



SL1200

Internet Security Router

User Manual

E2923/ November 2006

Copyright Information

E2923

First Edition

October 2006

Copyright © 2006 ASUSTeK COMPUTER INC. All Rights Reserved.

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).

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.

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.

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.

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.

Contact Information

ASUSTeK COMPUTER INC.

Company address: 15 Li-Te Road, Beitou, Taipei 11259
General (tel): +886-2-2894-3447
Web site address: www.asus.com.tw
General (fax): +886-2-2894-7798
General email: info@asus.com.tw

Technical support
General support (tel): +886-2-2894-3447
Online support: <http://support.asus.com>

ASUS COMPUTER INTERNATIONAL (America)

Company address: 44370 Nobel Drive, Fremont, CA 94538, USA
General (fax): +1-510-608-4555
Web site address: usa.asus.com

Technical support
General support (tel): +1-502-995-0883
Online support: <http://support.asus.com>
Notebook (tel): +1-510-739-3777 x5110
Support (fax): +1-502-933-8713

ASUS COMPUTER GmbH (Germany & Austria)

Company address: Harkort Str. 25, D-40880 Ratingen, Germany
General (tel): +49-2102-95990
Web site address: www.asus.com.de
General (fax): +49-2102-959911
Online contact: www.asus.com.de/sales

Technical support
Component support: +49-2102-95990
Online support: <http://support.asus.com>
Notebook support: +49-2102-959910
Support (fax): +49-2102-959911

Notices

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received including interference that may cause undesired operation.

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

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

Canadian Department of Communications Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This class B digital apparatus complies with Canadian ICES-003.

Table of Contents

1	Introduction.....	1
1.1	Features	1
1.2	System Requirements	1
1.3	Using this manual	2
1.1.1	Notational conventions.....	2
1.1.2	Typographical conventions.....	2
1.1.3	Symbols	2
2	Getting to Know the ASUS SL1200.....	3
2.1	Package contents	3
2.2	Front Panel	3
2.3	Rear Panel	3
2.4	Major Features	5
2.4.1	Firewall Features	5
2.4.2	VPN.....	9
3	Quick Start	11
3.1	Part 1 —Connecting the hardware	11
3.1.1	Connect to an ADSL or a cable modem	11
3.1.2	Connect computers or a LAN	11
3.1.3	Attach the power adapter	12
3.1.4	Turning on the ASUS SL1200	12
3.2	Part 2 — Configuring Your Computers	13
3.2.1	Before you begin	13
3.2.2	Windows® XP PCs.....	14
3.2.3	Windows® 2000 PCs	14
3.2.4	Windows® 95, 98, and ME PCs	15
3.2.5	Windows® NT 4.0 workstations	16
3.2.6	Assigning static IP addresses to your PCs	16

3.3 Part 3 — Quick Configuration of	
ASUS SL1200	18
3.3.1 Buttons Used in Setup Wizard	18
3.3.2 Setting up the ASUS SL1200	19
3.3.3 Testing Your Setup	25
3.3.4 Default Router Settings	25
4 Using the Configuration Manager.....	27
4.1 Log into the Configuration Manager.....	27
4.2 Functional Layout.....	29
4.2.1 Setup Menu Navigation Tips	29
4.2.2 Commonly used buttons and icons	30
4.3 Configuration Manager's Home Page	31
4.4 Overview of System Configuration	31
5 Configuring LAN Settings	32
5.1 LAN IP Address	32
5.1.1 LAN IP Configuration Parameters	33
5.1.2 Configuring the LAN IP Address	33
5.2 Dynamic Host Control Protocol (DHCP)	34
5.2.1 What is a DHCP?	34
5.2.2 Why use a DHCP?	34
5.2.3 Configuring a DHCP Server	35
5.2.4 Viewing Current DHCP Address Assignments	37
5.3 DNS	38
5.3.1 About DNS	38
5.3.2 Assigning DNS Addresses	38
5.3.3 Configuring DNS Relay	38
5.4 Viewing LAN Statistics	40

6 Configuring WAN Settings	41
6.1 WAN Connection Mode	41
6.2 PPoE	42
6.2.1 WAN PPoE	
Configuration Parameters	42
6.2.2 Configuring PPoE for WAN	43
6.3 Dynamic IP	44
6.3.1 WAN Dynamic IP	
Configuration Parameters	44
6.3.2 Configuring Dynamic IP for WAN	44
6.4 Static IP	45
6.4.1 WAN Static IP	
Configuration Parameters	45
6.4.2 Configuring Static IP for WAN	46
6.5 Viewing WAN Statistics	47
7 Configuring Routes	48
7.1 Overview of IP Routes	48
7.1.1 Do I need to define IP routes?	48
7.2 Dynamic Routing Using	
Routing Information Protocol (RIP)	49
7.2.1 Dynamic Routing (RIP)	
Configuration Parameters	49
7.2.2 Configuring RIP	50
7.3 Static Routing	51
7.3.1 Static Route Configuration Parameters	51
7.3.2 Adding a Static Route	52
7.3.3 Deleting a Static Route	52
7.3.4 Viewing the Routing Table	52

8	Configuring DDNS	54
8.1	DDNS Configuration Parameters	55
8.2	Access DDNS Configuration Page	56
8.3	Configuring HTTP DDNS Client	57
9	Configuring Firewall/NAT Settings	57
9.1	Firewall Overview	58
9.1.1	Stateful Packet Inspection	58
9.1.2	Denial of Service (DoS) Protection	59
9.1.3	Firewall and Access Control List (ACL)	59
9.1.4	Default ACL Rules	60
9.2	NAT Overview	60
9.2.1	Static (One to One) NAT	61
9.2.2	Dynamic NAT	62
9.2.3	Network Address and Port Translation (NAPT) or Port Address Translation (PAT)	63
9.2.4	Reverse Static NAT	64
9.2.5	Reverse NAPT/Virtual Server	64
9.3	Configuring Inbound ACL Rules	64
9.3.1	Inbound ACL Rule Configuration Parameters	65
9.3.2	Access Inbound ACL Rule Configuration Page (Firewall -> ACL)	69
9.3.3	Add Inbound ACL Rules	69
9.3.4	Modify Inbound ACL Rules	70
9.3.5	Delete Inbound ACL Rules	70
9.3.6	Display Inbound ACL Rules	70
9.4	Configuring Outbound ACL Rules	71
9.4.1	Outbound ACL Rule Configuration Parameters	72

9.4.2 Access Outbound ACL Rule Configuration	
Page (Firewall -> Outbound ACL)	69
9.4.3 Add Outbound ACL Rules	75
9.4.4 Modify Outbound ACL Rules	76
9.4.5 Delete Outbound ACL Rules	76
9.4.6 Display Outbound ACL Rules	77
9.5 Configuring URL Filters	77
9.5.1 URL Filter Configuration Parameters	77
9.5.2 Access URL Filter Configuration	
Page (Firewall -> URL Filter)	78
9.5.3 Add URL Filter Rules	78
9.5.4 Modify URL Filter Rules	79
9.5.5 Delete URL Filter Rules	79
9.5.6 View Configured URL Filter Rules	79
9.6 Configuring Advanced Firewall Features	
(Firewall -> Advanced)	80
9.6.1 Configuring Self Access Rules	81
9.6.2 Configuring Service List	83
9.6.3 Configuring DoS Settings	86
9.7 Firewall Policy List (Firewall -> Policy List)	90
9.7.1 Configuring IP Pool	90
9.7.2 Configuring NAT Pool	94
9.7.3 Configuring Time Range	98
9.8 Firewall Statistics	
(Firewall -> Statistics)	102
10 Configuring VPN	103
10.1 Default Parameters	103
10.2 VPN Tunnel	
Configuration Parameters	107

10.3 Establishing VPN Connection	
Using Automatic Keying	111
10.3.1 Add a Rule for VPN Connection	
Using Pre-shared Key	111
10.3.2 Modify VPN Rules	113
10.3.3 Delete VPN Rules	113
10.3.4 View VPN Rules	114
10.4 VPN Statistics	114
10.5 VPN Connection Examples	115
10.5.1 Intranet Scenario - firewall + VPN and no NAT for VPN traffic	116
10.5.2 Extranet Scenario - firewall + static NAT + VPN for VPN traffic	122
11 System Management	130
11.1 Configure System Services	130
11.2 Change the Login Password	131
11.3 Modify System Information	132
11.4 Setup Date and Time	131
11.4.1 View the System Date and Time	133
11.5 SNMP Setup	134
11.5.1 SNMP Configuration Parameters	134
11.5.2 Configuring SNMP	134
11.5.3 View the System Date and Time	133
11.5.4 View the System Date and Time	133
11.6 System Configuration Management	135
11.6.1 Reset System Configuration	135
11.6.2 Backup System Configuration	136
11.6.3 Restore System Configuration	137

11.7 Upgrade Firmware	138
11.8 Reset the Internet Security Router	139
11.9 Logout Configuration Manager	140
12 ALG Configuration	141
13 IP Addresses, Network Masks, and Subnets	145
13.1 IP Addresses	145
13.1.1 Structure of an IP Address	145
13.2 Network classes	146
13.3 Subnet masks	145
14 Troubleshooting	148
14.1 Diagnosing problems using IP utilities	151
14.1.1 ping	151
14.1.2 ns lookup	152
15 Glossary	153

List of Figures

Figure 2.1 Front Panel LEDs	3
Figure 2.2 Rear Panel Connections	4
Figure 3.1 Overview of Hardware Connections	12
Figure 3.2 Login Screen	19
Figure 3.3 Setup Wizard Home Page	20
Figure 3.4 Setup Wizard - Password Configuration Page	20
Figure 3.5 Setup Wizard - System Information Setup Page	21
Figure 3.6 Setup Wizard - Date/Time	

Configuration Page.....	21
Figure 3.7 Setup Wizard - LAN	
Configuration Page	22
Figure 3.8 Setup Wizard - DHCP Server	
Configuration Page	22
Figure 3.9 Setup Wizard - WAN PPOE	
Configuration Page	23
Figure 3.10 Setup Wizard - WAN Dynamic IP	
Configuration Page	23
Figure 3.11 Setup Wizard - WAN Static IP	
Configuration Page	24
Figure 4.1 Configuration Manager Login Screen	28
Figure 4.2 Typical Configuration Manager Page	29
Figure 4.3 Setup Wizard Home Page	31
Figure 4.4 System Information Page	31
Figure 5.1 LAN IP Address Configuration Page	33
Figure 5.2 DHCP Configuration Page	35
Figure 5.3 LAN Statistics Page	40
Figure 6.1 WAN PPOE Configuration Page	41
Figure 6.2 WAN Dynamic IP (DHCP client)	
Configuration Page	45
Figure 6.3 WAN Static IP Configuration Page	46
Figure 6.4 WAN Statistics Page	47
Figure 7.1 RIP Configuration	50
Figure 7.2 Static Route Configuration	52
Figure 7.3 Routing Table	53
Figure 8.1 Network Diagram for HTTP DDNS	55
Figure 8.2 HTTP DDNS Configuration Page	57
Figure 9.1 Static NAT - Mapping Four Private IP Addresses	

to Four Globally Valid IP Addresses	61
Figure 9.2 Dynamic NAT - Four Private IP Addresses	
Mapped to Three Valid IP Addresses	62
Figure 9.3 Dynamic NAT - PC-A can get a NAT Association	
after PC-B is disconnected	62
Figure 9.4 Map Any Internal PCs to a	
Single Global IP Address	63
Figure 9.5 Reverse Static NAT - Map a Global IP Address	
to An Internal PC	63
Figure 9.6 Reverse NAT - Relayed Incoming Packets to the	
Internal Host Base on the Protocol, Port	
Number or IP Address	63
Figure 9.7 Inbound ACL Configuration Page	65
Figure 9.8 Inbound ACL Configuration Example	69
Figure 9.9 Outbound ACL Configuration Page	71
Figure 9.10 Outbound ACL Configuration Example	76
Figure 9.11 URL Filter Configuration Page	78
Figure 9.12 URL Filter Example	80
Figure 9.13 Self Access Rule Configuration Page	81
Figure 9.14 Service List Configuration Page	84
Figure 9.15 DoS Configuration Page	89
Figure 9.16 IP Pool Configuration Page	91
Figure 9.17 Network Diagram	
for IP Pool Configuration	92
Figure 9.18 IP Pool Example - Add Two IP Pools -	
MISgroup1 and MISgroup2	93
Figure 9.19 IP Pool Example - Deny QUAKE-II	
Connection for MISgroup1	93
Figure 9.20 NAT Pool Configuration Page	95

Figure 9.21 Network Diagram for NAT Pool Example	96
Figure 9.22 NAT Pool Example - Create a Static NAT Pool	97
Figure 9.23 NAT Pool Example - Associate a NAT Pool to an ACL Rule	97
Figure 9.24 Time Range Configuration Page	99
Figure 9.25 Time Range Example - Create a Time Range	101
Figure 9.26 Time Range Example - Deny FTP Access for MISgroup1 During Office Hourss	101
Figure 9.27 Firewall Active Connection Statistics	102
Figure 10.1 VPN Tunnel Configuration Page - Pre-shared Key Mode	112
Figure 10.2 VPN Statistics Page	116
Figure 10.3 Typical Intranet Network Diagram	117
Figure 10.4 Intranet VPN Policy Configuration on ISR1	118
Figure 10.5 Intranet VPN Policy Configuration on ISR2	120
Figure 10.6 Typical Extranet Network Diagram	122
Figure 10.7 Extranet Example - VPN Policy Configuration on ISR1	124
Figure 10.8 Extranet Example - Outgoing NAT Pool Configuration on ISR1	124
Figure 10.9 Extranet Example - Incoming NAT Pool Configuration on ISR1	125
Figure 10.10 Extranet Example - Outbound ACL Rule on ISR1	125
Figure 10.11 Extranet Example - Inbound ACL Rule	

on ISR1	126
Figure 10.12 Extranet Example - VPN Policy	
Configuration on ISR2	126
Figure 10.13 Extranet Example - Outgoing NAT Pool	
Configuration on ISR2	127
Figure 10.14 Extranet Example - Incoming NAT Pool	
Configuration on ISR2	127
Figure 10.15 Extranet Example - Outbound ACL Rule	
on ISR2	128
Figure 10.16 Extranet Example - Inbound ACL Rule	
on ISR2	128
Figure 11.1 System Services Configuration Page	131
Figure 11.2 Password Configuration Page	131
Figure 11.3 System Information Configuration Page	132
Figure 11.4 Date and Time Configuration Page	133
Figure 11.5 SNMP Configuration	135
Figure 11.6 Existing SNMP Configuration	135
Figure 11.7 Default Setting Configuration Page	136
Figure 11.8 Backup System Configuration Page	137
Figure 11.9 Restore System Configuration Page	137
Figure 11.10 Windows File Browser	138
Figure 11.11 Firmware Upgrade Page	138
Figure 11.12 Configuration Manager Reset Page	139
Figure 11.13 Configuration Manager Logout Page	140
Figure 11.14 Confirmation for Closing Browser (IE)	140
Figure 14.1 Using the ping utility	151
Figure 14.2 Using the nslookup utility	152

List of Tables

Table 2.1 Front Panel Label and LEDs	3
Table 2.2 Rear Panel Connections	4
Table 2.3 DoS Attacks	8
Table 2.4 VPN Features	10
Table 3.1 LED Indicators	13
Table 3.2 Default Settings Summary	26
Table 4.1 Description of Commonly Used Buttons and Icons	30
Table 5.1 LAN IP Configuration Parameters	33
Table 5.2 DHCP Configuration Parameters	36
Table 5.3 DHCP Address Assignment	37
Table 6.1 WAN PPPoE Configuration Parameters	42
Table 6.2 WAN Dynamic IP Configuration Parameters	44
Table 6.3 WAN Static IP Configuration Parameters	45
Table 7.1 Dynamic Routing (RIP) Configuration Parameters	49
Table 7.2 Static Route Configuration Parameters	51
Table 8.1 DDNS Configuration Parameters	56
Table 9.1 Inbound ACL Rule Configuration Parameters	65
Table 9.2 Outbound ACL Rule Configuration Parameters	72
Table 9.3 URL Filter Configuration Parameters	77
Table 9.4 Self Access Configuration Parameters	81
Table 9.5 Service List Configuration Parameters	84
Table 9.6 DoS Protection Configuration Parameters	87
Table 9.7 IP Pool Configuration Parameters	90
Table 9.8 NAT Pool Configuration Parameters	94
Table 9.9 Time Range Configuration Parameters	98
Table 10.1 Default connections in the router	103

Table 10.2 Pre-configured IKE proposals in the router.....	104
Table 10.3 Pre-configured IPSec proposals in the router	105
Table 10.4 VPN Tunnel Configuration Parameter	107
Table 10.5 VPN Statistics	114
Table 10.6 Outbound Un-translated Firewall Rule for VPN Packets on ISR1	119
Table 10.7 Inbound Un-translated Firewall Rule for VPN Packets on ISR1	119
Table 10.8 Outbound Un-translated Firewall Rule for VPN Packets on ISR1	121
Table 10.9 Inbound Un-translated Firewall Rule for VPN Packets on ISR1	121
Table 11.1 Fixed DHCP Lease Configuration	134
Table 12.1 Supported ALG	141
Table 13.1 IP Address structure	146
Table 14.1 Problems and suggestions	148

1 Introduction

Thank you for buying the ASUS SL1200, the Internet Security Router!

Your Local Area Network (LAN) will now be able to access the Internet using high-speed broadband connection such as those with ADSL or cable modem.

This user manual will show you how to set up the ASUS SL1200, and how to customize its configuration to get the most out of this product.

1.1 Features

- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- Firewall, NAT (Network Address Translation), and IPSec VPN functions to provide secure Internet access for your LAN
- Automatic network address assignment through DHCP Server
- Services including IP route, DNS and DDNS configuration, RIP, and IP performance monitoring
- Configuration program accessible via a web browser, such as Microsoft Internet Explorer 5.5, Netscape 7.0.2 or later.

1.2 System Requirements

In order to use the ASUS SL1200 for Internet access, you must have the following:

- ADSL or cable modem and the corresponding service up and running, with at least one public Internet address assigned to your WAN
- One or more computers each containing an Ethernet 10Base-T/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 v5.5 or later.

1.3 Using this Manual

1.3.1 Notational conventions

- Acronyms are defined the first time they appear in the text and in the Glossary.
- The ASUS SL1200 is simply referred to as "**the router**" or "**Internet Security 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 defined in the Glossary.
- **Boldface** type text is used for items you select from menus and drop-down lists, and commands you type when prompted by the program.

1.3.3 Symbols

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



Note: Provides clarification or non-essential information on the current topic.



Definition: Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.



Warning: Provides messages of high importance, including messages relating to personal safety or system integrity.

2 Getting to Know the ASUS SL1200

2.1 Package contents

Check your ASUS SL1200 package for these items:

- ASUS SL1200
- Power adapter
- Ethernet cable (“straight-through” type)
- (Optional) console port cable (RJ-45)



If any of the above items is damaged or missing, contact your retailer.

2.2 Front Panel

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



Figure 2.1. 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
WAN	green	On: WAN link established and active Flashing: Data is transmitted via WAN connection Off: No WAN link
LAN1-LAN4	green	On: LAN link is established Flashing: Data is transmitted via LAN connection Off: No LAN link

2.3 Rear Panel

The rear panel contains the ports and power connections.

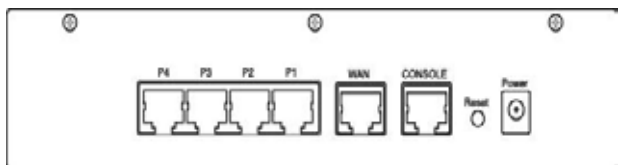


Figure 2.2. Rear Panel Connections

Table 2.2. Rear Panel Labels and LEDs

Label	Function
POWER	Connects to the supplied power adapter
Reset	Resets the device
CONSOLE	RJ-45 serial port for console management
WAN	Connects to your WAN device such as ADSL or cable modem.
P1-P4	Connects to the device to your PC's Ethernet port, or to the uplink port on your LAN's hub/switch using the cable provided

2.4 Major Features

2.4.1 Firewall Features

The ASUS SL1200's firewall provides features to protect your network from being attacked and to prevent your network from being used as the springboard for attacks.

The firewall features are:

- Address Sharing and Management
- Packet Filtering
- Stateful Packet Inspection
- Defense against Denial of Service Attacks
- Application Content Filtering
- Log and Alert
- Remote Access
- Keyword based URL Filtering

2.4.1.1 Address Sharing and Management

The ASUS SL1200's firewall provides Network Address Translation (NAT) to share a single high-speed Internet connection. NAT saves the cost of multiple connections required for the hosts on the LAN segments connected to the router. It conceals network address and prevents them from becoming public. It maps unregistered IP addresses of hosts connected to the LAN with valid ones for Internet access.

The router's firewall also provides reverse NAT capability, which enables SOHO users to host various services such as e-mail servers, web servers, etc. The NAT rules drive the translation mechanism at the NAT router.

The router supports these NAT types:

- **Static NAT:** It maps an internal host address to a globally valid Internet address (one-to-one). All packets are directly translated with the information contained in the map.

- **Dynamic NAT:** It dynamically maps an internal host address to a globally valid Internet address (m-ton). The map usually contains a pool of internal IP addresses (m) and a pool of globally valid Internet IP addresses (n) with **m** usually greater than **n**. Each internal IP address is mapped to one external IP address on a first come first serve basis.
- **Network Address and Port Translation (NAPT):** It is also called IP Masquerading. It maps many internal hosts to only one globally valid Internet address. The map usually contains a pool of network ports to be used for translation. Every packet is translated with the globally valid Internet address. The port number is translated with a free pool from the pool of network ports.
- **Reverse Static:** It is inbound mapping that maps a globally valid Internet address to an internal host address. All packets coming to that external address are relayed to the internal address. This is useful when hosting services in an internal machine.
- **Reverse NAPT:** It is also called inbound mapping, port mapping, and virtual server. Any packet coming to the router can be relayed to the internal host based on the protocol, port number or IP Address specified in the rule. This is useful when multiple services are hosted on different internal machines.



*For a complete listing of all NAT ALGs supported, refer to **Chapter 12: ALG Configuration**.*

2.4.1.1 Access Control List (ACL)

A firewall monitors each individual packet, decodes the header information of inbound and outbound traffic. It then either blocks the packet from passing or allows it to pass based on the contents of the source address, destination address, source port, destination port, protocol and other criterion such as application filter, and time ranges as defined in the Access Control List (ACL) rules.

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

The router's firewall's ACL methodology supports:

- Filtering based on destination and source IP address, port number and protocol

- Use of the wild card for composing filter rules
- Filter Rule priorities
- Time based filters
- Application specific filters
- User group based filters for remote access

2.4.1.2 Stateful Packet Inspection

The ASUS SL1200's firewall uses “stateful packet inspection” that extracts state-related information required for the security decision from the packet and maintains this information for evaluating subsequent connection attempts. It has awareness of application and creates dynamic sessions that allow dynamic connections so that no ports need to be opened other than the required ones. This provides a solution which is highly secure and that offers scalability and extensibility.

2.4.1.3 Defense against DoS Attacks

The firewall has an Attack Defense Engine that protects internal networks from known types of Internet attacks. It provides automatic protection from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. It can drop ICMP redirects and IP loose/strict source routing packets. For example, the router's firewall provides protection from “WinNuke”, a widely used program that remotely crash unprotected Windows systems in the Internet. The Internet Security Router Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, Reassembly and SYN flooding.

Table 2.3 lists the type of attack protections provided by the router.

Table 2.3. DoS Attacks

Type of Attack	Name of Attacks
Re-assembly attacks	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP Attacks	Ping of Death, Smurf, Twinge
Flooders	ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	TCP XMAS Scan, TCP Null Scan, TCP SYN Scan, TCP Stealth Scan
TCP Attacks	TCP sequence number prediction, TCP out-of sequence attacks
Protection with PF Rules	Echo-Chargen, Ascend Kill
Miscellaneous Attacks	IP Spoofing, LAND, Targa, Tentacle MIME Flood, Winnuke, FTP Bounce, IP unaligned time stamp attack

2.4.1.4 Application Level Gateway (ALG)

Applications such as FTP, and games dynamically open connections based on the respective application parameter. To go through the firewall on the router, packets pertaining to an application, require a corresponding allow rule. In the absence of such rules, the packets will be dropped by the router's firewall. As it is not feasible to create policies for numerous applications dynamically (without compromising security), intelligence in the form of Application Level Gateways (ALG), is built to parse packets for applications and open dynamic associations. The firewall provides a number of ALGs for popular applications such as FTP, H.323, RTSP, Microsoft Games, and SIP.

2.4.1.5 URL Filtering

A set of keywords that should not appear in the Uniform Resource Locator, (URL such as **www.yahoo.com**) can be defined. Any URL containing one or more of these keywords will be blocked. This is a policy independent feature. It cannot be associated to ACL rules. This feature can be independently enabled or disabled, but works only if firewall is enabled.

2.4.1.6 Log and Alerts

Events in the network, which could affect its security, are recorded in the router's System log file. Event details are recorded in the WebTrends Enhanced Log Format (WELF) format so that statistical tools can be

used to generate custom reports. The firewall can also forward Syslog information to a Syslog server on a private network.

The ASUS SL1200's firewall supports:

- Alerts sent to the administrator via e-mail.
- At a minimum, maintains log details such as, time of packet arrival, description of action taken by Firewall and reason for action.
- Supports the UNIX Syslog format.
- Sends log report e-mails as scheduled by the network administrator or by default when the log file is full.
- All the messages are sent in the WELF format.
- ICMP logging to show code and type.

2.4.2 VPN

The wide-use of a very open public network such as the Internet comes with a lot of advantages as well as risks. These risks include the lack of confidentiality of data being sent and the authenticity of the identities of the parties involved in the exchange of data. The VPN supported in the ASUS SL1200 is intended to resolve these issues.

The VPN supported by the router is IPSec compliant. Packets sent via VPN are encrypted to maintain privacy. The encrypted packets are then tunneled through a public network. As a result, tunnel participants enjoy the same security features and facilities that are available only to members of private network.

Table 2.4 lists the VPN features supported by the router.

Table 2.4. VPN Features

Features	
Transport Mode for Client-Client Connectivity	
Tunnel Mode for Network-Network Connectivity	
IP Fragmentation and Reassembly	
Hardware Encryption Algorithm	DES, 3DES
Hardware Authentication Algorithm	MD5, SHA-1
Transforms	ESP, AH
Key Management	IKE (Pre-shared key)
Mode configuration for IKE	Main Mode, Aggressive Mode, Quick Mode



Site-to-Site VPN connection is an alternative WAN infrastructure that is used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network.

3 Quick Start Guide

This chapter provides the basic instructions for connecting the ASUS SL1200 to a computer or a LAN and to the Internet.

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



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

3.1 Part 1 — Connecting the Hardware

This section gives you instructions on connecting the device to an ADSL or a cable modem (which in turn is connected to a phone jack or a cable outlet), the power outlet, and your computer or network.



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

3.1.1 Connect an ADSL or a cable modem

To connect the router

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

3.1.2 Connect computers or a LAN

If your LAN has less than four computers, you can use an Ethernet cable to connect computers directly to the built-in switch on the device. 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 your LAN has more than four computers, you can attach one end of an Ethernet cable to a hub or a switch, such as an uplink port (refer to the hub or switch documentations for instructions), and the other to the Ethernet switch port (labeled LAN1 – LAN4) on the router.



Either the crossover or straight-through Ethernet cable can be used to connect the built-in switch and computers, hubs or switches.

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 Turning on the ASUS SL1200

After plugging in, the router will be automatically turn on. Turn on your ADSL or cable modem, your computer(s), and any LAN devices such as hubs or switches.

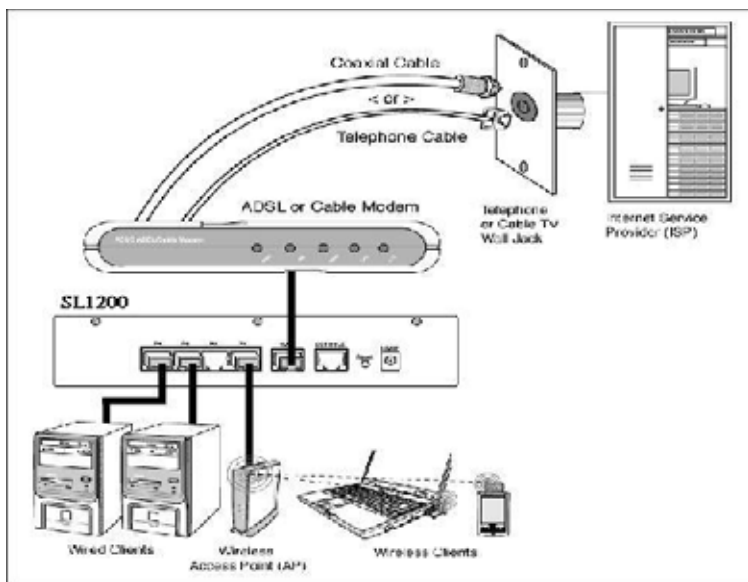


Figure 3.1. Overview of Hardware Connections



Check the LED indicators (refer to Table 3.1) to determine if the hardware setup is working properly.

Table 3.1. LED Indicators

LED	Description
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 the Internet Security Router 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.
WAN	Solid green to indicate that the device has successfully established a connection with your ISP or flashing when the device is sending or receiving data from the Internet.

3.2 Part 2 — Configuring Your Computers

This section provides instructions for configuring the Internet settings on your computers to work with the router.

3.2.1 Before you begin

By default, the ASUS SL1200 automatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information when it is assigned.



*In some cases, you may want to configure network settings manually to some or all of your computers rather than allow the Internet Security Router to do so. See **3.2.6: Assigning static IP addresses to your PCs** for instructions.*

If you have connected your PC via Ethernet to the router, 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 **Start -> 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



Check for the IP protocol and, if necessary, install it.

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

The **Local Area Connection Properties** dialog box displays a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

4. If **Internet Protocol (TCP/IP)** does not display as an installed component, click **<Install>**.
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 addresses assigned by the router.
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® 95, 98, and Me PCs

1. In the Windows task bar, click **Start -> Settings -> Control Panel**.
2. Double-click the **Network** icon.

In the Network dialog box, look for an entry started w/ "TCP/IP ->" and the name of your network adapter, and then click **<Properties>**. You may have to scroll down the list to find this entry.

If the list includes such an entry, then the TCP/IP protocol has already been enabled. Skip to step 8.

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

You may be prompted to install files from your Windows 95, 98 or Me installation CD or other media. Follow the instructions to install the files.

6. If prompted, click **<OK>** to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the router.

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

3.2.5 Windows® NT 4.0 workstations



Check for the IP protocol and, if necessary, install it.

1. In the Windows NT task bar, click **Start -> Settings -> Control Panel**.
2. In the **Control Panel** window, double click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.

The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP Protocol, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click <**Add**>.
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 addresses assigned by the router.

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**.

3.2.6 Assigning static IP addresses to your PCs

In some cases, you may want to assign IP addresses to some or all of your PCs directly (often called “statically”), rather than allowing the ASUS SL1200 to assign them. This option may be desirable (but not required) if:

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

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

On each PC to which you want to assign static information, follow the instructions on pages 13 through 17 relating only to checking for and 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.



Your PCs must have IP addresses that place them in the same subnet as the Internet Security Router's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Chapter 5 to change the LAN port IP address.

3.3 Part 3 — Quick Configuration of ASUS SL1200



This section gives instructions on logging in into the Configuration Manager, a preinstalled web-based program in the ASUS SL1200. This section also gives instructions on configuring the basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.



This section intends to quickly get the ASUS SL1200 up and running, and instructions in this section are concise. You may refer to corresponding chapters for more details.

3.3.1 Buttons Used in Setup Wizard

The ASUS SL1200 comes with a preinstalled software program called Configuration Manager that enables you to configure the router 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 the Setup Wizard. The following table shows the buttons that you will encounter in the Setup Wizard.

Button	Function
	Click this button to save the information and proceed to the next configuration page.
	Click this button to go back to the previous configuration page.

3.3.2 Setting up the ASUS SL1200

To set up the router

1. Before accessing the Configuration Manager in the router, make sure that the HTTP proxy setting is disabled in your browser. In IE, click **Tools -> Internet Options -> Connections -> LAN settings** and then uncheck "Use proxy server for your LAN ..."
2. On any PC connected to one of the four LAN ports on the router, 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 router. A login screen displays, as shown in Figure 3.2.



Figure 3.2. Login Screen

If you have problems connecting to the router, you may either: check if your PC is configured to accept IP address assignment from the router, or set the IP address of your PC to any IP address in the 192.168.1.0 network such as 192.168.1.2.

3. Enter your user name and password, and then click <OK> to enter the Configuration Manager. The first time you log into this program, use these default settings:

Default User Name: admin

Default Password: admin

The Setup Wizard home page displays each time you log into the Configuration Manager.



Figure 3.3. Setup Wizard Home Page



Figure 3.4. Setup Wizard - Password Configuration Page

- Click **<Next>** to enter the password configuration page as shown in Figure 3.4. Change the password, if desired. Otherwise, click **<Next>** to proceed to the next page.

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

- In the System Information setup page, enter the requested information and click **<Apply>** to save the changes. Otherwise, click **<Next>** to proceed to the next page.

Figure 3.5. Setup Wizard- System Information Setup Page

NTP Server ID	NTP Server IP	NTP Server Name
NTP Server 1	210.173.160.27	ASUS
NTP Server 2	210.173.160.67	
NTP Server 3	103.40.41.179	
NTP Server 4	100.40.191.23	
NTP Server 5	100.40.191.19	

Figure 3.6. Setup Wizard - Date/Time Configuration Page

- In the Date/Time Setup page, select your time zone from the Time Zone drop-down list. Click **<Apply>** to save the settings and then click the **<Next>** to go to the next configuration page.



There is no real time clock inside the router. The system date and time are maintained by the external network time server. There is no need to set the date and time here unless you do not have access to a time server and you want the router to maintain its own time.

7. 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 **<Next>** to proceed to the next configuration page.



Figure 3.7. Setup Wizard- LAN IP Configuration Page



Figure 3.8. Setup Wizard - DHCP Server Configuration Page

8. 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 **<Next>** to proceed to the next configuration page.

9. In the WAN Configuration page, you configure the WAN settings for the router. Depending on the connection mode required by your ISP, you can select from the three connection modes in the Connection Mode drop-down list (see Figure 3.9): **PPPoE**, **Dynamic**, and **Static**.



Figure 3.9. Setup Wizard - WAN PPPoE Configuration Page



Figure 3.10. Setup Wizard - WAN Dynamic IP Configuration Page

a) PPPoE Connection Mode (see Figure 3.9)

- You do not need to enter primary/secondary DNS IP addresses. PPPoE is able to automatically obtain this information for you from your ISP. However, if you prefer to use your favorite DNS servers, you may enter them in the space provided.
- Host name is optional. You may leave it empty if your ISP did not provide such information.
- Enter the user name and password provided by your ISP.
- Click **<Apply>** to save the PPPoE settings.

b) Dynamic IP Connection Mode (see Figure 3.10)

- You do not need to enter primary/secondary DNS IP addresses. DHCP client is able to automatically obtain this information for you from your ISP. However, if you prefer to use your favorite DNS servers, you may enter them in the space provided.
- Host name is optional. You may leave it empty if your ISP did not provide such information.
- If you had previously registered a specific MAC address with your ISP for Internet connections, enter the registered MAC address and make sure you check the MAC cloning check box.
- Click **<Apply>** to save the dynamic IP settings.



Figure 3.11. Setup Wizard - WAN Static IP Configuration Page

c) Static IP Connection Mode

- Enter WAN IP address in the IP Address field. This information should be provided by your ISP.
- Enter Subnet Mask for the WAN. This information should be provided by your ISP. Typically, it is 255.255.255.0.
- Enter gateway address provided by your ISP in the space provided.
- Enter at least the primary DNS IP address provided by your ISP. Secondary DNS IP address is optional. Enter it in the space provided if you have such information from your ISP.
- Click **<Apply>** to save the static IP settings.

You have now completed customizing the basic configuration settings. Read the next section to determine if you have access to the Internet.

3.3.3 Testing Your Setup

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

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

If the LEDs do not light up as expected or the web page does not display, see Chapter 14 for troubleshooting suggestions.

3.3.4 Default Router Settings

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

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

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

Table 3.2. Default Settings Summary

Option	Default Setting	Explanations/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.10 through 192.168.1.108	The Internet Security Router 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 5.2 for an explanation of the DHCP service.
LAN Port IP Address	Static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the Internet Security Router. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See section 5.1 LAN IP Address for instructions.

4 Using the Configuration Manager

The ASUS SL1200 includes a preinstalled program called the Configuration Manager, which provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You access it through your web browser from any PC connected to the router via the LAN or WAN ports.

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

4.1 Log into Configuration Manager

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

- A computer connected to the LAN or WAN port on the router as described in the Quick Start Guide chapter.
- A web browser installed on the computer. The program is designed to work best with Netscape 7.0.2 , Microsoft Internet Explorer® 5.5 or later.

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

To connect via the LAN ports

1. From a LAN computer, open your web browser, type the following in the web address (or location) box, and press <Enter>:
http://192.168.1.1

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

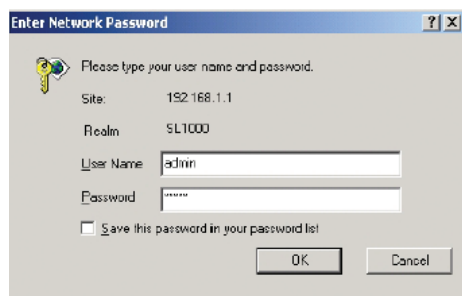


Figure 4.1. Configuration Manager Login Screen

2. Enter your user name and password, and then click <OK>.

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

Default User Name: admin

Default Password: admin



*You can change the password at any time. See section **11.2 Change the Login Password.***

The Setup Wizard page displays each time you log into the program. See Figure 4.3.

4.2 Functional Layout

A typical Configuration Manager page consists of two separate frames - the left frame and the right frame.

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, and WAN, and indicated by expandable folder icons. You can click on any of these folders to display a specific configuration page.

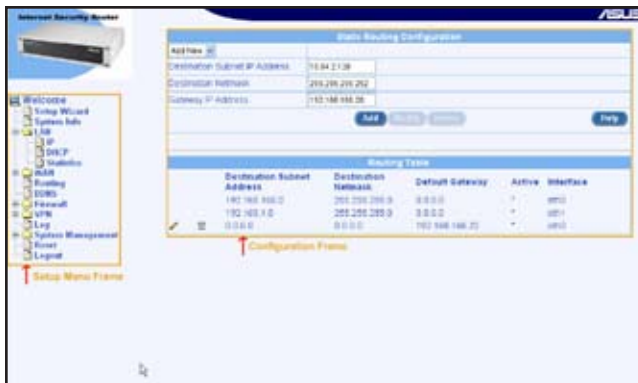





Figure 4.2. Typical Configuration Manager Page

The right frame displays the information for a selected Configuration page.









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

Table 4.1. Description of Commonly Used Buttons and Icons

Button/Icon	Function
	Stores any changes you have made on the current page.
	Adds the existing configuration to the system such as a static route or a firewall ACL rule.
	Modifies the existing configuration in the system such as a static route or a firewall ACL rule.
	Deletes the selected item, such as a static route or a firewall ACL rule.
	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.
	Redisplays the current page with updated statistics or settings.
	Selects the item for editing.
	Deletes the selected item.

4.3 Configuration Manager's Home Page

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



Figure 4.3. Setup Wizard Home Page

4.4 Overview of System Configuration

To view the overall system configuration, log into Configuration Manager as administrator, and then click the System Info menu. Figure 4.4 shows the information available in the System Info page.

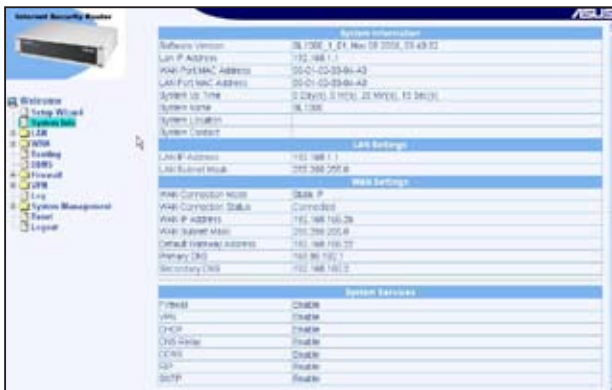


Figure 4.4. System Information Page

5 Configuring LAN Settings

This chapter describes how to configure LAN properties for the LAN interface on the router. You will learn to configure IP address, DHCP, and DNS server for your LAN in this chapter.

5.1 LAN IP Address

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



A network node can be thought of as any interface where a device connects to the network, such as the Internet Security Router's LAN port and the network interface cards on your PCs. See Chapter 13 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.



The Internet Security Router itself can function as a DHCP server for your LAN computers, as described in section 5.2.3 Configuring DHCP Server, but not for its own LAN port.

5.1.1 LAN IP Configuration Parameters

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

Table 5.1. LAN IP Configuration Parameters

Setting	Description
IP Address	The LAN IP address of the router. This IP is used by your computers to identify the router's LAN port. The public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN port on the router 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.

5.1.2 Configuring the LAN IP Address

To change the default LAN IP address

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

When the submenus of LAN Configuration displays, click IP submenu to display the IP Address configuration page as shown in Figure 5.1.



Figure 5.1. LAN IP Address Configuration Page

2. Enter a LAN IP address and subnet mask for the router.
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, **3.2 Part 2 — Configuring Your Computers**, for instructions.
5. Enter the new IP address in your Web browser's address/location box to log into the Configuration Manager.

5.2 Dynamic Host Control Protocol (DHCP)

5.2.1 What is a 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 router, 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.



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 the Internet Security Router.

The DHCP server draws from a defined pool of IP addresses and “leases” them for a specified duration 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.

5.2.2 Why use a DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from the router. 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.

5.2.3 Configuring a DHCP Server



By default, the router is configured as a DHCP server on the LAN side, with a predefined IP address pool from 192.168.1.10 to 192.168.1.42 (subnet mask 255.255.255.0). To change this range of addresses, follow the procedures described in this section.

To configure a DHCP server



You must first configure your PCs to accept DHCP information assigned by a DHCP server.

1. Log into Configuration Manager as administrator. Click **LAN -> DHCP**. The DHCP Configuration page displays as shown in Figure 5.2.

DHCP Server Assignments		
MAC Address	Assigned IP Address	IP Address Expires On
00:0C:29:00:00:00	192.168.1.10	09/20/2010 07:16:00

Figure 5.2. DHCP Configuration Page

2. Enter the information for the IP Address Pool (Begin/End Address), Subnet Mask, Lease Time and Default Gateway IP Address. Other fields, such as Primary/Secondary DNS Server IP Address and Primary/Secondary WINS Server IP Address, are optional. However, it is recommended that you enter the primary DNS server IP address. You may enter the LAN IP or your ISP's DNS IP in the primary DNS Server IP Address field. Table 5.2 describes the DHCP configuration parameters in detail.

Table 5.2. DHCP Configuration Parameters

Field	Description
IP Address Pool Begin/End	Specify the lowest and highest addresses in the DHCP address pool.
Subnet Mask	Enter the subnet mask to be used for the DHCP address pool.
Lease Time	The duration the assigned address will be used by a device connected on the LAN.
Default Gateway IP Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the device that the DHCP client computers first contacted to communicate with the Internet. Typically, it is the router's LAN port IP address.
Primary/Secondary DNS Server IP Address	The IP address of the Domain Name System server to be used by computers that receive IP addresses from this pool. The DNS server translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, the server(s) are located with your ISP. However, you may enter LAN IP address of the router as it 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. The primary and secondary DNS servers are optional.
Primary/Secondary WINS Server IP Address (optional)	The IP address of the WINS servers to be used by computers that receive IP addresses from the DHCP IP address pool. You do not need to enter this information unless your network has WINS servers.

3. Click **<Apply>** to save the DHCP server configurations.

5.2.4 Viewing Current DHCP Address Assignments

When the router 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, go to the DHCP Server Configuration page. A page displays similar to that shown in Figure 5.2. The bottom 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.

Table 5.3 lists the information for each leased addresses.

Table 5.3. DHCP Address Assignment

Field	Description
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.

5.3 DNS

5.3.1 About DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (such as “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.

5.3.2 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 the router and create an address pool that specify the DNS addresses to be distributed to the PCs. Refer to the section **5.2.3 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 Internet Security Router (such as 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the next section.



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

5.3.3 Configuring DNS Relay

When you specify the device's LAN port IP address as the DNS address, then the router automatically performs "DNS relay". Since 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 router must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

- **Learned through PPPoE or Dynamic IP Connection:** If the Internet Security Router uses a PPPoE (see section **6.2.2 Configuring PPPoE for WAN**) or Dynamic IP (see section **6.3.2 Configuring Dynamic IP for WAN**) connection to the ISP, the primary and secondary DNS addresses can be learned via the PPPoE protocol. Using this option provides the advantage that you will not need to reconfigure the PCs or the router if the ISP changes their DNS addresses.
- **Configured on the router:** You can also specify the ISP's DNS addresses in the WAN Configuration page as shown in Figure 6.1. WAN PPPoE Configuration Page, Figure 6.2. WAN Dynamic IP (DHCP client) Configuration Page, or Figure 6.3. WAN Static IP Configuration Page.

To configure DNS relay

1. Enter LAN IP in the DNS Server IP Address field in DHCP configuration page as shown in Figure 5.2.
2. Configure the LAN PCs to use the IP addresses assigned by the DHCP server on the router, or enter the router's LAN IP address as their DNS server address manually for each PC on your LAN.



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.

5.4 Viewing LAN Statistics

You can view statistics of your LAN traffic on the router. 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 5.3 shows the LAN Statistics page.



Figure 5.3. LAN Statistics Page

To display the updated statistics since you opened the page, click **<Refresh>**.

6 Configuring WAN Settings

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

6.1 WAN Connection Mode

The router supports three modes of WAN connection – PPPoE, dynamic IP, and static IP. You may select your ISP's required connection mode from the Connection Mode drop-down list in WAN Configuration page as shown in Figure 6.1.



Figure 6.1. WAN PPPoE Configuration Page

6.2 PPPoE

6.2.1 WAN PPPoE Configuration Parameters

Table 6.1 describes the configuration parameters available for PPPoE connection mode.

Table 6.1. WAN PPPoE Configuration Parameters

Setting	Description
Host Name	Host name is optional but may be required by some ISP.
User Name and Password	Enter the user name and password you use to log into your ISP. This is different from the information you used to log into Configuration Manager.
Primary/ Secondary DNS	IP address of the primary or secondary DNS are optional as PPPoE will automatically detect the DNS IP addresses configured at your ISP. However, if there are other DNS servers you would rather use, enter the IP addresses in the spaces provided.
Connection Options	The default setting for this option is "Disable". You can also select either Dial-On-Demand or Keep-Alive if desired. Dial-On-Demand enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. The minimum value of inactivity timeout is 30 seconds. RIP and SNTP services may interfere with this function if there are activities from these two services. Make sure that the update interval setting of the system date and time (see 11.4 Setup Date and Time for details) is greater than the inactivity timeout value.
Keep Alive	Enable this option if you wish to keep your Internet connection active, even when there is no traffic. Enter the value for the "Echo Interval" at which you want the router to send out some data periodically to your ISP. The default value of "Echo Interval" is 60 seconds.

6.2.2 Configuring PPPoE for WAN

To configure PPPoE settings

1. Select PPPoE from the Connection Mode drop-down list as shown in Figure 6.1.
2. (Optional) Enter the host name if required by your ISP.
3. If you are connecting to the Internet using PPPoE, you probably only have to enter User Name and Password in the PPPoE Configuration page as shown in Figure 6.1, unless you want to use your preferred DNS servers.
4. (Optional) Enter the IP addresses for the primary and secondary DNS servers if you want to use your preferred DNS servers. Otherwise, skip this step.
5. Choose a connection option and enter the appropriate setting if desired. The default setting is "Disable".
6. Click **<Apply>** to save the PPPoE settings when you are done with the configuration. You will see a summary of the WAN configuration at the bottom half of the configuration page. The default gateway address is not shown immediately. Click on the **WAN** menu to open the WAN configuration page again.

6.3 Dynamic IP

6.3.1 WAN Dynamic IP Configuration Parameters

Table 6.2 describes the configuration parameters available for dynamic IP connection mode.

Table 6.2. WAN Dynamic IP Configuration Parameters

Field	Description
Host Name	Host name is optional but may be required by some ISP.
Primary/ Secondary DNS	IP address of the primary and/or secondary DNS are optional as DHCP client will automatically obtain the DNS IP addresses configured at your ISP. However, if there are other DNS servers you would rather use, enter the IP addresses in the spaces provided.
MAC Cloning	The default is to use the MAC address of the WAN interface. However, if you had registered a MAC address previously with your ISP, you may need to enter that MAC address here.

6.3.2 Configuring Dynamic IP for WAN

To configure dynamic IP settings

1. Select **Dynamic** from the Connection Mode drop-down list as shown in Figure 6.2.
2. (Optional) Enter the host name if required by your ISP.
3. (Optional) Enter the IP addresses for the primary and secondary DNS servers if you want to use your preferred DNS servers. Otherwise, skip this step.
4. If you had previously registered a specific MAC address with your ISP for Internet access, enter the registered MAC address and make sure you check the MAC cloning check box.
5. Click **<Apply>** to save the Dynamic IP settings when you are done with the configuration. You will see a summary of the WAN configuration at the bottom half of the configuration page. The default gateway address is not shown immediately, click on the WAN menu to open the WAN configuration page again.



Figure 6.2. WAN Dynamic IP (DHCP client) Configuration Page

6.4 Static IP

6.4.1 WAN Static IP Configuration Parameters

Table 6.3 describes the configuration parameters available for static IP connection mode.

Table 6.3. WAN Static IP Configuration Parameters

Setting	Description
IP Address	WAN IP address provided by your ISP.
Subnet Mask	WAN subnet mask provided by your ISP. Typically, it is set as 255.255.255.0.
Gateway Address	Gateway IP address provided by your ISP. It must be in the same subnet as the WAN on the router.
Primary/ Secondary DNS	You must at least enter the IP address of the primary DNS server. Secondary DNS is optional.

6.4.2 Configuring Static IP for WAN



Figure 6.3. WAN Static IP Configuration Page

To configure static IP settings

1. Select **Static** from the Connection Mode drop-down list as shown in Figure 6.3.
2. Enter the WAN IP address in the IP Address field. This information should be provided by your ISP.
3. Enter the Subnet Mask for the WAN. This information should be provided by your ISP. Typically, it is 255.255.255.0.
4. Enter the gateway address provided by your ISP in the space provided.
5. Enter the IP address of the primary DNS server. This information should be provided by your ISP. Secondary DNS server is optional.
6. Click **<Apply>** to save the static IP settings. You will see a summary of the WAN configuration at the bottom half of the configuration page.

6.5 Viewing WAN Statistics

You can view statistics of your WAN traffic. You will not 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 IP statistics, click Statistics on the WAN submenu. Figure 6.4 shows the WAN Statistics page.



Figure 6.4. WAN Statistics Page

To see the updated statistics since you opened the page, simply click <Refresh>.

7 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.

7.1 Overview of IP Routes

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

7.1.1 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 router 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 router. 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. Refer to **3.2 Part 2 -- Configuring Your Computers** for more details.
- On the router 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. Refer to **7.3.2 Adding a Static Route** for more details on adding a default route.

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.

7.2 Dynamic Routing using Routing Information Protocol (RIP)

RIP enables routing information exchange between routers; thus, routes are updated automatically without human intervention. Please note that RIP service must be enabled first in the System Management / System Services configuration page if you want to use RIP to exchange routing information with other routers.

7.2.1 Dynamic Routing (RIP) Configuration Parameters

Table 7.1 defines the available configuration parameters for dynamic routing.

Table 7.1. Dynamic Routing (RIP) Configuration Parameters

Field	Description
Interface	Select the interface through which the routing information exchange is desired. You may configure all or some interfaces to support routing information exchange.
RIP	Click the Enable or Disable radio button to enable or disable RIP for the interface selected. You must enable RIP service first in the System Management -> System Services configuration page if you want to enable RIP to exchange routing information. The default setting is Enable .
Passive Mode	Enable this mode if RIP configured for this interface will only receive routing information from other routers and not send routing information to other routers. Disable this mode if you want this interface to send and receive routing information to/from other routers. The default setting is Enable .
RIP Version (Send)	Select the RIP version for sending the routing information. Three options are available: Version 1 , Version 2 , and Both . The default setting is Version 2 .
RIP Version (Receive)	Select the RIP version for receiving the routing information. Three options are available: Version 1 , Version 2 , and Both . The default setting is Both .

Field	Description
Authentication	Click on Enable or Disable radio button to enable/disable authentication for exchanging the routing information. All the routers exchanging routing information must use the same authentication key. The default setting is Disable .
RIP Authentication Mode	Select RIP authentication mode from the drop down list. Two modes are available - Clear Text , and MD5 . The default setting is Clear Text .
Authentication Key	Enter the authentication key for shared by all the routers exchanging routing information. The default authentication key is admin .

7.2.2 Configuring RIP

To configure RIP

1. Click the **Routing** menu to open the routing configuration page.
2. In the RIP Configuration page, click the **Enable** or **Disable** radio button depending on whether you want to enable or disable RIP service. Skip this step, if you have already done so.



Figure 7.1. RIP Configuration

3. Select an interface from the drop-down list via which the routing information is to be exchanged.
4. To enable or disable RIP for the specified interface, click the **Enable** or **Disable** radio button.

5. To enable or disable RIP passive mode, click the **Enable** or **Disable** radio button.
6. Select RIP version for sending and receiving routing information from the respective drop-down list.
7. To enable or disable authentication, click the **Enable** or **Disable** radio button. You must also select the RIP authentication mode and enter authentication key if authentication is enabled.
8. Repeat steps 1 to 5 if you want to configure another interface to support routing information exchange.
9. Click **<Apply>** to save the RIP configuration.

7.3 Static Routing

7.3.1 Static Route Configuration Parameters

Table 7.2 defines the available configuration parameters for static routing configuration.

Table 7.2. Static Route Configuration Parameters

Field	Description
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 13.1 IP Addresses for more details on IP addresses.
Destination Netmask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. The default route uses a netmask of 0.0.0.0. Refer to 13.3 Subnet masks for more details on network masks.
Gateway IP Address	Gateway IP address

7.3.2 Adding a Static Route

To add a static route to the routing table

1. To open the routing configuration page, click the **Routing** menu.
2. Enter static routes information such as destination IP address, destination netmask and gateway IP address in the corresponding fields.

For a description of these fields, refer to **Table 7.2. 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 Netmask** fields.

The image shows a web-based configuration form titled "Static Routing Configuration". At the top left is a dropdown menu labeled "Add New". Below it are three input fields: "Destination Subnet IP Address", "Destination Netmask", and "Gateway IP Address". At the bottom of the form are four buttons: "Add", "Modify", "Delete", and "Help".

Figure 7.2. Static Route Configuration

3. Click **<Add>** to add a new route.

7.3.3 Deleting a Static Route

To delete a static route from the routing table

1. In the Static Routes configuration page as shown in Figure 7.2, select the route from the service drop-down list or click on the icon of the route to be deleted in the Routing Table.
2. Click **<Delete>** to delete the selected route.



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

7.3.4 Viewing the 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 SL 1200's routing table, just open the Routing configuration page by clicking on the Routing menu. The Routing Table displays at the bottom half of the Routing configuration page, as shown in Figure 7.3.

Routing Table				
Destination Subnet Address	Destination Netmask	Default Gateway	Active	Interface
192.168.1.0	255.255.255.0	0.0.0.0	*	eth1

Figure 7.3. Routing Table

The routing table displays a row for each existing route containing the IP address and the subnet mask of the destination network and the IP address of the gateway that forwards the traffic to the destination network.

8 Configuring DDNS

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

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

HTTP Dynamic DNS Client

HTTP DDNS client uses the mechanism provided by the popular DDNS service providers for updating the DNS records dynamically. In this case, the service provider updates DNS records in the DNS. The router uses HTTP to trigger this update.

The router supports HTTP DDNS update with the following service providers:

- www.dyndns.org
- www.zoneedit.com
- www.dns-tokyo.jp

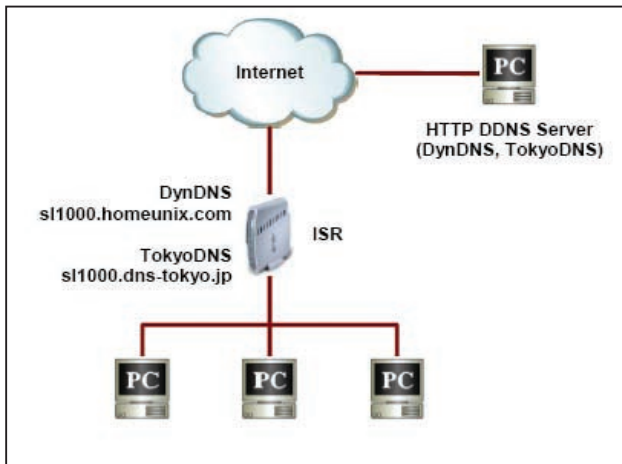


Figure 8.1. Network Diagram for HTTP DDNS

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

8.1 DDNS Configuration Parameters

Table 8.1 describes the configuration parameters available for DDNS service.

Table 8.1. DDNS Configuration Parameters

Field	Description
DDNS State	
Enable	Click on this radio button to enable the DDNS Service
Disable	Click on this radio button to disable the DDNS Service
DDNS Type – select a DDNS service type: HTTP or RFC-2136 DDNS	
HTTP DDNS	Click this radio button if HTTP DDNS is desired.
DNS Zone Name	
Enter the registered domain name provided by your ISP. The host name of the router has to be configured in the System Information Setup page properly. For example, If the host name of your router is “host1” and the DNS Zone Name is “yourdomain.com”. The fully qualified domain name (FQDN) is “host1.yourdomain.com”.)	
HTTP DDNS Specific Settings	
DDNS Service [For HTTP DDNS only]	
dyndns	Visit http://www.dyndns.org for more details.
zoneedit	Visit http://www.zoneedit.com for more details.
dyn-tokyo	Visit http://www.dns-tokyo.jp for more details.
DDNS User name [For HTTP DDNS only]	
Enter the user name provided by your DDNS service provider in this field.	
DDNS Password [For HTTP DDNS only]	
Enter the password provided by your DDNS service provider in this field.	

8.2 Access DDNS Configuration Page

Log into Configuration Manager as administrator, and click the **DDNS** menu. The DDNS Configuration page displays, as shown in Figure 8.2. When you open the DDNS Configuration page, a list of existing DDNS configuration is displayed at the bottom half of the configuration page such as those shown in Figure 8.2.

8.3 Configuring HTTP DDNS Client



Figure 8.2. HTTP DDNS Configuration Page

To configure the HTTP DDNS

1. You should have a registered domain name with a DDNS service provider. If you have not done so, visit <http://www.dns-tokyo.jp> or <http://www.dyndns.org> for more details.
2. Make sure that you have a host name configured for the router. Otherwise, go to **System Management -> System Identity** to configure one.
3. Open the DDNS Configuration page. See section **8.2 Access DDNS Configuration Page**.
4. In the DDNS Configuration page, select **Enable** for the DDNS State and **HTTP DDNS** for the DDNS Type. The HTTP DDNS Configuration is then displayed as shown in Figure 8.2.
5. Enter the domain name in the DNS Zone Name field.
6. Select a DDNS service from the DDNS Service drop-down list.
7. Enter the username and password provided by your DDNS service providers.
8. Click **<Apply>** to send a DNS update request to your DDNS service provider. The DNS update request will also be sent to your DDNS Service provider automatically whenever the WAN port status is changed.

9 Configuring Firewall/NAT Settings

The router provides built-in firewall/NAT functions. These functions 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 Access Control List (ACL) rules to control the data passing through your network. You will use firewall configuration pages to:

- Create, modify, delete, and view inbound/outbound ACL rules.
- Create, modify, and delete pre-defined services, IP pools, NAT pools, application filters and time ranges to be used in inbound/outbound ACL configurations.
- View firewall statistics.



When you define an ACL rule, you instruct the Internet Security Router to examine each data packet it receives to determine whether it meets the criteria set in the rule. The criteria can include the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data. If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

9.1 Firewall Overview

9.1.1 Stateful Packet Inspection

The stateful packet inspection engine in the router maintains a state table that is used to keep track of connection states of all the packets passing through the firewall. The firewall will open a “hole” to allow the packet to pass through if the state of the packet that belongs to an already established connection matches the state maintained by the stateful

packet inspection engine. Otherwise, the packet will be dropped. This “hole” will be closed when the connection session terminates. No configuration is required for stateful packet inspection. It is enabled by default when the firewall is enabled. Refer to section **11.1 Configure System Services** to enable or disable firewall service on the router.

9.1.2 Denial of Service (DoS) Protection

Both DoS protection and stateful packet inspection provide the first line of defense for your network. No configuration is required for both protections on your network as long as firewall is enabled for the router. By default, the firewall is enabled in the router. Refer to section **11.1 Configure System Services** to enable or disable firewall service on the router.

9.1.3 Firewall and Access Control List (ACL)

9.1.3.1 Priority Order of ACL Rule

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

9.1.3.2 Tracking Connection State

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

For example, an ACL rule allows outbound ICMP packet from 192.168.1.1 to 192.168.2.1. When 192.168.1.1 send an ICMP echo request (such as a ping packet) to 192.168.2.1, 192.168.2.1 will send an ICMP echo reply to 192.168.1.1. In the router, you do not need to create another inbound ACL rule because stateful packet inspection engine will remember the connection state and allows the ICMP echo reply to pass through the firewall.

9.1.4 Default ACL Rules

The router supports three 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.
- **Self Access Rules:** For controlling access to the Internet Security Router itself.

Default Inbound Access Rules

No default inbound access rule is configured. 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.



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

9.2 NAT Overview

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

The NAT modes supported are static NAT, dynamic NAT, NAPT, reverse static NAT, and reverse NAPT.

9.2.1 Static (One to One) NAT

Static NAT maps an internal host address to a globally valid Internet address (one-to-one). The IP address in each packet is directly translated with a globally valid IP contained in the mapping. Figure 9.1 illustrates the IP address mapping relationship between the four private IP addresses and the four globally valid IP addresses.



This mapping is static. This mapping will not change over time until this mapping is manually changed by the administrator. This means that a host will always use the same global valid IP address for all its outgoing traffic.

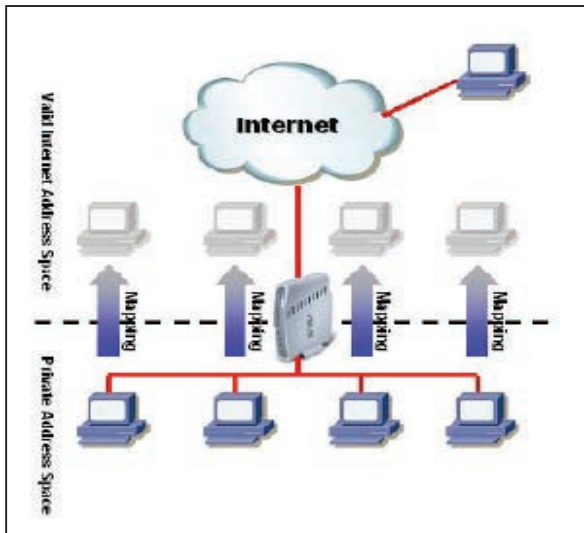


Figure 9.1 Static NAT – Mapping Four Private IP Addresses to Four Globally Valid IP Addresses

9.2.2 Dynamic NAT

Dynamic NAT maps an internal host dynamically to a globally valid Internet address (m-to-n). The mapping usually contains a pool of internal IP addresses (m) and a pool of globally valid Internet IP addresses (n) with m usually greater than n. Each internal IP address is mapped to one external IP address on a first come first serve basis. Figure 9.2 shows that PC B, C and D are mapped to a globally valid IP address respectively, while PC A does not map to any globally valid IP address. If PC A wants to go to the Internet, PC A must wait until a global valid IP address is available. For example, in Figure 9.3, PC B must disconnect from the Internet first to allow PC A to access Internet.

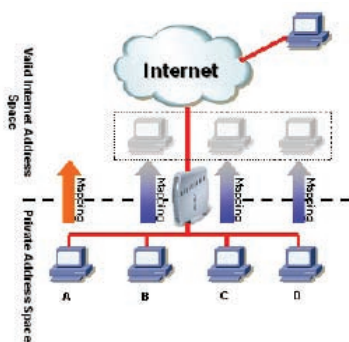


Figure 9.2 Dynamic NAT – Four Private IP addresses Mapped to Three Valid IP Addresses

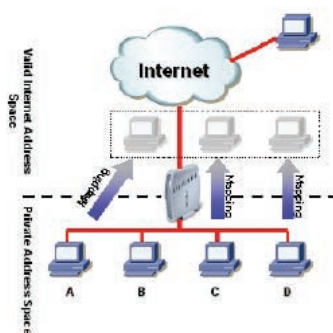


Figure 9.3 Dynamic NAT – PC-A can get a NAT association after PC-B is disconnected

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

This mapping is also called IP Masquerading. This maps many internal hosts to one globally valid Internet address. The mapping contains a pool of network ports to be used for translation. Every packet is translated with the globally valid Internet address and the port number is translated with an available port from the pool of network ports. Figure 9.4 shows that all the hosts on the local network gain access to the Internet by mapping to only one globally valid IP address and different port numbers from a free pool of network ports.

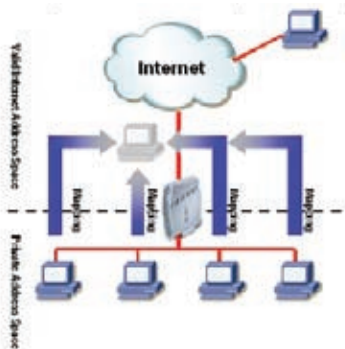


Figure 9.4 NAPT – Map Any Internal PCs to a Single Global IP Address

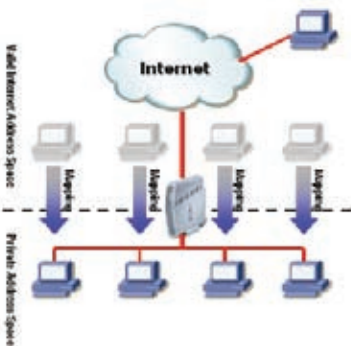


Figure 9.5 Reverse Static NAT – Map a Global IP Address to An Internal PC

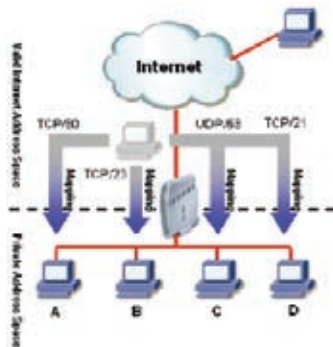


Figure 9.6 Reverse NAPT – Relay Incoming Packets to the Internal Host Base on the Protocol, Port Number or IP Address

9.2.4 Reverse Static NAT

Reverse static NAT maps a globally valid IP address to an internal host address for the inbound traffic. All packets coming to that globally valid IP address are relayed to the Internal address. This is useful when hosting services in an internal machine. Figure 9.5 shows that four globally valid IP addresses are mapped to four hosts on the internal network and each can be used to host some services for inbound traffic such as an FTP server.

9.2.5 Reverse NAPT / Virtual Server

Reverse NAPT is also called inbound mapping, port mapping, or virtual server. Any packet coming to the router can be relayed to the internal host based on the protocol, the port number or the IP address specified in the ACL rule. This is useful when multiple services are hosted on different internal machines. Figure 9.6 shows that web server (TCP/80) is hosted on PC A, telnet server (TCP/23) on PC B, DNS server (UDP/53) on PC C and FTP server (TCP/21) on PC D. This means that the inbound traffic of these four services will be directed to respective host hosting these services.

9.3 Configuring Inbound ACL Rules

By creating ACL rules in Inbound ACL configuration page as shown in Figure 9.7, 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

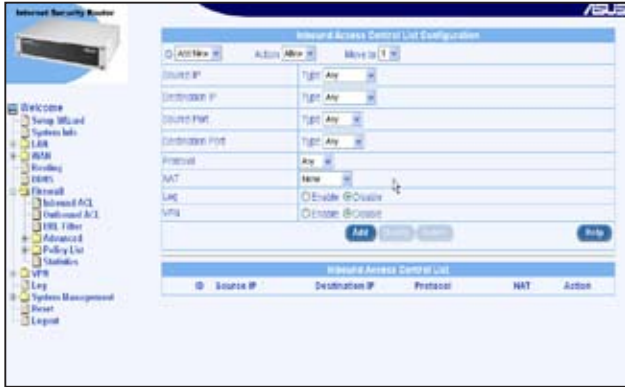


Figure 9.7. Inbound ACL Configuration Page

9.3.1 Inbound ACL Rule Configuration Parameters

Table 9.1 describes the configuration parameters available for firewall inbound ACL rule.

Table 9.1. Inbound ACL Rule Configuration Parameters

Field	Description
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 router's 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.

Field	Description
Source IP	
This option allows you to set the source network to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the source network such as those on the Internet.
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
Subnet	This option allows you to include all the computers that are connected in an IP subnet. When this option is selected, the following fields become available for entry:
Address	Enter the appropriate IP address.
Mask	Enter the corresponding subnet mask.
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:
Begin	Enter the starting IP address of the range
End	Enter the ending IP address of the range
IP Pool	This option allows you to associate a pre-configured IP pool with this rule. The available IP pool can be selected from the IP pool drop-down list.
Destination IP	
This option allows you to set the destination network to which this rule should apply. Use the dropdown list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the local network.
IP Address, Subnet, Range and IP Pool	Select any of these options and enter details as described in the Source IP section above.
Source Port	
This option allows you to set the source port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an arbitrary source port number.

Field	Description
Single	This option allows you to apply this rule to an application with a specific source port number.
Port Number	Enter the source port number
Range	Select this option if you want this rule to apply to applications with this port range. The following fields become available for entry when this option is selected.
Begin	Enter the starting port number of the range
End	Enter the ending port number of the range
Destination Port	
This option allows you to set the destination port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an arbitrary destination port number.
Single, Range	Select any of these and enter details as described in the Source Port section above.
Service	<p>This option allows you to select any of the pre-configured services from the drop-down list instead of the destination port. The following are examples of services:</p> <p>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.</p> <p>Note: Service is a combination of protocol and port number. They appear after you add them in the “Firewall Service” configuration page.</p>
Protocol	
This option allows you to select protocol type from a drop-down list. Available settings are All, TCP, UDP, ICMP, AH and ESP. If you select “service” for the destination port, this option will not be available.	

Field	Description
NAT	
This option allows you to select the type of NAT for the inbound traffic.	
None	Select this option if you do not intend to use NAT in this inbound ACL rule.
IP Address	Select this option to specify the IP address of the computer (usually a server in your LAN) that you want the incoming traffic to be directed. This option is called reverse NAT or virtual server.
NAT Pool	Select this option to associate a pre-configured NAT pool to the rule. Only reverse static NAT and reverse NAT pool can be used to associate with an inbound ACL rule.
Time Ranges	
Select a pre-configured time range during which the rule is active. Select “Always” to make the rule active at all times.	
Log	
Click on the “Enable” or “Disable” radio button to enable or disable logging for this ACL rule.	
VPN	
Click on the “Enable” radio button if you want the traffic to go through VPN. Otherwise, click on the “Disable” radio button.	

9.3.2 Access Inbound ACL Rule Configuration Page – (Firewall -> Inbound ACL)

Log into Configuration Manager as administrator. Click **Firewall -> Inbound ACL**.

The Firewall Inbound ACL Configuration page displays as shown in Figure 9.7.

When you open the Inbound ACL Configuration page, a list of existing ACL rules is also displayed at the bottom half of the configuration page such as those shown in Figure 9.8.



Figure 9.8. Inbound ACL Configuration Example

9.3.3 Add Inbound ACL Rules

To add an inbound ACL rule


1. Open the Outbound ACL Rule Configuration Page. See section **9.3.2 Access Inbound ACL Rule Configuration Page**.
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, time ranges, application filtering, log, and VPN. 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. 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 the **<Add>** button to create the new ACL rule. The new ACL rule will then be displayed in the inbound access control list table at the bottom half of the Inbound ACL Configuration page.

Figure 9.8 shows how to create a rule to allow inbound HTTP (such as web server) service. This rule allows inbound HTTP traffic to be directed to the host w/ IP address 192.168.1.28.


9.3.4 Modify Inbound ACL Rules

To modify an inbound ACL rule

1. Open the Outbound ACL Rule Configuration Page (see section **9.3.2 Access Inbound ACL Rule Configuration Page**).
2. Click on the  icon of the rule to be modified in the inbound ACL table or select the rule number from the “ID” drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, and VPN. See Table 9.1 for explanation of these fields.
4. Click **<Modify>** to modify this ACL rule. The new settings for this ACL rule will then be displayed in the inbound access control list table at the bottom half of the Inbound ACL Configuration page.

9.3.5 Delete Inbound ACL Rules

To delete an inbound ACL rule

1. Open the Outbound ACL Rule Configuration Page. See section **9.3.2 Access Inbound ACL Rule Configuration Page**.
2. Click on the  icon of the rule to be deleted in the inbound ACL table or select the rule number from the “ID” drop-down list.

3. Click <Delete> to delete this ACL rule. The ACL rule deleted will be removed from the ACL rule table located at the bottom half of the same configuration page.

9.3.6 Display Inbound ACL Rules

To see existing inbound ACL rules, open the **Inbound ACL Rule Configuration** page as described in section 9.3.2 **Access Inbound ACL Rule Configuration Page**.

9.4 Configuring Outbound ACL Rules

By creating ACL rules in outbound ACL configuration page as shown in Figure 9.9, 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



Figure 9.9. Outbound ACL Configuration Page

9.4.1 Outbound ACL Rule Configuration Parameters

Table 9.2 describes the configuration parameters available for firewall outbound ACL rule.

Table 9.2. Outbound ACL Rule Configuration Parameters

Field	Description
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. router's 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 option allows you to set the source network to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the 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
Subnet	This option allows you to include all the computers that are connected in an IP subnet. When this option is selected, the following fields become available for entry:
Address	Enter the appropriate IP address.
Mask	Enter the corresponding subnet mask.

Field	Description
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:
Begin	Enter the starting IP address of the range
End	Enter the ending IP address of the range
IP Pool	This option allows you to associate a pre-configured IP pool with this rule. The available IP pool can be selected from the IP pool drop-down list.
Destination IP	
This option allows you to set the destination network to which this rule should apply. Use the dropdown list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the destination network, such as those on the Internet.
IP Address, Subnet, Range and IP Pool	Select any of these and enter details as described in the Source IP section above.
Source Port	
This option allows you to set the source port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an arbitrary source port number.
Single	This option allows you to apply this rule to an application with a specific source port number.
Port Number	Enter the source port number
Range	Select this option if you want this rule to apply to applications with this port range. The following fields become available for entry when this option is selected.
Begin	Enter the starting port number of the range
End	Enter the ending port number of the range
Destination Port	
This option allows you to set the destination port to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	Select this option if you want this rule to apply to all applications with an arbitrary destination port number.
Single, Range	Select any of these and enter details as described in the Source Port section above.

Field	Description
Service	<p>This option allows you to select any of the pre-configured services from the drop-down list instead of the destination port. The following are examples of services:</p> <p>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.</p> <p>Note: Service is a combination of protocol and port number. They appear here after you add them in the "Firewall Service" configuration page.</p>
Protocol	
<p>This option allows you to select protocol type from a drop-down list. Available settings are All, TCP, UDP, ICMP, AH and ESP. If you select "service" for the destination port, this option will not be available.</p>	
NAT	
<p>This option allows you to select the type of NAT for the outbound traffic.</p>	
None	Select this option if you do not intend to use NAT in this outbound ACL rule.
IP Address	Select this option to specify the IP address that you want the outbound traffic to use. This option is called NAPT or overload.
NAT Pool	Select this option to associate a pre-configured NAT pool to the rule. Only static, dynamic and overload NAT pool can be used to associate with an outbound ACL rule.
Interface	Select this option to use the WAN interface IP address for the outbound traffic. WAN IP must be configured prior to selecting this option.
Time Ranges	
<p>Select a pre-configured time range during which the rule is active. Select "Always" to make the rule active at all times.</p>	
Log	
<p>Click on the "Enable" or "Disable" radio button to enable or disable logging for this ACL rule.</p>	
VPN	
<p>Click on the "Enable" radio button if you want the traffic to go through VPN. Otherwise, click on the "Disable" radio button.</p>	

9.4.2 Access Outbound ACL Rule Configuration Page – (Firewall -> Outbound ACL)

Log into Configuration Manager as administrator. Click **Firewall -> Outbound ACL**. The Firewall Outbound ACL Configuration page displays as shown in Figure 9.9.

When you open the Outbound ACL Configuration page, a list of existing ACL rules is also displayed at the bottom half of the configuration page such as those shown in Figure 9.9.

9.4.3 Add Outbound ACL Rules

To add an outbound ACL rule

1. Open the Outbound ACL Rule Configuration Page. See section **9.4.2 Access Outbound ACL Rule Configuration Page**.
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, NAT, time ranges, application filtering, 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. 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 bottom half of the Outbound ACL Configuration page.


Figure 9.10 shows 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.



Figure 9.10. Outbound ACL Configuration Example

9.4.4 Modify Outbound ACL Rules


To modify an outbound ACL rule

1. Open the Outbound ACL Rule Configuration Page. See section **9.4.2 Access Outbound ACL Rule Configuration Page**.
2. Click on the  icon of the rule to be modified in the outbound ACL table or select the rule number from the "ID" drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, source/destination port, protocol, NAT, time ranges, application filtering, log, and VPN. See Table 9.2 for explanation of these fields.
4. Click on the **<Modify>** button to modify this ACL rule. The new settings for this ACL rule will then be displayed in the outbound access control list table at the bottom half of the Outbound ACL Configuration page.

9.4.5 Delete Outbound ACL Rules

To delete an outbound ACL rule

1. Open the Outbound ACL Rule Configuration Page. See section **9.4.2 Access Outbound ACL Rule Configuration Page**.

2. Click on the  icon of the rule to be deleted in the outbound ACL table or select the rule number from the “ID” drop-down list.
3. Click on <Delete> to delete this ACL rule. The ACL rule deleted will be removed from the ACL rule table located at the bottom half of the same configuration page.

9.4.6 Display Outbound ACL Rules

To see existing outbound ACL rules, open the Outbound ACL Rule Configuration page as described in section 9.4.2 Access Outbound ACL Rule Configuration Page.

9.5 Configuring URL Filters

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

9.5.1 URL Filter Configuration Parameters

Table 9.3 describes the configuration parameters available for an URL filter rule.

Table 9.3. URL Filter Configuration Parameters

Field	Description
URL Filter State	Click on “Enable” or “Disable” radio button to enable or disable URL filtering.
Proxy Server Port	Enter the proxy server (web server) port number configured for your web browser. The proxy server port change requires you to disable and enable the firewall to take effect.
ID	
Add New	Click on this option to add a new URL filter rule.
Rule Number	Select a rule from the drop-down list to modify its attributes.
Keyword	Define a keyword that should not appear in the URL.

9.5.2 Access URL Filter Configuration Page – (Firewall -> URL Filter)

Log into Configuration Manager as administrator. Click **Firewall -> URL Filter**.

The Firewall URL Filter Configuration page displays as shown in Figure 9.11.

When you open the URL Filter Configuration page, a list of existing URL filter rules is also displayed at the bottom half of the configuration page such as those shown in Figure 9.11.

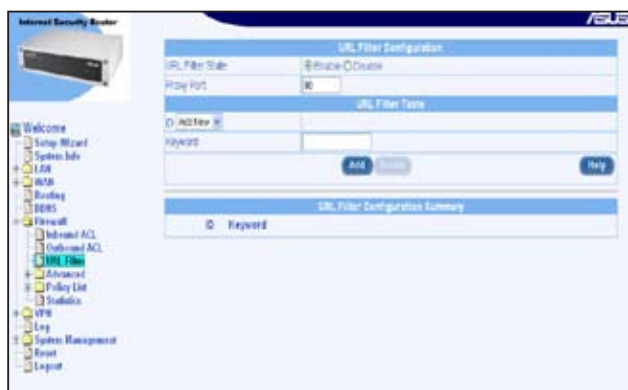


Figure 9.11. URL Filter Configuration Page

9.5.3 Add URL Filter Rules

To add an URL Filter


1. Open the URL Configuration page. See section **9.5.2 Access URL Filter Configuration Page**.
2. Select **Add New** from the **ID** drop-down list.
3. Enter a keyword to the Keyword field.
4. Click on **<Add>** to create the URL Filter rule. The new rule will then be displayed in the URL Filter Configuration Summary table.

9.5.4 Modify URL Filter Rules

To modify an URL Filter rule, you must first delete the existing URL filter rule (see Section 9.5.5) and then add a new one (see Section 9.5.3 Add an URL Filter Rule).

9.5.5 Delete URL Filter Rules

To delete an URL Filter rule

1. Open the URL Configuration page. See section **9.5.2 Access URL Filter Configuration Page**.
2. Click on the  icon of the rule to be deleted in the URL Filter Configuration Summary table or select the rule number from the “ID” drop-down list.
3. Click on **<Delete>** to delete this rule.

9.5.6 View Configured URL Filter Rules

To see existing URL filter rules, just open the URL Filter Configuration page as described in section 9.5.2 Access URL Filter Configuration Page.

9.5.7 URL Filter Rule Example

Figure 9.12 shows an URL filter rule example. It demonstrates:

- How to add the keyword “abcnews”. Any URL containing this keyword will be blocked.
- Set the proxy web server port number to 80 (you may use a different port number for your proxy server). This means that this URL filter rule will be applied over the proxy server port 80 in case a proxy web server is used. If you don’t use a proxy server for your browser, this setting will be ignored. You must disable and then enable the firewall for this change to take effect. Refer to 11.1 Configure System Services on details of enabling and disabling firewall services.

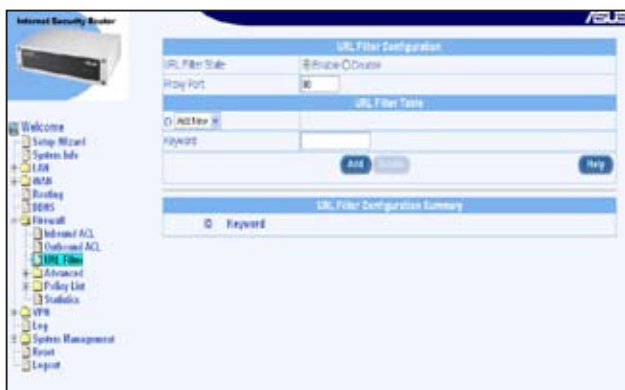


Figure 9.12. URL Filter Rule Example

9.6 Configuring Advanced Firewall Features – (Firewall -> Advanced)

This option sequence brings up the screen with the following sub-options for setting advanced firewall features:

- **Self Access:** This option allows you to configure rules for controlling packets targeting the Internet Security Router itself.
- **Services:** Use this option to configure services (applications using specified port numbers). Each service record contains the name of service record, the IP protocol value and its corresponding port number.
- **Denial of Service (DoS):** Use this option to configure DoS parameters. This option lists the default set of DoS attacks against which the router firewall provides protection.

The next sections describe usage of these options.

9.6.1 Configuring Self Access Rules

Self Access rules control access to the router itself. You may use Self Access Rule Configuration page to:

- Add a Self Access rule, and set basic parameters for it
- Modify an existing Self Access rule
- Delete an existing Self Access rule
- View existing Self Access rules



Figure 9.13. Self Access Rule Configuration Page

Table 9.4. Self Access Configuration Parameters

Field	Description
Protocol	Select protocol from drop down list - TCP/ UDP/ICMP
Port	Enter the Port Number.
Direction	
Select the direction from which the traffic will be allowed.	
From LAN	Select Enable or Disable to allow or deny traffic from the LAN (internal network) to the router.
From WAN	Select Enable or Disable to allow or deny traffic from WAN (external network) to the router.

9.6.1.2 Access Self Access Rule Configuration Page – (Firewall -> Advanced -> Self Access)

Log into Configuration Manager as administrator. Click **Firewall -> Advanced -> Self Access**. The Firewall Self Access Rule Configuration page displays as shown in Figure 9.13.

When you open the Self Access Configuration page, a list of existing Self Access rules is also displayed at the bottom half of the configuration page such as those shown in Figure 9.13.

9.6.1.3 Add a Self Access Rule

To add a Self Access rule

1. Open the Self Access Rule Configuration page. See section **9.6.1.2 Access Self Access Rule Configuration Page**.
2. Select **Add New** from the **Self Access** rule drop-down list.
3. Select a protocol from the **Protocol** drop-down list. If you select TCP or UDP protocol, you will need to enter port number as well.
4. Click on **<Add>** to create the new Self Access rule. The new rule will then be displayed in the Self Access Rule list table at the bottom half of the Self Access Rule Configuration page.

Example

Figure 9.13 displays the screen with entries to:


Add a new Self Access rule to:

- Allow TCP port 80 traffic (i.e. HTTP traffic) from the LAN and deny the HTTP traffic from the WAN port (i.e. from the external network) to the Internet Security Router.

9.6.1.4 Modify a Self Access Rule


To modify a Self Access rule

1. Open the Self Access Rule Configuration page. See section **9.6.1.2 Access Self Access Rule Configuration Page**.

2. Click on the  icon of the Self Access rule to be modified in the Self Access rule table or select the Self Access rule from the Self Access rule drop-down list.
3. You may then disable or enable the traffic from LAN or WAN or both. The port number cannot be changed if TCP or UCP protocol is selected. To modify the port number, you must first delete the existing Self Access rule and add a new rule instead.
4. Click on **<Modify>** to save the changes. The new settings for this Self Access rule will then be displayed in the Self Access rule table located at the bottom half of the Self Access Rule Configuration page.

9.6.1.5 Delete a Self Access Rule

To delete a Self Access rule

1. Open the Self Access Rule Configuration page. See section 9.6.1.2 Access Self Access Rule Configuration Page.
2. Click on the  icon of the Self Access rule to be deleted in the Self Access rule table or select the Self Access rule from the Self Access rule drop-down list.
3. Click on **<Delete>** to delete the rule. The rule deleted will be removed from the Self Access rule table located at the bottom half of the same configuration page.

9.6.1.6 View Configured Self Access Rules

To see existing Self Access Rules, just open the Self Access Rule Configuration page as described in section 9.6.1.2 Access Self Access Rule Configuration Page

9.6.2 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 9.14 shows the Firewall Service List Configuration page. The configured services are listed at the bottom half of the same page.

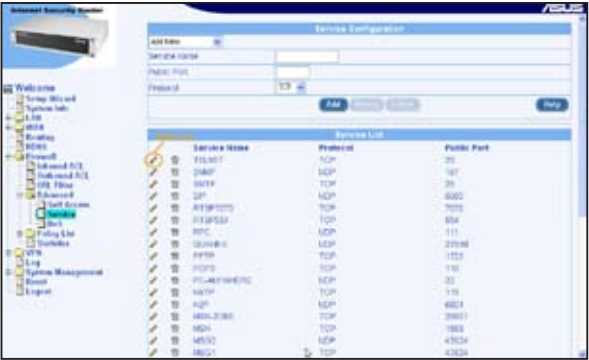


Figure 9.14. Service List Configuration Page

9.6.2.1 Service List Configuration Parameters

Table 9.5 describes the available configuration parameters for firewall service list.

Table 9.5. Service List Configuration Parameters

Field	Description
Service Name	Enter the name of the Service to be added. 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.

9.6.2.2 Access Service List Configuration Page – (Firewall -> Advanced -> Service)

Log into Configuration Manager as administrator. Click **Firewall -> Advanced -> Service**. The Service List Configuration page displays, as shown in Figure 9.14.

When you open the Service List Configuration page, a list of existing configured services is also displayed at the bottom half of the configuration page such as those shown in Figure 9.14.

9.6.2.3 Add a Service

To add a service, follow

1. Open the Service List Configuration Page. See section **9.6.2.2 Access Service List Configuration Page**.
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. Only alphanumeric characters are allowed in a name.
4. Make changes to any or all of the following fields: public port and protocol. See Table 9.5 for explanation of these fields.
5. Click on **<Add>** to create the new service. The new service will then be displayed in the service list table at the bottom half of the Service Configuration page.


9.6.2.4 Modify a Service

To modify a service

1. Open the Service List Configuration Page. See section **9.6.2.2 Access Service List Configuration Page**.
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. See Table 9.5 for explanation of these fields.
4. Click on **<Modify>** to modify this service. The new settings for this service will then be displayed in the service list table at the bottom half of the Service Configuration page.

9.6.2.5 Delete a Service

To delete a service

1. Open the Service List Configuration Page. See section **9.6.2.2 Access Service List Configuration Page**.
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. Click on **<Delete>** to delete this service. The service deleted will be removed from the service list table located at the bottom half of the same configuration page.

9.6.2.6 View Configured Services

To see a list of existing services

1. Open the Service List Configuration Page. See section **9.6.2.2 Access Service List Configuration Page**.
2. The service list table located at the bottom half of the Service Configuration page shows all the configured services.

9.6.3 Configuring DoS Settings

The router has a proprietary Attack Defense Engine that protects internal networks from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. It can drop ICMP redirects and IP loose/strict source routing packets. For example, a security device with the router's firewall provides protection from "WinNuke", a widely used program that remotely crash unprotected Windows systems in the Internet. The router's firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, Reassembly and SYN flooding. For a complete list of DoS protection provided by the Internet Security Router, see Table 2.3.

9.6.3.1 DoS Protection Configuration Parameters

Table 9.6 describes the configuration parameters available for DoS Protection.

Table 9.6. DoS Protection Configuration Parameters

Field	Description
SYN Flooding	Check or un-check this option to enable or disable protection against SYN Flood attacks. 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. By default, SYN Flood protection is enabled.
Winnuke	Check or un-check this option to enable or disable protection against Winnuke attacks. Some older versions of the Microsoft Windows OS are vulnerable to this attack. If the computers in the LAN are not updated with recent versions/patches, you are advised to enable this protection by checking this check box.
MIME Flood	Check or un-check this option to enable or disable protection against MIME attacks. You can select this box to protect the mail server in your network against MIME flooding.
FTP Bounce	Check or un-check this option to enable or disable protection against FTP bounce attack. In its simplest terms, the attack is based on the misuse of the PORT command in the FTP protocol. An attacker can establish a connection between the FTP server machine and an arbitrary port on another system. This connection may be used to bypass access controls that would otherwise apply.
IP Unaligned Time Stamp	Check or un-check this option to enable or disable protection against unaligned IP time stamp attack. Certain operating systems will crash if they receive a frame with the IP timestamp option that isn't aligned on a 32-bit boundary.
Sequence Number Prediction Check	Check or un-check this option to enable or disable protection against TCP sequence number prediction attacks. For TCP packets, sequence number is used to guard against accidental receipt of unintended data and malicious use by the attackers if the ISN (Initial Sequence Number) is generated randomly. Forged packets w/ valid sequence numbers can be used to gain trust from the receiving host. Attackers can then gain access to the compromised system. This attack affects only the TCP packets originated or terminated at the router.

Field	Description
Sequence Number Out of Range Check	Check or un-check this option to enable or disable protection against TCP out of range sequence number attacks. An attacker can send a TCP packet to cause an intrusion detection system (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent in that connection may then be ignored by the IDS. This may indicate an unsuccessful attempt to hijack a TCP session.
ICMP Verbose	Check or un-check this option to enable or disable protection against ICMP error message attacks. ICMP messages can be used to flood your network with undesired traffic. By default, this option is enabled.
Maximum IP Fragment Count	Enter the maximum number of fragments the Firewall should allow for every IP packet. This option is required if your connection to the ISP is through PPPoE. This data is used during transmission or reception of IP fragments. When large sized packets are sent via the router, the packets are chopped into fragments as large as MTU (Maximum Transmission Unit). By default, this number is set to 45. If 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 there can be more number of fragments and this number should be increased.
Minimum IP Fragment Size	Enter the Minimum size of IP fragments to be allowed through Firewall. This limit will not be enforced on the last fragment of the packet. If the Internet traffic is such that it generates many small sized fragments, this value can be decreased. This can be found if there are lots of packet loss, degradation in speed and if the following log message is generated very often: "fragment of size less than configured minimum fragment size detected".

9.6.3.2 Access DoS Configuration Page – (Firewall -> Advanced -> DoS)

Log into Configuration Manager as administrator. Click **Firewall -> Advanced -> DoS**. The DoS Configuration page displays as shown in Figure 9.15.

When you open the DoS Configuration page, a list of default DoS protection is also displayed at the bottom half of the configuration page such as those shown in Figure 9.15. These protections are enabled by default when firewall is enabled.

9.6.3.3 Configuring DoS Settings

By default, most DoS protection against all supported attack types are enabled. Figure 9.15 shows the default configuration for DoS settings. You may check or un-check individual type of attack defense to disable or enable protection against that specific type of attack.

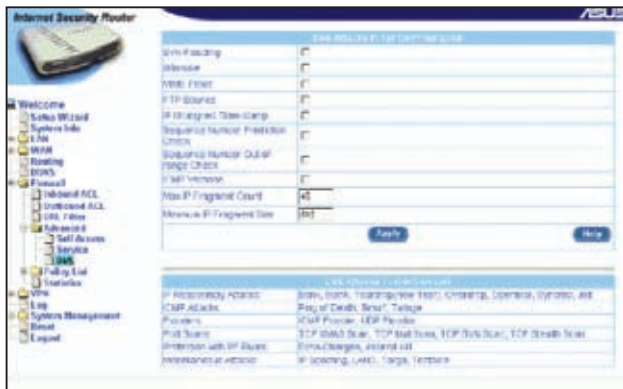


Figure 9.15. DoS Configuration Page

9.7 Firewall Policy List – (Firewall -> Policy List)

Firewall policy list provides a convenient way to manage firewall ACL rules (inbound/outbound ACL rules, and group ACL rules).

- **IP Pools:** This option allows you to configure logical names for IP Pools and set appropriate IP addresses. Each record contains the name of the IP record and the types of IP address (single IP address or a range of IP address or a subnet address).
- **NAT Pools:** This option allows you to configure NAT Pools that will ensure mapping of the internal IP address to public IP address. Configure NAT Pools here before attaching them to policies.
- **Time Ranges:** This option allows you to configure time-windows for user-access to the networks across the rRouter.

9.7.1 Configuring IP Pool

9.7.1.1 IP Pool Configuration Parameters

Table 9.7 describes the configuration parameters available for an IP pool.

Table 9.7. IP Pool Configuration Parameters

Field	Description
IP Pool Name	Enter the name of the local IP
IP Pool Type	Select the type of IP Pool.
IP Range	This option allows you to configure the range of IP addresses.
Start IP	Enter the starting IP address of the range.
End IP	Enter the ending IP address of the range.
Subnet	This option allows you to include all the computers that are connected in an IP subnet.
Subnet Address	Enter the appropriate IP address.
Subnet Mask	Enter the corresponding mask.
IP Address	This option allows you to configure single IP address.
IP Address	Enter the IP Address.

9.7.1.2 Access IP Pool Configuration Page – (Firewall -> Policy List -> IP Pool)

Log into Configuration Manager as administrator. Click Firewall menu, click the Policy List submenu and then click the IP Pool submenu. The IP Pool Configuration page displays, as shown in Figure 9.16.

When you open the IP Pool Configuration page, a list of existing IP pools is also displayed at the bottom half of the configuration page such as those shown in Figure 9.16.



Figure 9.16 IP Pool Configuration Page


9.7.1.3 Add an IP Pool

To add an IP Pool


1. Open the IP Pool Configuration page. See section **9.7.1.2 Access IP Pool Configuration Page**.
2. Select **Add New Pool** from the **IP Pool** drop-down list.
3. Enter a pool name into the Name field.
4. Select a pool type from the **IP Pool Type** drop-down list.
5. If “IP Range” pool type is selected, enter start IP address and end IP address. If “Subnet” pool type is selected, enter subnet address and subnet mask. If **IP Address** pool type is selected, enter an IP address.
6. Click on **<Add>** to create the new IP Pool. The new IP Pool will then be displayed in the IP Pool list table.


9.7.1.4 Modify an IP Pool

To modify an IP Pool

1. Open the IP Pool Configuration page. See section **9.7.1.2 Access IP Pool Configuration Page**.
2. Click on the  icon of the IP pool to be modified in the IP Pool List table or select the IP pool from the IP Pool drop-down list.
3. Make desired changes to any or all of the following fields: Pool name, Pool type and IP address.
4. Click on **<Modify>** to save the new settings. The new settings for this pool will then be displayed in the IP Pool list table.

9.7.1.5 Delete an IP Pool

To delete an IP Pool, click on the  icon of the IP pool to be deleted or follow the instruction below:

1. Open the IP Pool Configuration page. See section **9.7.1.2 Access IP Pool Configuration Page**.
2. Click on the  icon of the IP pool to be deleted in the IP Pool List table or select the IP pool from the IP Pool drop-down list.
3. Click on **<Delete>** to delete this IP pool.

9.7.1.6 IP Pool Example

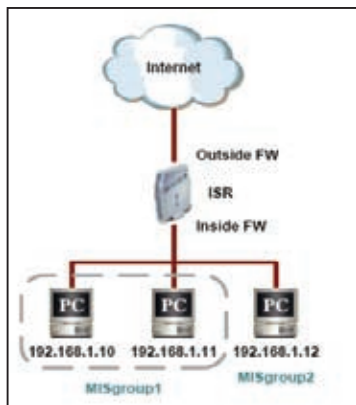


Figure 9.17. Network Diagram for IP Pool Configuration

1. Open the IP Pool Configuration page to create two IP groups – see Figure 9.18.



Figure 9.18. IP Pool Example – Add Two IP Pools – MISgroup1 and MISgroup2

2. Associate an IP pool to firewall ACL rules – inbound, outbound or group ACL by selecting **IP Pool** from the **Source IP Type** drop-down list and then choose an IP pool from the IP pool dropdown list. In this example, IP pool is used to associate to source IP. However, it can be used to associate to destination IP as well. As shown in Figure 9.19, MISgroup1 is not allow to play the network game, Quake-II, at all times.

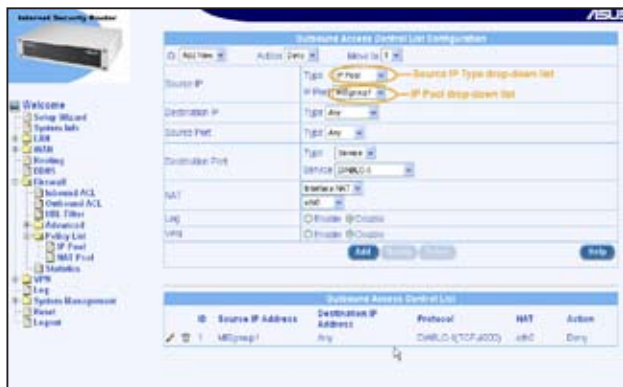


Figure 9.19. IP Pool Example – Deny QUAKE-II Connection for MISgroup1

9.7.2 Configuring NAT Pool

9.7.2.1 NAT Pool Configuration Parameters

Table 9.8 describes the configuration parameters available for a NAT pool.

Table 9.8. NAT Pool Configuration Parameters

Field	Description
NAT Pool Name	Enter a name for the NAT Pool.
NAT Pool Type	Select the type of NAT Pool and make appropriate IP Address entries.
Static	
Select this type of NAT to set a one-to-one Mapping between the Internal Address and the External Address.	
LAN IP range	For the Internal Address
Start IP	Enter the starting IP address.
End IP	Enter the ending IP address.
Internet IP Range	For the External Address
Start IP	Enter the starting IP address.
End IP	Enter the ending IP address.
Dynamic	
Select this type of NAT to map a set of internal (corporate) machines to a set of public IP addresses. Make entries for the LAN IP Range and the Internet IP Range as described above.	
Overload	
Select this type of NAT to use a single public IP address to connect multiple internal (corporate LAN) machines to external (Internet) network.	
NAT IP Address	Enter NAT IP address, for the overload.
Interface	
Select this type of NAT to specify the Dynamic Interface whose IP address should be used for subjecting traffic to NAT.	

9.7.2.2 Access NAT Pool Configuration Page – (Firewall -> Policy List -> NAT Pool)

Log into Configuration Manager as administrator. Click Firewall -> Policy List -> NAT Pool. The NAT Pool Configuration page displays as shown in Figure 9.20.

When you open the NAT Pool Configuration page, a list of existing NAT pools is also displayed at the bottom half of the configuration page such as those shown in Figure 9.20.

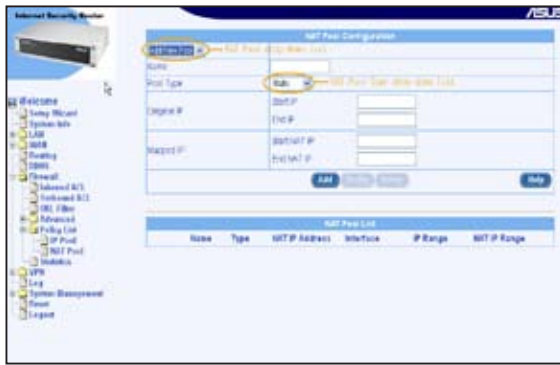


Figure 9.20. NAT Pool Configuration Page


9.7.2.3 Add a NAT Pool

To add a NAT Pool

1. Open the NAT Pool Configuration page. See section **9.7.2.2 Access NAT Pool Configuration Page**.
2. Select **Add New Pool** from the **NAT Pool** drop-down list.
3. Enter a pool name into the Name field.
4. Select a pool type from the Type drop-down list.
5. If **Static** or **Dynamic** pool type is selected, enter the original IP addresses (start IP Address, and end IP Address), and mapped IP addresses (start NAT IP Address and end NAT IP Address). If **Overload** pool type is selected, enter the NAT IP address. If you want to use the IP address assigned for the WAN port as the NAT IP address, select the Interface pool type.
6. Click on **<Add>** to create the new NAT pool. The new NAT pool will then be displayed in the NAT Pool List table.


9.7.2.4 Modify a NAT Pool

To modify a NAT Pool

1. Open the NAT Pool Configuration page. See section **9.7.2.2 Access NAT Pool Configuration Page**.
2. Click on the  icon of the NAT pool to be modified in the NAT Pool List table or select the NAT pool from the NAT Pool drop-down list.
3. Make desired changes to any or all of the following fields: Pool name, Pool type and IP address.
4. Click on **<Modify>** to save the new settings. The new settings for this pool will then be displayed in the NAT Pool List table.

9.7.2.5 Delete a NAT Pool

To delete a NAT Pool, click on the  icon of the NAT pool to be deleted or follow the instruction below:

1. Open the NAT Pool Configuration page. See section **9.7.2.2 Access NAT Pool Configuration Page**.
2. Click on the  icon of the NAT pool to be deleted in the NAT Pool List table or select the NAT pool from the NAT Pool drop-down list.
3. Click on **<Delete>** to delete this NAT pool.

9.7.2.6 NAT Pool Example

Figure 9.21 shows the network diagram for this NAT pool example.

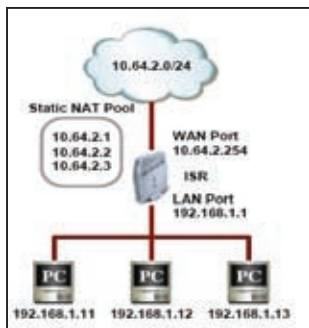


Figure 9.21. Network Diagram for NAT Pool Example

1. Create a NAT pool for static NAT – see Figure 9.22.



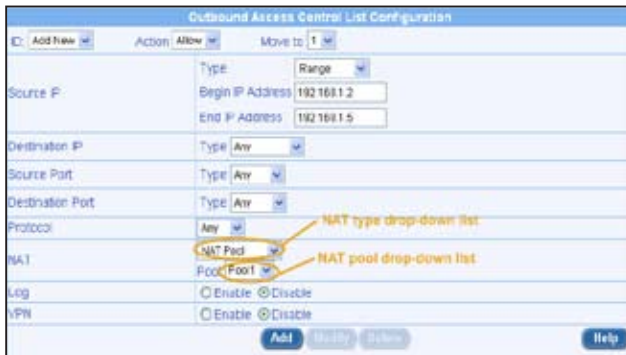
The NAT Pool Configuration window is shown. It has a title bar 'NAT Pool Configuration'. Below the title bar is a button 'Add New Pool'. The form contains the following fields:

Field	Value
Name	Pool1
Pool Type	Static
Original IP	Start IP: 192.168.1.2, End IP: 192.168.1.5
Mapped IP	Start NAT IP: 10.64.2.205, End NAT IP: 10.64.2.205

At the bottom right are buttons 'Add', 'Modify', 'Delete', and 'Help'.

Figure 9.22. NAT Pool Example – Create a Static NAT Pool

2. Associate the NAT pool to an outbound ACL rule by selecting **NAT Pool** from the NAT type drop-down list and then choose an existing NAT pool from the NAT pool drop-down list.



The Outbound Access Control List Configuration window is shown. It has a title bar 'Outbound Access Control List Configuration'. Below the title bar are buttons 'Add New', 'Action', 'Allow', and 'Move to: 1'. The form contains the following fields:

Field	Value
Type	Range
Source IP	Begin IP Address: 192.168.1.2, End IP Address: 192.168.1.5
Destination IP	Type: Any
Source Port	Type: Any
Destination Port	Type: Any
Protocol	Any
NAT	NAT type: NAT Pool, Pool: Pool1
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

At the bottom right are buttons 'Add', 'Modify', 'Delete', and 'Help'. Two orange arrows point to the 'NAT type' and 'Pool' drop-down lists, with labels 'NAT type drop-down list' and 'NAT pool drop-down list' respectively.

Figure 9.23. NAT Pool Example – Associate a NAT Pool to an ACL Rule

9.7.3 Configuring Time Range

With this option you can configure access time range records for eventual association with ACL rules. ACL rules associated with a time range record will be active only during the scheduled period. If the ACL rule denies HTTP access during 10:00hrs to 18:00hrs, then before 10:00hrs and after 18:00hrs the HTTP traffic will be permitted to pass through. One time range record can contain up to three time periods. For example:

Office hours on weekdays (Mon-Fri) can have the following periods:

- Pre-lunch period between 9:00 and 13:00 Hrs
- Post-lunch period between 14:00 and 18:30 Hrs

Office hours on weekends (Saturday-Sunday) can have the following periods:

- 9:00 to 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.

9.7.3.1 Time Range Configuration Parameters

Table 9.9 describes the configuration parameters available for a time range.

Table 9.9. Time Range Configuration Parameters

Field	Description
Time Range dropdown list	Select "Add New Time Range" to add a new time range or select an existing time range from the drop-down list.
Time Range Name	Enter a name for the Time Range.
Schedule drop-down list	Select "Add New Schedule" to add a new schedule or select an existing schedule from the drop-down list.
Days of Week	Set the days for the schedule.
Time (hh:mm)	Set the time windows for the schedule in hh:mm format.

9.7.3.2 Access Time Range Configuration Page – (Firewall -> Policy List -> Time Range)

Log into Configuration Manager as administrator. Click **Firewall -> Policy List -> Time Range**. The Time Range Configuration page displays as shown in Figure 9.24.

When you open the Time Range Configuration page, a list of existing time ranges is also displayed at the bottom half of the configuration page such as those shown in Figure 9.24.

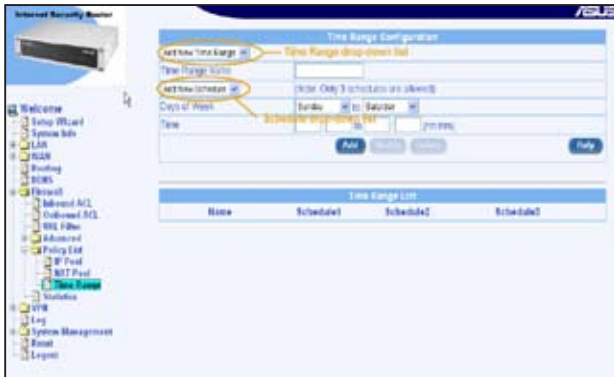


Figure 9.24. Time Range Configuration Page


9.7.3.3 Add a Time Range

To add a Time Range


1. Open the Time Range Configuration page. See section **9.7.3.2 Access Time Range Configuration Page**.
2. Select **Add New Time Range** from the **Time Range** drop-down list.
3. Enter a name into the Time Range Name field.
4. Select **Add New Schedule** from the Schedule drop-down list.
5. Select Days of Week. For example, from Sunday to Saturday.
6. Enter day hours, For example, from 08:00 to 18:00.
7. Click on **<Add>** to create the new schedule.

9.7.3.4 Modify a Time Range

To modify a Time Range


1. Open the Time Range Configuration page. See section **9.7.3.2 Access Time Range Configuration Page**.
2. Click on the  icon of the Time Range to be modified in the Time Range list table or select the Time Range from the Time Range drop-down list.
3. Select the **Schedule** from the schedule drop-down list.
4. Make desired changes to any or all of the following fields: Days of week and hours.
5. Click on **<Modify>** to save the new settings.

9.7.3.5 Delete a Time Range

To delete a Time Range, click on the  icon of the Time Range to be deleted.

9.7.3.6 Delete a Schedule in a Time Range

To delete a schedule in a Time Range

1. Open the Time Range Configuration page. See section **9.7.3.2 Access Time Range Configuration Page**.
2. Click on the  icon of the Time Range to be deleted in the Time Range list table or select the Time Range from the Time Range drop-down list.
3. Select the **Schedule** from the drop-down list.
4. Click on **<Delete>** to delete this schedule.

9.7.3.7 Time Range Example

1. Create a time range – see Figure 9.22.



The screenshot shows the 'Time Range Configuration' window. It has a title bar with the text 'Time Range Configuration'. Below the title bar, there is a dropdown menu labeled 'Add New Time Range'. The 'Time Range Name' field contains the text 'Office Hours'. Below this, there is another dropdown menu labeled 'Add New Schedule'. The 'Days of Week' field shows 'Sunday' and 'Friday' with arrows indicating a range. The 'Time' field shows '08:00 to 17:00 (hh:mm)'. At the bottom right, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

Figure 9.25. Time Range Example – Create a Time Range

2. Associate the time range to an outbound ACL rule by selecting an existing time range from the Time Range drop-down list. Figure 9.26 shows that MISgroup1 is denied FTP access during office hours.



The screenshot shows the 'ASUS SL1200' Firewall Configuration window. The left sidebar shows a tree view with 'Firewall' selected. The main area shows the 'Time Range Configuration' window. The 'Time Range Name' field contains 'Office Hours'. The 'Days of Week' field shows 'Sunday' and 'Friday'. The 'Time' field shows '08:00 to 17:00 (hh:mm)'. Below the configuration fields, there is a table titled 'Time Range List' with columns 'Name', 'Schedule1', 'Schedule2', and 'Schedule3'. The table is currently empty.

Figure 9.26. Time Range Example – Deny FTP Access for MISgroup1 During Office Hours

Advanced Security Monitor

Active Connections

Source Interface	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	TCP	192.168.1.101 - 1985	192.168.1.1 - 33	0.0.0.0 - 0	56	0	320
LAN	TCP	192.168.1.66.26 - 1827	192.168.1.68.26 - 83	0.0.0.0 - 0	93	6803	8
LAN	TCP	192.168.1.66.26 - 1827	168.96.152.1 - 83	0.0.0.0 - 0	43	1684	8
LAN	TCP	192.168.1.66.26 - 1826	192.168.1.68.26 - 83	0.0.0.0 - 0	48	160	8
LAN	TCP	192.168.1.66.26 - 1826	168.96.152.1 - 83	0.0.0.0 - 0	47	140	8
LAN	TCP	192.168.1.10 - 1648	192.168.1.1 - 80	0.0.0.0 - 0	599	177	874
LAN	TCP	192.168.1.10 - 1648	192.168.1.1 - 80	0.0.0.0 - 0	39	0	340

Total Connections Count

TCP	UDP	ICMP	Others
1	5	0	0

Buttons: Refresh

ASUS SL1200

10 Configuring VPN

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

10.1 Default Parameters

The router 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 router are as follows:

Default Connections

Each connection represents a rule that can 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 the router

Name	Type	Port	Protocol	State	Purpose
allow-ike-io	passby	500	UDP	Enabled	To allow the IKE traffic to the Internet Security Router
allow-all	passby			Enabled	To allow the plain traffic



Do not delete or modify default VPN policies.

Proposals

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. 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.

Pre-configured IKE proposals

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. Table 10.2 lists the pre-configured IKE proposals.

Table 10.2. Pre-Configured IKE proposals in the router

Name	Encryption Algorithm	Authentication Algorithm	Diffie-Hellman Group	Key Management	Lifetime (secs)
ike-preshared-3des-sha1-dh2	3DES	SHA-1	2	Pre-shared Keys	3600
ike-preshared-3des-md5-dh2	3DES	MD5	2	Pre-shared Keys	3600
ike-pre-shareddes-sha1-dh2	DES	SHA-1	2	Pre-shared Keys	3600
ike-pre-shareddes-md5-dh2	DES	MD5	2	Pre-shared Keys	3600
ike-preshared-3des-sha1-dh1	3DES	SHA-1	1	Pre-shared Keys	3600
ike-preshared-3des-md5-dh1	3DES	MD5	1	Pre-shared Keys	3600
			1		
ike-pre-shareddes-sha1-dh1	DES	SHA-1	1	Pre-shared Keys	3600
ike-pre-shareddes-md5-dh1	DES	MD5	1	Pre-shared Keys	3600
ike-preshared-3des-sha1-dh5	3DES	SHA-1	5	Pre-shared Keys	3600

Name	Encryption Algorithm	Authentication Algorithm	Diffie-Hellman Group	Key Management	Lifetime (secs)
ike-preshared-3des-md5-dh5	3DES	MD5	5	Pre-shared Keys	3600
ike-pre-shareddes-sha1-dh5	DES	SHA-1	5	Pre-shared Keys	3600
ike-pre-shareddes-md5-dh5	DES	MD5	5	Pre-shared Keys	3600

Pre-configured IPSec proposals

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

Table 10.3 lists the default IPSec proposals available on the router.

Table 10.3. Pre-configured IPSec proposals in the Internet Security Router

Name	Encryption Algorithm	Authentication Algorithm	Encapsulation	Lifetime (Mbytes/sec)
ipsec-esp-3des-sha1	3DES	SHA-1	ESP	75/3600
ipsec-esp-3des-md5	3DES	MD5	ESP	75/3600
ipsec-esp-des-sha1	DES	SHA-1	ESP	75/3600
ipsec-esp-des-md5	DES	MD5	ESP	75/3600
ipsec-ah-sha1	-	SHA-1	AH	75/3600
ipsec-ah-md5	-	MD5	AH	75/3600
ipsec-esp-3des	3DES	-	ESP	75/3600
ipsec-esp-des	-	SHA-1	ESP	75/3600
ipsec-esp-sha1	-	SHA-1	ESP	75/3600
ipsec-esp-md5	-	MD5	ESP	75/3600

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 50characters. 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.

These 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 the VPN configuration page. This way you can control the proposals that become part of a connection.



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

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

- Basic Access List Configuration
 - Access List using IKE
- Advanced Access List Configuration
 - Access List using IKE

10.2 VPN Tunnel Configuration Parameters

Table 10.4 describes all the VPN tunnel configuration parameters available for various VPN configurations.

Table 10.4. VPN Tunnel Configuration Parameter

Field	Description
VPN Connection Settings	
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.
Name	Enter a unique name, preferably a meaningful name that signifies the tunnel connection. 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 router's 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.
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	Enter the appropriate IP address for the local secure group.
Subnet	This option allows you to include all the computers that are connected in an IP subnet. The following fields become available when this option is selected:
Subnet Address	Specify the appropriate network address.
Subnet Mask	Enter the subnet mask.

Field	Description
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 (only available for site to site VPN mode)	
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 Gateway	
You have a choice of entering either the IP address or the FQDN (fully qualified domain name) for the remote secure gateway.	
Any	Select this option to accept connection request from any computer.
IP Address	Select this option to specify an IP address for the remote secure gateway.
FQDN	Select this option to enter the fully qualified domain name for the remote secure gateway.
IKE Proposal Settings (only available for pre-shared key)	
Note that all options for the IKE proposal settings are available only when pre-shared key is selected.	
IKE Mode	Main mode and aggressive mode are supported. Click the proper radio button for the desired IKE mode.
Preshared Key	Enter the shared secret (this should match the secret key at the other end).

Field	Description
IKE Encryption / Authentication	<p>Select the IKE authentication and encryption from the drop-down list.</p> <p>All 3DES & SHA1-DH2 3DES & MD5-DH2 DES & SHA1-DH2 DES & MD5-DH2 3DES & SHA1-DH1 DES & MD5-DH1 DES & SHA1-DH1 DES & MD5-DH1 3DES & SHA1-DH5 DES & SHA1-DH5 DES & MD5-DH5</p> <p>Note: It is recommended that you choose All to have all the IKE proposals associated with the current tunnel and allow IKE to automatically select one (among the set of IKE proposals) to communicate with its peer. However, if a specific proposal is required, then it can be chosen from the list.</p>
Life Time	Enter the IKE security association life time in seconds, minutes, hours or days.

Field	Description
IPSec Proposal Settings	
IPSec Encryption / Authentication	<p>Select one of the following pre-configured IKE proposals from the dropdown 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.</p> <p>All</p> <p>Strong Encryption & Authentication (ESP 3DES HMAC SHA1)</p> <p>Strong Encryption & Authentication (ESP 3DES HMAC MD5)</p> <p>Encryption & Authentication (ESP DES HMAC SHA1)</p> <p>Encryption & Authentication (ESP DES HMAC MD5)</p> <p>Authentication (AH SHA1)</p> <p>Authentication (AH MD5)</p> <p>Strong Encryption (ESP 3DES)</p> <p>Encryption (ESP DES)</p> <p>Authentication (ESP SHA1)</p> <p>Authentication (ESP MD5)</p>
PFS Group	<p>PFS stands for perfect forward secrecy. You may choose to use the same keys (generated when the IKE tunnel is created) for all re-negotiations or you can choose to generate new keys for every re-negotiation. Select None to use the same keys for all the re-negotiations. Select a specific DH (Diffie-Hellman) group to generate new keys for every re-negotiation. The supported DH groups are DH-1, DH-2 and DH-5. The greater the group number, the more secure the connection is. However, the greater the group number, the more time it takes to negotiate a tunnel.</p> <p>Note: With PFS selected, keys are changed during the course of a connection and the tunnel is more secure. However, enabling this option slows down the tunnel negotiation.</p>
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.

10.3 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.
- pre-shared secret for remote gateway authentication.
- appropriate priority for the connection.

This option sequence brings up the screen as illustrated in Figure 4.2. Fields and buttons represent the basic VPN parameters. 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

10.3.1 Add a Rule for VPN Connection Using Pre-shared Key

VPN Tunnel Configuration Page, as shown in the Figure 10.1, is used to configure a rule for VPN connection using pre-shared key

To add a rule for a VPN connection

1. Log into Configuration Manager as administrator. Click **VPN -> VPN Tunnel**. The VPN Tunnel Configuration page displays as shown in Figure 10.1.

When you open the VPN Tunnel Configuration page, a list of existing rules for VPN connections are also displayed at the bottom 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. Only alphanumeric characters are allowed in a name.
5. Click on **Enable** or **Disable** radio button to enable or disable this rule.



Figure 10.1. VPN Tunnel Configuration Page – Pre-shared Key Mode

6. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select Preshared Key), pre-shared 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 **<Add>** to create the new VPN rule. The new VPN rule will then be displayed in the VPN Connection Status table at the bottom half of the VPN Configuration page.


10.3.2 Modify VPN Rules

To modify a VPN rule

1. Log into Configuration Manager as administrator. Click **VPN -> VPN Tunnel**.
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), pre-shared 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 **<Modify>** to modify this VPN rule. The new settings for this VPN rule will then be displayed in the VPN Connection Status table at the bottom half of the VPN Configuration page.

10.3.3 Delete VPN Rules

To delete an outbound ACL rule

1. Log into Configuration Manager as administrator. Click **VPN -> VPN Tunnel**.
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 **<Delete>** to delete this VPN rule. The VPN rule deleted will be removed from the VPN Connection Status table located at the bottom half of the same configuration page.

10.3.4 View VPN Rules

To view existing VPN rules

1. Log into Configuration Manager as administrator. Click **VPN -> VPN Tunnel**.
2. The VPN rule table located at the bottom 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 10.5 gives description for the VPN statistics parameters.

Table 10.5. VPN Statistics

Entry	Descriptions
VPN Statistics	
Global IPSEC SA Statistics	Overall packet statistics
AH Packets	Number of AH packets
ESP Packets	Number of ESP packets
Triggers	Number of triggers
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

Entry	Descriptions
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 -1negotiations
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
IKE SA	
IPSec SA	

Figure 10.2 shows all the parameters available for VPN connections. To see an updated statistics, click on **<Refresh>**.

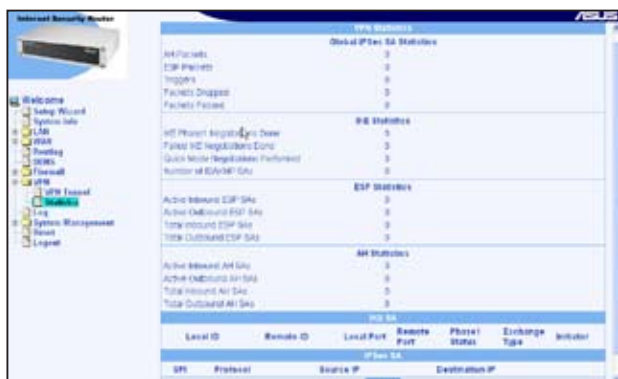


Figure 10.2. VPN Statistics Page

10.5 VPN Connection Examples

Gateways with integrated VPN and Firewall are useful in scenarios where:

- The traffic between branch offices is protected by VPN and
- Traffic destined for public Internet goes through Firewall/NAT.

To avoid NAT/IPSec interoperability issues, outgoing traffic is first processed by Firewall/NAT and then by IPSec. Hence, you must ensure that appropriate Firewall rules are configured to let the VPN traffic go through. This section describes these scenarios and presents step-by-step instructions for configuring these scenarios.

10.5.1 Intranet Scenario – firewall + VPN and no NAT for VPN traffic

This is a common scenario where traffic to the public Internet goes through the Firewall/NAT only and traffic between private networks is allowed without NAT before IPSec processing. The same authority administers the networks that are protected by VPN to avoid any possible address clash. Configure each of the router for the Intranet scenario using the following steps:

- Configure VPN connection rules.
- Configure Firewall access rules to allow inbound and outbound VPN traffic.
- Configure a Firewall self rule to allow IKE packets into the router

10.5.1.1 Configure Rules on Internet Security Router 1 (ISR1)

This section describes the steps to establish the VPN/Firewall for the Internet scenario. Figure 10.3 shows the typical Intranet connections. The ADSL or cable modem is not required if the two networks are connected via Ethernet connections. The setting of each configuration step is illustrated in a figure. For instructions on configuration of each step, refer to the next section for details.

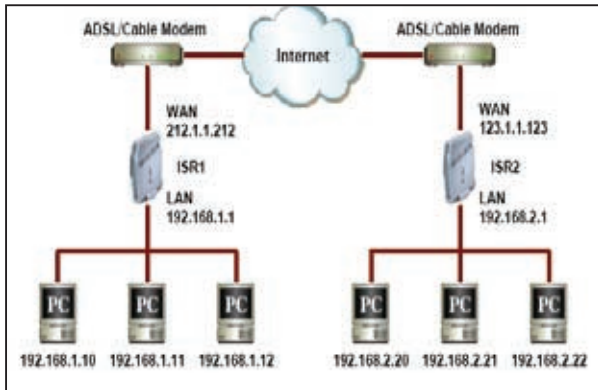


Figure 10.3. Typical Intranet Network Diagram

Figure 10.4. Intranet VPN Policy Configuration on ISR1

Step 1: Configure VPN connection rules

Refer to the section **10.3 Establish VPN Connection Using Automatic Keying** to configure VPN policies on ISR1 using automatic keying.

Step 2: Configure Firewall rules

1. Configure outbound Firewall rule to allow packets from 192.168.1.0/255.255.255.0 to 192.168.2.0/255.255.255.0 without any NAT
2. Configure inbound Firewall rule to allow packets from 192.168.2.0/255.255.255.0 to 192.168.1.0/255.255.255.0 without any NAT.

Table 10.6 and Table 10.7 provide the parameters to be configured for the outbound and inbound Firewall rule fields. For a general description on configuring any inbound/outbound Firewall rule, refer to sections 9.3 and 9.4.

Table 10.6. Outbound Un-translated Firewall Rule for VPN Packets on ISR1

Field		Value
Source IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable



The outbound Un-translated Firewall rule has to be added the existing rule ID 1001.

Table 10.7. Inbound Un-translated Firewall Rule for VPN Packets on ISR1

Field		Value
Source IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable

10.5.1.2 Configure Rules on Internet Security Router 2 (ISR2)

Step 1: Configure VPN connection rules

Refer to the section **10.3 Establish VPN Connection Using Automatic Keying** to configure VPN policies on ISR2 using automatic keying.

The screenshot displays the 'VPN Connection Settings' configuration window. It includes fields for 'Local Secure Group' (Type: Subnet, Address: 192.168.2.0, Mask: 255.255.255.0), 'Remote Secure Group' (Type: Subnet, Address: 192.168.1.0, Mask: 255.255.255.0), 'Local Gateway' (interface: eth0), and 'Remote Gateway' (Type: IP Address, IP Address: 192.168.1.1). Below these are sections for 'IKE Proposal Settings' (IKE Mode: Main, Preshared Key: *****, IKE Encryption/Authentication: AES, Life Time: 1000) and 'IPsec Proposal Settings' (IPsec Encryption/Authentication: AES, IPS Group: DH-7, Life Time: 1000).

Figure 10.5. Intranet VPN Policy Configuration on ISR2

Step 2: Configure Firewall rules

1. Configure outbound Firewall rule to allow packets from 192.168.2.0/255.255.255.0 to 192.168.1.0/255.255.255.0 without any NAT.
2. Configure inbound Firewall rule to allow packets from 192.168.1.0/255.255.255.0 to 192.168.2.0/255.255.255.0 without any NAT.

Table 10.8 and Table 10.9 provide the parameters to be configured for the outbound and inbound Firewall rule fields. For a general description on configuring any inbound/outbound Firewall rule, refer to sections 9.3 and 9.4.

Table 10.8. Outbound Un-translated Firewall Rule for VPN Packets on ISR1

Field		Value
Source IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable



The outbound Un-translated Firewall rule has to be added the existing rule ID 1001.

Table 10.9. Inbound Un-translated Firewall Rule for VPN Packets on ISR1

Field		Value
Source IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable

10.5.1.3 Establish Tunnel and Verify

- Ping continuously from a host in the LAN behind ISR1 to a host in the LAN behind ISR2. The first few pings might fail. After a few seconds, the host in the LAN behind ISR1 should start getting ping response.

10.5.2 Extranet Scenario – firewall + static NAT + VPN for VPN traffic

In case of the extranet scenario, the networks protected by the routers could be under different administrative authorities. Hence, there is a possibility that the IP addresses of both networks are in the same subnet. The typical extranet set up is shown in Figure 10.6.

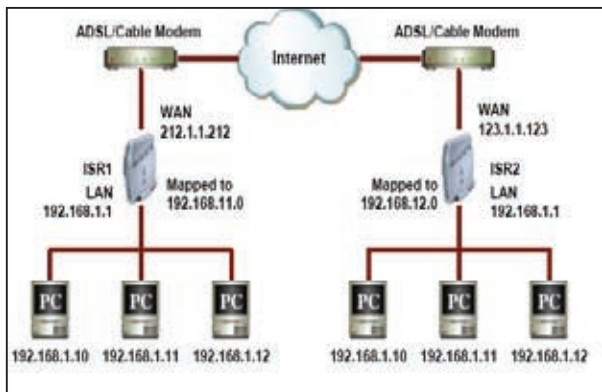


Figure 10.6. Typical Extranet Network Diagram



Both networks behind the ISR1 and ISR2 are 192.168.1.0/255.255.255.0.

To avoid routing problems in such scenario, network IP addresses must be mapped to different ones:

- Network 192.168.1.0/255.255.255.0 behind ISR1 is translated to 192.168.11.0/255.255.255.0 before VPN processing.
- Network 192.168.1.0/255.255.255.0 behind ISR2 is translated to 192.168.12.0/255.255.255.0 before VPN processing.

The results are:

- The LAN behind ISR1 would be viewed as 192.168.11. 0/24 by the LAN behind ISR2.
- The LAN behind ISR2 would be viewed as 192.168.12. 0/24 by the LAN behind ISR1.

The configuration of each of the routers for extranet scenario consists of the following steps:

- Configure VPN Connection rules.
- Configure Firewall rules to allow inbound and outbound VPN traffic by performing one-to-one NAT.
- Configure a Firewall Self Access rule to allow IKE packets into the Internet Security Router.

10.5.2.1 Setup the Routers

On ISR1

1. Configure LAN interface of ISR1 with IP address 192.168.1.1.
2. Configure DHCP pool with IP addresses from 192.168.1.10 to 192.168.1.110 on ISR1.
3. Configure WAN interface of ISR1 with IP address 212.1.1.212.
4. Add a route on ISR1 with gateway as 123.1.1.123.
5. Save the configuration.

On ISR2

1. Configure LAN interface of ISR2 with IP address 192.168.1.1.
2. Configure DHCP pool with IP addresses from 192.168.1.10 to 192.168.1.110 on ISR2.
3. Configure WAN interface of ISR2 for IP address 123.1.1.123.
4. Add a default route on ISR2 with gateway as 212.1.1.212.
5. Save the configuration.

10.5.2.2 Configure VPN Rules on ISR1

Step 1: Configure VPN Rule

Refer to the section **10.3 Establish VPN Connection Using Automatic Keying** to configure VPN policies on ISR1 using automatic keying with the following addresses:

1. Use 192.168.11.0/255.255.255.0 for the Local Secure Group
2. Use 192.168.12.0/255.255.255.0 for the Remote Secure Group

The screenshot shows the Cisco ASA configuration interface for the 'Local Secure Group'. The configuration is as follows:

- Local Secure Group:**
 - Type: **Subnet**
 - Address: **192.168.1.0**
 - Mask: **255.255.255.0**
- Remote Secure Group:**
 - Type: **Subnet**
 - Address: **192.168.1.0**
 - Mask: **255.255.255.0**
- Local Gateway:**
 - Interface: **eth0**
 - Type: **IP Address**
- Remote Gateway:**
 - IP Address: **192.168.1.254**

Below the group configurations, the **IKE Proposal Settings** are shown:

- IKE Mode:** **Aggressive**
- Pre-shared Key:** *********
- IKE Encryption/Authentication:** **AE**
- Life Time:** **1440**

Below the IKE settings, the **IPsec Proposal Settings** are shown:

- IPsec Encryption/Authentication:** **Strong Encryption & Authentication (ESP 3DES HMAC SHA1)**
- IPsec Group:** **None**
- Life Time:** **3600**

The bottom of the page shows navigation buttons: **Back**, **Cancel**, **Apply**, and **Help**.

Figure 10.7. Extranet Example –VPN Policy Configuration on ISR1

Step 2: Configure Static NAT Pools

1. Configure outgoing static NAT pool (static-NAT) for translating addresses in range 192.168.1.1-192.168.1.254 to 192.168.11.1-192.168.11.254

NAT Pool Configuration			
Add New Pool			
Name	Outgoing_NAT		
Pool Type	Static		
Original IP	Start IP	192.168.1.1	
	End IP	192.168.1.254	
Mapped IP	Start NAT IP	192.168.11.1	
	End NAT IP	192.168.11.254	
		Add Modify Delete	
		Help	

Figure 10.8. Extranet Example – Outgoing NAT Pool Configuration on ISR1

2. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.11.1-192.168.11.254 to 192.168.1.1-192.168.1.254

NAT Pool Configuration	
Add New Pool	
Name	Incoming_NAT
Pool Type	Static
Original IP	Start IP: 192.168.11.1
	End IP: 192.168.11.254
Mapped IP	Start NAT IP: 192.168.1.1
	End NAT IP: 192.168.1.254
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	

Figure 10.9. Extranet Example – Incoming NAT Pool Configuration on ISR1

Step 3: Configure Extranet access rules

1. Configure outbound Firewall rules to map the source IP address of outbound packets from 192.168.1.x range to 192.168.11.x (defined by Outgoing_NAT pool) range before sending the packet to VPN.

Outbound Access Control List Configuration	
Add New	
Action	Allow
Move to	1
Source IP	Type: Subnet
	Address: 192.168.1.0
	Mask: 255.255.255.0
Destination IP	Type: Subnet
	Address: 192.168.12.0
	Mask: 255.255.255.0
Source Port	Type: Any
Destination Port	Type: Any
Protocol	Any
NAT	NAT Pool
Log	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	

Figure 10.10. Extranet Example – Outbound ACL Rule on ISR1

2. Configure inbound Firewall rules to map the destination IP address of inbound packets from 192.168.11.x range to 192.168.1.x (defined by Incoming_NAT pool) range after the packet is processed by VPN.

ID	Add New	Action	Move to
1		Deny	1

Source IP: Type: Subnet, Address: 192.168.12.0, Mask: 255.255.255.0

Destination IP: Type: Subnet, Address: 192.168.11.0, Mask: 255.255.255.0

Source Port: Type: Any

Destination Port: Type: Any

Protocol: All

Port Mapping: NAT Pool: [None], Protocol: [Any]

Time Range: Always

Log: ☐ Enable ☐ Disable

PN: ☐ Enable ☐ Disable

Buttons: Add, Edit, Delete, Help

Figure 10.11. Extranet Example – Inbound ACL Rule on ISR1

10.5.2.3 Configure VPN Rules on ISR2

Step 1: Configure VPN rules

Refer to the section **10.3 Establish VPN Connection Using Automatic Keying** to configure VPN policies on ISR2 using automatic keying with the following addresses:

1. Use 192.168.12.0/255.255.255.0 as Local Secure Group
2. Use 192.168.11.0/255.255.255.0 as Remote Secure Group

VPN Connection Settings

Name: IP2_TC_IPR1

Buttons: Add New, Enable, Disable, Move to

Local Secure Group: Type: Subnet, Address: 192.168.12.0, Mask: 255.255.255.0

Remote Secure Group: Type: Subnet, Address: 192.168.11.0, Mask: 255.255.255.0

Local Gateway: Interface: eth0

Remote Gateway: Type: IP Address, IP Address: 212.1.1.212

IKE Proposal Settings

IKE Mode: ☒ Main ☐ Aggressive

Pre-shared Key: *****

IKE Encryption/Authentication: All

Life Time: 3600 Sec

IPsec Proposal Settings

Encryption/Authentication: ESP:DES+MAC (SHA1)

PFS Group: None

Life Time: 3600 Sec, 72000 KByte

Buttons: Add, Edit, Delete, Help

Figure 10.12. Extranet Example –VPN Policy Configuration on ISR2

Step 2: Configure Static NAT Pools

1. Configure outgoing static NAT pool (static-NAT) for translating addresses in range 192.168.1.1- 192.168.1.254 to 192.168.12.1-192.168.12.254



The screenshot shows the 'NAT Pool Configuration' window. The 'Add New Pool' dropdown is set to 'Add'. The 'Name' field contains 'Outgoing_NAT'. The 'Pool Type' is set to 'Static'. Under 'Original IP', the 'Start IP' is 192.168.1.1 and the 'End IP' is 192.168.1.254. Under 'Mapped IP', the 'Start NAT IP' is 192.168.12.1 and the 'End NAT IP' is 192.168.12.254. At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

Figure 10.13. Extranet Example – Outgoing NAT Pool Configuration on ISR2

2. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.12.1-192.168.12.254 to 192.168.1.1-192.168.1.254

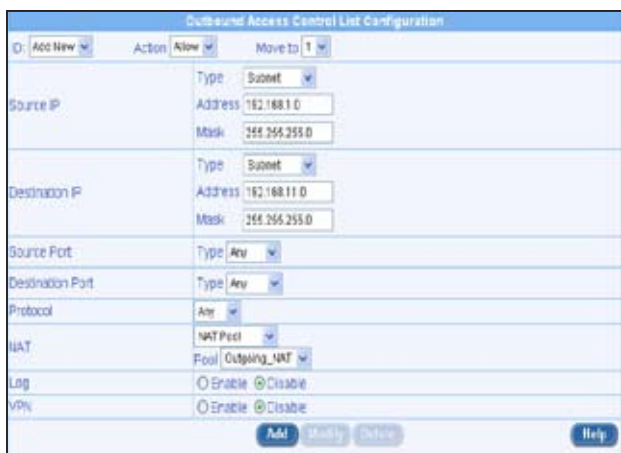


The screenshot shows the 'NAT Pool Configuration' window. The 'Add New Pool' dropdown is set to 'Add'. The 'Name' field contains 'Incoming_NAT'. The 'Pool Type' is set to 'Static'. Under 'Original IP', the 'Start IP' is 192.168.12.1 and the 'End IP' is 192.168.12.254. Under 'Mapped IP', the 'Start NAT IP' is 192.168.1.1 and the 'End NAT IP' is 192.168.1.254. At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

Figure 10.14. Extranet Example – Incoming NAT Pool Configuration on ISR2

Step 3: Configure Extranet rules

1. Configure outbound Firewall rules to map the source IP address of outbound packets from 192.168.1.x range to 192.168.12.x (defined by Outgoing_NAT pool) range before sending the packet to VPN.



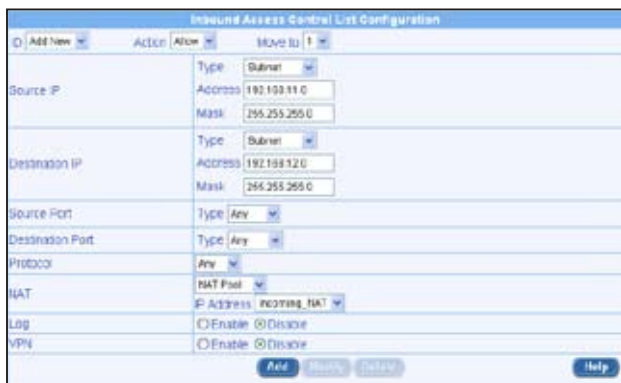
The screenshot shows the 'Outbound Access Control List Configuration' window. At the top, there are buttons for 'Add New', 'Action', 'Allow', and 'Move to 1'. The configuration fields are as follows:

Field	Type	Value
Source IP	Subnet	192.168.1.0
	Mask	255.255.255.0
Destination IP	Subnet	192.168.1.0
	Mask	255.255.255.0
Source Port	Any	
Destination Port	Any	
Protocol	Any	
NAT	NAT Pool	
	Pool	Outgoing_NAT
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

Figure 10.15. Extranet Example – Outbound ACL Rule on ISR2

2. Configure inbound Firewall rules to map the destination IP address of inbound packets from 192.168.12.x range to 192.168.1.x range after the packet is processed by VPN.



The screenshot shows the 'Inbound Access Control List Configuration' window. At the top, there are buttons for 'Add New', 'Action', 'Allow', and 'Move to 1'. The configuration fields are as follows:

Field	Type	Value
Source IP	Subnet	192.168.12.0
	Mask	255.255.255.0
Destination IP	Subnet	192.168.1.0
	Mask	255.255.255.0
Source Port	Any	
Destination Port	Any	
Protocol	Any	
NAT	NAT Pool	
	P Address	Incoming_NAT
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

Figure 10.16. Extranet Example – Inbound ACL Rule on ISR2

10.5.2.4 Establish Tunnel and Verify

- Start continuous ping from a host on the LAN behind ISR1 to a host on the LAN behind ISR2. The first few pings would fail. After a few seconds, The host on the LAN behind ISR1 should start getting ping response.
- Ping from a host on the LAN behind ISR2 to a host on the LAN behind ISR1. Ping should be successful.
- The ping might fail due to any of the following:
 - The IP address of the host on the LAN behind ISR2 used in the ping command may not be correct. Check and give the correct IP address.
 - Default route is not configured for ISR1 or ISR2. Configure the default routes as necessary.
 - Firewall rules corresponding to VPN connection may not be configured properly. If any of the network addresses is not correctly configured, correct the parameters and apply the configuration.
 - Local and remote network addresses may not be configured correctly. The network addresses used in VPN connection rule are 192.168.11.0/255.255.255.0 and 192.168.12.0/255.255.255.0

11 System Management

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

- Configure system services
- Modify password
- Modify system Information
- Modify system date and time
- Reset, backup and restore system configuration
- Update firmware
- Logout of Configuration Manager

You can access these tasks from the System Management menu.

11.1 Configure System Services

As shown in Figure 11.1, you can use the System Services Configuration page to enable or disable services supported by the Internet Security Router. All services, firewall, VPN, DNS, DHCP and RIP, are all enabled at the factory. To disable or enable individual service, follow the steps below:

1. Log into Configuration Manager as administrator. Click **System Management -> System Services**. The System Services Configuration page displays, as shown in Figure 11.1.
2. Click on the corresponding **Enable** or **Disable** radio button to enable or disable the desired services.
3. Click on **<Apply>** to save the changes.



Figure 11.1. System Services Configuration Page

11.2 Change the Login Password

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 users – **administrator** (username: admin) and **guest** (username: guest).

Administrator has the privilege to modify the system settings while guest can only view the system settings. Passwords of both the admin and guest accounts can be changed by the administrator.



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.



Figure 11.2. Password Configuration Page

The Password Configuration page 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 the User Account submenu. The User Account Configuration page displays, as shown in Figure 11.2.
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.

11.3 Modify System Information

As illustrated in Figure 11.3, you can use System Information Setup 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. All fields allow only alphanumeric characters. When you are done entering system specific information, click **<Apply>** to save the changes.



Figure 11.3. System Information Configuration Page

11.4 Setup Date and Time

The Internet Security Router keeps a record of the current date and time, which it uses to calculate and report various performance data.



Figure 11.4. Date and Time Configuration Page

There is no real time clock inside the Internet Security Router. The system date and time are maintained by external network time server. The only fields configurable in this configuration page are the "Time Zone", IP address of time servers and the desired update interval. Select your time zone from the "Time Zone" dropdown list, change the IP address of the time servers and the update interval if desired and then click on button to save the changes.

11.4.1 View the System Date and Time

To view the updated system date and time

1. Log into Configuration Manager as administrator. Click **System Management -> Date/Time Setup**. The Date/Time Configuration page displays as shown in Figure 11.4.
2. Click **<Apply>** to see the updated system date and time.

11.5 SNMP Setup

Simple Network Management Protocol (SNMP) is used for network management. You may use the SNMP configuration page to enable or disable the SNMP support.

11.5.1 SNMP Configuration Parameters

Table 11.1 describes the configuration parameters available for SNMP setup.

Table 11.1. Fixed DHCP Lease Configuration

Field	Description
SNMP	Click on the Enable or Disable radio button to enable or disable the SNMP support.
RO Community Name	Community string is a clear text string that is used as password between the SNMP management station and the ASUS SL1200. This Read Only community name is used by the SNMP management station to read the settings in the ASUS SL1200.
RW Community Name	Community string is a clear text string that is used as password between the SNMP management station and the ASUS SL1200. This Read and Write community name is used by the SNMP management station to read and configure the settings in the ASUS SL1200.
Trap Address	Trap message is sent by the ASUS SL1200 to tell the SNMP management station that something has happened on the router. This field is used to enter the IP address of the SNMP management station that is supposed to receive trap messages from the ASUS SL1200.

11.5.2 Configuring SNMP

1. To open the SNMP configuration page, click the **System Management** -> **SNMP** menu.
2. Click on the **Enable** or **Disable** radio button to enable or disable the SNMP support.
3. Enter the RO (read only) and R/W (read and write) community names.
4. Enter the IP address of the SNMP management station that receives trap messages from the ASUS SL 1200.

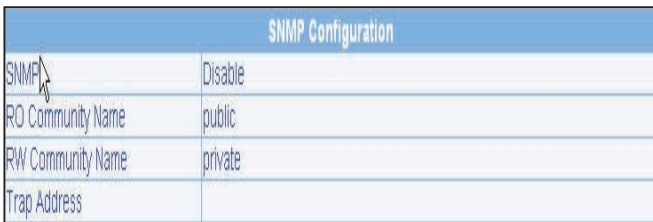


The image shows a web-based configuration form titled "SNMP Configuration". It contains the following fields and controls:

SNMP Configuration	
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RO Community Name	<input type="text" value="public"/>
RW Community Name	<input type="text" value="private"/>
Trap Address	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 11.5. SNMP Configuration

5. Click **<Apply>** to save the configuration. You can verify your settings in the existing SNMP configuration table displayed at the bottom of the configuration page.



The image shows a table titled "SNMP Configuration" with the following data:

SNMP Configuration	
SNMP	Disable
RO Community Name	public
RW Community Name	private
Trap Address	

Figure 11.6. Existing SNMP Configuration

11.6 System Configuration Management

11.6.1 Reset System Configuration

At times, you may want to revert to factory default settings to eliminate problems resulted from incorrect system configuration.

To reset system configuration

1. Log into Configuration Manager as administrator. Click **System Management -> Configuration -> Default Settings**. The Default Settings Configuration page displays, as shown in Figure 11.7.
2. Click **<Apply>** to set the system configuration back to factory default. The Internet Security Router will reboot to make the factory default configuration in effect.

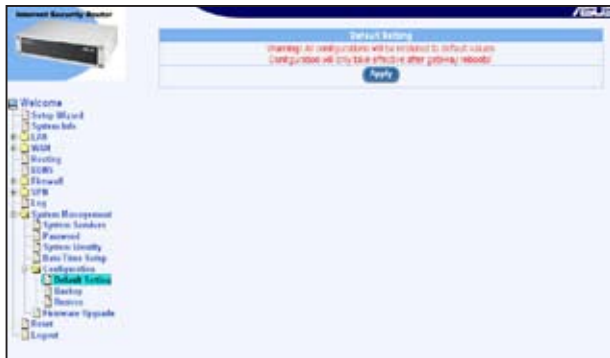


Figure 11.7. Default Setting Configuration Page

Sometimes, you may find that you have no way to access the Internet Security Router, such as when you forget your password. The only way out in this scenario is to reset the system configuration to the factory default.

To reset the router

1. Power down the Internet Security Router and wait for at least five seconds.
2. Power on the Internet Security Router and wait for at least five seconds before pressing the reset switch the first time. You will see the Alarm LED flash once in about 5 seconds.
3. When you see the Alarm LED flash once, press the reset switch again. You will then see the Alarm LED flash twice in about five seconds. This indicates that the Internet Security Router is about to revert to the factory default settings. If you change your mind, you may press the reset switch again or turn the power off to cancel this action.

11.6.2 Backup System Configuration

To backup system configuration

1. Log into Configuration Manager as administrator. Click **System Management -> Configuration -> Backup**. The Backup Configuration page displays, as shown in Figure 11.8.
2. Click **<Apply>** to backup the system configuration.



Figure 11.8. Backup System Configuration Page

11.6.3 Restore System Configuration

To restore system configuration

1. Log into the Configuration Manager as administrator. Click **System Management -> Configuration -> Restore**. The Restore Configuration page displays, as shown in Figure 11.9.



Figure 11.9. Restore System Configuration Page

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 **<Browse>** to search for the system configuration file on your hard drive. A window similar to the one shown in Figure 11.10 will pop up for you to select the configuration file to restore.

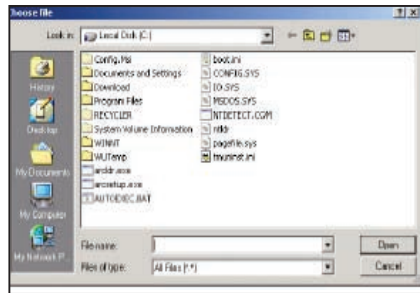


Figure 11.10. Windows File Browser

3. Click **<Apply>** to restore the system configuration. The Internet Security Router will reboot to make the new system configuration in effect.

11.7 Upgrade Firmware

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



Figure 11.11. Firmware Upgrade Page

1. Log into Configuration Manager. Click **System Management -> Firmware Upgrade**. The Firmware Upgrade page displays as shown in Figure 11.11.

2. In the Firmware text box, enter the path and name of the firmware image file. Alternatively, you may click on button to search for it on your hard drive.
3. Click **<Apply>** to update the firmware. It may take up to 5 minutes for the firmware upgrade. After the transfer of firmware is completed, the Internet Security Router will reboot to make the new firmware in effect.

11.8 Reset the Internet Security Router

To reset the Internet Security Router, click **<Apply>** in the Configuration Manager Reset page.



Figure 11.12. Configuration Manager Reset Page

11.9 Logout Configuration Manager

To logout of Configuration Manager, click **<Apply>** in the Configuration Manager Logout page. If you are using IE as your browser, a window similar to the one shown in Figure 11.14 will prompt for confirmation before closing your browser.

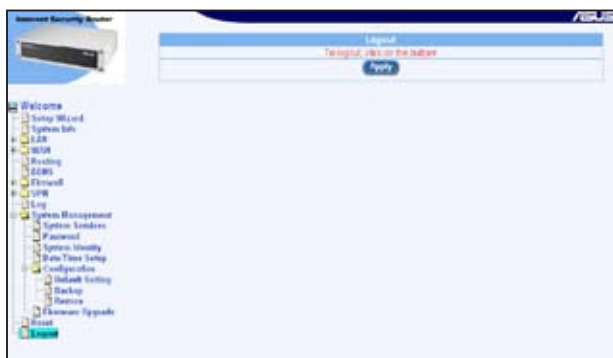


Figure 11.13. Configuration Manager Logout Page

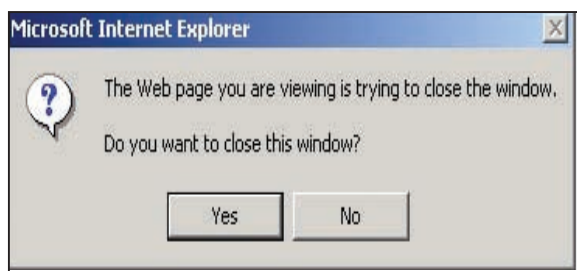


Figure 11.14. Confirmation for Closing Browser (IE)

12 ALG Configuration

Table 12.1 lists all the supported ALGs (Application Layer Gateway).

Table 12.1. Supported ALG

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
PCAnywhere	UDP/22	PC-ANYWHERE	pcAnywhere 9.0.0
RTSP-554	TCP/554	RTSP554	RealPlayer 8 Plus QuickTime Version 6
	UDP/53	DNS	
	TCP/80	HTTP	
RTSP-7070	TCP/7070	RTSP7070	RealPlayer 8 Plus
	UDP/53	DNS	QuickTime Version 6
	TCP/80	HTTP	
Net2Phone	UDP/6801	N2P	Net2Phone CommCenter Release 1.5.0
	TCP/80	HTTP	
	TCP/443	HTTPS	
	UDP/53	DNS	
CUSeeMe	TCP/7648	CUSEEME	CUSeeMe Version 5.0.0.043
	TCP/80	HTTP	
	UDP/53	DNS	
Netmeeting	TCP/1720	H323	
	UDP/53	DNS	
Netmeeting with ILS	TCP/1720	H323	Windows Netmeeting Version 3.01 Opengk Version 1.2.0
	TCP/389	ILS	
	UDP/53	DNS	

Chapter 12 - ALG Configuration

ALG/Application Name	Protocol Port	and	Pre defined Service Name	Tested Software Version
Netmeeting with GK	TCP/1720		H323	W i n d o w s Netmeeting Version 3.01 OpengK Version 1.2.0
	UDP/1719		H323GK	
	UDP/53		DNS	
SIP	UDP/5060		SIP	SIP User Agent 2.0
Intel Video Phone	TCP/1720		H323	Intel Video Phone Version 5.0
	UDP/53		DNS	
FTP	TCP/21		FTP	WFTPD version 2.03 Redhat Linux 7.3
	UDP/53		DNS	
Security ALGs				
L2TP	UDP/1701		L2TP	Windows 2000 Server built-in
	UDP/53		DNS	
PPTP	TCP/1723		PPTP	Windows 2000 Server built-in
	UDP/53		DNS	
IPSec (Only Tunnel Mode with ESP)	UDP/500		IKE	Windows 2000 Server built-in
	ESP			
	UDP/53		DNS	
Chats				
AOL Chat	TCP/ 5190		AOL	AOL Instant Messenger Version 5.0.2938
	TCP/80		HTTP	
	UDP/53		DNS	
ICQ Chat NB: Application should be configured to use TCP/5191	TCP /5191		ICQ_2000	ICQ 2000b
	TCP/80		HTTP	
	UDP/53		DNS	
IRC	TCP/ 6667		IRC	MIRC v6.02
	TCP/80		HTTP	
	UDP/53		DNS	

ALG/Application Name	Protocol Port	and P r e d e f i n e d Service Name	Tested Software Version
Chats			
MSIM	TCP/1863	MSN	MSN Mes- senger Service Version 3.6.0039
	TCP/80	HTTP	
	UDP/53	DNS	
Games			
Flight Simulator 2002 (Gaming Zone)	TCP/47624	MSG1	Flight Simulator 2002, Profes- sional Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Quake II (Gaming Zone)	UDP/ 27910	QUAKE	Quake II
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Age Of Empires(Gaming Zone)	TCP/47624	MSG1	Age of Empires, Gold Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Diablo II (BATTLENET- TCP, BATTLENET-UDP)	TCP/4000	DIABLO-II	DIABLO II
	TCP/ 6112	BATTLE-NET-TCP, BATTLE-NET-UDP	
	UDP/53	DNS	
	UDP/6112	Diablo II	

Chapter 12 - ALG Configuration

ALG/Application Name	Protocol and Port	Predefined Service Name	Tested Software Version
Chats			
POP3	TCP/110	POP3	Outlook Express 5
	UDP/53	DNS	
IMAP	TCP/143	IMAP4	Outlook Express 5
	UDP/53	DNS	
SMTP	TCP/25	SMTP	Outlook Express 5
	UDP/53	DNS	
HTTPS / TLS / SSL	TCP/443	HTTPS	Internet Explorer 5
	TCP/80	HTTP	
	UDP/53	DNS	
LDAP	TCP/389	ILS	Openldap 2.0.25
	UDP/53	DNS	
NNTP	TCP/119	NNTP	Outlook Express 5
	UDP/53	DNS	

13 IP Addresses, Network Masks, and Subnets

13.1 IP Addresses



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.

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."

13.1.1 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 13.1 shows the structure of an IP address.

Table 13.1. IP Address structure

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

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

13.2 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.

13.3 Subnet masks



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.



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.

14 Troubleshooting

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

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

Table 14.1. Problems and suggestions

Problem	Troubleshooting Suggestion
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 Internet Security Router and a wall socket/power strip.
LINK WAN LED does not illuminate after Ethernet cable is attached.	Verify that an Ethernet cable like the one provided is securely connected to the Ethernet port of your ADSL or cable modem and the WAN port of the Internet Security Router. Make sure that your ADSL or cable modem is powered on. Wait 30 seconds to allow the Internet Security Router to negotiate a connection with your broadband modem.
LINK LAN LED does not illuminate after Ethernet cable is attached.	<p>Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Internet Security Router. Make sure the PC and/or hub is turned on.</p> <p>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.</p>

Problem	Troubleshooting Suggestion
Internet Access	
PC cannot access Internet	<p>Use the ping utility, discussed in the following section, to check whether your PC can communicate with the Internet Security Router's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling.</p> <p>If you statically assigned a private IP address to the computer, (not a registered public address), verify the following:</p> <ul style="list-style-type: none"> • 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 Internet Security Router to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules. Or, configure the PC to accept an address assigned by another device (see section 3.2 "Part 2 — Configuring Your Computers"). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool.
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.

Chapter 14 - Troubleshooting

Problem	Troubleshooting Suggestion
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 following the instructions provided in section 11.5.1 “Reset System Configuration”. 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 Internet Security Router’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, Netscape 7.0.2 or later. 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 Internet Security Router.
Changes to Configuration Manager are not being retained.	Be sure to click on <Apply> button to save any changes.

14.1 Diagnosing problems using IP utilities

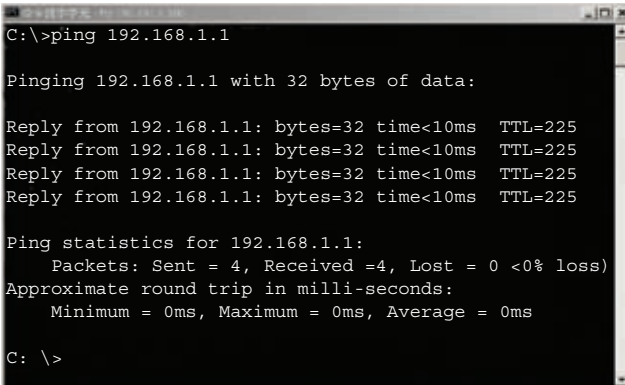
14.1.1 ping

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

On Windows-based computers, you can execute a ping command from the Start menu. Click the **Start** button, and then click **Run**. In the Open text box, type a statement such as the following: **ping 192.168.1.1**

Click **<OK>**. You can substitute any private IP address you know on your LAN or a public IP address for an Internet site.

If the target computer receives the message, a Command Prompt window appears as shown in Figure 14.1.



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms TTL=225

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

C: \>
```

Figure 14.1 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 switch is working (using the pre-configured 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.

14.1.2 nslookup

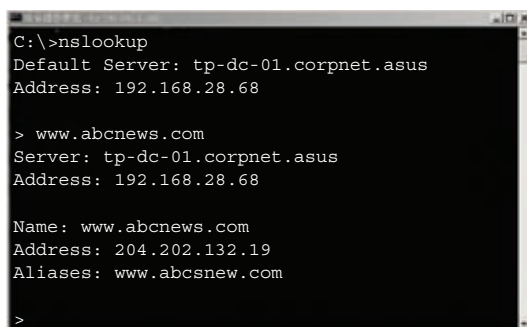
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred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

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

nslookup

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

The window displays the associate IP address you know. See Figure 14.2.



```
C:\>nslookup
Default Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

> www.abcnews.com
Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

Name: www.abcnews.com
Address: 204.202.132.19
Aliases: www.abcnews.com

>
```

Figure 14.2. 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.

15 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.
1000BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 1000 Mbps.
binary	The “base two” system of numbers, which 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
CoS	Class of Service. Defined in 802.1Q, the value range is from 0 to 7.
broadcast	To send data to all computers on a network.

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.
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.
host	A device (usually a computer) connected to a network.
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.
IGMP Snooping	Snoop the IGMP packets on each port and associate the port with a layer 2 multicast group.
mask	See network mask.
Multicast	To send data to a group of network devices.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

Monitor	Also called “Roving Analysis”, allow you to attach a network analyzer to one port and use it to monitor the traffics of other ports on the switch.
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.
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 intranet is a remote user.
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.
RMON	Remote Monitoring Extensions to SNMP, provide comprehensive network monitoring capabilities.
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.
SNMP	Simple Network Management Protocol The TCP/IP protocol used for network management.
STP	Spanning Tree Protocol The bridge protocol to avoid packet looping in a complicate network.
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/SSH	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 / SSH 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.
Trunk	Two or more ports are combined as one virtual port, also called as Link Aggregation.
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.
VLAN	Virtual Local Area Network
WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the SL-1000, 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.