.1.10	0:10:43 1/2/1970
00:00:4c:2e:0f:ca	192.168.1.11	3:6:55 1/1/1970
00:e0:18:0f:ab:51	192.168.1.23	2:30:20 1/1/1970
00:e0:18:88:7c:58	192.168.1.22	2:29:52 1/1/1970
00:e0:18:18:86:e8	192.168.1.21	2:25:45 1/1/1970
00:e0:18:9a:53:a4	192.168.1.20	2:16:11 1/1/1970
00:e0:18:18:ac:44	192.168.1.18	2:8:14 1/1/1970
00:80:c6:e3:fb:1a	192.168.1.16	1:34:41 1/1/1970
00:80:88:33:00:e7	192.168.1.19	1:26:40 1/1/1970
00:e0:18:75:c0:5d	192.168.1.17	1:13:24 1/1/1970
00:e0:18:2e:1b:2d	192.168.1.15	0:57:34 1/1/1970
00:01:24:f0:08:3f	192.168.1.14	0:50:51 1/1/1970
00:e0:18:9e:13:e3	192.168.1.12	0:46:51 1/1/1970
00:20:e0:e0:a1:a6	192.168.1.13	0:46:11 1/1/1970

Figure 3.10 Setup Wizard DHCP Server Configuration Page

8. Now we are at the last page of the Setup Wizard, which is to configure the WAN settings for SL6000/SL6300. Depending on the connection mode required from your ISP, you may select from the following connection modes from the Connection Mode drop-down list (see Figure 3.12): MPoA Bridged, PPPoE Relay, MPoA Routed, IPoA Routed, PPPoA Routed and PPPoE Routed.

Figure 3.12 Setup Wizard WAN Configuration Page

Configuration Parameters

1. Channel: Select the ATM Interface that is to be configured or viewed
2. VPI and VCI: These settings are used to specify the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) that is used for connecting the Broadband Gateway to the ISP's ATM Switch using the specified ATM Interface.
 - VPI: Enter the VPI of the ATM Connection to the ISP's ATM Switch
 - VCI: Enter the VCI of the ATM Connection to the ISP's ATM Switch
3. Select the option VC Mux to carry your Internet Service without encapsulation over the ATM Interface, else select the option LLC - contact your ISP for details

Chapter 3

4. **Default Gateway:** Select this channel as default gateway of the Broadband Gateway
5. **RIP Tx/Rx:** Select send/accept routing updates on the channel via RIPv1 or RIPv2, this setting will only be effective if RIP is enabled in Global Setting page
6. **QoS:** These settings are used to specify the service category and traffic parameters that are to be applied for traffic over the specified ATM interface. Choose one of the following options depending on your traffic requirements.
 - **None:** The traffic carried over this interface will be on a best effort basis without any guarantee of quality-of-service
 - **CBR:** The quality-of-service applied to traffic over this interface is that applied to Constant-Bit-Rate (CBR) traffic.
 - **VBR-rt:** The quality-of-service applied to traffic over this interface is that applied to Real-Time-Variable-Bit-Rate (VBR-rt) traffic.
 - **VBR-nrt:** The quality-of-service applied to traffic over this interface is that applied to Non-Real-Time-Variable-Bit-Rate (VBR-nrt) traffic.
 - **UBR:** The quality-of-service applied to traffic over this interface is that applied to Unspecified-Bit-Rate (UBR) traffic

ATM Service Configuration Parameters

- a) **MPoA Bridged and PPPoE Relay:**
 - * No further configuration parameters need to be specified for MpoA Bridged and PPPoE Relay services.
- b) **MPoA Routed:**
 - * **DHCP IP Address Assignment:** Select this option if the MPoA Routed Service interface is to obtain its IP address from your ISP via DHCP.
 - * **Static IP Address Assignment:** Select this option if the MPoA Routed Service interface is to have its IP address configured statically.
 - * **IP Address:** Enter the MPoA Routed service interface's IP Address. Contact your ISP for details
 - * **Subnet Mask:** Enter the MPoA Routed service interface's Subnet Mask. Contact your ISP for details
- c) **IPoA Routed**

- * DHCP IP Address Assignment: Select this option if the IPoA Service interface is to obtain its IP address from your ISP via DHCP.
 - * Static IP Address Assignment: Select this option if the IPoA Service interface is to have its or remote host's IP addresses configured statically.
 - * IP Address: Enter the IPoA service interface's IP Address. Contact your ISP for details.
 - * Subnet Mask: Enter the IPoA service interface's Subnet Mask. Contact your ISP for details.
- d) PPPoA Routed and PPPoE Routed
- * User Name: The user name for setting up the PPPoA/PPPoE Service. Contact your ISP for the specific user name to be used.
 - * Password: The password for setting up the PPPoA/PPPoE Service. Contact your ISP for the specific password to be used for initial setup.
- e) Bridge IP Settings: These settings must be specified if any LAN interface is in bridge mode, or if any ATM interface carries bridged services (MPoA Bridge, PPPoE Relay) - the Broadband Gateway software will automatically prompt you for the bridge interface settings in this case.
- * IP Address: Enter the IP address for the bridge interface
 - * Subnet Mask Address: Enter the Subnet Mask for the bridge interface

You are now finished customizing basic settings. Read the following section to determine if you have access to the Internet.

Notes:

- If you specify a new service using an ATM interface that has an existing service, the Broadband Gateway software will automatically delete the existing service and replace it with the new service
- If you change your PPPoA/PPPoE password through your ISP, you need to set the new password for the configured PPPoA/PPPoE service, in order to setup the service successfully
- The Bridge IP Settings are the same for all Interfaces that are in bridge mode or that have bridge services running over them
- RIP Rx is always enabled as RIP is enabled

3.3.3 Testing Your Setup

At this point, SL6000/SL6300 should enable any computer on your LAN to use the SL6000/SL6300's ADSL 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.yahoo.com>). You should be able to surf the Internet from now on.

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

3.3.4 Default Router Settings

In addition to handling the DSL connection to your ISP, the SL6000/SL6300 VPN ADSL Router 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, 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

DHCP (Dynamic Host Configuration Protocol)
<i>Default: DHCP server enabled with the following pool of addresses: 192.168.1.10 through 192.168.1.108</i>
SL6000/SL6300 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 6.2 for an explanation of the DHCP service.
LAN Port IP Address
<i>Default: Static IP address: 192.168.1.1 Subnet mask: 255.255.255.0</i>
This is the IP address of the LAN port on SL6000/SL6300. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See section 6.1 LAN IP Address for instructions.

4. Starting the Configuration Manager

The SL6000/SL6300 includes a pre-installed 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 SL6000/SL6300 via the LAN ports.

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

4.1 Log into Configuration Manager

The Configuration Manager program is pre-installed on the SL6000/SL6300. To access the program, you need the following:

A computer connected to the LAN port of SL6000/SL6300 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® 5.5, or later versions. Note that Netscape is not supported.

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 SL6000/SL6300. A login screen displays, as shown in Figure 4.1.



Figure 4.1 Configuration Manager Login Screen

Chapter 4

2. Enter your user name and password, and then click .

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

Default User Name: **admin**

Default Password: **admin**

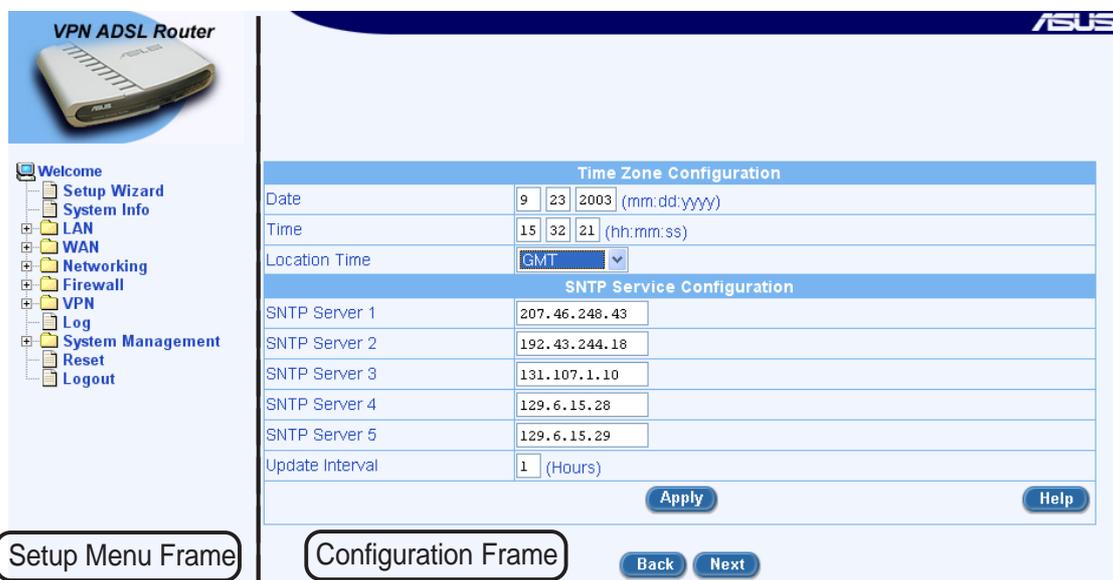


Note: You can change the password at any time (see section 12.2 User Account Management).

The Setup Wizard page displays each time you log into the program (shown in Figure 4.3).

4.2 Functional Layout

Typical Configuration Manager page consists of two separate frames. The left frame, as shown in Figure 4.2, contains all the menus available for device configuration. Menus are indicated by file icons, , and related menus are grouped into categories, such as LAN, WAN and etc., and indicated by folder icons,  or,  depending on whether the group of menus are expanded or not. You can click on any of these to display a specific configuration page.



Time Zone Configuration			
Date	9	23	2003 (mm:dd:yyyy)
Time	15	32	21 (hh:mm:ss)
Location Time	GMT		

SNTP Service Configuration	
SNTP Server 1	207.46.248.43
SNTP Server 2	192.43.244.18
SNTP Server 3	131.107.1.10
SNTP Server 4	129.6.15.28
SNTP Server 5	129.6.15.29
Update Interval	1 (Hours)

Figure 4.2 Typical Configuration Manager Page

A separate page displays in the right-hand-side frame for each menu. For example, the configuration page displayed in Figure 4.2 is intended for DHCP configuration.

4.2.1 Setup Menu Navigation Tips

- To expand a group of related menus: click on the + sign next to the corresponding file folder icon, 
- To contract a group of related menus: click on the - sign next to the “opened” file folder icon, 
- To open a specific configuration page, click on the file icons, , next to the desired menu item.

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

[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 the existing configuration in the system, e.g. a static route or a firewall ACL rule and etc.
[Delete]
Deletes the selected item, e.g. a static route or a firewall ACL rule and etc.
[Help]
Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.
[Refresh]
Re-displays the current page with updated statistics or settings.

Selects the item for editing.

Deletes the selected item.

4.3 The Home Page of Configuration Manager

The Setup Wizard page displays when you first access the Configuration Manager.



Figure 4.3 Setup Wizard Page

5. System Information

This chapter describes your SL6000/SL6300 system information and configuration summary when you click the “System Info” in the left column. You may get all information as shown in Figure 5.1.



System Information	
Software Version	323.058_A
IP Address	192.168.1.1
MAC Address	00-00-00-00-00-00
ADSL Line Status	Activating
System Up Time	0:15:45:37 (dd:hh:mm:ss)
System Name	SL6000
System Location	TAIPEI
System Contact	ASUS TAIWAN

Configuration Summary	
Firewall	Enabled
VPN	Disabled
DHCP	Enabled
DNS Relay	Enabled
RIP	Enabled
SNTP	Disabled

Figure 5.1. LAN IP Address Configuration Page

6. Configuring LAN Settings

This chapter describes how to configure LAN properties for the LAN interface on the SL6000/SL6300 that communicates with your LAN computers. You'll learn to configure IP address, DHCP and DNS server for your LAN in this chapter.

6.1 LAN IP Address

If you are using the SL6000/SL6300 with multiple PCs on your LAN, you must connect the LAN via the Ethernet ports on the built-in Ethernet switch. You must assign a unique IP address to each device residing on your LAN. The LAN IP address identifies the SL6000/SL6300 as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN. The default LAN IP for SL6000/SL6300 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 SL6000/SL6300's LAN port and the network interface cards on your PCs. See Appendix A for an explanation of subnets.

You can change the default to reflect the set of IP addresses that you want to use with your network.



Note: The SL6000/SL6300 itself can function as a DHCP server for your LAN computers, as described in section 6.2.3 Configuring DHCP Server, but not for its own LAN port.

6.1.1 LAN IP Configuration Parameters

Table 6.1 describes the configuration parameters available for LAN IP configuration.

Table 6.1 LAN IP Configuration Parameters

IP Address
The LAN IP address of SL6000/SL6300. This IP is used by your computers to identify SL6000/SL6300'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 SL6000/SL6300 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 pre-configured with a default subnet mask of 255.255.255.0.

6.1.2 Configuring the LAN IP Address

Follow these steps to change the default LAN IP address.

1. Log into Configuration Manager as administrator, and then click the LAN menu.

When the sub-menus of the LAN Configuration displays, click Ethernet submenu to display the IP Address configuration page as shown in Figure 6.1.

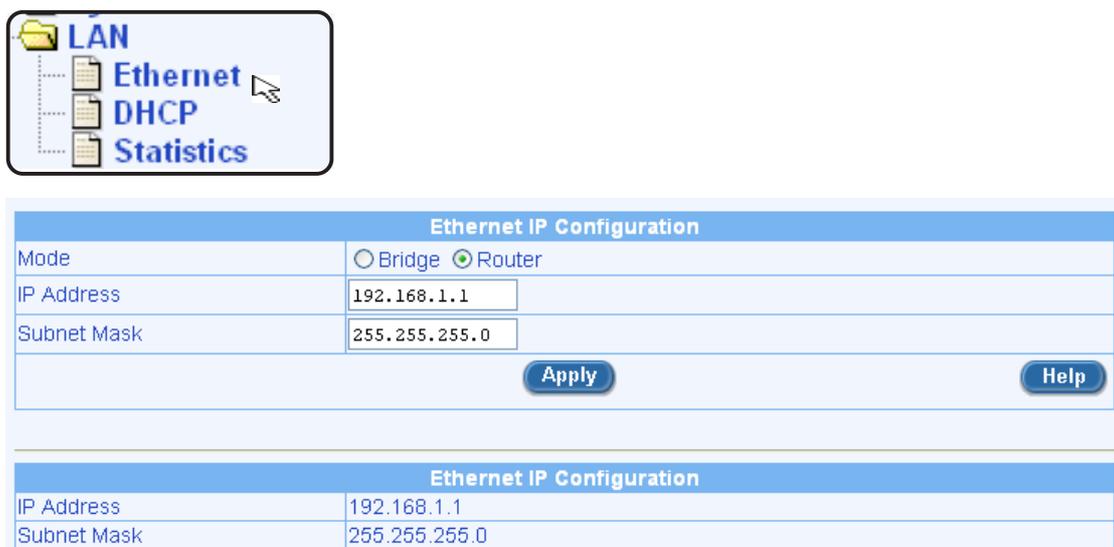


Figure 6.1 LAN IP Address Configuration Page

Chapter 6

2. Enter a LAN IP address and subnet mask for SL6000/SL6300 in the space provided.
3. Click [**Apply**] to save the LAN IP address.
If you were using an Ethernet connection for the current session, and changed the IP address, the connection will be terminated.
4. Reconfigure your PCs, if necessary, so that their IP addresses place them in the same subnet as the new IP address of the LAN port. See the Quick Start Guide chapter, “Configuring Your Computers,” for instructions.
5. Log into Configuration Manager by typing the new IP address in your Web browser’s address/location box.

6.2 DHCP (Dynamic Host Configuration Protocol)

6.2.1 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 SL6000/SL6300 - 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 DHCP server such as SL6000/SL6300.

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.

6.2.2 Why use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from SL6000/SL6300. 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.

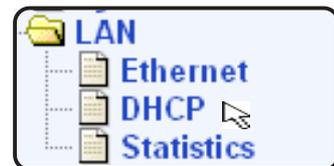
6.2.3 Configuring DHCP Server



Note: By default, SL6000/SL6300 is configured as a DHCP server on the LAN side, with a predefined IP address pool of 192.168.1.10 through 192.168.1.108 (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. Log into Configuration Manager as administrator, click the LAN menu, and then click the DHCP submenu.



The DHCP Configuration page displays as shown in Figure 6.2:

DHCP Server Configuration	
IP Address Pool	Begin <input type="text" value="192.168.1.10"/> End <input type="text" value="192.168.1.108"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Lease Time	<input type="text" value="00:23:59"/> (dd:hh:mm)
Default Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS Server	<input type="text" value="192.168.1.1"/> (Optional)
Secondary DNS Server	<input type="text"/> (Optional)
Primary WINS Server	<input type="text" value="192.168.1.1"/> (Optional)
Secondary WINS Server	<input type="text"/> (Optional)
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

DHCP Configuration	
IP Address Pool	192.168.1.10 ~ 192.168.1.108
Lease Time	00:23:59 (dd:hh:mm)
Default Gateway	192.168.1.1
Primary DNS Server	192.168.1.1
Secondary DNS Server	
Primary WINS Server	192.168.1.1
Secondary WINS Server	

DHCP Server Assignments		
MAC Address	Assigned IP Address	IP Address Expires On
00:e0:18:00:e1:3b	192.168.1.25	15:12:57 1/2/1970
00:e0:18:75:c0:2a	192.168.1.24	3:19:32 1/2/1970

Figure 6.2 DHCP Configuration Page

Chapter 6

2. To add an IP address pool, click **[Add]**.
The DHCP Server Pool - Add page displays.
3. Enter the Start IP Address, End IP Address, Net Mask, and Default Gateway IP Address, fields are required; the others, such as DNS Server IP Address and WINS Server IP Address are optional. However, it is recommended that you enter DNS server IP address in the space provided. You may enter the LAN IP or your ISP's DNS IP in the DNS Server IP Address field. The following table describes the DHCP configuration parameters in detail.

Table 6.2 DHCP Configuration Parameters

IP Address Pool Begin/End
Specify the lowest and highest addresses in the DHCP address pool.
Lease Time
The amount of time 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 IP address that the computers first contact to communicate with the Internet. Typically, it is SL6000/SL6300's LAN port IP address.
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 here as SL6000/SL6300 will serve as DNS proxy for the LAN computers and forward the DNS request from the LAN to DNS servers and relay the results back to the LAN computers.
WINS Server IP Address (optional)
The WINS server IP address 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 a WINS server.

4. Click **[Apply]** to save the DHCP server configurations.

NOTE: If you change the LAN IP address and subnet mask, the DHCP Server Pool will be automatically configured to fall into the same subnet as the new LAN IP address.



6.2.4 Viewing Current DHCP Address Assignments

When the SL6000/SL6300 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 go to the DHCP Server Configuration page. A page displays similar to that shown in Figure 6.2; the lower half of the same page shows the existing DHCP address assignments.

The DHCP Server Address Table lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

Table 6.3 DHCP Address Assignment

MAC Address
A hardware ID of the device that leases an IP address from the DHCP server.
Assigned IP Address
The address that has been leased from the pool.
IP Address Expired on
The time when the leased address is to be terminated.

6.3 DNS

6.3.1 About DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., “yahoo.com”) to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

6.3.2 Assigning DNS Addresses

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

Statically: If your ISP provides you with their DNS server addresses, you can assign them to each PC by modifying the PCs' IP properties.

Dynamically from a DHCP pool: You can configure the DHCP Server SL6000/SL6300 and create an address pool that specify the DNS addresses to be distributed to the PCs. Refer to the section Configuring DHCP Server for instructions on creating DHCP address pools.

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the VPN ADSL Router (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the following section.



Note: If you specify the actual DNS addresses on the PCs or in the DHCP pool, the DNS relay feature is not used.

6.3.3 Configuring DNS Relay

When you specify the device's LAN port IP address as the DNS address, then SL6000/SL6300 automatically performs "DNS relay"; i.e., because the device itself is not a DNS server, it forwards domain name lookup requests from the LAN PCs to a DNS server at the ISP. It then relays the DNS server's response to the PC.

When performing DNS relay, the SL6000/SL6300 must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

Follow these steps to configure DNS relay:

1. Enter LAN IP in the DNS Server IP Address field in DHCP configuration page as shown in Figure 6.2.
2. Configure the LAN PCs to use the IP addresses assigned by the DHCP server on SL6000/SL6300, or enter SL6000/SL6300's LAN IP address as their DNS server address manually for each PC on your LAN.

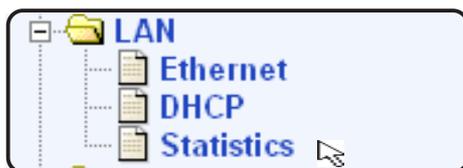


Note: DNS addresses that are assigned to LAN PCs prior to enabling DNS relay will remain in effect until the PC is rebooted. DNS relay will only take effect when a PC's DNS address is the LAN IP address. Similarly, if after enabling DNS relay, you specify a DNS address (other than the LAN IP address) in a DHCP pool or statically on a PC, then that address will be used instead of the DNS relay address.

6.4 Viewing LAN Statistics

You can view statistics of your LAN traffic on SL6000/SL6300. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

To view LAN IP statistics, click “**Statistics**” on the LAN submenu. Figure 6.3 shows the LAN Statistics page



LAN Statistics	
Total Bytes Received	113394
Unicast Packets Received	783
Multicast Packets Received	0
Packets Received and Discarded	0
Packets Received with Errors	0
Packets Received with unknown Protocols	0
Total Bytes Transmitted	349543
Unicast Packets Transmitted	772
Multicast Packets Transmitted	0
Packets Discarded while Transmission	0
Packets Sent with Errors	0

[Refresh](#)

Figure 6.3 LAN Statistics Page

To display the updated statistics since you opened the page, click [**Refresh**].

7. Configuring WAN/ADSL Settings

This chapter describes how to configure WAN/ADSL settings for the WAN/ADSL interface on the SL6000/SL6300 that communicates with your ISP. You'll learn how to configure ADSL, IP address, and connection mode for your WAN in this chapter.

7.1 ADSL Connection

There are several ADSL line configurations available on SL6000 and SL6300, for Annex A and Annex B, respectively. Figure 7.1 shows the available modes of SL6000: Multi, G.DMT, G.Lite and ANSI. You may click **[Connect]** to create the ADSL connection and click **[Disconnect]** to end down your ADSL connection.

The ADSL line status is also shown, no matter it's activating, connected, or disconnect (Figure 7.1)

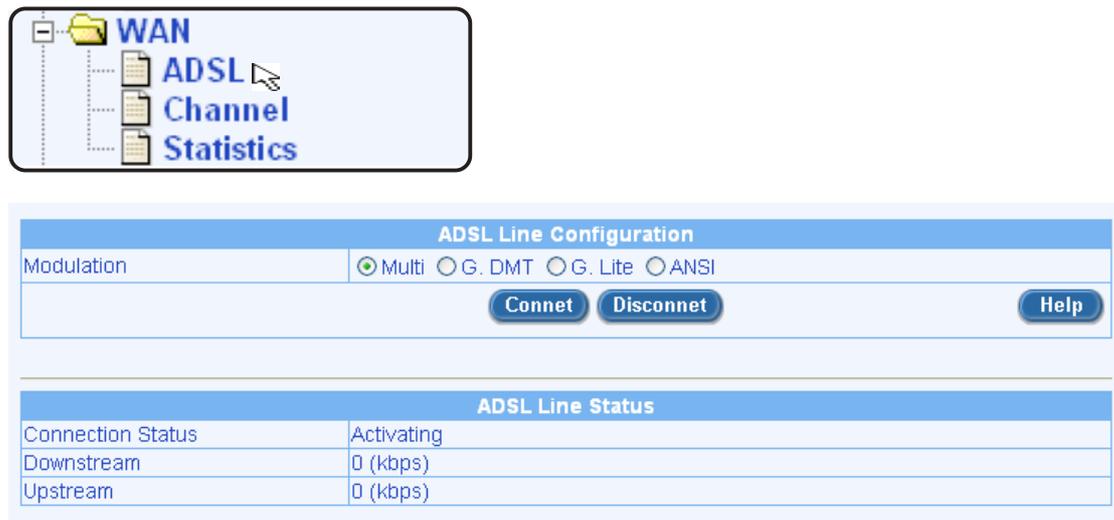


Figure 7.1 ADSL Connection Page

7.2 WAN Configuration

For WAN port configuration, there are several different protocols supported by SL6000/SL6300 to match your ISP's requirement, including MPoA Bridged, PPPoE Relay, MPoA Routed, IPoA Routed, PPPoA Routed and PPPoE Routed.

7.2.1 MPoA Bridged and PPPoE Relay:

No further configuration parameters need to be specified for MpoA Bridged and PPPoE Relay services.

7.2.2 MPoA Routed:

- * DHCP IP Address Assignment: Select this option if the MPoA Routed Service interface is to obtain its IP address from your ISP via DHCP.
- * Static IP Address Assignment: Select this option if the MPoA Routed Service interface is to have its IP address configured statically.
- * IP Address: Enter the MPoA Routed service interface's IP Address. Contact your ISP for details
- * Subnet Mask: Enter the MPoA Routed service interface's Subnet Mask. Contact your ISP for details.

7.2.3 IPoA Routed:

- * DHCP IP Address Assignment: Select this option if the IPoA Routed Service interface is to obtain its IP address from your ISP via DHCP.
- * Static IP Address Assignment: Select this option if the IPoA Routed Service interface is to have its IP address configured statically.
- * IP Address: Enter the IPoA Routed service interface's IP Address. Contact your ISP for details
- * Subnet Mask: Enter the IPoA Routed service interface's Subnet Mask. Contact your ISP for details.

7.2.4 PPPoA Routed and PPPoE Routed:

- * **Username:** The user name for setting up the PPPoA/PPPoE Service. Contact your ISP for the specific user name to be used.
- * **Password:** The password for setting up the PPPoA/PPPoE Service. Contact your ISP for the specific password to be used for initial setup.
- * **DoD :** Dial on Demand. The SL6000/SL6300 attempts to connect to your ISP when an outgoing traffic is detected.
- * **Inactivity Timeout:** The amount of time that specifies the PPP connection must elapse due to inactivity.

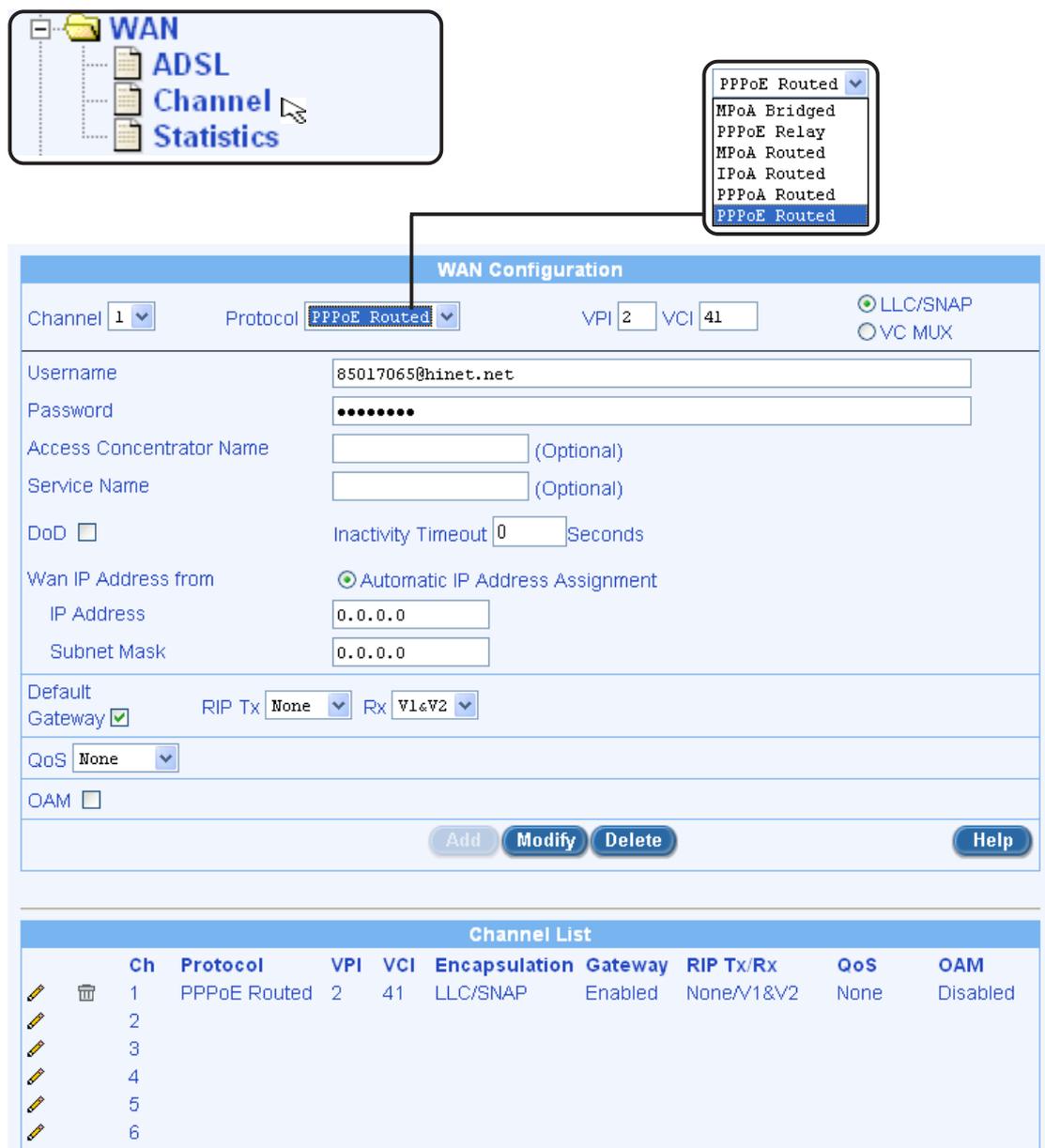


Figure 7.2 WAN Configuration Page

7.3 Viewing WAN/ADSL Statistics

You can view statistics of your WAN/ADSL traffic. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

To view WAN/ADSL statistics, click Statistics on the WAN submenu. Figure 7.3 shows the WAN/ADSL Statistics page.



WAN Statistics		
Modem Statistics	Downstream	Upstream
SNR Margin	0 (db)	0 (db)
Attenuation	0 (db)	0 (db)
Data Rate	0 (Kbps)	0 (Kbps)
Latency	0	0
Performance Errors	Downstream	Upstream
HEC Errors	0	0
CRC Errors	0	0
FEC Errors	0	0
Refresh		

Figure 7.3 WAN Statistics Page

To see the updated statistics since you opened the page, simply click **[Refresh]**.

8. Configuring 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 routes.

Note that most users do not need to define routes.

8.1 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 SL6000/SL6300 uses to make these decisions.

8.1.1 Do I need to define IP routes?

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the SL6000/SL6300 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 SL6000/SL6300. 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 SL6000/SL6300 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 8.3.2 Adding Static Routes.)

You may need to define 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.

8.2 DNS Relay Configuration

You may input your ISP's Primary/Secondary DNS server address here if your PC's DNS server address is directed to SL6000/SL6300, instead of automatically getting DNS server address from the ISP. Click **[Apply]** after typing your ISP's Primary/Secondary DNS server address.



DNS Relay Configuration	
Primary DNS Server	168.95.192.1
Secondary DNS Server	
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

DNS Relay Configuration	
Primary DNS Server	168.95.192.1
Secondary DNS Server	

Figure 8.1 DNS Relay Configuration Page

8.3 Static Routing

8.3.1 Static Route Configuration Parameters

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

Chapter 8

Table 8.1 Static Route Configuration Parameters

Destination IP 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 A for an explanation of network ID.
Destination Subnet
Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix A, for an explanation of network masks. The default route uses a netmask of 0.0.0.0.
Gateway IP Address
Gateway IP address

8.3.2 Adding Static Routes

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

1. In the Static Routes Configuration page (as shown in Figure 8.2.), enter static routes information such as destination IP address, Destination Subnet and Gateway IP address in the corresponding fields.

For a description of these fields, refer to Table 8.1 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 Destination Subnet fields.

2. Click **[Add]** to add a new route.

8.3.3 Modifying Static Routes

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

1. In the Static Routes Configuration page (as shown in Figure 8.2.), select the route from the service drop-down list or click on the  icon of the route to be modified in the Static Routing Table.
2. Click **[Modify]** to modify the selected route.

8.3.4 Deleting Static Routes

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

- In the Static Routes Configuration page (as shown in Figure 8.2), select the route from the service drop-down list or click on the  icon of the route to be deleted in the Static Routing Table.
- Click **[Delete]** to delete the selected route.



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.

8.3.5 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 SL6000/SL6300's routing table, click the **Routing** sub menu under Networking. The Static Routing Table displays in the lower half of the Static Routing Configuration page, as shown in Figure 8.2:

The Static 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. This table shows only user-added routes.



Static Routing Configuration	
Add New <input type="button" value="v"/>	
Destination IP	<input type="text"/>
Destination Subnet	<input type="text"/>
Gateway	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	
Static Routing Table	
Destination IP	Destination Subnet Gateway

Figure 8.2 Static Routing Configuration Page

9. Configuring Firewall/NAT Settings

SL6000/SL6300 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 who should be automatically notified.

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

- Create, modify and delete inbound/outbound ACL rules.
- Create, modify and delete predefined services to be used in inbound/outbound ACL configurations.
- Create service list (DOS)
- View ACL inbound/outbound rules
- View firewall statistics.



Note: When you define an ACL rule, you instruct the SL6000/SL6300 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 DoS Protection and Stateful Packet Inspection

The firewall as implemented in SL6000/SL6300 provides DoS (Denial of Service) protection and stateful packet inspection as the first line security for your network. No configuration is required for this protection on your network as long as firewall is enabled for SL6000/SL6300. By default, the firewall is enabled at the factory. Please refer to section 12.1 Global Setting Configuration to enable or disable firewall service on SL6000/SL6300.

9.2 Default ACL Rules

SL6000/SL6300 supports four types of default access rules:

- Inbound Access Rules: for controlling incoming access to computers on your LAN.
- Outbound Access Rules: for controlling outbound access to external networks for hosts on your LAN.
- Group Access Rules: for controlling users and user group information on your LAN.
- Self Access Rules: for controlling access privilege to SL6000/SL6300 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.

9.3 Configuring Inbound ACL Rules

By creating ACL rules in Inbound ACL configuration page as shown in Figure 9.1, 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 ACL rules

Chapter 9



Figure 9.1 Inbound ACL Configuration Page

Inbound Access Control Configuration				
ID	<input type="button" value="Add New"/>	Action	<input type="button" value="Allow"/>	Move to <input type="button" value="1"/>
Source IP	Type	WAN		
Destination IP	Type	LAN		
Source Port	Type	Any		
Destination Port	Type	Any		
Protocol	All			
Port Mapping	Type	None		
Time Range	Always			
Application Filters	FTP	None	HTTP	None
			RPC	None
				SMTP
				None
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable			
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>				<input type="button" value="Help"/>

Inbound Access Control List				
ID	Source IP	Destination IP	Protocol	Act

The diagram illustrates the configuration of an Inbound Access Control rule. The main configuration window is shown with several dropdown menus open to show their options:

- Source IP Type:** WAN
- Destination IP Type:** LAN
- Port Mapping Type:** IP Address (Value: 192.168.8.28)
- Service:** HTTP
- Application Filters:** HTTP
- Log:** Disable
- VPN:** Disable

The 'Service' dropdown menu is expanded to show a list of services, including:

- L2TP
- H323GK
- CUSEEME
- MSN-ZONE
- ILS
- ICQ_2002
- ICQ_2000
- MSN
- AOL
- RPC
- RTSP7070
- RTSP554
- QUAKE
- N2P
- PPTP
- MSG2
- MSG1
- IRC
- IKE
- H323
- IMAP4
- HTTPS
- DNS
- SNMP
- NNTP
- POP3
- SMTP
- HTTP
- FTP
- TELNET

9.3.1 Options in Inbound ACL Configuration Page

Table 9.1 describes the options available for an inbound ACL rule.

Table 9.1 Options in the Firewall Inbound ACL Configuration Page

ID
Add New
Click on this option to add a new 'basic' Firewall rule.
Rule Number
Select a rule from the drop-down list, to modify its attributes.
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.
Move to
This option allows you to set a priority for this rule. The SL6000/SL6300 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.

Source IP
This section allows you to set the source network to which this rule should apply. Use the drop-down list to select one of the following:
WAN
This option allows you to apply this rule inclusively on all computers in the external network.
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 in the blank field.
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: Subnet Address: Enter the appropriate IP address in the blank field. Subnet Mask: Enter the corresponding subnet mask in the blank field.
IP Range
This option allows you to include a range of IP addresses for applying this rule. The following fields become available for entry when this option is selected: Start IP: Enter the starting IP address of the range End IP: Enter the ending IP address of the range
IP Pool
This option allows you to include a pool of IP addresses for applying this rule. The following fields become available for entry when this option is selected. IP Pool: You can associate a pre-configured IP pool (see section 9.9.3) that you had added to the rule.

Destination IP
This section allows you to set the destination network to which this rule should apply. Use the drop-down list to select one of the following:
LAN
This option allows you to apply this rule inclusively on all computers in the local network.
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 in the blank field.
Subnet
This option allows you to include all computers that are connected in an IP subnet. When selected, the following fields become available for entry: Subnet Address: Enter the appropriate IP address in the blank field. Subnet Mask: Enter the corresponding subnet mask in the blank field.
IP Range
This option allows you to include a range of IP addresses for applying this rule. The following fields become available for entry when this option is selected: Start IP: Enter the starting IP address of the range End IP: Enter the ending IP address of the range
IP Pool
This option allows you to include a pool of IP addresses for applying this rule. The following fields become available for entry when this option is selected: IP Pool: You can associate a pre-configured IP pool (see section 9.9.3) that you had added to the rule.

Source Port	
Any	Select this option if you want this rule to apply to all applications with an arbitrary source port number.
Single	This option allows you to apply this rule to an application with a specific source port number. Port: 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. Begin Port: Enter the starting port number of the range End Port: Enter the ending port number of the range
Destination Port	
Any	Select this option if you want this rule to apply to all applications with an arbitrary source port number.
Single	This option allows you to apply this rule to an application with a specific source port number. Port: Enter the destination 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. Begin Port: Enter the starting port number of the range End Port: Enter the ending port number of the range
Service	This option allows you to select any of the pre-configured services (selectable from the drop-down list) instead of the destination port. The following are examples of services: BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. Note: service is a combination of protocol and port number. They appear here after you add them in the “Firewall Service” configuration page.

Protocol
You may select proper protocols here, including “All”, “TCP”, “UDP”, “ICMP”, “AH” and “ESP”.
Port Mapping
None
Select this to not use Port Mapping.
NAT Pool
Select this to use the IP addresses in the NAT Pool (see section 9.9.2).
IP Address
Select this option to specify the IP address of the computer that you want the incoming traffic to be directed.
Time Range
Only “Always” available for the time being.
Application Filters
FTP: Only “None” available for the time being. HTTP: Only “None” available for the time being. RPC: Only “None” available for the time being. SMTP: Only “None” available for the time being.
Log
Select “Enable” radio button to enable logging for this ACL rule; otherwise, select “Disable”.
VPN
This option allows you to select the check box if this policy corresponds to VPN policy.

9.3.2 Add Inbound ACL Rules

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

1. Log into Configuration Manager as admin, click the Firewall menu, and then click Inbound ACL submenu. The Firewall Inbound ACL Configuration page displays, as shown in Figure 9.1.

Note that when you open the Inbound ACL Configuration page, a list of existing ACL rules are also displayed in the lower half of the configuration page such as those shown in Figure 9.2. By default, no inbound access rule is configured.

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, port mapping, log, and VPN. Please see Table 9.1 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 lower half of the Inbound ACL Configuration page.

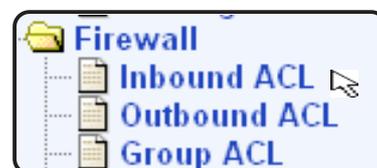


Figure 9.2 illustrates how to create a rule to allow inbound HTTP (i.e. web server) service. This rule allows inbound HTTP traffic to be directed to the

Inbound Access Control Configuration		
ID	<input type="button" value="Add New"/>	Action <input type="button" value="Allow"/> Move to <input type="button" value="1"/>
Source IP	Type	<input type="button" value="WAN"/>
Destination IP	Type	<input type="button" value="LAN"/>
Source Port	Type	<input type="button" value="Any"/>
Destination Port	Type	<input type="button" value="Service"/>
	Service	<input type="button" value="HTTP"/>
Port Mapping	Type	<input type="button" value="IP Address"/>
	IP Address	<input type="text" value="192.168.8.28"/>
Time Range	<input type="button" value="Always"/>	
Application Filters	FTP <input type="button" value="None"/> HTTP <input type="button" value="None"/> RPC <input type="button" value="None"/> SMTP <input type="button" value="None"/>	
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>		

9.3.3 Modify Inbound ACL Rules

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

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Inbound ACL** submenu.
2. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be modified in the inbound ACL table.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, port mapping, log, and VPN. Please see Table 9.1 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 lower half of the Inbound ACL Configuration page.

9.3.4 Delete Inbound ACL Rules

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

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Inbound ACL** submenu.
2. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be modified in the inbound ACL table.
3. Click on the [**Delete**] button to delete this ACL rule. Note that the ACL rule deleted will be removed from the ACL rule table located at the lower half of the same configuration page.

9.3.5 Display Inbound ACL Rules

To see existing inbound ACL rules, follow the instructions below:

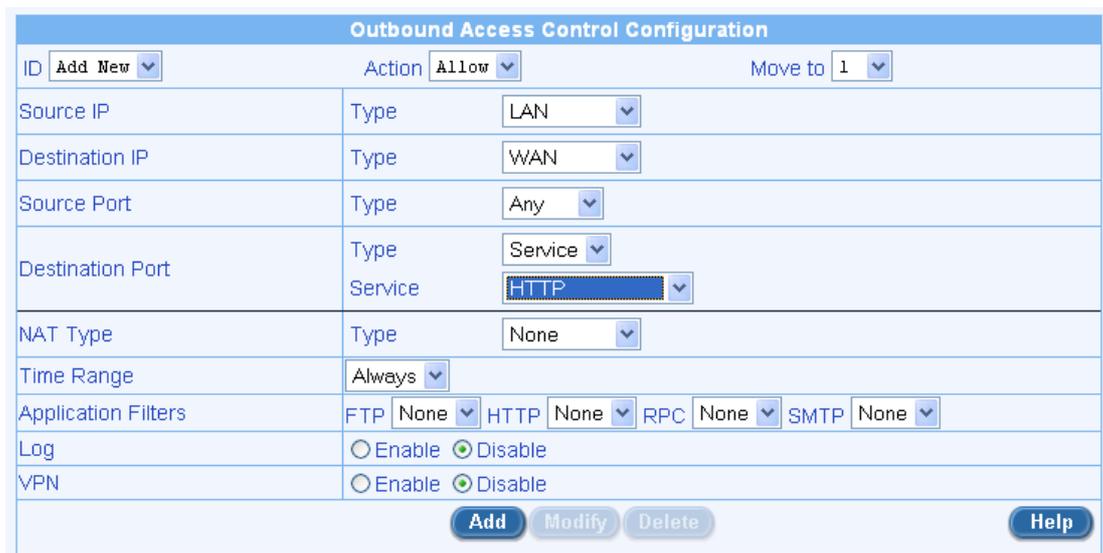
1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Inbound ACL** submenu.
2. The inbound ACL rule table located at the lower half of the Inbound ACL Configuration page shows all the configured inbound ACL rules.

9.4 Configuring Outbound ACL Rules

By creating ACL rules in outbound ACL configuration page as shown in Figure 9.3, 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 ACL rules



Outbound Access Control Configuration	
ID <input type="button" value="Add New"/>	Action <input type="button" value="Allow"/> Move to <input type="button" value="1"/>
Source IP	Type <input type="button" value="LAN"/>
Destination IP	Type <input type="button" value="WAN"/>
Source Port	Type <input type="button" value="Any"/>
Destination Port	Type <input type="button" value="Service"/> Service <input type="button" value="HTTP"/>
NAT Type	Type <input type="button" value="None"/>
Time Range	<input type="button" value="Always"/>
Application Filters	FTP <input type="button" value="None"/> HTTP <input type="button" value="None"/> RPC <input type="button" value="None"/> SMTP <input type="button" value="None"/>
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	

Figure 9.3 Outbound ACL Configuration Page

9.4.1 Options in Outbound ACL Configuration Page

Table 9.2 describes the options available for an outbound ACL rule.

Table 9.2 Options in the Firewall Outbound ACL Configuration Page

ID
Add New
Click on this option to add a new 'basic' Firewall rule.
Rule Number
Select a rule from the drop-down list, to modify its attributes.
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.
Move to
This option allows you to set a priority for this rule. The SL6000/SL6300 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.

Source IP
This section allows you to set the source network to which this rule should apply. Use the drop-down list to select one of the following:
LAN
This option allows you to apply this rule inclusively on all computers in your local network.
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 in the blank field.
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: Subnet Address: Enter the appropriate IP address in the blank field. Subnet Mask: Enter the corresponding subnet mask in the blank field.
IP Range
This option allows you to include a range of IP addresses for applying this rule. The following fields become available for entry when this option is selected: Start IP: Enter the starting IP address of the range End IP: Enter the ending IP address of the range
IP Pool
This option allows you to include a pool of IP addresses for applying this rule. The following fields become available for entry when this option is selected: IP Pool: You can associate a pre-configured IP pool (see section 9.9.3) that you had added to the rule.

Destination IP
This section allows you to set the destination network to which this rule should apply. Use the drop-down list to select one of the following:
WAN
This option allows you to apply this rule inclusively on all computers in the external network.
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 in the blank field.
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: Subnet Address: Enter the appropriate IP address in the blank field. Subnet Mask: Enter the corresponding subnet mask in the blank field.
IP Range
This option allows you to include a range of IP addresses for applying this rule. The following fields become available for entry when this option is selected: Start IP: Enter the starting IP address of the range End IP: Enter the ending IP address of the range
IP Pool
This option allows you to include a pool of IP addresses for applying this rule. The following fields become available for entry when this option is selected: IP Pool: Enter the IP pool number in the blank field.
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. Begin Port: Enter the starting port number of the range End Port: Enter the ending port number of the range

Chapter 9

Source Port
Any
Select this option if you want this rule to apply to all applications with an arbitrary source port number.
Single
This option allows you to apply this rule to an application with a specific source port number. Port: Enter the source port number
Destination Port
Any
Select this option if you want this rule to apply to all applications with an arbitrary source port number.
Single
This option allows you to apply this rule to an application with a specific source port number. Port: Enter the destination 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. Begin Port: Enter the starting port number of the range End Port: Enter the ending port number of the range
Service
This option allows you to select any of the pre-configured services (selectable from the drop-down list) instead of the destination port. The following are examples of services: BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. Note: service is a combination of protocol and port number. They appear here after you add them in the “Firewall Service” configuration page.

Protocol
You may select proper protocols here, including “All”, “TCP”, “UDP”, “ICMP”, “AH” and “ESP”.
NAT Type
None
Select this to not use NAT.
NAT Pool
Select this to use the associated IP addresses in the NAT Pool (see section 9.9.2).
IP Address
Select this option to specify the IP address of the computer that you want the incoming traffic to be directed.
Interface
Select the external interface as the NAT IP address.
Time Range
Only “Always” available for the time being.
Application Filters
FTP: Only “None” available for the time being. HTTP: Only “None” available for the time being. RPC: Only “None” available for the time being. SMTP: Only “None” available for the time being.
Log
Select “Enable” radio button to enable logging for this ACL rule; otherwise, select “Disable”.
VPN
This option allows you to select the check box if this policy corresponds to VPN policy.

9.4.2 Add an Outbound ACL Rule

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

1. Log into Configuration Manager as admin, click the Firewall menu, and then click Outbound ACL submenu. The Firewall Outbound ACL Configuration page displays, as shown in Figure 9.3.



Note that when you open the Outbound ACL Configuration page, a list of existing ACL rules are also displayed in the lower half of the configuration page such as those shown in Figure 9.3.

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, port mapping, log, and VPN. Please see Table 9.2 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 outbound access control list table at the lower half of the Outbound ACL Configuration page.

Figure 9.4 illustrates how to create a rule to allow outbound HTTP traffic. This rule allows outbound HTTP traffic to be directed to any host on the external network for a host in your LAN w/ IP address 192.168.1.15.

Outbound Access Control Configuration	
ID	Add New
Action	Allow
Move to	1
Source IP	Type: IP Address IP Address: 192.168.1.15
Destination IP	Type: WAN
Source Port	Type: Any
Destination Port	Type: Service Service: HTTP
NAT Type	Type: None
Time Range	Always
Application Filters	FTP: None HTTP: None RPC: None SMTP: None
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	

Figure 9.4 Outbound ACL configuration example. (No predefined ACL rule.)

9.4.3 Modify Outbound ACL Rules

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

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Outbound ACL** submenu.
2. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be modified in the outbound ACL table.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, port mapping, log, and VPN. Please see Table 9.1 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 lower half of the Outbound ACL Configuration page.

9.4.4 Delete Outbound ACL Rules

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

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Outbound ACL** submenu.
2. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be deleted in the outbound ACL table.
3. Click on the [**Delete**] button to delete this ACL rule. Note that the ACL rule deleted will be removed from the ACL rule table located at the lower half of the same configuration page.

9.4.5 Display Outbound ACL Rules

To see existing outbound ACL rules, follow the instructions below:

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Outbound ACL** submenu.
2. The outbound ACL rule table located at the lower half of the Outbound ACL Configuration page shows all the configured outbound ACL rules.

9.5 Configuring Group ACL Rules

With this option, you can allow users belonging to different groups to access different services at any desired time-frame. For instance, you can configure user1 belonging to group1 to have access to services like NetMeeting during morning and configure user2 of group2 to deny access to ICQ chat during office hours. This user login is quite different from administrator's login to SL6000/SL6300.

Prior to configuring the access rule for user groups, you should have: (See section 9.9.4 "Firewall User".)

- Created a user group
- Created a user within that group

9.5.1 Add/Delete a User Group

1. To add a new user groups access rule, choose the **Add New** option in the drop down list, select the action as either **Allow** or **Deny**. (Figure 9.5)
2. Choose the Rule Type that you'd like to add from the drop down list.
3. Select the user group from the drop down list.
4. Choose the Source IP from the drop down list, from where you'd like to allow the traffic.
5. Choose the Destination IP from the drop down list, to where you'd like to allow the traffic.
6. Choose the Source Port from the drop down list, from where you'd like to allow the traffic.
7. Choose the Destination Port from the drop down list, to where you'd like to allow the traffic.
8. Select the protocol of traffic. If you'd like to allow the traffic using NAT, select the **NAT Pool** or **Interface**.
9. If you'd like to allow the traffic during any specific time, choose the Time range option.
10. You can associate any Application Filter by selecting the filters from the drop down list.
11. You can enable log and VPN for this Rule.
12. You can set the priority of the rule by making the rule first or second depending on your wish.

13. Finally, click on the **[Add]** button. To view the existing or the configured rules, choose the rule id from the drop down list. To delete an existing rule, choose the rule id in the drop down list and click on **[Delete]** the button.

The detail inbound/outbound ACL rule configurations are also described in **9.3 Configuring Inbound ACL Rules** and **9.4 Configuring Outbound ACL Rules**.



Group Access Control Configuration								
ID	<input type="button" value="Add New"/>	Action	<input type="button" value="Allow"/>	Type	<input type="button" value="Outbound"/>	Group	<input type="button" value="1"/>	
Source IP	Type		<input type="button" value="LAN"/>					
Destination IP	Type		<input type="button" value="WAN"/>					
Source Port	Type		<input type="button" value="Any"/>					
Destination Port	Type		<input type="button" value="Any"/>					
Protocol	<input type="button" value="All"/>							
NAT Type	Type <input type="button" value="None"/>							
Time Range	<input type="button" value="Always"/>							
Application Filters	FTP	<input type="button" value="None"/>	HTTP	<input type="button" value="None"/>	RPC	<input type="button" value="None"/>	SMTP	<input type="button" value="None"/>
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable							
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable							
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>							<input type="button" value="Help"/>	

Figure 9.5 Group Access Control Configuration Page

9.6 Configuring Self Access Rules

With this option, you can configure the rules for controlling packets addressed to SL6000/SL6300 itself.



9.6.1 Add a Self Access Rule

1. To add a new user groups access rule, choose the **Add New** option in the drop down list.
2. Select the protocol from the drop down list and enter the port number that you want to configure.
3. Choose the direction (from LAN/WAN) that you want to add.
4. Finally, click on the **[Add]** button (Figure 9.6).

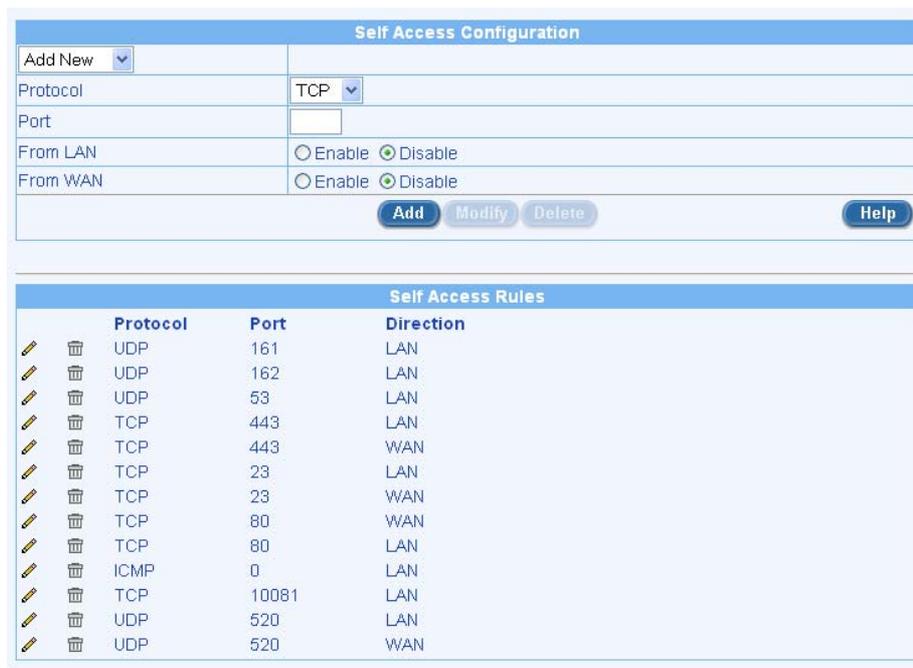


Figure 9.6 Self Access Configuration Page

9.6.2 View Self Access Summary

You can see the list of all the self access rules that are currently configured for your SL6000/SL6300 with all their attributes.

9.6.3 Delete Self Access Rule

To delete an existing self access rule, choose the rule in the drop down list and click on the **Delete** button.

9.7 Configuring Service List

Services are a combination of Protocol and Port number. It is used in inbound and outbound ACL rule configuration. You may use Service Configuration Page to:

- Add a service, and set parameters for it
- Modify an existing service
- Delete an existing service
- View configured services

Figure 9.7 shows the Firewall Service Configuration page. The configured services are listed at the lower half of the same page.



Service Configuration

Add New ▼

Service Name

Public Port

Protocol TCP ▼

Add
Modify
Delete

Help

Service List

		Name	Protocol	Public Port
		BATTLE-NET	TCP	6112
		PC-ANYWHERE	UDP	22
		FINGER	TCP	79
		DIABLO-II	TCP	4000
		L2TP	UDP	1701
		H323GK	UDP	1719
		CUSEEME	TCP	7648
		MSN-ZONE	TCP	28801
		ILS	TCP	389
		ICQ_2002	TCP	5190
		ICQ_2000	TCP	5191
		MSN	TCP	1863
		AOL	TCP	5190
		RPC	UDP	111
		RTSP7070	TCP	7070
		RTSP554	TCP	554
		QUAKE	UDP	27910
		N2P	UDP	6801
		PPTP	TCP	1723
		MSG2	UDP	47624
		MSG1	TCP	47624
		IRC	TCP	6667
		IKE	UDP	500
		H323	TCP	1720
		IMAP4	TCP	143
		HTTPS	TCP	443
		DNS	UDP	53
		SNMP	UDP	161
		NNTP	TCP	119
		POP3	TCP	110
		SMTP	TCP	25
		HTTP	TCP	80
		FTP	TCP	21
		TELNET	TCP	23

Figure 9.7 Firewall Service Configuration Page

Chapter 9

9.7.1 Options in Service Configuration Page

Table 9.3 describes the available configuration parameters for firewall service list.

Table 9.3. Service List configuration parameters

Service Name
Enter the name of the Service to be added. Note that only alphanumeric characters are allowed in a name.
Protocol
Enter the type of protocol the service uses.
Port
Enter the port number that is set for this service.

9.7.2 Add a Service

To add a service, follow the instructions below:

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Service** submenu. The Firewall Service Configuration page displays, as shown in Figure 9.7.



Note that when you open the Service Configuration page, a list of existing services are also displayed in the lower half of the configuration page such as those shown in Figure 9.7.

2. Select “**Add New**” from the service drop-down list.
3. Enter a desired name, preferably a meaningful name that signifies the nature of the service, in the “**Service Name**” field. Note that only alphanumeric characters are allowed in a name.
4. Specify any or all of the following fields: public port and protocol. Please see Table 9.3 for explanation of these fields.
5. Click on the [**Add**] button to create the new service. The new service will then be displayed in the service list table at the lower half of the Service Configuration page.

9.7.3 Modify a Service

To modify a service, follow the instructions below:

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Service** submenu.

2. Select the service from the service drop-down list or click on the  icon of the service to be modified in the service list table.
3. Make desired changes to any or all of the following fields: service name, public port and protocol. Please see Table 9.3 for explanation of these fields.
4. Click on the [**Modify**] button to modify this service. The new settings for this service will then be displayed in the service list table at the lower half of the Service Configuration page.

9.7.4 Delete a Service

To delete a service, follow the instructions below:

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Service** submenu.
2. Select the service from the service drop-down list or click on the  icon of the service to be deleted in the service list table.
3. Click on the [**Delete**] button to delete this service. Note that the service deleted will be removed from the service list table located at the lower half of the same configuration page.

9.7.5 View Configured Services

To see a list of existing services, follow the instructions below:

1. Log into Configuration Manager as admin, click the **Firewall** menu, and then click **Service** submenu.
2. The service list table located at the lower half of the Service Configuration page shows all the configured services.

9.8 DoS (Denial of Service)

SL-600/SL6300 is able to protect your network against the following attacks by proper configuration in this page (Figure 9.8)

9.8.1 SYN Flooding Attack Check

This attack involves sending connection requests to a server, but never fully completing the connections. This will cause some computers to get into a “stuck state” where they cannot accept connections from legitimate users. (“SYN” is short for “SYNchronize”; this is the first step in opening an Internet connection). You can select this box if you wish to protect the network from TCP Syn flooding.

9.8.2 Winnuke Attack Check

Certain older versions of the MS 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 the check box.

9.8.3 MIME Flood Attack Check

You can select this box to protect the mail server in your network against MIME flooding.

9.8.4 Maximum IP Fragment Count

This data is used during transmission or reception of IP fragments. When large sized packets are sent via SL6000/SL6300, SL6000/SL6300 fragments the large sized packets (depending on the Maximum Transmission Unit). By default, it's set to 45. If the Maximum Transmission Unit (MTU) of the interface is 1500 (default for Ethernet) then there can be a maximum of 45 fragments per IP packet. If the MTU is less then this number, there can be more number of fragments.



DoS Attacks Filter Configuration	
SYN Flooding	<input checked="" type="checkbox"/>
Winnuke	<input type="checkbox"/>
MIME Flood	<input type="checkbox"/>
Max IP Fragment Count	45
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

DoS Attacks Protection List	
<ul style="list-style-type: none"> IP Reassembly Attacks <ul style="list-style-type: none"> - Bonk - Boink - Teardrop(New Tear) - Overdrop - Opentear - Syndrop - Jolt ICMP Attacks <ul style="list-style-type: none"> - Ping of Death 	

Figure 9.8 DoS Configuration Page

If any of the above check is disabled then Firewall will no longer offer protection against the disabled item(s) and the LAN network might become vulnerable.

9.9 Policy List

9.9.1 Application Filter

With this option, you can define filters that can be associated with access rules for filtering commands of SMTP, FTP and RPC services and HTTP file extensions.

- * For FTP, SMTP and RPC service filters: If an application filter is configured to allow certain commands, SL6000/SL6300 will allow **ONLY** those commands. If an application filter is configured to deny certain commands, SL6000/SL6300 will deny **ONLY** those commands.
- * For HTTP application filter: The application filter can be set only to deny file extensions.
 1. To add a new application filter, choose the Filter type first from the drop down list.
 2. Then choose the Add New option in the drop down list, enter the Filter name in the text box.
 3. Choose the Protocol from the drop down list.
 4. Enter the Port value
 5. Choose the action as Allow or Deny depending on whether you'd like to allow or deny the commands. You can also chose to log messages whenever SL6000/SL6300 drops or allows a packet based on the filter you've selected.
 6. You'd also have to type the commands in the Command text boxes depending the type of the filter you're adding or modifying.
 7. Finally click on the [**Add**] button to create a new application filter. To view the existing or the configured application filters, choose the Filter name in the drop down list. To delete an existing application filter, choose the Filter name in the drop down list and click on the button.

Table 9.4 Application Filter configuration parameters

Filter Type
You can select the Filter Type from the drop down list.
Filter Name
Type the Filter name that you would like to add.
Protocol
You can select the protocol from the drop down list.
Port
Type the port number. For example, if you're adding a HTTP filter the port would be 80
Log
You can enable or disable logging of messages whenever Broadband Gateway denies or allows a packet based on the filter that you've set. By clicking on enable you'd enable logging of such messages.
Commands
<p>You can refer to the commands by clicking on the [Help] button.</p> <ul style="list-style-type: none"> * FTP: You can filter any or all of FTP commands such as PORT, RETR, STOR, PASV etc. * HTTP: You can filter certain file extensions such *.java, *.ocx etc. * SMTP: You can filter any or all of SMTP commands such as VRFY * RPC: You can filter the specified RPC program numbers



Application Filter Configuration

Filter Type	FTP ▼												
Add New ▼													
Name	<input style="width: 90%;" type="text"/>												
Protocol	TCP ▼												
Port	<input style="width: 80%;" type="text"/>												
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable												
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny												
FTP Commands	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 33%; height: 20px;"></td><td style="width: 33%; height: 20px;"></td><td style="width: 33%; height: 20px;"></td></tr> <tr><td style="height: 20px;"></td><td style="height: 20px;"></td><td style="height: 20px;"></td></tr> <tr><td style="height: 20px;"></td><td style="height: 20px;"></td><td style="height: 20px;"></td></tr> <tr><td style="height: 20px;"></td><td style="height: 20px;"></td><td style="height: 20px;"></td></tr> </table>												
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input style="float: right;" type="button" value="Help"/>													

Application Filter List

Name	Type	Protocol	Action	Commands

Figure 9.9 Application Filter Configuration

9.9.2 NAT Pool

With this option you can configure NAT Pools and NAT IP Addresses and eventually you can associate NAT pools with policies. The NAT database and access rule database (or the Rule database) are closely associated. Interpretation of NAT database records is based on the usage of the records in the access rule database. A general idea about the access rule database is useful for understanding the NAT database.

1. To add a new NAT Pool, choose the **Add New** option in the drop down list.
2. Enter the NAT Pool name in the text box and choose the NAT pool type from the drop down list.
3. Enter the LAN and Internet IP address values depending on the NAT pool type you chose and finally click on the **[Add]** button.
4. To view the existing or the configured NAT pools, choose the NAT pool name in the drop down list.
5. To delete an existing NAT pool, choose the NAT pool name in the drop down list and click on the **[Delete]** button.

Table 9.5 NAT Pool configuration parameters

NAT Pool Name
Type the NAT pool name that you would like to add.
NAT Pool Type
You can select the NAT Pool Type from the drop down list. * Static: This type of NAT allows one address to be mapped exactly to one computer in the network. When a packet matches a policy with static NAT record, no port change will occur. The number of Internet IP addresses should be equal to the number of LAN IP Addresses. * Start IP: Specify the starting IP address in LAN and WAN (Internet) * End IP: Specify the ending IP address in LAN and WAN (Internet) * Dynamic: This type of NAT allows you to map a set of LAN computers to a set of Internet IP addresses, in a NAT Record. When this record is associated with an outbound policy, the source IP address of packets will be subjected to NAT and directed to one of the available Internet IP address. If no Internet IP address is free, the packet will be dropped. As an IP address is assigned to a single computer at any instant of time, there is no need for port translation.

- * **Start IP:** Specify the starting IP address in LAN and WAN (Internet)
- * **End IP:** Specify the ending IP address in LAN and WAN (Internet)
- * **Overload:** This is also referred to as NAPT. This type of NAT record allows you to use a single Internet IP address to connect multiple LAN machines to Internet.. When this NAT record is associated with a policy, matching packets will be subject to NAT using this Internet IP address. It also manages port translation.
- * **NAT IP Address:** Specify a single NAT IP Address
- * **Interface:** This is similar to NAPT (Internet IP). The only difference is that this setting takes the external interface as the Internet IP address. The IP address of the interface connected to the Internet will be used as the NAT IP address.

Note: If the static type NAT record is used in an Internet policy then packets from LAN to Internet with attributes that match this policy will be subject to NAT such that the source IP address of the packet gets modified to the corresponding IP address which is a public address. The source IP address of the packet should fall into the set of LAN IP Addresses. If the static type NAT record is used in an Internal Service policy then packets from Internet to LAN with attributes that match this policy will be subject to NAT such that the destination IP address of the packet gets modified to the corresponding IP address which is a private network address. The destination IP address of the packet should fall into the set of LAN IP addresses.



NAT Pool Configuration

Add New ▼

Name

Pool Type

Type Static ▼

LAN IP Start

LAN IP End

WAN IP Start

WAN IP End

Add
Modify
Delete
Help

NAT Pool List

Name	Type	IP Address	Interface	LAN IP Range	WAN IP Range

Figure 9.10 NAT Pool Configuration Page

9.9.3 IP Pool

With this option, you can configure IP addresses and eventually you can associate IP pools with access rules. Each IP pool contains:

- * The name of IP pool
 - * The type of the IP address: single IP address, range of IP addresses or a subnet address.
1. To add a new IP Pool name, choose the Add New option in the drop down list
 2. Enter the IP pool name in the text box and choose the IP pool type from the drop down list.
 3. Enter the IP address values depending on the pool type you chose and finally click on the **[Add]** button.
 4. To view the existing or the configured IP pools, choose the IP pool name in the drop down list.
 5. To delete an existing IP pool, choose the IP pool name in the drop down list and click on the **[Delete]** button.

Table 9.6 IP Pool configuration parameters

IP Pool Name	
Type the IP pool name that you would like to add.	
IP Pool Type	
*	You can select the IP Pool Type from the drop down list.
	• If you select IP Range, you have to specify
*	Start IP: Starting IP address in the IP Range
*	End IP: Ending IP address in the IP Range
	• If you select Subnet, you have to specify
*	IP Address: IP address in the respective Subnet
*	Subnet Mask: Subnet mask of the corresponding network
	• If you select IP Address, you have to specify
*	IP Address: Single IP Address



IP Pool Configuration

Add New

Name

Type

IP Pool Type

Start IP

End IP

IP Pool List

Name	Type	Start Address	End Address

Figure 9.11 IP Pool Configuration Page

9.9.4 Firewall User

With this option, you can add user groups and set users for each group. These user groups and users will be used to create rules that can permit remote access to users to access their LANs without compromising on security. You can configure individual groups with a set of access rules that will:

- * Define the resources for which they are allowed access
- * Be activated upon user login

When a user belonging to a group logs in via the Internet or from a local network, the SL6000/SL6300 creates dynamic policies by:

- * Activating all the rules configured for the group
- * Replacing the source IP address in the rule with IP address of the machine from which the user logged in.

SL6000/SL6300 stores them in a dynamic rule list and uses them for every connection from the user. It deletes this list after the user logs out of the GoC System's firewall.

1. To add a new User, you've to add a User-group first. Choose the Add New option in the drop down list, enter the User Group Name in the text box.
2. Choose the Add New option in the drop down list, enter the User Name in the text box.
3. Enter the Password that you'd like the user to have. Make sure that the Password entered is at least of 8 characters in length and it's alphanumeric. Type the same Password in Confirm Password text box.
4. Enter the Inactivity timeout value that you'd like to set. Finally, click on the button to make the changes effective.
5. To view the existing or the configured Users, choose the User name in the drop down list.
6. To delete an existing User or User group, choose the User name or the User group in the drop down list and click on the button.

Table 9.7 Firewall User configuration parameters

User Group Name
Type the User group name that you would like to add.
User Name
Type the User name that you would like to add.
Confirm Password
Type the User's password again to confirm.
Inactivity Timeout
Type the timeout period, which is used to delete the User related associations whenever there is no traffic across this connection.



Firewall User Configuration

<input style="border: none; background-color: #e0e0e0; padding: 2px 5px; font-size: small; vertical-align: top;" type="button" value="Add New"/>	
User Group Name	<input style="width: 95%;" type="text"/>
<input style="border: none; background-color: #e0e0e0; padding: 2px 5px; font-size: small; vertical-align: top;" type="button" value="Add New"/>	
User Name	<input style="width: 95%;" type="text"/>
Password	<input style="width: 95%;" type="password"/>
Confirm Password	<input style="width: 95%;" type="password"/>
Inactivity Timeout	<input style="width: 80%;" type="text"/> (Secs)

Firewall User List

User Name	Group Name	Inactivity Timeout

Figure 9.12 Firewall User Configuration Page

9.9.5 Time Range

With this option, you can configure access time range records for eventual association with access rules. Access rules associated with time range record will be active only during the scheduled period of time. If the Access rule denies HTTP access during 10.00hrs to 18hrs then before 10.00hrs and after 1800 hrs the HTTP traffic will be permitted to pass through.

When you configure Time range record they are saved in the Time Range (or schedules) database. One time range record can contain multiple time periods, for example:

- * Office hours on week days (Mon-Fri) can have the following periods:
 - a. Pre-lunch period between 9:00 and 13:00 Hrs
 - b. Post-lunch period between 14:00 and 18:30 Hrs
- * Office hours on week ends (Saturday) can have the following periods:
 - a. 9:00 and 12:00 Hrs

Such varying time periods can be configured into a single time range record. Access rules can be activated based on these time periods.

1. To add a new Time Range, choose the Add New option in the drop down list, enter the Time Range Name in the text box.
2. Only if you'd like to have a multiple time period range such as the one mentioned above you need to add a Schedule and not otherwise. In such a case, you can choose the Add New option in the drop down list. Select the starting and ending days of the week. Enter the time during which you'd like to allow the traffic in the Time field in hh:mm format.
3. Finally click on the **[Add]** button to create a new Time Range or Schedule.
4. To view the existing or the configured time ranges, choose the Time-range name in the drop down list.
5. To delete an existing Time-range or Schedule, choose the Time-range name or the Schedule in the drop down list and click on the **[Delete]** button.

Table 9.8 Time Range configuration parameters

Time Range Name
Enter the name of the Time range Record
Days of week
You can set the days-range for the new schedule: * In the left-side list - You can select the starting day of the range * In the right-side list - You can select the ending day of the range
Time
Type the time during which you'd like to allow the traffic in hh:mm format.



Time Range Configuration

Add New ▼

Time Range Name

Add New ▼

Days of Week

Time

Sunday ▼
to
Saturday ▼

:
to
 :
(hh:mm)

Add
Modify
Delete
Help

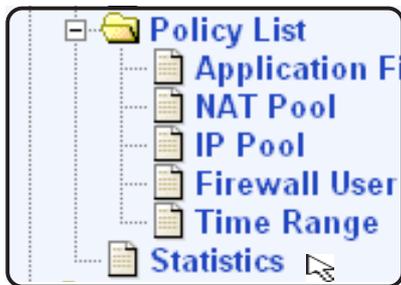
Time Range List

Name	Schedule1	Schedule2	Schedule3

Figure 9.13 Time Range Configuration Page

9.10 Firewall Statistics

The Firewall Statistics page displays details regarding the active connections. Figure 9.14 shows a sample firewall statistics for active connections. To see an updated statistics, click on [**Refresh**] button.



Active Connections							
Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	TCP	192.168.1.25 - 1252	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
LAN	TCP	192.168.1.25 - 1251	192.168.1.1 - 80	0.0.0.0 - 0	20	0	0
LAN	TCP	192.168.1.25 - 1250	192.168.1.1 - 80	0.0.0.0 - 0	8	0	0
Local	UDP	192.168.1.1 - 520	224.0.0.9 - 520	0.0.0.0 - 0	60	0	0

Total Connections Count			
TCP	UDP	ICMP	Others
3	1	0	0

[Refresh](#)

Figure 9.14 Firewall active connections statistics

10. Configuring VPN

The chapter contains instructions for configuring VPN connections using automatic keying and manual keys.

10.1 Default Parameters

The SL6000/SL6300 is pre-configured with a default set of proposals/connections. They cover the most commonly used sets of parameters, required for typical deployment scenarios. It is recommended that you use these pre-configured proposals/connections to simplify VPN connection setup. The default parameters provided in the SL6000/SL6300 are as follows:

Default Connections

Each connection represents a rule that will be applied on traffic originating from/terminating at the security gateway. It contains the parameters: local/remote IP-Addresses and ports. Table 10.1 lists the default connections that are provisioned on the gateway:

Table 10.1 Default connections in SL6000/SL6300

Name	Type	Port	Protocol	State	Purpose
allow-ike-io	passby	500	UDP	Enabled	To allow IKE traffic
allow-all	passby	---	---	Enabled	To allow plain traffic
Proposals					
<p>Each proposal represents a set of authentication/encryption parameters. Once configured, a proposal can be tied to a connection. Upon session establishment, one of the proposals specified is selected and used for the tunnel.</p> <p>Note that multiple proposals can be specified for a connection. If you do not specify the proposal to be used for a connection, all the pre-configured proposals will be included for that connection.</p>					
Pre-configured IKE proposals					
<p>IKE proposals decide the type of encryption, hash algorithms and authentication method that will be used for the establishment of the session keys between the endpoints of a tunnel.</p>					

Chapter 10

Pre-configured IPsec proposals

IPsec proposals decide the type of encryption and authentication of the traffic that flows between the endpoints of the tunnel.

Default lifetime

Default lifetime for the pre-configured IKE proposals and IPsec proposals is 3600 seconds. (One hour). It is recommended to set lifetime value greater than 600 seconds, for a new IKE proposal or IPsec proposal. This will reduce quick re-keying which will unnecessarily burden the system.

Limits for key length

The maximum key length for pre shared key, cipher key and Authentication Key is 50 characters. If the cipher key length is greater than the length specified by the encryption algorithm, the key is truncated to the appropriate length.

Priority of the connections

The allow-ike-io default rule has the highest priority (1). The allow-all default rule has the lowest priority. At any point of time it is recommended to maintain this priority. If you add connections below the allow-all rule (lower priority), it will not have any effect as the corresponding packets will match the allow-all rule and go without encryption.



Important: Note that pre-configured Proposals/Connections are read-only and cannot be modified. If you have to specify a proposal (other than the default), you should add a new one via VPN configuration page. This way you can control the proposals that become part of a connection.



Note: For the negotiation to succeed the peer gateway should also be configured with matching parameters. However if needed any specific proposal can be chosen.

This chapter includes the procedure to configure the Access List through GUI:

- Basic Access List Configuration
 - * Access List using IKE
 - * Access List using Manual Keys
- Advanced Access List Configuration
 - * Access List using IKE
 - * Access List using Manual Keys

10.2 Establish VPN Connection Using Automatic Keying

This section describes the steps to establish the VPN tunnel using the Configuration Manager. Internet Key Exchange (IKE) is the automatic keying protocol used to exchange the key that is used to encrypt/authenticate the data packets according to the user-configured rule. The parameters that should be configured are:

- the network addresses of internal and remote networks.
- the remote gateway address and the local gateway address.
- preshared secret for remote gateway authentication.
- appropriate priority for the connection.

Use them to configure basic Access Rule that will be used to establish a tunnel from local secure group to remote secure group with basic parameters.

Options in this screen allow you to:

- Add an Access List, and set basic parameters for it
- Modify an Access List
- Delete an existing Access List

10.2.1 VPN Tunnel Configuration Parameters for Automatic Keying

Table 10.4 describes the VPN tunnel configuration parameters using preshared key as key management mode.

Table 10.4 VPN tunnel configuration parameters using preshared key for key management

VPN Connection Settings

ID
Add New: Click on this option to add a new VPN rule. Rule number: Select a rule from the drop-down list, to modify its attributes.
Name
Enter a unique name, preferably a meaningful name that signifies the tunnel connection. Note that only alphanumeric characters are allowed in this field.
Enable
Select this radio button to enable this rule (default).
Disable
Select this radio button to disable this rule.
Move to
This option allows you to set a priority for this rule. The VPN service in SL6000/SL6300 acts on packets based on the priority of the rule, with 1 being the highest priority. Set a priority by specifying a number for its position in the list of rules: 1: This number marks the highest priority. Other numbers: Select other numbers to indicate the priority you wish to assign to the rule.
Local Secure Group
This option allows you to set the local secure network to which this rule should apply. This option allows you to apply this rule inclusively on all computers in the internal network. Use the "Type" drop-down list to select one of the following:
IP Address
This option allows you to specify an IP address on which this rule will be applied. IP Address: Enter the appropriate IP address.
Subnet
This option allows you to include all the computers that are connected in an IP subnet. The following fields become available for entry when this option is selected: Subnet Address: Specify the appropriate network address. Subnet Mask: Enter the subnet mask.

Chapter 10

Life Time

Enter the IKE security association life time in seconds, minutes, hours or days.

IPSec Proposal Settings

Encryption / Authentication

Select one of the following pre-configured IKE proposals from the drop-down list. If "All" is selected, all the pre-configured proposals will be associated with existing tunnel and one (among the set of IPSec proposals) will be selected automatically and used by IPSec to communicate with its peer.

- All
- Strong Encryption & Authentication (ESP 3DES HMAC SHA1)
- Strong Encryption & Authentication (ESP 3DES HMAC MD5)
- Encryption & Authentication (ESP DES HMAC SHA1)
- Encryption & Authentication (ESP DES HMAC MD5)
- Authentication (AH SHA1)
- Authentication (AH MD5)
- Strong Encryption (ESP 3DES)
- Encryption (ESP DES)
- Authentication (ESP SHA1)
- Authentication (ESP MD5)

Operation Mode

PFS Group

Select one of the following Perfect Forward Secrecy Diffie-Hellman Group from the drop-down list.

- NO PFS (default)
- DH-1
- DH-2
- DH-5

Note: Using PFS, keys will be changed during the course of a connection and make the tunnel more secure. However, enabling this option slows down the data transfer.

Life Times

Enter the life time of IPSec security association in seconds, minutes, hours or days and kilo bytes. Default value is 3600 seconds and 75000 kilo bytes.

10.2.2 Add a Rule for VPN Connection Using Preshared Key

VPN Tunnel Configuration Page, as illustrated in the Figure 10.1, is used to configure a rule for VPN connection using preshared key.



VPN Connection Settings

ID Add New Name Enable Disable Move to 1

Local Secure Group Type IP Address
 IP Address

Local Secure Gateway 1 : PPPoE Routed

Remote Secure Group Type IP Address
 IP Address

Remote Security Gateway

Key Management Preshared Key

IKE Proposal Settings

Authentication Preshared Key

Encryption/Authentication All

Life Time 3600 sec

IPSec Proposal Settings

Encryption/Authentication ALL

Encapsulation Tunnel Transport

PFS Group None

Life Time 3600 Sec or 75000 KByte

Add
Modify
Delete
Help

VPN Connection Status

	ID	Name	Local Gateway	Remote Gateway	Key Mgmt.	IPSec	Status
	1	New		192.168.8.1	Auto(IKE)	Tunnel	Enable
	2	allow-ike-io			Auto(IKE)	Tunnel	Enable
	3	allow-all			Auto(IKE)	Tunnel	Enable

Figure 10.1 VPN Tunnel Configuration Page - Preshared Key Mode

Chapter 10

To add a rule for a VPN connection, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu. The VPN Tunnel Configuration page displays, as shown in Figure 10.1.

Note that when you open the VPN Tunnel Configuration page, a list of existing rules for VPN connections are also displayed in the lower half of the configuration page such as those shown in Figure 10.1.

2. Prior to adding a VPN rule, make sure that the VPN service is enabled in System Service Configuration page.
3. Select “**Add New**” from the “**ID**” drop-down list.
4. Enter a desired name, preferably a meaningful name that signifies the nature of the VPN connection, in the “**Name**” field. Note that only alphanumeric characters are allowed in a name.
5. Click on “**Enable**” or “**Disable**” radio button to enable or disable this rule.
6. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select **Preshared Key**), preshared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec. Please see Table 10.4 for explanation of these fields.
7. 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 two being the highest as one is used by the rule, allow-ike-io, which is needed by IKE. Higher priority rules will be examined prior to the lower priority rules by the VPN.
8. Click on the [**Add**] button to create the new VPN rule. The new VPN rule will then be displayed in the VPN Connection Status table at the lower half of the VPN Configuration page.

10.2.3 Modify VPN Rules

To modify a VPN rule, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. Prior to modifying a VPN rule, make sure that the VPN service is enabled in System Service Configuration page.
3. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be modified in the VPN Connection Status table.

4. Click on “**Enable**” or “**Disable**” radio button to enable or disable this rule.
5. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select **Preshared Key**), preshared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec. Please see Table 10.4 for explanation of these fields.
6. Click on the [**Modify**] button to modify this VPN rule. The new settings for this VPN rule will then be displayed in the VPN Connection Status table at the lower half of the VPN Configuration page.

10.2.4 Delete VPN Rules

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

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. Prior to deleting a VPN rule, make sure that the VPN service is enabled in System Service Configuration page.
3. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be deleted in the VPN Connection Status table.
4. Click on the [**Delete**] button to delete this VPN rule. Note that the VPN rule deleted will be removed from the VPN Connection Status table located at the lower half of the same configuration page.

10.2.5 Display VPN Rules

To see existing VPN rules, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. The VPN rule table located at the lower half of the VPN Configuration page shows all the configured VPN rules.

10.3 Establish VPN Connection Using Manual Keys

This section describes the steps to establish the VPN tunnel-using manual keying. Manual keying is a method to achieve security when ease of configuration and maintenance is more important or automatic keying is not feasible due to interoperability issues between IKE implementations on the gateways. However, this is a weak security option as all packets use the same keys unless you - as the network administrator, use different key for authentication.

Chapter 10

10.3.1 VPN Tunnel Configuration Parameters - Manual Key

Table 10.5 describes the VPN tunnel configuration parameters using manual key.

Table 10.5 VPN tunnel configuration parameters using manual key for key management

VPN Connection Settings

ID
Add New: Click on this option to add a new VPN rule. Rule number: Select a rule from the drop-down list, to modify its attributes.
Name
Enter a unique name, preferably a meaningful name that signifies the tunnel connection. Note that only alphanumeric characters are allowed in this field.
Enable
Select this radio button to enable this rule (default).
Disable
Select this radio button to disable this rule.
Move to
This option allows you to set a priority for this rule. The VPN service in SL6000/SL6300 acts on packets based on the priority of the rule, with 1 being the highest priority. Set a priority by specifying a number for its position in the list of rules:
1: This number marks the highest priority.
Other numbers: Select other numbers to indicate the priority you wish to assign to the rule.
Local Secure Group
This option allows you to set the local secure network to which this rule should apply. This option allows you to apply this rule inclusively on all computers in the internal network. Use the "Type" drop-down list to select one of the following:
IP Address
This option allows you to specify an IP address on which this rule will be applied. IP Address: Enter the appropriate IP address.

Subnet
This option allows you to include all the computers that are connected in an IP subnet. The following fields become available for entry when this option is selected:
Subnet Address
Specify the appropriate network address.
Subnet Mask
Enter the subnet mask.
IP Range
This option allows you to include a range of IP addresses for applying this rule. The following fields become available for entry when this option is selected:
Start IP
Enter the starting IP address of the range.
End IP
Enter the ending IP address of the range.
Remote Secure Group
This option allows you to set the remote (destination) secure network to which this rule should apply. This option allows you to apply this rule inclusively on all computers in the external network. Use the "Type" drop-down list to select one of the following: IP Address, Subnet, IP Range: Select any of these and enter details as described in the Local Secure Group above.
Remote Secure Gateway
Enter the appropriate IP address for the remote secure gateway.
Key Management
Two modes are supported: preshared key and manual key.
Manual Key
Select Manual Key from the Key Management drop-down list.

IPSec Proposal Settings

Encryption / Authentication

Select one of the following pre-configured IKE proposals from the drop-down list. If “All” is selected, all the pre-configured proposals will be associated with existing tunnel and one will be selected automatically and used by IPSec to communicate with its peer.

All

Strong Encryption & Authentication (ESP 3DES HMAC SHA1)

Strong Encryption & Authentication (ESP 3DES HMAC MD5)

Encryption & Authentication (ESP DES HMAC SHA1)

Encryption & Authentication (ESP DES HMAC MD5)

Authentication (AH SHA1)

Authentication (AH MD5)

Strong Encryption (ESP 3DES)

Encryption (ESP DES)

Authentication (ESP SHA1)

Authentication (ESP MD5)

Operation Mode

Encryption Key

Enter the encryption key to be used. To enter in hex start with 0x.

Authentication Key

Enter the authentication key to be used. To enter in hex start with 0x.

Inbound SPI

Enter the inbound security parameter index.

Outbound SPI

Enter the outbound security parameter index.

10.3.2 Add a Rule for VPN Connection Using Manual Key

VPN Tunnel Configuration Page, as illustrated in the Figure 10.2, is used to configure a rule for VPN connection using manual key.

VPN Connection Status						
ID	Name	Local Gateway	Remote Gateway	Key Mgmt.	IPsec	Status

Figure 10.2 VPN Tunnel Configuration Page - Manual Key Mode

To add a rule for a VPN connection, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu. The VPN Tunnel Configuration page displays, as shown in Figure 10.2.



Note that when you open the VPN Tunnel Configuration page, a list of existing rules for VPN connections are also displayed in the lower half of the configuration page such as those shown in Figure 10.2.

2. Prior to adding a VPN rule, make sure that the VPN service is enabled in System Service Configuration page (see section 12.1 Global Setting Configuration).
3. Select “**Add New**” from the “**ID**” drop-down list.

4. Enter a desired name, preferably a meaningful name that signifies the nature of the VPN connection, in the “**Name**” field. Note that only alphanumeric characters are allowed in a name.
5. Click on “**Enable**” or “**Disable**” radio button to enable or disable this rule.
6. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select **Manual Key**), preshared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec. Please see Table 10.5 for explanation of these fields.
7. 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 two being the highest as one is used by the rule, allow-ike-io, which is needed by IKE. Higher priority rules will be examined prior to the lower priority rules by the VPN.
8. Click on the [**Add**] button to create the new VPN rule. The new VPN rule will then be displayed in the VPN Connection Status table at the lower half of the VPN Configuration page.

10.3.3 Modify VPN Rules

To modify a VPN rule, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. Prior to modifying a VPN rule, make sure that the VPN service is enabled in System Service Configuration page.
3. Select the rule number from the “**ID**” drop-down list or click on the  icon of the rule to be modified in the VPN Connection Status table.
4. Click on “**Enable**” or “**Disable**” radio button to enable or disable this rule.
5. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select **Preshared Key**), preshared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec. Please see Table 10.5 for explanation of these fields.
6. Click on the [**Modify**] button to modify this VPN rule. The new settings for this VPN rule will then be displayed in the VPN Connection Status table at the lower half of the VPN Tunnel Configuration page.

10.3.4 Delete VPN Rules

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

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. Prior to deleting a VPN rule, make sure that the VPN service is enabled in System Service Configuration page.
3. Select the rule number from the “**ID**” drop-down list or click on the icon of the rule to be modified in the VPN Connection Status table.
4. Click on the [**Delete**] button to delete this VPN rule. Note that the VPN rule deleted will be removed from the VPN Connection Status table located at the lower half of the same configuration page.

10.3.5 Display VPN Rules

To see existing VPN rules, follow the instructions below:

1. Log into Configuration Manager as admin, click the **VPN** menu, and then click **Tunnel** submenu.
2. The VPN rule table located at the lower half of the VPN Configuration page shows all the configured VPN rules.

10.4 VPN Statistics

Statistics option allows you to view the information about the VPN statistics - Global, IKE SAs and IPsec SAs. Table 10.6 gives description for the VPN statistics parameters.

Table 10.6 VPN Statistics

Global IPSEC SA
Overall packet statistics
AH Packets
Number of AH packets
ESP Packets
Number of ESP packets
Triggers
Number of triggers

Chapter 10

Packets Dropped
Number of packets dropped
Packets Passed
Total number of packets passed by VPN
Partial Packets
Total count of partial packets
Packets Currently Reassembled
Number of partial packets currently being reassembled
Non-First Fragments Currently in the Engine
Number of non-first fragments currently in the engine
IKE Statistics
IKE negotiation statistics
IKE Phase1 Negotiation Done
Number of IKE phase-1 negotiations performed
Failed IKE Negotiations Done
Number of failed IKE phase -1 negotiations
Quick Mode Negotiation Performed
Number of IKE quick mode negotiations performed
Number of ISAKMP SAs
Number of phase 1 SA's
ESP Statistics
Number of ESP statistics
Active Inbound ESP SAs
Number of active inbound ESP SA's
Active Outbound ESP SAs
Number of active outbound ESP SA's
Total Inbound ESP SAs
Number of inbound ESP SA's since the system has started

Total Outbound ESP SAs
Number of active outbound ESP SA's since the system has started
AH Statistics
SA statistics for all AH SAs
Active Inbound AH SAs
Number of active inbound AH SA's
Active Outbound AH SAs
Number of active outbound AH SA's
Total Inbound AH SAs
Number of inbound AH SA's since the system has started
Total Outbound AH SAs
Number of outbound AH SA's since the system has started

Figure 10.3 shows all the parameters available for VPN connections. To see an updated statistics, click on the **[Refresh]** button.



VPN Statistics
Global IPSec SA Statistics

AH Packets
 ESP Packets
 Triggers
 Packets Dropped
 Packets Passed
 Partial Packets
 Packets Currently Reassembled
 Non-First Fragments Currently in the Engine

IKE Statistics

IKE Phase1 Negotiations Done
 Failed IKE Negotiations Done
 Quick Mode Negotiations Performed
 Number of ISAKMP SAs

ESP Statistics

Active Inbound ESP SAs
 Active Outbound ESP SAs
 Total Inbound ESP SAs
 Total Outbound ESP SAs

AH Statistics

Active Inbound AH SAs
 Active Outbound AH SAs
 Total Inbound AH SAs
 Total Outbound AH SAs

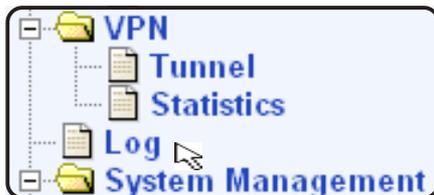
IKE SA

Local Address	Remote Address	Local Port	Remote Port	Phase1 Status	Exchange Type	Initiator
IPSec SA						
SPI	Protocol	Source Address	Destination Address			
<div style="background-color: #4f81bd; color: white; padding: 2px 10px; border-radius: 5px; display: inline-block;">Refresh</div>						

Figure 10.3 VPN Statistics Page

11. System Log

This chapter shows the System Log Configuration page, which you might enable/disable the log files for Access, System, Firewall & VPN. On the other hand, you might also enable the log file backup via Email function here (Figure 11.1)



System Log Configuration				
Log Category	Access	System	Firewall	VPN
File	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Log File Backup via Email	<input type="checkbox"/>			
Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Syslog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Log File List

Figure 11.1 System Log Configuration Page

12. System Management

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

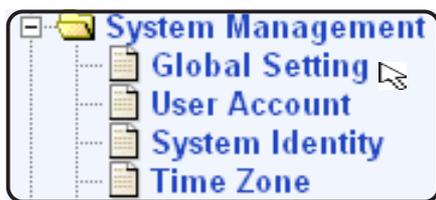
- Global Setting Configuration
- User Account Management
- Modify system Information
- System time setting
- Reset, backup and restore system configuration
- Update system firmware

You can access these tasks from the System Management menu.

12.1 Global Setting Configuration

As shown in Figure 12.1, you can use the **Global Setting** page to enable or disable services supported by SL6000/SL6300, including firewall, VPN, DNS Relay, DHCP RIP and SNTP. To disable or enable individual service, follow the steps below:

1. Log into Configuration Manager as admin, click the **System Management** menu, and then click **Global Setting** submenu. (Figure 12.1)
2. Click on the corresponding “enable” or “Disable” radio button to enable or disable the desired services.
3. Click on [**Apply**] button to save the changes.



Global Setting	
Firewall	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DNS Relay	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RIP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SNTP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 12.1 Global Setting Page

12.2 User Account Management

The first time you log into the Configuration Manager, you use the default username and password (admin and admin). The system allows two types of accounts - “Supervisor” (username/password: admin/admin) and “User” (username/password: guest/guest). “Supervisor” has the privilege to modify the system settings while “User” can only view the system settings. Passwords of both the “Supervisor” and “User” accounts can only be changed by the “Supervisor”.



Note: This username and password is only used for logging into the Configuration Manager; it is not the same as the login password you may use to connect to your ISP.



User Account Configuration	
Login Password	<input type="text"/>
Supervisor's Password	New Password <input type="text"/>
	Confirm New Password <input type="text"/>
User's Password	New Password <input type="text"/>
	Confirm New Password <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 12.2 User Account Setting Page

Password configuration page, see Figure 12.2, allows you to change supervisor or user’s password. Follow the steps below to change password:

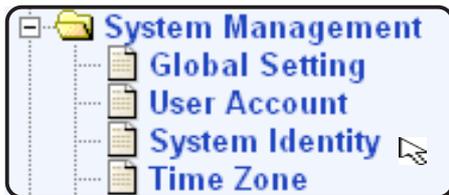
1. Log into Configuration Manager as admin, click the System Management menu, and then click User Account submenu. The User Account Configuration page displays, as shown in Figure 12.2.
2. Enter existing password in the Login Password field.
3. Type the new password in the New Password text field and again in the Confirm New 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 use here.

4. Click on button to save the new password.

12.3 Modify System Information

As illustrated in Figure 12.3, you can use System Identity page to enter system specific information such as system name (unique name for this device), system location (where this device is located), and contact person information for this device. Note that all fields allow only alphanumeric characters. When you are done entering system specific information, click on **[Apply]** button to save the changes.



System Information Configuration		
System Name	<input type="text" value="SL6000"/>	(Optional)
System Location	<input type="text" value="TAIPEI"/>	(Optional)
System Contact	<input type="text" value="ASUS TAIWAN"/>	(Optional)
<input type="button" value="Apply"/>		

Figure 12.3 System Identity Page

12.4 Setup Time Zone

SL6000/SL6300 keeps a record of the current date and time, which it uses to calculate and report various performance data.



Note: Changing the SL6000/SL6300 date and time does not affect the date and time on your PCs.

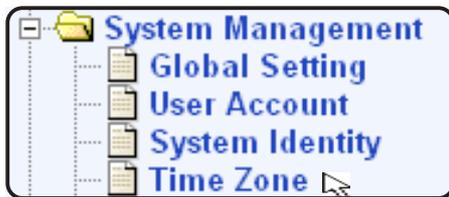
Chapter 12

12.4.1 Change/View the System Time Zone

1. Log into Configuration Manager as admin, click the System Management menu, and then click Time Zone submenu. Since there is no real time clock inside SL6000/SL6300, the system date and time are maintained by external network time server. Time Zone configuration parameters:

Date: Current Date
Time: Current Time
Location Time: Time Zone
SNTP Server: Maximum of 5 services can be configured
Update Interval: SNTP update time interval.

2. Click on **[Apply]** button to save the changes.



Time Zone Configuration	
Date	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1970"/> (mm:dd:yyyy)
Time	<input type="text" value="16"/> <input type="text" value="24"/> <input type="text" value="12"/> (hh:mm:ss)
Location Time	GMT <input type="button" value="v"/>
SNTP Service Configuration	
SNTP Server 1	<input type="text" value="207.46.248.43"/>
SNTP Server 2	<input type="text" value="192.43.244.18"/>
SNTP Server 3	<input type="text" value="131.107.1.10"/>
SNTP Server 4	<input type="text" value="129.6.15.28"/>
SNTP Server 5	<input type="text" value="129.6.15.29"/>
Update Interval	<input type="text" value="1"/> (Hours)
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 12.4 Time Zone Configuration Page

12.5 System Configuration Management

12.5.1 Reset System Configuration to Default

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

1. Log into Configuration Manager as admin, click the System Management menu, click the Configuration submenu and then click Default Setting submenu. The Default Setting Configuration page displays, as shown in Figure 12.5.
2. Click on **[Apply]** button to set the system configuration back to factory default. Note that SL6000/SL6300 will reboot to make the factory default configuration in effect.

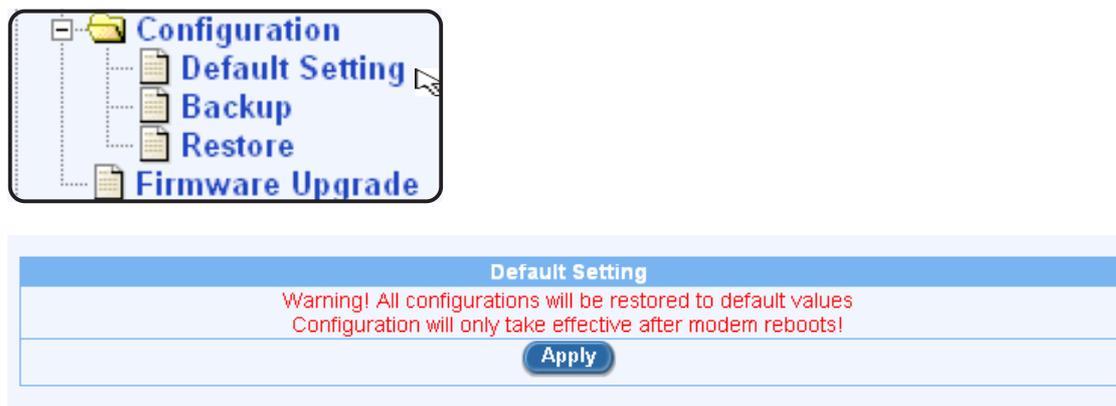


Figure 12.5 Default Setting Configuration Page

12.5.2 Backup System Configuration

Follow the steps below to backup system configuration:

1. Log into Configuration Manager as admin, click the System Management menu, click the Configuration submenu and then click Backup submenu. The Backup Configuration page displays, as shown in Figure 12.6.
2. Click on **[Apply]** button to backup the system configuration.

Chapter 12

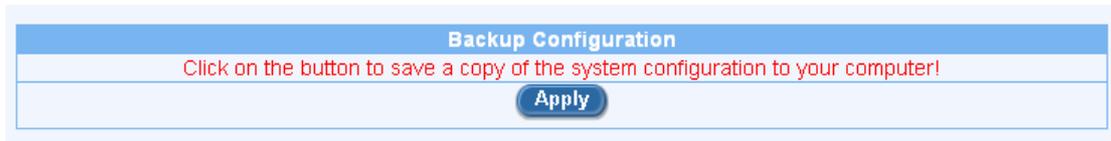


Figure 12.6 Backup System Configuration Page

12.5.3 Restore System Configuration

Follow the steps below to backup system configuration:

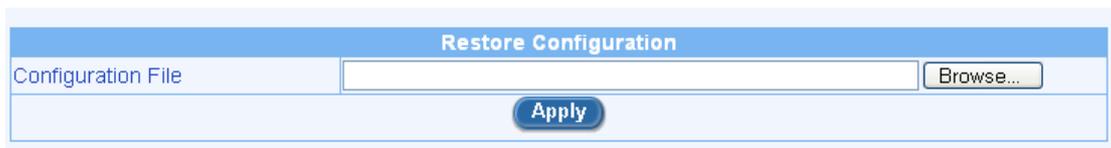


Figure 12.7 Restore System Configuration Page

1. Log into Configuration Manager as admin, click the **System Management** menu, click the Configuration submenu and then click **Restore** submenu. The Restore Configuration page displays, as shown in Figure 12.7.
2. Enter the path and name of the system configuration file that you want to restore in the “Configuration File” text box. Alternatively, you may click on the [**Browse**] button to search for the system configuration file on your hard drive.
3. Click on [**Apply**] button to restore the system configuration. Note that SL6000/SL6300 will reboot to make the new system configuration in effect.

12.6 Upgrade Firmware

ASUS may from time to time provide you with an update to the firmware running on the SL6000/SL6300. All system software is contained in a single file, called an image. Configuration Manager provides an easy way to upgrade the new firmware image. To upgrade the image, follow this procedure:

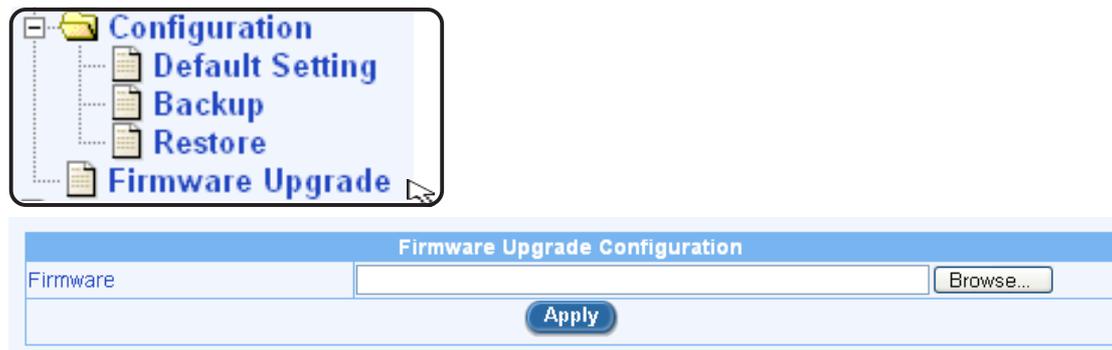


Figure 12.8 Firmware Upgrade Page

1. Log into Configuration Manager, click the System Management menu and then click Firmware Upgrade submenu. The Firmware Upgrade page displays, as shown in Figure 12.8.
2. In the Firmware text box, enter the path and name of the firmware image file. Alternatively, you may click on [**Browse**] button to search for it on your hard drive.
3. Click on [**Apply**] button to update the firmware. Note: it may take up to 5 minutes for the firmware upgrade. Note that after the transfer of firmware is completed, SL6000/SL6300 will reboot to make the new firmware in effect.

13. System Reset

To reset your SL6000/SL6300, log into Configuration Manager, click the **System Management** menu and then click Reset submenu. Click on the **[Apply]** button to reset the modem/router.



Figure 13.1 System Reset Page

14. Logout Configuration Manager

To logout of Configuration Manager, click **Logout** then click on the **[Apply]** button in the Configuration Manager Logout.



Figure 14.1 Configuration Manager Logout

A. IP Addresses, Network Masks, & Subnets

A.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 A.

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."

A.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 A.1 shows the structure of an IP address.

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

Table A.1. IP Address structure

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)

A.1.2 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.

A.2 Subnet masks



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.

B. Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the SL6000 / SL6300, and provides instructions for using several IP utilities to diagnose problems.

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

LEDs

Power LED does not illuminate after product is turned on.

Verify that you are using the power adapter provided with the device and that it is securely connected to the SL6000/SL6300 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 SL6000 / SL6300. Make sure that your ADSL or cable modem is powered on. Wait 30 seconds to allow SL6000/SL6300 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 SL6000 / SL6300. 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.

Appendix

Internet Access

PC cannot access Internet

Use the ping utility, discussed in the following section, to check whether your PC can communicate with the SL6000 / SL6300'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 SL6000/SL6300 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 the Quick Start Guide, Part 2). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool

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 both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the rear panel of SL6000/SL6300 three times. **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 SL6000 / SL6300’s LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.

Verify that you are using Internet Explorer v5.5 or later. Netscape is not supported. 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 SL6000 / SL6300.

Changes to Configuration Manager are not being retained.

Be sure to click on **Apply** button to save any changes.

Appendix

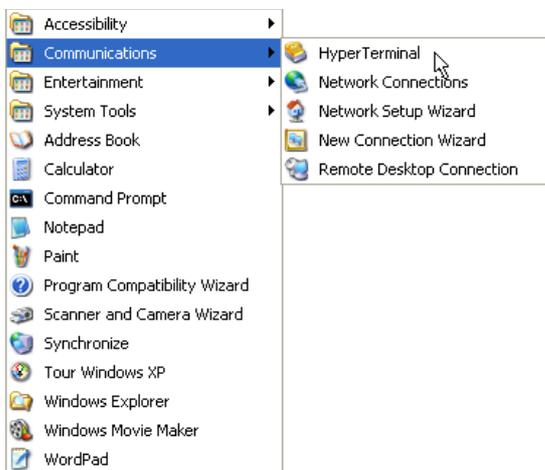
B.1 Recall default configuration by “RESET” button



WARNING: Resetting the device removes all custom settings and returns all settings to their default values.

To ensure the reset process correctly, please attach the RS232 to RJ45 cable between the router’s console port and your PC’s COM port after the router is powered ON.

1. Start Windows HyperTerminal software.



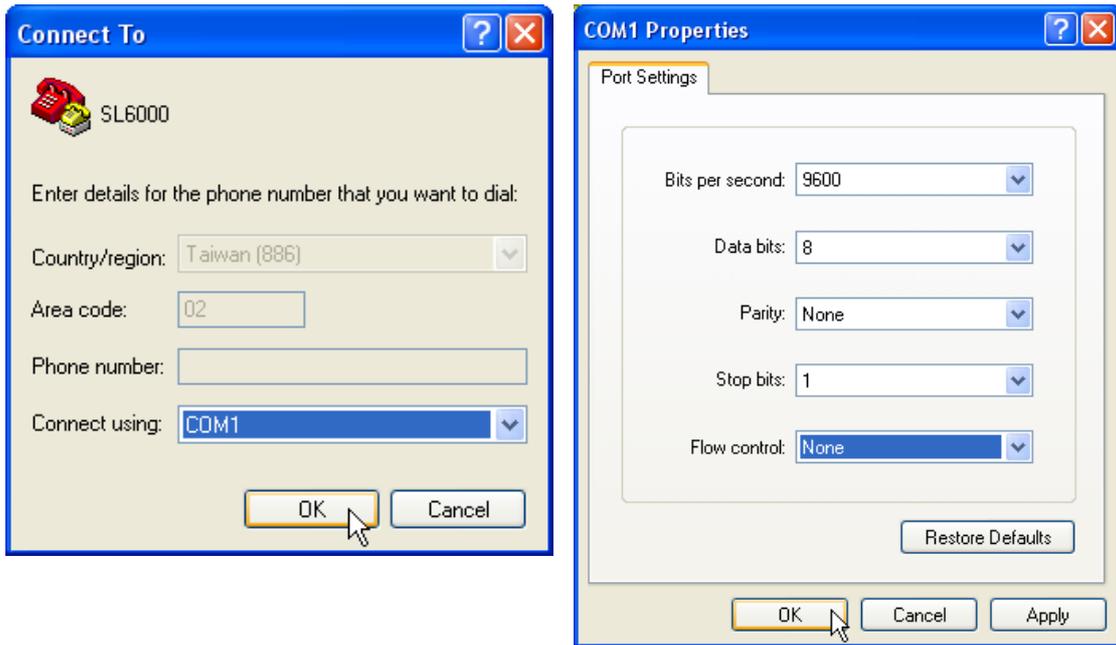
*. In Windows operating system, click “START” | “Program” | “Accessories” | “Communications” | “HyperTerminal”

* You can choose Yes if you do not normally use other telnet software.

2. Setup the telnet connection to the SL6000/SL6300 as follows:

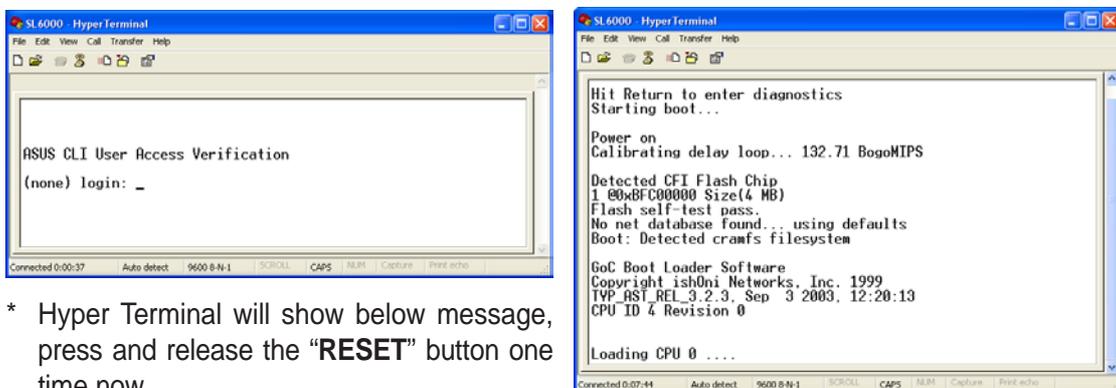


* Enter any name for this New Connection.



- * Select **COM1** or **COM2** (depends on your serial port configuration) and click **OK**.
- * Select: Bits per second: **9600**, Data bits: **8**, Parity: **None**, Stop bits: **1**, Flow Control: **NONE** and click **OK**.

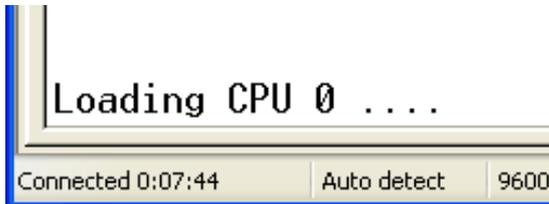
3. Press the **RESET** button on the back of the SL6000/SL6300.



- * Hyper Terminal will show below message, press and release the **“RESET”** button one time now.
- * The router will reboot and show some system messages.

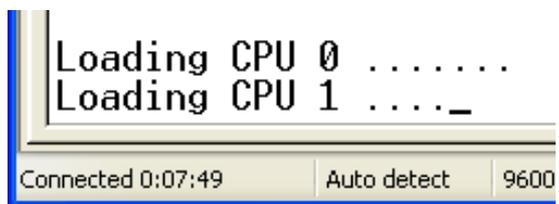
Appendix

- Press the RESET button on the back of the SL6000/SL6300 a second time.



```
Loading CPU 0 ....
Connected 0:07:44 Auto detect 9600
```

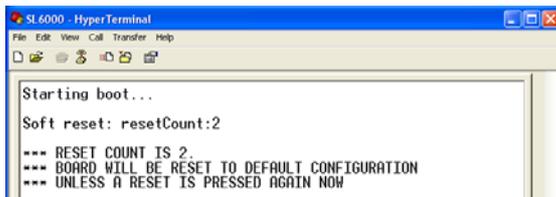
* When you see **Loading CPU 0 ...** while the dots are increasing (about 5 sec after pushing the RESET button.)



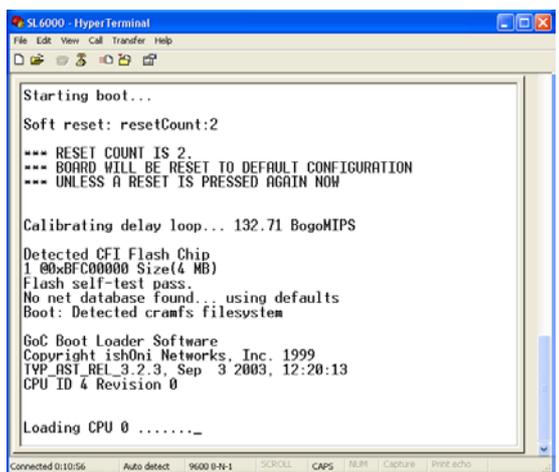
```
Loading CPU 0 .....
Loading CPU 1 .....
Connected 0:07:49 Auto detect 9600
```

* If you see “Loading CPU 1 ...”, it would be too late to press the RESET button a second time.

- This time the router will show below message to indicate the system is going to be reset to default.



```
Starting boot...
Soft reset: resetCount:2
--- RESET COUNT IS 2.
--- BOARD WILL BE RESET TO DEFAULT CONFIGURATION
--- UNLESS A RESET IS PRESSED AGAIN NOW
```



```
Starting boot...
Soft reset: resetCount:2
--- RESET COUNT IS 2.
--- BOARD WILL BE RESET TO DEFAULT CONFIGURATION
--- UNLESS A RESET IS PRESSED AGAIN NOW

Calibrating delay loop... 132.71 BogoMIPS

Detected CFI Flash Chip
1 @0xBF00000 Size(4 MB)
Flash self-test pass.
No net database found... using defaults
Boot: Detected cramfs filesystem

GoC Boot Loader Software
Copyright ishOni Networks, Inc. 1999
TVP_AST_REL_3.2.3, Sep 3 2003, 12:20:13
CPU ID 4 Revision 0

Loading CPU 0 .....
Connected 0:10:56 Auto detect 9600 B-N-1 SCROLL CAPS NUM Capture Print echo
```

* After the router reboots, don't push the RESET button this time when you see “**Loading CPU 0 ...**”.

- This process is complete and the SL6000/SL6300 will recover its factory default settings after a few minutes.

B.2 Diagnosing Problem using IP Utilities

B.2.1 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 B.1.

```
C:\Documents and Settings>ping 192.168.8.1
Pinging 192.168.8.1 with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time=15ms TTL=255
Reply from 192.168.8.1: bytes=32 time=5ms TTL=255
Reply from 192.168.8.1: bytes=32 time=3ms TTL=255
Reply from 192.168.8.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 15ms, Average = 6ms
```

Figure B.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 SL6000/SL6300 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.

Appendix

B.2.2 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: **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 B.2.



```
C:\Documents and Settings\Victor_Shar>nslookup 192.168.8.1
Server:   tp-dc-01.corpnet.asus
Address:  192.168.28.68
```

Figure B.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.

C. Glossary

10BASE-T

A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See also data rate, Ethernet.

100BASE-T

A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See also data rate, Ethernet.

ADSL (Asymmetric Digital Subscriber Line)

The most commonly deployed “flavor” of DSL for home users. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.

ATM authenticate)

To verify a user’s identity, such as by prompting for a password.

Binary

The “base two” system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See also bit, IP address, network mask.

Bit

Short for “binary digit,” a bit is a number that can have two values, 0 or 1. See also binary.

bps

bits per second

Appendix

Broadband

A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.

Broadcast

To send data to all computers on a network.

DHCP

Dynamic Host Configuration Protocol

DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.

DHCP relay (Dynamic Host Configuration Protocol relay)

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the SL6000 / SL6300's interfaces can be configured as a DHCP relay. See DHCP.

DHCP server (Dynamic Host Configuration Protocol server)

A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.

DNS (Domain Name System)

The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See also domain name.

Domain name

A domain name is a user-friendly name used in place of its associated IP address. For example, www.globespan.net is the domain name associated with IP address 209.191.4.240. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site, e.g., <http://www.globespan.net/index.html>. See also DNS.

Download

To transfer data in the downstream direction, i.e., from the Internet to the user.

DSL (Digital Subscriber Line)

A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.

Ethernet

The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.

Filtering

To screen out selected types of data, based on filtering rules. Filtering can be applied in one direction (upstream or downstream), or in both directions.

Filtering rule

A rule that specifies what kinds of data the a routing device will accept and/or reject. Filtering rules are defined to operate on an interface (or multiple interfaces) and in a particular direction (upstream, downstream, or both).

firewall Any method of protecting a computer or LAN connected to the Internet from intrusion or attack from the outside. Some firewall protection can be provided by packet filtering and Network Address Translation services.

FTP (File Transfer Protocol)

A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

GGP

Gateway to Gateway Protocol. An Internet protocol that specifies how gateway routers communicate with each other.

Hop

When you send data through the Internet, it is sent first from your computer to a router, and then from one router to another until it finally reaches a router that is directly connected to the recipient. Each individual “leg” of the data’s journey is called a hop.

Appendix

Hop count

The number of hops that data has taken on its route to its destination. Alternatively, the maximum number of hops that a packet is allowed to take before being discarded (see also TTL).

Host

A device (usually a computer) connected to a network.

HTTP (Hyper-Text Transfer Protocol)

HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See also web browser, web site.

ICMP (Internet Control Message Protocol)

An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

IGMP (Internet Group Management Protocol)

An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers. A multicast group of computers is one whose members have designated as interested in receiving specific content from the others. Multicasting to an IGMP group can be used to simultaneously update the address books of a group of mobile computer users or to send company newsletters to a distribution list.

Internet

The global collection of interconnected networks used for both private and business communications.

Intranet

A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP (See TCP/IP)

IP address (Internet Protocol address)

The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network

mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See also domain name, network mask.

ISP (Internet Service Provider)

A company that provides Internet access to its customers, usually for a fee.

LAN (Local Area Network)

A network limited to a small geographic area, such as a home, office, or small building.

LED (Light Emitting Diode)

An electronic light-emitting device. The indicator lights on the front of the SL6000/SL6300 are LEDs.

MAC address (Media Access Control address)

The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of characters.

Mask (See network mask)

Mbps

Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

NAT

Network Address Translation

A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.

NAT rule

A defined method for translating between public and private IP addresses on your LAN.

Appendix

Network

A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.

Network mask

A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean “select this bit” while bits set to 0 mean “ignore this bit.” For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See also binary, IP address, subnet, “IP Addresses Explained” section.

NIC (Network Interface Card)

An adapter card that plugs into your computer and provides the physical interface to your network cabling, which for Ethernet NICs is typically an RJ-45 connector. See Ethernet, RJ-45.

packet

Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

Ping (Packet Internet (or Inter-Network) Groper)

A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

Port

A physical access point to a device such as a computer or router, through which data flows into and out of the device.

PPP (Point-to-Point Protocol)

A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the SL6000/SL6300 uses two forms of PPP called PPPoA and PPPoE. See also PPPoA, PPPoE.

PPPoE (Point-to-Point Protocol over Ethernet)

One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.

Protocol

A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

Remote

In a physically separate location. For example, an employee away on travel who logs in to the company's Internet is a remote user.

RIP (Routing Information Protocol)

The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.

RJ-11 (Registered Jack Standard-11)

The standard plug used to connect telephones, fax machines, modems, etc. to a telephone jack. It is a 6-pin connector usually containing four wires.

RJ-45 (Registered Jack Standard-45)

The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

Routing

Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

Rule (See filtering rule, NAT rule.)

SDNS (Secondary Domain Name System (server))

A DNS server that can be used if the primary DSN server is not available. See DNS.

SNMP (Simple Network Management Protocol)

The TCP/IP protocol used for network management.

Appendix

Subnet

A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask which selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See also network mask.

Subnet mask

A mask that defines a subnet. See also network mask.

TCP (See TCP/IP)

TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.

Telnet

An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.

TFTP (Trivial File Transfer Protocol)

A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.

TTL (Time To Live)

A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packet decrements this field by one. When the TTL reaches zero, the packet is discarded.

Twisted pair

The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed

with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See also 10BASE-T, 100BASE-T, Ethernet.

Upstream

The direction of data transmission from the user to the Internet.

WAN (Wide Area Network)

Any network spread over a large geographical area, such as a country or continent. With respect to the SL6000 / SL6300, WAN refers to the Internet.

Web browser

A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See also HTTP, web site, WWW.

Web page

A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See also hyperlink, web site.

Web site A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See also hyperlink, web page.

WWW (World Wide Web)

Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

