Set-up instructions for

Solwise SAR110
ADSL Router

www.solwiseforum.co.uk

The Solwise Forum is designed to be the first port-of-call for technical support and sales advice for the whole Solwise product range.

Please check the forum for coverage on any technical problems you have. Many people have trodden your path before you, and a quick check on the forum will reduce the pressure on our support staff.

Mar 29, 2003
Covers Solwise-270303/1.38.030131a13
Notification is hereby given that Solwise Ltd. reserves the right to modify, change, update or revise this document from time to time as required without the prior obligation to notify any person, company or organization. Further, Solwise makes no warranty or representation, either express or implied, with respect to merchantability, or fitness of its products for a particular purpose.

Solwise Ltd.
13/15 Springfield Way
Anlaby
Hull   HU10 6RJ
UK
Tel  0845 458 4558 (local rate)
Fax 0845 458 4559
Email sales@solwise.co.uk
Http www.solwise.co.uk

Copyright
All rights reserved. No part of this document may be reproduced in any form or by any means without written permission from the product manufacturer.

Changes are periodically made to the information in this document. They will be incorporated in subsequent editions. The product manufacturer may take improvement and/or changes in the product described in this document at any time.

FCC compliance
This equipment complies with Part 68 of the FCC Rules. On this equipment is a label that contains, among other information, the FCC registration number and Ringer Equivalence Number (REN) for this equipment. You must, upon request, provide this information to your telephone company.

If your telephone equipment causes harm to the telephone network, the Telephone Company may discontinue your service temporarily. If possible, they will notify in advance. But, if advance notice isn’t practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect proper operation of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service. The FCC prohibits this equipment to be connected to party lines or coin-telephone service.

In the event that this equipment should fail to operate properly, disconnect the equipment from the phone line to determine if it is causing the problem. If the problem is with the equipment, discontinue use and contact your dealer or vendor.
DOC compliance information

NOTICE: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user’s satisfaction.

Before installing this equipment, users ensure that it is permissible to be connected to the facilities of the local Telecommunications Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the sum of the Load Numbers of all the devices does not exceed 100.

European CTR 21 compliance

The equipment has been approved in accordance with Council Decision 98/482/EC for pan-European single terminal connection to the public switched telephone network (PSTN). However, due to differences between the individual PSTNs provided in different countries, the approval does not, of itself, give an unconditional assurance of successful operation on every PSTN network termination point. In the event of problem, you should contact your equipment supplier in the first instance.
Table of Contents

1 Introduction
   1.1 Features
   1.2 System Requirements
   1.3 Using this Document
      1.3.1 Notational conventions
      1.3.2 Typographical conventions
      1.3.3 Special messages

2 Getting to Know the SAR110
   2.1 Parts Check
   2.2 Front Panel
   2.3 Rear Panel

3 Quick Start
   3.1 Part 1 — Connecting the Hardware
      3.1.1 Step 1. Connect the ADSL cable and optional telephone
      3.1.2 Step 2. Connect the Ethernet cable
      3.1.3 Step 3. Attach the power connector
      3.1.4 Step 4. Turn on the SAR110 and power up your systems
   3.2 Part 2 — Configuring Your Computers
      3.2.1 Before you begin
      3.2.2 Windows® XP PCs
      3.2.3 Windows 2000 PCs
      3.2.4 Windows Me PCs
      3.2.5 Windows 95, 98 PCs
      3.2.6 Windows NT 4.0 workstations
      3.2.7 Apple Mac
   3.3 Part 3 — Quick Configuring the SAR110
      3.3.1 Logging in to the SAR110 Quick Configuration Page
      3.3.2 Default Router Settings

4 Basic for Configuration using the Web Interface
   4.1 Accessing the Configuration Manager
   4.2 Functional Layout
4.2.1 Commonly used buttons.................................38
4.3 The Home Tab and System View Table ...............39
4.4 Changing the System Date and Time .................40
4.5 Changing Your Login Password............................41
4.6 Committing Your Changes and Rebooting the Device..................................................43
  4.6.1 Committing your changes............................43
  4.6.2 Rebooting the device using Configuration Manager........................................43
5 Setting IP Properties for the LAN-side Interfaces..........................................................45
  5.1 Configuring the LAN IP Address..........................45
6 Viewing System IP Information and Performance Statistics ..............................................49
  6.1 Viewing the SAR110’s IP addresses..................49
  6.2 Viewing IP Global Statistics..............................50
7 Configuring Dynamic Host Configuration Protocol ............................................................53
  7.1 Overview of DHCP ........................................53
    7.1.1 What is DHCP?........................................53
    7.1.2 Why use DHCP?........................................53
    7.1.3 SAR110 DHCP modes................................54
  7.2 Configuring DHCP Server................................55
    7.2.1 Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool..............................58
    7.2.2 Viewing current DHCP address assignments ..........................................................59
  7.3 Configuring DHCP Relay ................................60
  7.4 Setting the DHCP Mode..................................61
8 Configuring Network Address Translation .................63
  8.1 Overview of NAT ..........................................63
  8.2 Viewing NAT Global Settings and Statistics........64
  8.3 Viewing NAT Rules and Rule Statistics................67
  8.4 Viewing Current NAT Translations......................68
  8.5 Adding NAT Rules.........................................70
    8.5.1 The napt rule: Translating between private and public IP addresses..........................70
8.5.2 The rdr rule: Allowing external access to a LAN computer ...................................................72

8.5.3 The basic rule: Performing 1:1 translations ........................................................................75

8.5.4 The filter rule: Configuring a basic rule with additional criteria ........................................77

8.5.5 The bimap rule: Performing two-way translations ................................................................79

8.5.6 The pass rule: Allowing specific addresses to pass through untranslated ..........................80

9 Configuring DNS Server Addresses ......................81

9.1 About DNS .............................................................................................................................81

9.2 Assigning DNS Addresses ....................................................................................................81

9.3 Configuring DNS Relay ........................................................................................................82

10 Configuring IP Routes ..........................................................85

10.1 Overview of IP Routes .........................................................................................................85

10.1.1 Comparing IP routing to telephone switching ................................................................85

10.1.2 Hops and gateways ......................................................................................................86

10.1.3 Using IP routes to define default gateways .....................................................................86

10.1.4 Do I need to define IP routes? .......................................................................................86

10.2 Viewing the IP Routing Table ...........................................................................................87

10.3 Adding IP Routes ................................................................................................................88

11 Configuring the Routing Information Protocol ........................................................................91

11.1 RIP Overview .......................................................................................................................91

11.1.1 When should you configure RIP? ...................................................................................91

11.2 Configuring the SAR110's Interfaces with RIP ....................................................................91

11.3 Viewing RIP Statistics .......................................................................................................93

12 Configuring the ATM VCC ..............................................................95

12.1 Viewing Your ATM VC Setup .............................................................................................95

12.2 Adding ATM VCCs ..............................................................................................................96

12.3 Modifying ATM VCCs ........................................................................................................97

13 Configuring PPP Interfaces ..........................................................99

13.1 Viewing Your Current PPP Configuration ...........................................................................99

13.2 Viewing PPP Interface Details .........................................................................................101

13.3 Adding a PPP Interface Definition ....................................................................................103
13.4 Modifying and Deleting PPP Interfaces.................105

14 Configuring EOA Interfaces ..........................106
14.1 Overview of EOA .........................................106
14.2 Viewing Your EOA Setup .............................107
14.3 Adding EOA Interfaces ................................108

15 Configuring IPoA Interfaces ..........................111
15.1 Viewing Your IPoA Interface Setup ..................111
15.2 Adding IPoA Interfaces .................................112

16 Configuring Bridging .....................................115
16.1 Overview of Bridges ....................................115
16.2 Using the Bridging Feature ...........................116
16.3 Defining Bridge Interfaces ............................117
16.4 Deleting a Bridge Interface .........................118

17 Configuring Firewall Settings .......................119
17.1 Configuring Global Firewall Settings ...............119
17.2 Managing the Black List ..............................122

18 Configuring IP Filters and Blocking Protocols ..........125
18.1 Configuring IP Filters ................................125
18.1.1 Viewing Your IP Filter Configuration ..........125
18.1.2 Configuring IP Filter Global Settings ..........126
18.1.3 Creating IP Filter Rules ..........................127
18.1.4 IP filter rule examples ..........................133
18.1.5 Viewing IP Filter Statistics ......................136
18.1.6 Managing Current IP Filter Sessions ..........136
18.2 Blocking Protocols .....................................137

19 Viewing DSL Parameters ...............................141

20 Administrative Tasks ......................................145
20.1 Viewing System Alarms ...............................145
20.1.1 Viewing the Alarm Table ..........................145
20.1.2 Displaying the Alarm Monitor in a Separate Window ........................................146
20.2 Upgrading the Software ................................146
20.2.1 What if something goes wrong? .................147
20.3 Using Diagnostics .......................................149
20.4 Modifying Port Settings ..............................150
20.4.1 Overview of IP port numbers ..................150
20.4.2 Modifying the ADSL/Ethernet routers’ port numbers .......................................................... 151

21 Committing Your Changes and Rebooting the Device .......................................................... 153
21.1 Committing Your Changes ................................................. 153
21.2 Rebooting the Device ........................................... 153

22 How to .............................................................................. 154
22.1 How to enter Command Line Interface mode .............................................................................. 154
22.1.1 Telnet ........................................................................ 154
22.1.2 Using terminal program via serial console port ............................................................ 155
22.1.3 Basic CLI syntax .......................................................... 157
22.2 Common CLI Commands .................................................. 159
22.2.1 commit ................................................................. 159
22.2.2 reboot < default|backup|last|clean|minimum> .................................................. 160
22.2.3 get ip <address | cfg | route | stats> ............... 160
22.2.4 modify ethernet intf ifname <name> [ip,mask,usedhcp,speed,duplex] ........................... 160
22.2.5 modify nbsize maxipsess ’value’ ................. 161
22.2.6 create user name <name> passwd <name> [root | user] ............................................... 161
22.3 Altering the WAN IP address of the router .............. 161
22.4 eMule/eDonkey ☺ .......................................................... 162
22.4.1 What’s the problem? .............................................. 162
22.4.2 How do I fix it? ..................................................... 163
22.5 Enabling ZIPB ............................................................... 163
22.5.1 What’s ZIPB? ......................................................... 163
22.5.2 How it works ........................................................ 163
22.5.3 Here’s how to do it .............................................. 164
22.5.4 Testing it’s worked .............................................. 169
22.6 Operation with multiple IP’s ............................................. 170
22.6.1 IP Unnumbered PPP interface ......................... 170
22.6.2 Configuration ......................................................... 171
22.6.3 Limitations .......................................................... 172
22.6.4 IP Unnumbered with NAT ................................. 173
22.7 Blocking remote access to your SAR110 router .............................................................................. 173
1 Introduction

Congratulations on becoming the owner of the SAR110 ADSL Ethernet bridge/router. Your LAN (local area network) will now be able to access the Internet using your high-speed ADSL connection.

This User Guide will show you how to set up the SAR110 ADSL Bridge/Router, and how to customize its configuration to get the most out of your new product.

1.1 Features

- Internal ADSL modem for high-speed Internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT), Firewall, and IP filtering functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Relay
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- Configuration program you access via an HTML browser

1.2 System Requirements

In order to use the SAR110 ADSL/Ethernet router, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network.
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later
1.3 Using this Document

1.3.1 Notational conventions

- Acronyms are defined the first time they appear in text and in the glossary (Appendix 27).
- For brevity, the SAR110 is referred to as “the router.”
- The terms LAN and network are used interchangeably to refer to a group of Ethernet-connected computers at one site.

1.3.2 Typographical conventions

- Italics are used to identify terms that are defined in the glossary (Appendix 27).
- Bolded text is used for items you select from menus and drop-down lists, and text strings you type when prompted by the program.

1.3.3 Special messages

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

**Note**

Provides clarifying 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 SAR110

2.1 Parts Check

In addition to this document, your SAR110 should arrive with the following:

- SAR110 ADSL Ethernet Bridge/Router
- Power adapter and power cord
- Ethernet cable ("straight-through" type)
- Standard phone/DSL line cable
- Documentation CD

Figure 1. SAR110 ADSL/Ethernet Router
2.2 Front Panel

The front panel contains lights called LEDs that indicate the status of the unit.

![Front Panel and LEDs](image)

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>Function</th>
</tr>
</thead>
</table>
| POWER | green  | On: Unit is powered on
Off: Unit is powered off                                                   |
| DIAG  | yellow | Flashes on/off at boot-up to indicate that the device software is operational. Turns off after 10-15 seconds. |
| PC    | green  | On: LAN link established and active
Off: No LAN link                                                              |
| ADSL  | green  | On: ADSL link established and active
Off: No ADSL link                                                             |
| TX/RX | yellow | Flashes when ADSL data activity occurs.
May appear solid when data traffic is heavy.                                 |
2.3 Rear Panel

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

![Rear Panel Connections](image)

**Figure 3. Rear Panel Connections**

<table>
<thead>
<tr>
<th>Label</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>Connects the device to a telephone jack for DSL communication</td>
</tr>
<tr>
<td>10/100Base-T</td>
<td>Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided</td>
</tr>
<tr>
<td>DC</td>
<td>Connects to the supplied power converter cable</td>
</tr>
<tr>
<td>On Off</td>
<td>Switches the unit on and off (on side of case)</td>
</tr>
</tbody>
</table>
3 Quick Start

This Quick Start provides basic instructions for connecting the SAR110 to a computer or LAN and to the Internet.

- Part 1 describes setting up the hardware.
- Part 2 describes how to configure Internet properties on your computers.
- Part 3 shows you how to configure basic settings on the SAR110 to get your LAN connected to the Internet.

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

3.1 Part 1 — Connecting the Hardware

In Part 1, you connect the device to the phone jack, the power outlet, and your computer or network.

**WARNING**

*Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the SAR110.*

![Diagram of hardware connections](image)

Figure 4 illustrates the hardware connections. The layout of the
ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

Figure 4. Overview of Hardware Connections

3.1.1 Step 1. Connect the ADSL cable and optional telephone.

Connect one end of the provided phone cable to the port labeled ADSL on the rear panel of the device. Connect the other end to your wall phone jack.

You can attach a telephone line to the device. This is helpful when the ADSL line uses the only convenient wall phone jack. If desired, connect the telephone cable to the port labeled PHONE.

**WARNING**

Although you use the same type of cable, the ADSL and PHONE ports are not interchangeable. Do not route the ADSL connection through the PHONE port.

3.1.2 Step 2. Connect the Ethernet cable.

If you are connecting a LAN to the SAR110 ADSL/Ethernet router, attach one end of a provided Ethernet cable to a crossover hub port and the other to the Ethernet port on the SAR110. If you want to connect the 110 to a ‘normal’ LAN port then you need to use a crossover adapter or cable.

If you are using the SAR110 with a single computer and no hub, you must use a “standard” Ethernet cable to attach the PC directly to the device.
3.1.3 **Step 3. Attach the power connector.**

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

3.1.4 **Step 4. Turn on the SAR110 and power up your systems.**

Press the Power switch on the back panel of the device to the ON position.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

3.2 **Part 2 — Configuring Your Computers**

Part 2 of the Quick Start provides instructions for configuring the Internet settings on your computers to work with the SAR110.

3.2.1 **Before you begin**

By default, the SAR110 is on IP address 192.168.7.1 with subnet mask 255.255.255.0. In order to configure the router you must ensure that the IP settings on your computer suite the default address of the SAR110.

*Note*

Your computers must have IP addresses that place them in the same subnet as the SAR110’s LAN port. If you want to use a different subnet range then you can follow the instructions in Chapter 5 to change the LAN port IP address of the SAR110 accordingly.

3.2.2 **Windows® XP PCs:**

1. In the Windows task bar, click the Start button, and then click **Control Panel**.

2. Double-click the Network Connections icon.

3. In the LAN or High-Speed Internet window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (Often this icon is labeled **Local Area Connection**).

   The Local Area Connection dialog box displays with a list of currently installed network items.

4. Ensure that the check box to the left of the item labeled **Internet Protocol TCP/IP** is checked, and click **Properties**.

5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Specify an IP address**. Enter a suitable IP address for the PC e.g. 192.168.7.2 (remember that each computer/device on an IP network must have it’s own, unique IP address). Use the subnet mask 255.255.255.0.
6. Set the router/default gateway address to the address of the SAR110 which is 192.168.7.1.

7. Enter the DNS address as given to you by your ISP. Please note that you will need a DNS address. If you don’t know the DNS address for your ISP then you can, temporarily use the own from our ISP which is 212.50.160.100 but you should get the correct DNS address of your ISP and use that value as soon as possible.

8. Click twice to confirm your changes, and close the Control Panel.

3.2.3 Windows 2000 PCs:

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

1. In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network and Dial-up Connections icon.

3. In the Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select Properties. The Local Area Connection Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click Install.

5. In the Select Network Component Type dialog box, select Protocol, and then click Add.

6. Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK.

You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

7. If prompted, click to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the SAR110:

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 **Specify an IP address**. Enter a suitable IP address for the PC e.g. 192.168.7.2 (remember that each computer/device on an IP network must have it's own, unique IP address). Use the subnet mask 255.255.255.0.

12. Set the router/default gateway address to the address of the SAR110 which is 192.168.7.1.

13. Enter the DNS address as given to you by your ISP. Please note that you **will** need a DNS address. If you don't know the DNS address for your ISP then you can, temporarily use the own from our ISP which is 212.50.160.100 but you should get the correct DNS address of your ISP and use that value as soon as possible.

14. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

### 3.2.4 Windows Me PCs

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.

2. Double-click the Network and Dial-up Connections icon.

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

   The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add...**.

5. In the Select Network Component Type dialog box, select **Protocol**, and then click **Add...**.

6. Select **Microsoft** in the Manufacturers box.

7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.

   You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
8. If prompted, click OK to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the SAR110:

9. In the Control Panel, double-click the Network and Dial-up Connections icon.

10. In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.

11. In the Network Properties dialog box, select TCP/IP, and then click Properties.

12. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Specify an IP address. Enter a suitable IP address for the PC e.g. 192.168.7.2 (remember that each computer/device on an IP network must have its own, unique IP address). Use the subnet mask 255.255.255.0.

13. Then goto the tab labeled Gateway and set the router/default gateway address to the address of the SAR110 which is 192.168.7.1.

14. Next goto the DNS tab and enable DNS, enter a host name (can be anything you like) and then enter the DNS address as given to you by your ISP. Please note that you will need a DNS address. If you don’t know the DNS address for your ISP then you can, temporarily use the own from our ISP which is 212.50.160.100 but you should get the correct DNS address of your ISP and use that value as soon as possible.

15. Click OK twice to confirm and save your changes, and then close the Control Panel.

### 3.2.5 Windows 95, 98 PCs:

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

16. In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

17. Double-click the Network icon.

The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 24.

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

The Select Network Component Type dialog box displays.
19. Select **Protocol**, and then click **Add...**

The Select Network Protocol dialog box displays.

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

21. Click **OK** to return to the Network dialog box, and then click **OK** again.

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

22. Click **OK** to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the SAR110:

23. Open the Control Panel window, and then click the Network icon.

24. Select the network component labeled TCP/IP, and then click **Properties**.

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

25. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Specify an IP address**. Enter a suitable IP address for the PC e.g. 192.168.7.2 (remember that each computer/device on an IP network must have it’s own, unique IP address). Use the subnet mask 255.255.255.0.

26. Then goto the tab labeled Gateway and set the router/default gateway address to the address of the SAR110 which is 192.168.7.1.

27. Next goto the DNS tab and enable DNS, enter a host name (can be anything you like) and then enter the DNS address as given to you by your ISP. Please note that you will need a DNS address. If you don’t know the DNS address for your ISP then you can, temporarily use the own from our ISP which is 212.50.160.100 but you should get the correct DNS address of your ISP and use that value as soon as possible.

28. Click **OK** twice to confirm and save your changes.

You will be prompted to restart Windows.

29. Click **Yes**.
3.2.6 Windows NT 4.0 workstations:

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

1. In the Windows NT task bar, click the Start button, point to Settings, and then click Control Panel.

2. In the Control Panel window, double click the Network icon.

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

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

5. In the Select Network Protocol dialog box, select TCP/IP, and then click OK.
   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

6. Click Yes to continue, and then click OK if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the SAR110:

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 Specify an IP address. Enter a suitable IP address for the PC e.g. 192.168.7.2 (remember that each computer/device on an IP network must have its own, unique IP address). Use the subnet mask 255.255.255.0. Then set the router/default gateway address to the address of the SAR110 which is 192.168.7.1. Next enter the DNS address as given to you by your ISP. Please note that you will need a DNS address. If you don’t know the DNS address for your ISP then you can, temporarily use the own from our ISP which is 212.50.160.100 but you should get the correct DNS address of your ISP and use that value as soon
as possible. A list of common DNS values is given later in the manual appendices.

11. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

### 3.2.7 Apple Mac:


![Image of manual TCP setup for Apple Mac](image)

2. Enter a suitable IP address (e.g. 192.168.7.2) and the netmask as shown above and click on **Apply Now**.

3. Now enter the IP address of the router in ‘Router’ box.
4. You also need to enter an address for your 'Domain Name Server'. Ideally you should get the DNS address to use from your ISP. However, if you don’t know the ISPs’ DNS address then you can temporarily use the address 212.50.160.23. Add the DSN address to the Domain Name Server list. A list of common DNS values is given later in the manual appendices.

5. That’s all you should have to do. Click on Apply Now and your new settings should be set.

Note: Your computers must have IP addresses that place them in the same subnet as the SAR110'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 accordingly.

3.3 Part 3 — Quick Configuring the SAR110

In Part 3, you log into the program on the SAR110 and configure basic settings for your Internet connection. Your ISP should provide you with the necessary information to complete this step.

3.3.1 Logging in to the SAR110 Quick Configuration Page

The SAR110 provides a preinstalled software program called Configuration Manager which enables you to configure the operation of the device via your Web browser. The settings that you
are most likely to need to change before using the device are grouped onto a single Quick Configuration page.

Follow these instructions to configure the device settings:

At any computer connected to the SAR110 via Ethernet, open your Web browser, and type the following URL in the address/location box:

192.168.7.1

When you press <Return>, a login screen displays, as shown below.

Enter your configuration user name and password, and then click OK.

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

Default User Name: DSL
Default Password: DSL

The page shown below should then display (see Appendix 26, “Appendix C Troubleshooting,” if you receive an error message or the page does not display).
If you are unsure of the existing set-up on the SAR110 e.g. you have a half completed or faulty set-up already configured then you are advised to clear and reset the configuration. To do this click on Admin,

Now click on 'Commit & Reboot',

---

Chapter 3. Quick Start Solwise SAR110 ADSL Ethernet Router User's Guide
Now select Reboot From Default Configuration (under Reboot Mode) and then click on Reboot.

Now wait about 30 seconds before clicking on Home; the status page should then display again.

To enter your configuration click on the Quick Configuration link at the top of the Home/status screen:
The fields are described in the table below and after this table specific settings are shown for BT and KC phone lines:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM Interface</td>
<td>Select the ATM interface you want to use (usually atm-0). You system may be configured with more than one ATM interface if you are using different types of services with your ISP.</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>This setting enables or disables the SAR110. When set to “No”, the device cannot be used to provide Internet connectivity for your network. Set it to “Yes” now, if necessary.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>This setting determines the type of data link your ISP uses to communicate with your ADSL/Ethernet router. Contact them to determine the appropriate setting: For a BT phone line you set this to PPPoA VC-MUX. For a KC phone line you set this to PPPoA LLC.</td>
</tr>
<tr>
<td>VCI and VPI</td>
<td>These values are provided by your ISP and determine the unique path your connection uses to communicate with your ISP: For a BT phone line you set VPI to 0 and VCI to 38. For a KC phone line you set VPI to 1 and VCI to 50.</td>
</tr>
<tr>
<td>Bridge</td>
<td>This setting enables or disables bridging between the SAR110 and your ISP. Your ISPs may also refer to this using “RFC 1483” or “Ethernet over ATM”. This setting should be left as disabled for normal, PPPoA UK use.</td>
</tr>
<tr>
<td>IGMP</td>
<td>This setting enables or disables the Internet Group Management Protocol, which some ISPs use to perform remote configuration of your device. As of time of writing no UK ISP’s support IGMP so you can leave this as disabled.</td>
</tr>
<tr>
<td>IP Address and Subnet Mask</td>
<td>If your ISP has assigned a public IP address to your LAN, enter the address and the associated subnet mask in the boxes provided. Note: please refer to the section in “How to…” concerning multiple IP setup before changing this entry.</td>
</tr>
<tr>
<td>Default Route</td>
<td>When enabled, this setting specifies that the IP address specified above will be used as the default route for your LAN. Whenever, one of your LAN computers</td>
</tr>
</tbody>
</table>
attempts to access the Internet, the data will be sent via the WAN interface. For normal UK operation this should be set to enabled.

**Gateway**
Specify the IP address that identifies the ISP server through which your Internet connection will be routed. Normally this should be left as 0.0.0.0.

**Primary/Secondary DNS Server**
Enter the Primary and Secondary DNS addresses provided by your ISP. If you selected Auto Discovery + User Configured, you are not required to enter addresses here; they will be used in addition to any addresses discovered automatically.

**User Name and Password**
Enter the username and password you use to log in to your ISP. (Note: this is different from the information you used to log in to Configuration Manager.) Please note, if your ISP DOESN'T provide you with a login password you MUST still enter something in this field.

Now enter the configuration required for your ISP set-up:

**For a BT phone line…**

- **ATM Interface:** 0
- **Operation Mode:** Yes
- **Encapsulation:** PPPoA VC-Mux
- **VPI:** 0
- **VCI:** 38
- **Bridge:** Disabled
- **IGMP:** Disabled
- **IP Address:** 0.0.0.0
  (assumes WAN IP assigned by ISP, LEAVE as 0.0.0.0!)

**For a KC phone line…**

- **ATM Interface:** 0
- **Operation Mode:** Yes
- **Encapsulation:** PPPoA LLC
- **VPI:** 1
- **VCI:** 50
- **Bridge:** Disabled
- **IGMP:** Disabled
- **IP Address:** 0.0.0.0
  (assumes WAN IP assigned by ISP, LEAVE as 0.0.0.0!)
Chapter 3. Quick Start

Solwise SAR110 ADSL Ethernet Router User’s Guide

When finished customizing these settings, click Submit.

The settings are now in effect; however, if you reboot or if the power is disconnected, your settings will be lost. In step 3, you save the changes to permanent memory:

Finally you need to modify this new ppp connection to do normal UK CHAP authentication (this option is not offered when doing setup by Quick Configuration.

Click on ‘Home’ to display the main screen again…
You should now save (Commit) the new settings and then reboot the router. To do this click on Admin,

Now click on ‘Commit & Reboot’,

Now click on Commit and wait for the saved message to appear,

Then click on Reboot
Now wait until the ADSL light stops flashing (assuming the ADSL line is connected and operational – otherwise wait for about 30 seconds) and then click on Home.

The main status page should then display.

First of all check the DSL, Operational Status. It should be green with the message Showtime/Data - this means you are successfully connected to the ADSL line.

Next check the entry ppp-0 in WAN Interfaces. The Status should be green and also the IP Address, Mask, and Gateway should have values entered (i.e., not 0.0.0.0).
IF YOU CANNOT SEE A VALID WAN IP ADDRESS THEN PLEASE GO TO APPENDIX C TO TROUBLESHOOT THE CONNECTION.

You are now finished customizing basic settings. The next Chapter covers the configuration settings in more details.
3.3.2 Default Router Settings

In addition to handling the DSL connection to your ISP, the SAR110 ADSL/Ethernet router can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

Table 1 lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review the settings in Table 1 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>
<thead>
<tr>
<th>Option</th>
<th>Default Setting</th>
<th>Explanation/Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP (Dynamic Host Configuration Protocol)</td>
<td>DHCP server disabled</td>
<td>If you enable DHCP then the SAR110 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. See below for an explanation of the DHCP service.</td>
</tr>
<tr>
<td>NAT (Network Address Translation)</td>
<td>napt rule enabled</td>
<td>Your computers’ private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See below for a description of the NAT service.</td>
</tr>
<tr>
<td>LAN Port IP Address</td>
<td>Static IP address: 192.168.7.1 subnet mask: 255.255.255.0</td>
<td>This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See below for instructions.</td>
</tr>
</tbody>
</table>
4 Basic for Configuration using the Web Interface

The SAR110 includes a preinstalled web configuration interface 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 SAR110 via the LAN port.

This chapter describes how to use the Configuration Manager.

### 4.1 Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on the SAR110. To access the program, you need the following:

- A PC or laptop connected to the LAN port on the device as described in the Quick Start chapter.
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions.

You can access the program from any computer connected to the SAR110 via the LAN port.

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

   [http://192.168.7.1](http://192.168.7.1)

   These are the predefined IP addresses for the LAN port on the SAR110.

A login screen displays, as shown in Figure 5.

![Figure 5. Login Screen](image)
2. Enter your user name and password, and then click **OK**.

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

- **Default User Name:** DSL
- **Default Password:** DSL

You can change the password at any time (see Changing Your Login Password later on). The user name cannot be changed.

The System View page on the Home tab displays each time you log into the program (shown above).

### 4.2 Functional Layout

Configuration Manager tasks are grouped into categories, which you can access by clicking the tabs at the top of each page. Each tab displays the available tasks horizontally the top of the page. You can click on these to display the specific configuration options.

A separate page displays for each task in the task bar. The left-most task displays by default when you click on a new tab. The same task may appear in more than one tab, when appropriate. For example, the LAN Config task displays in both the LAN tab and the Routing tab.

#### 4.2.1 Commonly used buttons

The following buttons are used throughout the application.

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Submit" /></td>
<td>Stores in temporary system memory any changes you have made on the current page. See “Committing your changes” for instructions on storing changes permanently.</td>
</tr>
</tbody>
</table>
4.3 The Home Tab and System View Table

The System View page displays when you first access the program. This page is one of two options available in the Home tab (the other is the Quick Start page, as described above).

The System View table provides a snapshot of your system configuration, and provides links to the software pages that enable you to configure each setting (if available). The following table describes each section of the system view table.

| Table Heading | Description |
### Table Heading | Description
---|---
**Device** | Displays basic information about the SAR110 hardware and software versions, the system uptime (since the last reboot), and the preconfigured operating mode.

**DSL** | Displays performance statistics for the DSL line. You can click **DSL** in WAN tab to display additional DSL settings, which are described below.

**WAN Interfaces** | Displays the software name(s) and various settings for the device interfaces that communicate with your ISP via DSL. Although you only have one physical DSL port, multiple software-defined interfaces can be configured to use it. See the ATM VCC, PPP, EOA, and IPoA chapter, respectively for more information about the interfaces defined on your system.

**LAN Interfaces** | Displays the software names and various settings for the device interfaces that communicate directly with your network. These typically include an Ethernet interface named **eth-0**. For information on modifying properties of these interfaces, see below.

**Services Summary** | Displays the following services that the SAR110 performs to help you manage your network:
- Translating private IP addresses to your public IP address (NAT, see Chapter 8).
- Setting up filtering rules that accept or deny incoming or outgoing data. (IP Filter, see Chapter 18).
- Enabling router-to-router communication (RIP, see Chapter 9).
- Dynamic assignment or receipt of IP information (DHCP, see Chapter 7).
- Message forwarding based on Internet Group assignment (IGMP, not configurable).

### 4.4 Changing the System Date and Time

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

*Note* Changing the SAR110 date and time does not affect the date and time on your PCs.

Follow these instructions to change the date and time:

1. At the bottom of the System View page, click **Modify**.
The System – Modify page displays in a separate browser window:

![System - Modify Page](image)

2. Use the drop-down lists to select a new date and time.

3. Click [Submit].

A page displays to confirm your change.

4. Click [Close] to return to the System View page.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click [Commit] to save your changes to permanent memory.

### 4.5 Changing Your Login Password

The first time you log into the Configuration Manager, you use the default user ID and password (*root* and *root*). The system allows only one user ID and password. Only the password can be changed.

*This user ID and password is only used for logging into the Configuration Manager; it is not the same as the login you may use to connect to your ISP (described in Chapter 12).*
To change the Configuration Manager login password:

1. Click the Admin tab.

   The User Password Configuration page displays by default.

   ![User Password Configuration Page](image)

   Figure 8. User Password Configuration Page

2. To change the standard user password click on the pencil under Action

   ![User Config - Modify](image)

   User Configuration Modification

<table>
<thead>
<tr>
<th>User ID:</th>
<th>DSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old Password:</td>
<td></td>
</tr>
<tr>
<td>New Password:</td>
<td></td>
</tr>
<tr>
<td>Confirm New:</td>
<td></td>
</tr>
</tbody>
</table>

   Copyright © 2001-2002 GlobespanVirata, Inc. All rights reserved.

3. Type your current password in the Old Password text box.

4. Type the new password in the New Password text box and again in the Confirm New text box.

   The password can be up to eight ASCII characters long. When logging in, you must type the new password in the same upper and lower case characters that you use here.

5. Click Submit.
6. Click the Admin tab, and then click Commit & Reboot in the task bar.

7. Click Commit to save your changes to permanent memory.

### 4.6 Committing Your Changes and Rebooting the Device

#### 4.6.1 Committing your changes

Whenever you use the Configuration Manager to change system settings, the changes are initially placed in temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

To save your changes for future use, you can use the commit function. This function saves your changes from RAM to permanent storage (called flash memory).

**Note**

Submitting changes activates them immediately, but saves them only until the device is reset or powered down. Committing changes saves them permanently.

Follow these steps to commit changes to permanent storage.

1. Click the Admin tab, and then click Commit & Reboot in the task bar.

   The Commit & Reboot page displays:

   ![Commit & Reboot Page](image)

   **Figure 9. Commit & Reboot Page**

2. Click Commit. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)

   The changes are saved to permanent storage.

   The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions below).

#### 4.6.2 Rebooting the device using Configuration Manager

To reboot the device, display the Commit & Reboot page, select the appropriate reboot mode from the drop-down menu, and then click Reboot.

You can select from the following three options when rebooting:
### Option | Description
--- | ---
Reboot from Last Configuration | Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration | Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Default Configuration | Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.
5 Setting IP Properties for the LAN-side Interfaces

This chapter describes how to configure IP properties the interfaces on the ADSL/Ethernet router that communicate with your LAN computers.

5.1 Configuring the LAN IP Address

The LAN IP address identifies the LAN port (eth-0) as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN.

A network node can be thought of as any interface where a device connects to the network, such as the SAR110’s LAN port and the network interface cards on your PCs. See Appendix 24 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.

If your network uses a DHCP server (other than the ADSL/Ethernet router) to assign IP addresses, you can configure the device to accept and use a LAN IP address assigned by that server. Similarly, if your ISP performs DHCP serving for your network, you can configure the device to accept an IP address assigned from the ISP’s server. In this mode, the ADSL/Ethernet router is considered a DHCP client of your (or your ISP’s) DHCP server.

The SAR110 itself can function as a DHCP server for your LAN computers, as described below, but not for its own LAN port.

Follow these steps to change the default LAN IP address or to configure the LAN port as a DHCP client.

1. Log into Configuration Manager, and then click the LAN tab. The LAN Configuration page displays, as shown in Figure 10.
Figure 10. LAN Configuration Page
The LAN Configuration table displays the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Mode</strong></td>
<td>The preconfigured mode for your device, such as Routing or Bridging mode. This setting is not user-configurable.</td>
</tr>
<tr>
<td><strong>LAN IP Address</strong></td>
<td>The IP address your computers use to identify the device’s LAN port. Note that the public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN (ADSL) port on your ADSL/Ethernet router to the Internet.</td>
</tr>
<tr>
<td><strong>LAN Network Mask</strong></td>
<td>The LAN Network mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network. Your device is preconfigured with a default network mask of 255.255.255.0.</td>
</tr>
<tr>
<td><strong>Use DHCP</strong></td>
<td>Use this setting if you want device to accept LAN IP information assigned dynamically from another DHCP server. If the server is on your network, click Local. If the server is on your ISP's network, click Remote. The SAR110 cannot act as a DHCP server for its own LAN port.</td>
</tr>
</tbody>
</table>

2. Enter a LAN IP address and network mask, or click the DHCP Enable radio button.

- **Entering a fixed address:** If you are using routing services on your LAN such as DHCP and NAT, you will want to assign a fixed LAN IP address and mask. This ensures that your LAN computers have a fixed address that they use to communicate with the device.

  The IP address you assign must be on the same subnet as your LAN computers that connect to this port (that is, the network ID portion of their IP addresses and their subnet masks must be the same). See Appendix 24 for an explanation of IP addresses and network masks.

  You may need to update the DHCP configuration so that the addresses that the DHCP server dynamically assigns to your computers are on the same subnet as the new LAN IP address. See Chapter 7 for instructions on changing the pool of dynamically assigned addresses. In addition, if you change the DHCP pool, you will also need to update the NAT configuration so the new IP addresses are translated properly. See Chapter 8 for instructions on NAT.

- **Enabling DHCP:** If another computer on your LAN provides DHCP services for your network, you can click the Use DHCP checkbox to enable the LAN port to accept a dynamically assigned address from the server.

  When you click the Enable radio button, the LAN Network Mask field will be dimmed (made unavailable for entry). The LAN IP Address field will remain editable, however. The address that you specify here will be used as a
requested IP address from the DHCP server. This is referred to as a "Configured IP Address" in the program. If the configured IP address is not available from the DHCP server, the server will distribute another address to the LAN port. Even if another number is assigned, the same configured IP address will continue to display in this field.

For a description of how DHCP works, see Chapter 7.

3. Click **Submit**.
   - If you were using an Ethernet connection for the current session, and changed the IP address, the connection will be terminated.
   - If you enabled the DHCP service, the ADSL/Ethernet router will initiate a request for an IP address from your LAN's DHCP server. Assuming a different IP address is assigned, your current 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 chapter, "Part 2 — Configuring Your Computers," for instructions.

5. Log into Configuration Manager by typing the new IP address in your Web browser’s address/location box.
   If you enabled DHCP, you may need to check the DHCP server on your LAN to determine the IP address actually assigned to the LAN port.

6. If the new settings work properly click the Admin tab, and then click **Commit & Reboot** in the task bar.

7. Click **Commit** to save your changes to permanent memory.
6 Viewing System IP Information and Performance Statistics

The interfaces on the SAR110 that communicate with other network and Internet devices are identified by unique Internet protocol (IP) addresses. You can use the Configuration Manager to view the list of IP addresses that your device uses, and to view other system and network performance data.

See Appendix 24 for a description of IP addresses and masks.

6.1 Viewing the SAR110’s IP addresses

To view the SAR110’s IP addresses, click the Routing tab, and then click **IP Addr** in the task bar. The IP Address Table page displays, as shown in Figure 11:

**Figure 11. IP Address Table Page**

The table lists the IP addresses, network masks (“Net Mask”), and interface names (“IF Name”) for each of its IP-enabled interfaces.

The listed IP addresses may include:

- The IP address of the device’s LAN (Ethernet) port, called **eth-0**. See Chapter 5 for instructions on configuring this address.
- The IP address of the WAN (ADSL line) interface, which your ISP and other external devices use to identify your network. It may be identified in the Configuration Manager by the names **ppp-0** or **eoa-0**, or **ipoa-0**, depending on the protocol your device uses to communicate with your ISP. Your ISP may assign the same address each time, or it may change each time you reconnect.
- The “loopback” IP address, named **lo-0**, of 127.0.0.1. This special address enables the device to keep any data addressed directly to it, rather than route the data through the WAN or LAN ports.
If your device has additional IP-enabled interfaces, the IP addresses of these will also display.

### 6.2 Viewing IP Global Statistics

You can view statistics on the processing of Internet protocol packets (a packet is a collection of data that has been bundled for transmission). 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 global IP statistics, click [Global Stats] on the IP Address Table page. Figure 12 shows the IP Global Statistics page:

![IP Global Statistics](image)

**Figure 12. IP Global Statistics Page**
To display updated statistics showing any new data since you opened the page, click "Refresh".
7 Configuring Dynamic Host Configuration Protocol

You can configure your network and SAR110 to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides an overview of DHCP and instructions for implementing it on your network.

7.1 Overview of DHCP

7.1.1 What is DHCP?

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

When you enable DHCP on a network, you allow a device — such as the SAR110 or a router located with your ISP — 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 used the Quick Start 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 SAR110.

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

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

7.1.2 Why use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from a central computer. Without DHCP, you would have to configure each computer separately with IP addresses and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.
7.1.3 SAR110 DHCP modes

The device can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

- If you configure the device as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation service, so that the private addresses can be translated to your public IP address on the Internet. Both DHCP server and NAT are enabled in the default configuration.

- If your ISP performs the DHCP server function for your network, then you can configure the device as a DHCP relay agent. When the SAR110 receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.

- If you have another PC or device on your network that is already performing the DHCP server function, then you can configure the LAN port on the SAR110 to be a DHCP client of that server (as are your PCs). This configuration is not discussed in this chapter. See Chapter 5 for instructions.

![Note]

You can input settings for both DHCP server and DHCP relay mode, and then activate either mode at any time. De-activated settings are retained for your future use.
7.2 Configuring DHCP Server

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.7.3 through 192.168.7.34 (subnet mask 255.255.255.0). To change this range of addresses, see “Viewing, modifying, and deleting address pools” below.

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

1. Open the Windows Control Panel and display the computer’s Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). For detailed instructions, see the Quick Start chapter, "Part 2 — Configuring Your Computers.'

Next, you define the pools of IP addresses you want to make available for distribution to your computers. These addresses can be multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. (LAN administrators often create private IP addresses for use only on their networks. See “Overview of NAT” below.)

2. Log into Configuration Manager, click the LAN tab, and then click DHCP Server in the task bar.

   The DHCP Server Configuration page displays:

   ![DHCP Server Configuration](image)

   **Figure 13. DHCP Configuration Page**

   Each pool you create displays in a row on the table on this page.

   You can create up to eight pools; however, most users will need to create only one for their LAN.

3. To add an IP address pool, click **Add**.

   The DHCP Server Pool – Add page displays.
### DHCP Server Pool – Add

<table>
<thead>
<tr>
<th>DHCP Pool Information</th>
<th>Start IP Address: 192.168.51.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>End IP Address: 192.168.51.254</td>
</tr>
<tr>
<td></td>
<td>Mac Address: 00:00:00:00:00</td>
</tr>
<tr>
<td></td>
<td>Net Mask: 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>Domain Name: PoolName</td>
</tr>
<tr>
<td></td>
<td>Gateway Address: 192.168.51.239</td>
</tr>
<tr>
<td></td>
<td>DNS Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>SDNS Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>SMTP Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>POP3 Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>NNTP Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>WWW Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>IRC Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>WINS Address: 0 0 0 0</td>
</tr>
<tr>
<td></td>
<td>SWINS Address: 0 0 0 0</td>
</tr>
</tbody>
</table>

*Figure 14. DHCP Server Pool – Add Page*
4. Enter the **Start IP Address**, **End IP Address**, **Net Mask**, and **Gateway Address** fields are required; the others are optional. The following table describes each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start/End IP Addresses</strong></td>
<td>Specify the lowest and highest addresses in the pool.</td>
</tr>
<tr>
<td><strong>Mac Address</strong></td>
<td>Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network.) If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.</td>
</tr>
<tr>
<td><strong>Net Mask</strong></td>
<td>Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer). For a description of network masks and LAN network masks, see Appendix 24. You can use the network mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (called a subnet).</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>A user-friendly name that refers to the group of computers (subnet) that will be assigned addresses from this pool.</td>
</tr>
<tr>
<td><strong>Gateway Address</strong></td>
<td>The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the IP address that the computers first contact to communicate with the Internet. Typically, it is the device’s LAN port IP address. See “Hops and gateways” below for an explanation of gateway addresses.</td>
</tr>
<tr>
<td><strong>DNS/SDNS Address</strong></td>
<td>The IP address of the Domain Name System server and Secondary Domain Name System server to be used by computers that receive IP addresses from this pool. These DNS servers translate common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, these servers are located with your ISP.</td>
</tr>
</tbody>
</table>
### Chapter 7. Configuring Dynamic Host Configuration Protocol

**Solwise SAR110 ADSL Ethernet Router User’s Guide**

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP...SWINS</td>
<td>The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or Simple Mail Transfer Protocol, server which handles e-mail traffic). Contact your ISP for these addresses.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

A confirmation page displays briefly to indicate that the pool has been added successfully. After a few seconds, the DHCP Server Pool – Add page displays with the newly added pool.

6. Follow the instructions in “Setting the DHCP Mode” below to set the DHCP mode to DHCP Server.

### 7.2.1 Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool

To view, modify, or delete an existing address pool, display the DHCP Server Configuration page, and click the icons in the corresponding row in the address pool table.

- To delete an IP address pool, click **Submit**, then **Delete** and commit your changes.
- To view details on an IP address pool, click **View Details**. A page displays with all the same information you entered when adding the pool.

To modify the domain name associated with an IP address pool, or to exclude addresses from the pool, click **Modify**. The DHCP Server Pool – Modify page displays, as shown in Figure 15.

#### DHCP Server Pool – Modify

<table>
<thead>
<tr>
<th>DHCP Pool Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start IP Address: 192.168.1.2</td>
</tr>
<tr>
<td>End IP Address: 192.168.1.10</td>
</tr>
<tr>
<td>Net Mask: 255.255.255.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Name:</th>
<th>Excluded IP Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No Excluded IP</td>
<td></td>
</tr>
<tr>
<td>192.168.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 15. DHCP Server Pool – Modify Page**

Excluded addresses are those that you have designated for fixed use with specific devices, or for some other reason do not want to make available to your network.
To exclude an address from distribution, type it in the fields provided and click [Add]. Click [Submit] after entering your changes. Be sure to use the Commit feature to save your changes to permanent memory, as described above.

### 7.2.2 Viewing current DHCP address assignments

When the SAR110 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, display the DHCP Server Configuration page, and then click [Address Table].

A page displays similar to that shown in Figure 16:

![Figure 16. DHCP Server Address Table Page](image)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>The address that has been leased from the pool.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td>The network mask associated with the leased address, which identifies the network ID and host ID portions of the address (see Appendix A).</td>
</tr>
<tr>
<td><strong>Mac Address</strong></td>
<td>A hardware ID for the device to which the number has been assigned.</td>
</tr>
<tr>
<td><strong>Pool Start</strong></td>
<td>The lower boundary of the address pool (provided to identify the pool from which the leased number came).</td>
</tr>
<tr>
<td><strong>Address Type</strong></td>
<td>Static or Dynamic. <em>Static</em> indicates that the IP number has been assigned permanently to the specific hardware device. <em>Dynamic</em> indicates that the number has been leased temporarily for a specified length of time.</td>
</tr>
<tr>
<td><strong>Time Remaining</strong></td>
<td>The amount of time left for the device to use the assigned address.</td>
</tr>
</tbody>
</table>
7.3 Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers’ home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the SAR110 contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

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

1. Open the Windows Control Panel and display the computer’s Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system). For detailed instructions, see the Quick Start chapter, "Part 2 — Configuring Your Computers."

Next, you specify the IP address of the DHCP server and select the interfaces on your network that will be using the relay service.

2. Log into the Configuration Manager, click the LAN tab, and then click DHCP Relay in the task bar.

The DHCP Relay Configuration page displays:

![Figure 17. DHCP Relay Configuration Page](image)

3. Type the IP address of your ISP’s DHCP server in the fields provided.

If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

4. If the interface named eth-0 is not already displaying, select it from the drop-down list and click Add.

The eth-0 interface specifies that your default Ethernet (LAN) interface is running DHCP relay for your LAN. Typically, this is the only interface you need to specify here. If the SAR110 has additional interfaces that you want to perform DHCP relay, you can select and add them.

(You can also delete an interface from the table by clicking " in the right column.)
5. Click **Submit**.

A page displays to confirm your changes, and then the program returns to the DHCP Relay Configuration page.

6. Follow the instructions in “Setting the DHCP Mode” below to set the DHCP mode to DHCP Relay.

### 7.4 Setting the DHCP Mode

You should set the DHCP mode only after you have configured DHCP relay or DHCP server settings. See “Configuring DHCP Server” or “Configuring DHCP Relay” above for additional instructions.

Follow these instructions to set the DHCP mode:

1. Click the LAN tab, and then click **DHCP Mode** in the task bar.

The DHCP Configuration page displays, as shown in Figure 18.

2. From the DHCP Mode drop-down list, choose **DHCP Server**, **DHCP Relay**, or **none**.

If you choose **none**, your LAN computers must be configured with static IP addresses.

3. Click **Submit**.

4. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

5. Click **Commit** to save your changes to permanent memory.
8 Configuring Network Address Translation

This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your device.

8.1 Overview of NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

A **private IP address** is created by a network administrator for use only on a LAN, whereas a **public IP address** is purchased from the Internet Corporation for Assigned Names and Numbers (ICANN) for use on the Internet. Typically, your ISP provides a public IP address for your entire LAN, and you define the private addresses for computers on your LAN.

In a typical NAT setup, your ISP provides you with a single public IP address to use for your entire network. Then, you assign each computer on your LAN a unique private IP address. (Or, you define a pool of private IP addresses for dynamic assignment to your computers, as described in Chapter 7.) On the SAR110, you set up a NAT rule to specify that whenever one of your computers communicates with the Internet, (that is, it sends and receives IP data packets) its private IP address—which is referenced in each packet—will be replaced by the LAN’s public IP address.

An **IP data packet** contains bits of data bundled together in a specific format for efficient transmission over the Internet. Such packets are the building blocks of all Internet communication. Each packet contains header information that identifies the IP address of the computer that initiates the communication (the **source IP address**), the port number that the router associates with that computer (the **source port number**), the IP address of the targeted Internet computer (the **destination IP address**), and other information.

When this type of NAT rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are actually originating from the computer assigned your public IP address (in this case, the SAR110).

The NAT rule could further be defined to disguise the source port in the data packet (i.e., change it to another number), so that outside computers will not be able to determine the actual port from which the packet originated. Data packets that arrive in response contain the public IP address as the destination IP address and the
disguised source port number. The SAR110 changes the IP address and source port number back to the original values (having kept track of the changes it made earlier), and then routes the packet to the originating computer.

NAT rules such as these provide several benefits:

- They eliminate the need for purchasing multiple public IP addresses for computers on your LAN. You can make up your own private IP addresses at no cost, and then have them translated to the public IP address when your computers access the Internet.
- They provide a measure of security for your LAN by enabling you to assign private IP addresses and then have these and the source port numbers swapped out before your computers access the Internet.

The type of NAT function described above is called network address port translation (napt). You can use other types, called flavors, of NAT for other purposes; for example, providing outside access to your LAN or translating multiple private addresses to multiple public addresses.

By default, NAT is enabled, with an napt rule configured that translates any private address on the LAN side to your ISP-assigned public IP address on the WAN side. (For a description of napt rules, see below.)

8.2 Viewing NAT Global Settings and Statistics

To view your NAT settings, log into Configuration Manager, click the Services tab. The NAT Configuration page displays by default, as shown in Figure 19.

![Figure 19. NAT Configuration Page](image-url)
The NAT Configuration page contains the following elements:

- The NAT Options drop-down list, which provides access to the Global Information page (shown by default), the NAT Rule Configuration page, and the NAT Translations page, which shows current translations.
- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays the following settings that apply to all NAT rule translations:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Idle Timeout (sec)</td>
<td>For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.</td>
</tr>
<tr>
<td>TCP Close Wait (sec)</td>
<td>For a NAT translation on data using the TCP protocol, after a communication session has been closed, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.</td>
</tr>
<tr>
<td>TCP Def Timeout (sec)</td>
<td>For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.</td>
</tr>
<tr>
<td>UDP Timeout (sec)</td>
<td>Same as TCP Idle Timeout, but for UDP packets.</td>
</tr>
<tr>
<td>ICMP Timeout (sec)</td>
<td>Same as TCP Idle Timeout, but for ICMP packets.</td>
</tr>
<tr>
<td>GRE Timeout (sec)</td>
<td>Same as TCP Idle Timeout, but for GRE packets.</td>
</tr>
<tr>
<td>Default Nat Age (sec)</td>
<td>For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.</td>
</tr>
<tr>
<td>NAPT Port Start/End</td>
<td>When an napt rule is defined, the source ports will be translated to sequential numbers in this range.</td>
</tr>
</tbody>
</table>

If you change any values, click **Submit**, and then click the Admin tab and commit your changes to permanent system memory.

You can click **Global Stats** to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one shown below.
### NAT Rule Global Statistics

#### Total NAT Sessions

<table>
<thead>
<tr>
<th>Type</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Translation Sessions</td>
<td>491</td>
</tr>
<tr>
<td>Number of FTP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of SNMP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of Real Audio ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of Remote-Command Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of L2TP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of MIRC ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of CUICME ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of H323 Q931 ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of H323 RAS ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of H323 H245 ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of H323 RTP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of CUSEME UDP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of PPTP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of RTSP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of Timbuktu ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of T120 ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of LDAP ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of SG1 Compcore ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of MSN Messenger ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of IKE ALG Sessions</td>
<td>0</td>
</tr>
<tr>
<td>Number of ESP ALG Sessions</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Translation Statistic

- Packets w/o Matching Translation Rules: 12 Packets
- Number Of In-Packets Translated: 9685 Packets
- Number Of Out-Packets Translated: 8279 Packets
- Number Of Fragments Processed: 0 Packets

#### Active NAT Sessions

<table>
<thead>
<tr>
<th>Type</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Translation Sessions</td>
<td>28</td>
</tr>
<tr>
<td>Active Rules</td>
<td>1</td>
</tr>
<tr>
<td>Active Session Using FTP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using SNMP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using Real Audio ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using Remote-Command-Session</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using L2TP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using MIRC ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using CUICME ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using H323 Q931 ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using H323 RAS ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using H323 H245 ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using H323 RTP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using CUSEME UDP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using PPTP ALG</td>
<td>0</td>
</tr>
<tr>
<td>Active Session Using RTSP ALG</td>
<td>0</td>
</tr>
</tbody>
</table>
Figure 20. NAT Rule Global Statistics Page

The table provides basic information for each NAT rule you have set up. You can click **Clear** to restart the accumulation of the statistics at their initial values.

### 8.3 Viewing NAT Rules and Rule Statistics

To view the NAT rules currently defined on your system, select **NAT Rule Entry** in the NAT Options drop-down list. The NAT Rule Configuration page displays, as shown in Figure 21.

Figure 21. NAT Rule Configuration Page

The NAT Rule Configuration table displays a row containing basic information for each rule. For a description of these fields, refer to the instructions for adding rules given below.

From the NAT Rule Configuration page, you can click **Add** to add a new rule, or use the icons in the right column to delete (🗑️) or view details on (🔍) a rule.

To view data on how often a specific NAT rule has been used, click **Stats** in the Action(s) column. A page similar to the one show in Figure 22 displays:

Figure 22. NAT Rule Statistics Page

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can
To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **NAT Translations** from the NAT Options drop-down list. The NAT Translations page displays, as shown in Figure 23:

**Figure 23. NAT Translations Page**

For each current NAT translation session, the table contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trans Index</td>
<td>The sequential number assigned to the IP session used by this NAT translation session.</td>
</tr>
<tr>
<td>Rule ID</td>
<td>The ID of the NAT rule invoked.</td>
</tr>
<tr>
<td>Interface</td>
<td>The device interface on which the NAT rule was invoked (from the rule definition).</td>
</tr>
<tr>
<td>Protocol</td>
<td>The IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.</td>
</tr>
<tr>
<td>Alg Type</td>
<td>The Application Level Gateway (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).</td>
</tr>
<tr>
<td>NAT Direction</td>
<td>The direction (incoming or outgoing) of the translation (from the port definition).</td>
</tr>
<tr>
<td>Entry Age</td>
<td>The elapsed time, in seconds, of the NAT</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
| | translation session.

You can click ± in the Action(s) column to view additional details about a NAT translation session, as shown in Figure 24.

![NAT Translation - Details](image)

**Figure 24. NAT Translation – Details Page**

In addition to the information displayed in the NAT Translations table, this table displays the following for the selected current translation sessions:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translated InAddress</td>
<td>The public IP address to which the private IP address was translated.</td>
</tr>
<tr>
<td>In Address</td>
<td>The private IP address that was translated.</td>
</tr>
<tr>
<td>Out Address</td>
<td>The IP address of the outside destination (web, ftp site, etc.)</td>
</tr>
<tr>
<td>In/Out Packets</td>
<td>The number of incoming and outgoing IP packets that have been translated in this translation session.</td>
</tr>
<tr>
<td>In Ports</td>
<td>The actual port number corresponding to the LAN computer.</td>
</tr>
<tr>
<td>Out Ports</td>
<td>The port number associated with the destination address.</td>
</tr>
<tr>
<td>Translated In Ports</td>
<td>The port number to which the LAN computer’s actual port number was translated.</td>
</tr>
</tbody>
</table>
8.5 Adding NAT Rules

This section explains how to create rules for the various NAT flavors.

*Note*

You cannot edit existing NAT rules. To change a rule setup, delete it and add a new rule with the modified settings.

One of the exciting features of the SAR110 router is its very powerful port forwarding rules. In all the 110 has six different types of port forwarding. Full details covering port forwarding are given below or in the online web help. For those users familiar with other manufacturers router products, 'normal' port forwarding is covered by the RDR port rule (see below).

8.5.1 The napt rule: Translating between private and public IP addresses

Follow these instructions to create a rule for translating the private IP addresses on your LAN to your public IP address. This type of rule uses the NAT flavor napt, which was used in your default configuration. The napt flavor translates private source IP addresses to a single public IP address. The napt rule also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page. The Introduction to NAT on describes how the napt rule works.

1. Click the NAT tab, then select **NAT Rule Entry** from the NAT Options drop-down list on the right side of the page.

   The NAT Rule entry page displays a row for each currently configured NAT rule.

2. Click **Add** to display the NAT Rule – Add page.

   The NAPT flavor displays by default in the Rule Flavor drop-down list. The NAT Rule – Add page displays, as shown in Figure 25.
3. Enter a Rule ID.

The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority rules. It is recommended that you select rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules.

Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

4. From the IF Name drop-down list, select the interface on the device to which this rule applies.

Typically, NAT rules are used for communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named ppp-0 or eoa-0) to connect your LAN to your ISP, it is the usual IF Name selection.

5. In the Local Address From field and Local Address To fields, type the starting and ending IP addresses, respectively, of the range of private address you want to be translated. Or, type the same address in both fields to specify a single value.

To specify that data from all LAN addresses should be translated, type 0 (zero) in each From field and 255 in each To field.

If you have several non-sequential private addresses, you can create an additional napt rule for each address.

These addresses should correspond to private addresses already in use on your network (either assigned statically to
your PCs, or assigned dynamically using DHCP, as discussed in the Quick Start).

6. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.

If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on other PPP interfaces.

If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

7. When you have completed entering all information, click **Submit**.

A page displays to confirm the change.

8. Click **Close** to return to the NAT Configuration page.

The new rule should display in the NAT Rule Configuration table.

9. Ensure that the Enable radio button is selected, and then click **Submit**.

A page displays to confirm your changes.

10. Click the Admin tab, and then click **Commit and Reboot** in the task bar.

11. Click **Commit** to save your changes to permanent memory.

### 8.5.2 The rdr rule: Allowing external access to a LAN computer

You can create an rdr rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer’s private IP address is translated to your public IP address in all incoming and outgoing data packets.

The RDR rule will be the type of port rule that users of other routers might be more familiar with: an rdr rule would be the type of rule you could use to forward, for example, incoming traffic to a local web server.

**Note**

Without an rdr rule (or bimap rule described below), the SAR110 blocks attempts by external computers to access your LAN computers.

The following example illustrates using the rdr rule to provide external access to your web server:
Your ADSL/Ethernet router receives a packet containing a request for access to your Web server. The packet header contains the public address for your LAN as the destination IP address, and a destination port number of 80. Because you have set up an rdr rule for incoming packets with destination port 80, the device recognizes the data as a request for Web server access. The device changes the packet's destination address to the private IP address of your Web server and forwards the data packet to it.

Your Web server sends data packets in response. Before the ADSL/Ethernet router forwards them on to the Internet, it changes the source IP address in the data packets from the Web server's private address to your LAN's public address. To an external Internet user then, it appears as if your Web server uses your public IP address.

Figure 26 shows the fields used to establish an rdr rule:

![Figure 26. NAT Rule – Add Page (rdr Flavor)](image)

Follow these instructions to add an rdr rule (see steps 1-4 under "The napt rule" for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **RDR** as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. Select a protocol to which this rule applies, or choose **ALL**.
This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the same private IP address, or the lowest and highest addresses in a range:
   - If you type the same IP address in both fields, incoming traffic that matches the criteria you specify in steps 5 and 6 will be redirected to that IP address.
   - If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers to help ensure efficient network performance.
   These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start, Part 2).

5. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.
   If you have multiple WAN (PPP) interfaces, this rule will not be enforced for data that arrives on other PPP interfaces. This rule will not be enforced for data that arrives on WAN interfaces not specified here.
   If you have multiple WAN interfaces and want the rule to be enforced on more than one of them (or all), type the starting and ending IP addresses of the range.

6. In the Destination Port From and Destination Port To fields, enter the port ID (or a range) that you expect to see on incoming packets destined for the LAN computer for which this rule is being created.
   Incoming traffic that meets this criteria will be redirected to the Local Port number you specify in the next field.
   To simplify matters, the common ports are listed and can be selected using the drop down lists. For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the well-known web server port number, 80. This setting serves as a filter; data packets not containing this port number would not be granted access to your local computer.

7. If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the Local Port field.
   This option translates the standard port number in packets destined for your LAN computer to the non-standard number
you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 here and 80 in the Destination Port fields. The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet can then be routed appropriately to the web server.

8. Follow steps 7-12 under “The napt rule” to submit your changes.

For example, to forward incoming port 80 traffic to a single local web server at address 192.168.7.20 enter the values as shown below and then click on Submit…. Finally save your configuration and then reboot.

8.5.3 The basic rule: Performing 1:1 translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like napt rules. However, unlike napt rules, basic rules do not also translate the port numbers in the packet header; they are passed through untranslated. Therefore, the basic rule does not provide the same level of security as the napt rule.

Figure 27 shows the fields used for adding a basic rule.
Follow these instructions to add an basic rule (see steps 1-4 under "The napt rule" for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **BASIC** as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

   You can create a basic rule for each specific address translation to occur. The range of addresses should correspond to private addresses already in use on your network, whether assigned statically to your PCs, or assigned dynamically using DHCP.

5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the pool of public IP addresses that the private addresses should be translated to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. Follow steps 7-12 under "The napt rule" to submit your changes.

8.5.4 The filter rule: Configuring a basic rule with additional criteria

Like the basic flavor, the filter flavor translates public and private IP addresses on a one-to-one basis. The filter flavor extends the capability of the basic rule. Refer to "The basic Rule" for a general description.

You can use the filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both.

Figure 28 shows the fields used to establish a filter rule.

---

**Figure 28. NAT Rule—Add Page (filter Flavor)**

Follow these instructions to add a filter rule (see steps 1-4 under "The napt rule" for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select FILTER as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. Select a protocol to which this rule applies, or choose ALL.
This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

The address (or range of addresses) should correspond to a private addresses (or addresses) already in use on your network. These may be assigned statically to your PCs or assigned dynamically using DHCP, as discussed in the Quick Start.

5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 4).

6. Specify a Destination Address or addresses, Destination Port (or ports), or both. You can specify a single value by entering that value in both fields.

- Specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range).
  
  If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network.

- Specify a destination ports (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.
  
  For example, if you do not specify a destination address, but specify a Destination Port From/To of 21, then this translation will occur on all accesses by your LAN to all external FTP servers. That is, when one of your LAN computers communicates with an external FTP server, the source IP address in the packet headers is changed to the public address, replacing the initiator's private IP address.

  Port number assignments are maintained in RFCs maintained by IANA. Common port numbers are given in drop down lists e.g.:

  21—FTP (file transfer protocol) server
  25—SMTP (simple mail transfer protocol) server
  80—HTTP (World Wide Web) server

- Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to
apply to accesses to the specified server type at the specified IP address or network.

7. Follow steps 7-12 under "The napt rule" to submit your changes.

8.5.5 The bimap rule: Performing two-way translations

Unlike the other NAT flavors, the bimap flavor performs address translations in both the outgoing and incoming directions.

In the incoming direction, when the specified SAR110 interface receives a packet with your public IP address as the destination address, this address is translated to the private IP address of a computer on your LAN. To the external computer, it appears as if the access is being made to the public IP address, when, in fact, it is communicating with a LAN computer.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN’s public IP address. To the rest of the Internet, it appears as if the data packet originated from the public IP address.

Bimap rules can be used to provide external access to a LAN device. They do not provide the same level of security as rdr rules, because rdr rules also reroute incoming packets based on the port ID. Bimap rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.

Figure 29 shows the fields used to establish a bimap rule.

Follow these instructions to add a bimap rule (see steps 1-4 under "The napt rule" for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select BIMAP as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. In the Local Address field, type the private IP address of the computer to which you are granting external access.
4. In the Global Address field, type the address that you want to serve as the publicly known address for the LAN computer.

5. Follow steps 7-12 under “The napt rule” to submit your changes.

8.5.6 The pass rule: Allowing specific addresses to pass through untranslated

You can create a pass rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.

![Figure 30. NAT Rule – Add Page (pass Flavor)](image)

The pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. In you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a pass rule with ID #1 through #4.

Follow these instructions to add a pass rule (see steps 1-4 under “The napt rule” for detailed instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select PASS as the Rule Flavor, and enter a Rule ID.

2. Select the interface on which this rule will be effective.

3. In the Local Address From and Local Address To fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

   If you want the pass rule to act on only one address, type that address in both fields.

4. Follow steps 7-12 under “The napt rule” to submit your changes.
9 Configuring DNS Server Addresses

9.1 About DNS

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

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

9.2 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 feature on the ADSL/Ethernet router and create an address pool that specify the DNS addresses to be distributed to the PCs. Refer to Chapter 7, “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 ADSL/Ethernet router (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the following section.

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

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

When performing DNS relay, the SAR110 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 PPP:** If the device uses a PPP connection to the ISP, the primary and secondary DNS addresses can be learned via the PPP protocol. To use this method, the "Use DNS" checkbox must be selected in the PPP interface properties. (See Chapter 13 for instructions on configuring your PPP interface. Note that you cannot change this property by modifying an existing PPP interface; you must delete the interface and recreate it with the new setting.)

  Using this option provides the advantage that you will not need to reconfigure the PCs or the ADSL/Ethernet router if the ISP changes their DNS addresses.

- **Configured on the ADSL/Ethernet router:** You can use the device's DNS feature to specify the ISP's DNS addresses. If the device also uses a PPP interface with the "Use DNS" property enabled, then these configured addresses will be used in addition to the two addresses learned through PPP. If "Use DNS" is not enabled, or if a protocol other than PPP is used (such as EoA), then these configured addresses will be used as the primary and secondary DNS addresses.

Follow these steps to configure DNS relay:

1. Configure the LAN PCs to use the ADSL/Ethernet router's LAN IP address as their DNS server address—by assigning the LAN IP address statically to each PC, or by inputting the LAN IP address or the address 0.0.0.0 as the DNS address in the DHCP server pool used by the PCs.

2. If using a PPP connection to the ISP, click the "Use DNS" check box so that the DNS server addresses it learns are used for DNS relay.

   Or, ...

If not using a PPP connection (or if you want to specify DNS addresses in addition to those learned through PPP), configure the DNS addresses on the ADSL/Ethernet router as follows:
a. Click the Services tab, and then click **DNS** in the task bar. The DNS Configuration page displays.

![Figure 31. DNS Configuration Page](image)

b. Type the IP address of the DNS server in an empty row and click **Add**.

You can enter only two addresses.

c. Click the **Enable** radio button, and then click **Submit**.

3. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

4. Click **Commit** to save your changes to permanent memory.

*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.*

**Note**

*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.*
10 Configuring IP Routes

You can use Configuration Manager to define specific routes for your Internet and network data. This chapter describes basic routing concepts and provides instructions for creating routes.

Note that most users do not need to define IP routes.

10.1 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 a computer uses to make these decisions.

10.1.1 Comparing IP routing to telephone switching

IP routing decisions are similar to those made by switchboards that handle telephone calls.

When you dial a long distance telephone number, you are first connected to a switchboard operated by your local phone service carrier. All calls you initiate go first to this main switchboard.

If the phone number you dialed is outside your calling area, the switchboard opens a connection to a higher-level switchboard for long distance calls. That switchboard looks at the area code you dialed and connects you with another switchboard that serves that area. This new switchboard, in turn, may look at the prefix in the number you dialed (the middle set of three numbers) and connect to a more localized switchboard that handles numbers with that prefix. This final switchboard can then look at the last four digits of the phone number to open a connection with the person or company you dialed.

In comparison, when your computer initiates communication over the Internet, such as viewing a web page connecting to a web server, the data it sends out includes the IP address of the destination computer (the "phone number"). All your outgoing requests first go to the same router at your ISP (the first "switchboard"). That router looks at the network ID portion of the destination address (the "area code") and determines which next router to send the request to. After several such passes, the request arrives at a router for the destination network, which then uses the host ID portion of the destination IP address (the local "phone number") to route the request to the appropriate computer. (The network ID and host ID portions of IP addresses are explained in Appendix 24.)

With both the telephone and the computer, all transactions are initially sent to the same switchboard or router, which serves as a gateway to other higher- or lower-level devices. No single device knows at the outset the eventual path the data will take, but each uses a specific part of the destination address/phone number to make a decision about which device to connect to next.
10.1.2 Hops and gateways

Each time Internet data is passed from one Internet address to another, it is said to take a hop. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a gateway. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company’s web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company’s web servers.

10.1.3 Using IP routes to define default gateways

IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined default gateway. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to its default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

10.1.4 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 SAR110 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 SAR110. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the Quick Start instructions, Part 2.)
- On the SAR110 itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described below.)

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.
10.2 Viewing the IP 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 SAR110’s routing table, click the Routing tab. The IP Route page displays by default, as shown in Figure 32:

**Figure 32. IP Route Table Page**

The IP Route Table displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.
The following table defines the fields in the IP Routing Table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Specifies the IP address of the destination computer. The destination can be specified as the IP address of a specific computer or an entire 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).</td>
</tr>
<tr>
<td>Netmask</td>
<td>Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix 24, for an explanation of network masks. The default gateway uses a netmask of 0.0.0.0.</td>
</tr>
<tr>
<td>NextHop</td>
<td>Specifies the next IP address to send data to when its final destination is that shown in the destination column.</td>
</tr>
<tr>
<td>IFName</td>
<td>Displays the name of the interface on the device through which data is forwarded to the specified next hop.</td>
</tr>
<tr>
<td>Route Type</td>
<td>Displays whether the route is direct or indirect. In a direct route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an indirect route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.</td>
</tr>
<tr>
<td>Route Origin</td>
<td>Displays how the route was defined. Dynamic indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled Local. Other routes can be created automatically (using RIP, as described in Chapter 9), or defined remotely through various network management protocols (LCL or ICMP).</td>
</tr>
<tr>
<td>Action</td>
<td>Displays an icon (🗑️) you can click on to delete a route.</td>
</tr>
</tbody>
</table>

10.3 Adding IP Routes

Follow these instructions to add an IP route to the routing table.

1. From the IP Route Table page, click [Add].

The IP Route – Add page displays, as shown in Figure 33.
2. Specify the destination, network mask, and gateway or next hop for this route.

For a description of these fields, refer to the table above.

To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Net Mask fields. Enter your ISP’s IP address in the Gateway/NextHop field.

Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click **Submit**.

4. On the confirmation page, click **Close** to return to the IP Route table page.

The IP Routing Table will now display the new route.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click **Commit** to save your changes to permanent memory.
11 Configuring the Routing Information Protocol

The SAR110 can be configured to communicate with other routing devices to determine the best path for sending data to its intended destination. Routing devices communicate this information using a variety of IP protocols. This chapter describes how to configure the SAR110 to use one of these, called the Routing Information Protocol (RIP).

11.1 RIP Overview

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP’s location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on autonomous networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

11.1.1 When should you configure RIP?

Most small home or office networks do not need to use RIP; they have only one router, such as the SAR110, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the SAR110). The SAR110 and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

11.2 Configuring the SAR110’s Interfaces with RIP

The following instructions describe how to enable RIP on the SAR110.
In order for the SAR110 to communicate with other devices using RIP, you must also enable the other devices to use the protocol. See the product documentation for those devices.

1. Log into the Configuration Manager, click the Services tab, and then click RIP in the task bar.

The RIP Configuration page displays, as shown in Figure 34.

![Figure 34. RIP Configuration Page](image)

The page contains radio buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

2. If necessary, change the Age and Update Time.

These are global settings for all interfaces that use RIP.

- **Age** is the amount of time in seconds that the device’s RIP table will retain each route that it learns from adjacent computers.
- **Update Time** specifies how frequently the SAR110 will send out its routing table to its neighbors.

3. In the IFName column, select the name of the interface on which you want to enable RIP.

For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

4. Select a metric value for the interface.

RIP uses a “hop count” as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.

For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others.
You can select any integer from 1 to 15.

5. Select a Send Mode and a Receive Mode.

The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

The Receive Mode setting indicates the RIP version(s) in which information must be passed to the SAR110 in order for it to be accepted into its routing table.

RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.

6. Click Add.

The new RIP entry will display in the table.

7. Click the Enable radio button to enable the RIP feature.

If you disable the RIP feature, the interface settings you have configured will remain available for future activation.

8. When you are finished defining RIP interfaces, click Submit.

A page displays to confirm your changes.

9. Click the Admin tab, and then click Commit & Reboot in the task bar.

10. Click Commit to save your changes to permanent memory.

You can delete an existing RIP entry by clicking in the Action column.

11.3 Viewing RIP Statistics

From the RIP Configuration page, you can click Global Stats to view statistics on attempts to send and receive route table data over RIP-enabled interfaces on the SAR110.
Figure 35. RIP Global Statistics Page

You can click **Clear** to reset all statistics to zero and **Refresh** to display any newly accumulated data.
12 Configuring the ATM VCC

As your LAN computers access the Internet via the SAR110, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called Asynchronous Transfer Mode (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This chapter describes how to configure the ATM virtual channel connection (VCC). The VCC properties define the path the SAR110 uses to communicate with your ISP over the ATM network.

12.1 Viewing Your ATM VC Setup

To view your current configuration, log into Configuration Manager, click the WAN tab, and then click ATM VCC in the task bar. The ATM VCC Configuration page displays, as shown in Figure 36.

![ATM VC Configuration](image)

*Figure 36. ATM VCC Configuration Page*
Chapter 12. Configuring the ATM VCC

The ATM VCC Configuration table displays the following fields (contact your ISP to determine these settings):

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.</td>
</tr>
<tr>
<td>Vpi, Vci, and Mux Type</td>
<td>These settings identify a unique ATM data path for communication between your ADSL/Ethernet router and your ISP.</td>
</tr>
<tr>
<td>Max Proto per AAL5</td>
<td>If you are using an AAL5-type of interface, this setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.</td>
</tr>
<tr>
<td>Actions</td>
<td>Displays an icon ( ) you can click on to delete the associated interface.</td>
</tr>
</tbody>
</table>

12.2 Adding ATM VCCs

You may need to create a VCC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VCC. Follow these instructions to add a VCC:

1. From the ATM VCC Configuration page, click Add.

The ATM VCC – Add page displays, as shown in Figure 37.

Figure 37. ATM VCC – Add Page
2. Select an interface name from the VCC Interface drop-down list.

3. Enter the VPI and VCI values assigned by your ISP, and select the mux type from the drop-down list.

4. Click Submit.

5. On the confirmation page, click to return to the ATM VCC Configuration page.

6. Click the Admin tab, and then click Commit & Reboot in the task bar.

7. Click Commit to save your changes to permanent memory.

The new interface should now display in the ATM VCC Configuration table.

You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VCC. See the instructions for configuring a PPP (Chapter 12), EoA (Chapter 14), or IPoA (Chapter 10) interfaces, depending on the type you use to communicate with your ISP.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.

### 12.3 Modifying ATM VCCs

Your device may already be preconfigured with the necessary ATM VCC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VCC values. Follow these instructions to modify a preconfigured VCC:

1. From the ATM VCC Configuration page, click in the Actions column for the interface you want to modify.

   The ATM VCC Interface – Modify page displays, as shown in Figure 37.
2. Enter the new VPI and VCI values, select the MUX type, or change the maximum number of protocols that the VCC can carry, as directed by your ISP.

You cannot modify the interface type over which an existing VCC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. Click [Submit].

4. On the confirmation page, click [Close] to return to the ATM VCC Configuration page.

5. Click the Admin tab, and then click [Commit & Reboot] in the task bar.

6. Click [Commit] to save your changes to permanent memory.

You can verify that the new settings work by attempting to access the Internet from a LAN computer. Contact your ISP for troubleshooting assistance.
13 Configuring PPP Interfaces

When powered on, the SAR110 initiates a connection through your DSL line to your ISP.

The point-to-point (PPP) protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password login
- Enabling the ISP to assign Internet information to the customer’s computers

Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

13.1 Viewing Your Current PPP Configuration

To view your current PPP setup, log into Configuration Manager, click the WAN tab, and then click PPP in the task bar. The PPP Configuration page displays, as shown in Figure 39.

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the SAR110 can be defined with more than one group of PPP settings. Each group of settings is called a PPP interface and is given a name, such as ppp-0, ppp-1, etc.
You can configure the following settings on the PPP Configuration page:

- **Inactivity TimeOut (mins):** The time in minutes that must elapse before a PPP connection times-out due to inactivity.
- **Ignore WAN to LAN traffic:** When enabled, data traffic traveling in the incoming direction—from the WAN port to the LAN port—will not count as activity on the WAN port; i.e., it will not prevent the connection from being terminated if inactive for the specified time.

The PPP Configuration Table displays the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The predefined name of the PPP interface.</td>
</tr>
<tr>
<td>VCC</td>
<td>The Virtual Channel Connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP. See Chapter 12 for more information.</td>
</tr>
</tbody>
</table>
| **IPF Type** | The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ):
  | - A public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.
  | - A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.
  | - The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. |
| Protocol  | The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPoE) or PPP-over-ATM (PPoA). |
| WAN IP    | The IP address currently assigned to your WAN (DSL) port by your ISP.                            |
| Gateway IP| The IP address of the server at your ISP that provides you access to the Internet. See "Hops and gateways" for a description of gateway addresses. |
| Default Route | Indicates whether the ADSL/Ethernet router should use the IP address assigned to this connection as its default route. Can be Enabled or Disabled. See Chapter 10 for an explanation of default routes. |
### 13. Configuring PPP Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use DHCP</td>
<td>When set to Enable, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With Use DHCP enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).</td>
</tr>
<tr>
<td>User DNS</td>
<td>When set to Enable, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the ADSL/Ethernet Router is configured to act as a DHCP Server for your LAN. When set to Disable, LAN hosts will use the DNS address(es) preconfigured in the DHCP pool (see &quot;Configuring DHCP Server&quot;) and in the DNS feature (see Chapter 9, &quot;Configuring DNS Server Addresses&quot;).</td>
</tr>
<tr>
<td>Oper. Status</td>
<td>Indicates whether the link is currently up or down or if a specific type of data exchange is under way (e.g., password authorization or DHCP).</td>
</tr>
<tr>
<td>Actions</td>
<td>You can use these icons to modify (-pencil), delete (trash), and view additional details on (窴) the PPP interface.</td>
</tr>
</tbody>
</table>

#### 13.2 Viewing PPP Interface Details

When you click (窴) to view additional details, the PPP Interface - Detail page displays, as shown in Figure 40.
Chapter 13. Configuring PPP Interfaces

In addition to the properties defined above, the Detail page displays these fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status         | Indicates whether the interface has been specified in the system as:  
|                | - Enabled: A connection will be established for use when the device is turned on or rebooted.  
|                | - Disabled: The PPP interface cannot currently be used.  
|                | - Start On Data: The PPP connection will be made only when data is sent to the interface (e.g., when a LAN user attempts to use the Internet).  
| Service Name   | The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties. |
### Field Description

**Last Fail Cause**
Indicates the action that ended the previous PPP session:
- **No Valid PADO Recvd**: The unit initiated a PPoE handshake but did not receive a packet in reply from the ISP.
- **No Valid PADS Recvd**: After the initial handshake, the unit did not receive a confirmation packet from the ISP.
- **Stopped by User**: The user stopped the connection (for example, by changing the Configuration Manager settings for the PPP interface.)
- **No Activity**: The PPP communication timed out, in accordance with the timeout period specified on the PPP Configuration page.
- **Auth Failure**: The ISP could not authorize the connection based on the user name and/or password provided.
- **PADT recvd**: The ISP issued a special packet type to terminate the PPP connection.
- **VC down**: The Virtual Circuit between the unit and the ISP is down.
- **Internal failure**: A system software failure occurred.

**DNS**
The IP address of the DNS server (located with your ISP) used on this PPP connection.

**SDNS**
The IP address of the secondary DNS server (located with your ISP) used on this PPP connection.

**Security Protocol**
The type of PPP security your ISP uses: PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

**Login Name**
The name you use to log in to your ISP each time this PPP connection is established.

### 13.3 Adding a PPP Interface Definition

If you intend to use more than one type of service from your ISP, the device may be configured with multiple PPP interfaces, each with unique logon and other properties. Follow this procedure to define properties for a PPP interface:

1. From the PPP Configuration Page, click **Add**.

The PPP Interface – Add page displays, as shown in Figure 41.
2. Select a PPP interface name from the drop-down list, and then enter or select data for each field.

**Note**
You can create multiple PPP interfaces only if you are using the PPoA protocol; only one PPP interface can be define if you are using PPoE. Check with your ISP which version of the protocol they require.

The fields are defined in the tables above.

3. Click **Submit**.

A page displays to confirm your changes.

4. Click **Close** to return to the PPP page and view the new interface in the table.

5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

6. Click **Commit** to save your changes to permanent memory.
### 13.4 Modifying and Deleting PPP Interfaces

To modify a PPP interface, display the PPP Configuration page and click ![pencil](pencil.png) in the Action(s) column for the interface you want to modify. The PPP Interface – Modify page displays, as shown in Figure 42.

![PPP Interface – Modify](image.png)

*Figure 42. PPP Interface – Modify*

You can change only the status of the PPP connection, the security protocol, your login name, and your password. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP interface, display the PPP Configuration page and click ![trash](trash.png) in the Action(s) column for the interface you want to delete. You should not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP interface, click ![Submit](submit.png). Then, click ![Commit & Reboot](commit.png) in the task bar, and click ![Commit](commit.png) to save your changes to permanent memory.
14 Configuring EOA Interfaces

This chapter describes how to configure an Ethernet-over-ATM interface on the SAR110, if one is needed to communicate with your ISP.

14.1 Overview of EOA

The Ethernet-over-ATM (EOA) protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EOA protocol for data transfer with their customers' DSL modems.

EOA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP’s network and their customer’s as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EOA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

Before creating an EOA interface or modifying the default settings, contact your ISP to determine which type of protocol they use.

Note

PPP vs. EOA: Your ISP may use a protocol other than EOA for communication with the SAR110, such as the point-to-point protocol (PPP). One type of PPP, named PPP over Ethernet (PPPoE), actually works “on top” of the EOA protocol. The other type, PP over ATM (PPPoA), does not. However, if your ISP uses either type of PPP, you do not need to separately create an EOA interface. See Chapter 12 for instructions on creating or configuring a PPP interface.
14.2 Viewing Your EOA Setup

To view your current EOA configuration, log into Configuration Manager, click Advanced in the task bar, and then click EOA. Figure 43 shows the EOA Configuration page.

![EOA Configuration Page](image)

Figure 43. EOA Configuration Page

The EOA table contains a row for each EOA interface currently defined on the device. The table may contain no entries if your ISP does not use the EOA protocol.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name the software uses to identify the EOA interface.</td>
</tr>
<tr>
<td>IPF Type</td>
<td>The type of IP Firewall protections in effect on the interface (public, private, or DMZ):</td>
</tr>
<tr>
<td></td>
<td>- Public interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.</td>
</tr>
<tr>
<td></td>
<td>- A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.</td>
</tr>
<tr>
<td></td>
<td>- The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.</td>
</tr>
<tr>
<td>Lower interface</td>
<td>EOA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port—the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EOA interface will operate. This will be an ATM VCC interface, such as aal5-0, as described in Chapter 12.</td>
</tr>
</tbody>
</table>
14. Configuring EOA Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config IP Address and</td>
<td>The IP address and network mask you want to assign to the interface. If the interface will be used for</td>
</tr>
<tr>
<td>Net Mask</td>
<td>bridging with your ISP and you will not be using the SAR110 as a router on your LAN, then you do not need</td>
</tr>
<tr>
<td></td>
<td>to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve</td>
</tr>
<tr>
<td></td>
<td>only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address</td>
</tr>
<tr>
<td></td>
<td>is not available.</td>
</tr>
<tr>
<td>Use DHCP</td>
<td>When checked, this setting instructs the device to accept IP information assigned dynamically by your ISP's</td>
</tr>
<tr>
<td></td>
<td>DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data</td>
</tr>
<tr>
<td></td>
<td>through it, leave this checkbox unselected.</td>
</tr>
<tr>
<td>Default Route</td>
<td>Indicates whether the SAR110 uses the IP address assigned to this interface, if any, as its default route</td>
</tr>
<tr>
<td></td>
<td>for your LAN. Your system can have only one default route. See Chapter 9 for an explanation of default routes.</td>
</tr>
<tr>
<td>Status</td>
<td>A green or red ball will display to indicate that the interface is currently up or down, respectively. You</td>
</tr>
<tr>
<td></td>
<td>cannot manually enable or disable the interface; a red ball may indicate a problem with the DSL connection.</td>
</tr>
<tr>
<td>Action</td>
<td>Icons you can click on to edit (&gt;Edit) or delete (\text{Trash}) the associated EOA interface.</td>
</tr>
</tbody>
</table>

### 14.3 Adding EOA Interfaces

Follow these instructions to add an EOA interface:

1. Click the WAN tab, and then click **EOA** in the task bar.
2. Click **Add**. The EOA Interface – Add page displays, as shown in Figure 44.
3. Select one of the predefined interface names from the EOA Interface drop down list.

4. From the IPF Type drop-down list, select the level of IP Firewall to be used on this interface, as defined above.

5. In the Lower Interface field, select the lower-level interface name over which this protocol is being configured. Typically, an EOA interface is configured to operate over an aal5 interface, such as `aal5-0`.

   If you are using the SAR110 as a bridge only, skip to step 7.

6. If you are using the SAR110 as a router on your LAN, enter the IP address and network mask you want to assign to the interface. This address serves as the public IP address for your entire LAN and is usually assigned by your ISP.

   Or, if your ISP will assign this information, click the Enable radio button to set up the DHCP service.

   Also, specify whether this interface should serve as the default route for your LAN for accessing the Internet.

7. Click [Submit].

   A confirmation page display to confirm your changes.
8. Click **Close** to return to the EOA page and view the new interface in the table.

9. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

10. Click **Commit** to save your changes to permanent memory.
15 Configuring IPoA Interfaces

This chapter describes how to configure an IPoA (Internet Protocol-over-ATM) interface on the SAR110.

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. Typically, this type of interface is used only in product development and test environments, to eliminate unneeded variables when evaluating IP layer processing.

15.1 Viewing Your IPoA Interface Setup

To configure an IPoA interface, log into Configuration Manager, click the WAN tab, and then click IPoA in the task bar. The IPoA page displays, as shown in Figure 45.

Figure 45. IPoA Configuration Page

The IPoA table contains a row for each EOA interface currently defined on the device. The table may initially contain no entries.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name the software uses to identify the IPoA interface</td>
</tr>
<tr>
<td>IPoA Type</td>
<td>Specifies whether the IPoA protocol to be used complies with the IETF RFC 1577 &quot;Classical IP and ARP over ATM&quot; (contact your ISP if unsure).</td>
</tr>
<tr>
<td>Lower Interface</td>
<td>IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port -- the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VCC interface, such as aal5-0, as described in Chapter 12.</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>The IP address of the remote computer you will be connecting to via the WAN interface.</td>
</tr>
</tbody>
</table>
### Field Description

**IPF Type**
The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ):

- **A public interface** connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software.

- **A private interface** connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.

- **The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company’s public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.

**Config IP Address and Net Mask**
The IP address and network mask you want to assign to the interface.

**Status**
A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a down interface may indicate a problem with the DSL connection.

**Action**
Icons you can click on to edit (✏️) or delete (🗑️) the associated EOA interface.

### 15.2 Adding IPoA Interfaces

Follow these instructions to add an IPoA interface:

1. Display the IPoA page and click Add.
   - The IPoA Interface – Add page displays, as shown in Figure 46.
2. Select the next available interface name from the IPoA Interface drop-down list.

3. In the Configured IP Address and Net Mask boxes, type the address and mask that you want to assign to the IPoA interface.

4. Select the level of firewall security to apply to the interface by selecting the IPF Type as Public, Private, or DMZ.

5. In the Lower Interface dialog box, select the lower-level interface name over which this protocol is being configured and click Add. Typically, an IPoA interface is configured to operate over an aal5 interface.

6. Click Submit.

   A confirmation page will display to confirm your changes.

7. Click Close to return to the EOA page and view the new interface in the table.
8. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

9. Click **Commit** to save your changes to permanent memory.
16 Configuring Bridging

The SAR110 can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This chapter describes how to configure the SAR110 to operate as a bridge.

Before changing your bridge configuration, check with your ISP to determine the type of connection they use to exchange data with their customer's DSL modems (such as Ethernet bridging or IP routing).

16.1 Overview of Bridges

A bridge is a device used to connect two or more networks so they can exchange data. A bridge learns the unique manufacturer-assigned hardware IDs of each computer or device on both (or all) networks it is attached to. It learns that some of the IDs represent computers attached via one of the device's interfaces and others represent computers connected via other interfaces. For example, the hardware IDs of your home computers are attached via the Ethernet port, and the hardware IDs of your ISP's computers are attached via the WAN (DSL) port. It stores the ID list and the interface associated with each ID in its bridge forwarding table.

When the bridge receives a data packet, it compares its destination hardware ID to the entries in the bridge forwarding table. When the packet's ID matches one of the entries, it forwards the packet through the interface that connects to the corresponding network. Note that the bridge does not send the data directly to the receiving computer, but broadcasts it to the receiving network, making it available to any node on that network. On the receiving network, a LAN protocol such as Ethernet takes over, helping the packet reaches its destination.

When the bridge does not recognize a packet's destination hardware ID, it broadcasts the packet through all of its interfaces – to each network it is attached to.
Chapter 16. Configuring Bridging

Bridges vs. Routers: The essential difference between a bridge and a router is that a router uses a higher-level protocol (such as IP) to determine how to pass data. IP data packets contain IP addresses that specifically identify the destination computer. Routers can read this information and pass the data to the destination computer, or determine which next router to send the data to if the destination is not on a connected network.

Bridges cannot read IP information, but instead refer to the hardware ID of the destination computer, which is also included in data packets. The hardware ID is a unique number that the manufacturer assigns to each piece of hardware it sells. A bridge learns to recognize the hardware IDs accessible through each of its ports. When it receives a packet, the bridge simply forwards the packet through the port it associates with the given hardware ID, or through all its ports if it does not recognize the ID. The hardware ID is often referred to as the Media Access Control (MAC) address.

Routers are considered more intelligent and flexible devices than bridges, and often provide a variety of security and network administration services based on the IP protocols.

16.2 Using the Bridging Feature

Although the SAR110 is preconfigured to serve as a router for providing Internet connectivity to your LAN, there are several instances in which you may also want to configure bridging:

- Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using layer-3 protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

In both cases, you need to specify the device’s interfaces as bridge interfaces.
16.3 Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode:

1. Log into Configuration Manager and click the Bridging tab. The Bridge Configuration page displays, as shown in Figure 47.

   ![Bridge Configuration page](image)

   **Figure 47. Bridge Configuration page**

   The table may be empty if bridging has not yet been configured.

2. Select the interface names on which you want to perform bridging and click Add.

   For example, select eth-0 (LAN) and eoa-0 (WAN) interfaces.

   If you do not have an eoa-0 interface, but instead have an interface named ppp-0 or ipoa-0, your device is not currently configured with a WAN interface that allows bridging with your ISP. You may want to check with your ISP to determine whether they use the eoa protocol. See Chapter 14 for instructions on creating an eoa interface.

   **Note**
If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.

You can determine whether the Ethernet (eth-0) interfaces have been assigned IP addresses by displaying the IP Address Table (display the Routing tab, and then click IP Address). These interfaces will display in the table only if they have been assigned IP addresses.

You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (click the WAN tab, and then click EOA). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.

3. Click the Enable radio button to turn on bridging.

4. Click Submit. A page will briefly display to confirm your changes, and will return you to the Bridge Configuration page.

5. Click the Admin tab, and then click Commit & Reboot in the task bar.

6. Click Commit to save your changes to permanent memory.

### 16.4 Deleting a Bridge Interface

To make an interface non-bridgeable, display the Bridge Configuration page and click next to the interface you want to delete. Click OK to confirm the deletion. The interface remains defined in the system, but is no longer capable of performing bridging.
17 Configuring Firewall Settings

Configuration Manager provides built-in firewall functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

17.1 Configuring Global Firewall Settings

Follow these instructions to configure global firewall settings:

1. Log into Configuration Manager, click the Services tab, and then click **Firewall** in the task bar.

   The Firewall Configuration page displays, as shown in Figure 48.

![GlobespanVirato](image)
Note that the Firewall Configuration page contains a drop-down list on the right side of the page that enables you to view firewall settings, as discussed in this chapter, or configure IP filters, as discussed in Chapter 18.
2. Configure any of the following settings that display in the Firewall Global Information table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Black List Status</strong></td>
<td>If you want the device to maintain and use a black list, click <strong>Enable</strong>. Click <strong>Disable</strong> if you do not want to maintain a list.</td>
</tr>
<tr>
<td><strong>Black List Period(min)</strong></td>
<td>Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the ADSL/Ethernet router). For more information, see &quot;Managing the Black List&quot;.</td>
</tr>
<tr>
<td><strong>Attack Protection</strong></td>
<td>Click the <strong>Enable</strong> radio button to use the built-in firewall protections that prevent the following common types of attacks:</td>
</tr>
<tr>
<td></td>
<td>- IP Spoofing: Sending packets over the WAN interface using an internal LAN IP address as the source address.</td>
</tr>
<tr>
<td></td>
<td>- Tear Drop: Sending packets that contain overlapping fragments.</td>
</tr>
<tr>
<td></td>
<td>- Smurf and Fraggle: Sending packets that use the WAN or LAN IP broadcast address as the source address.</td>
</tr>
<tr>
<td></td>
<td>- Land Attack: Sending packets that use the same address as the source and destination address.</td>
</tr>
<tr>
<td></td>
<td>- Ping of Death: Illegal IP packet length.</td>
</tr>
<tr>
<td><strong>DoS Protection</strong></td>
<td>Click the <strong>Enable</strong> radio button to use the following denial of service protections:</td>
</tr>
<tr>
<td></td>
<td>- SYN DoS</td>
</tr>
<tr>
<td></td>
<td>- ICMP DoS</td>
</tr>
<tr>
<td></td>
<td>- Per-host DoS protection</td>
</tr>
<tr>
<td><strong>Max Half open TCP Connection</strong></td>
<td>Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.</td>
</tr>
<tr>
<td><strong>Max ICMP Connection</strong></td>
<td>Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as they are initiated.</td>
</tr>
<tr>
<td><strong>Max Single Host Connection</strong></td>
<td>Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Log Destination | Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility (Trace) or can be mailed to specified administrators.

E-mail ID of Admin 1/2/3 | Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format, e.g., jxsmith@onecompany.com.

The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

3. Click Submit.

4. Click the Admin tab, and then click Commit & Reboot in the task bar.

5. Click Commit to save your changes to permanent memory.

17.2 Managing the Black List

If data packets are received that violate the firewall settings or any of the IP Filter rules, then the source IP address of the offending packets can be blocked from such accesses for a specified period of time. You can enable or disable use of the black list using the settings described above. The source computer remains on the black list for the period of time that you specify.

To view the list of currently blacklisted computers, click Black List at the bottom of the Firewall Configuration page. The Firewall Blacklisted Hosts page displays, as shown in Figure 49.

![Firewall Blacklisted Hosts](image)

**Figure 49. Firewall Blacklisted Hosts Page**

The table displays the following information for each entry:
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host IP Address</strong></td>
<td>The IP address of the computer that sent the packet(s) that caused the violation.</td>
</tr>
<tr>
<td><strong>Reason</strong></td>
<td>A short description of the type of violation. If the packet violated an IP Filter rule, the custom text from the Log Tag field will display. (See “Creating IP Filter Rules”.)</td>
</tr>
<tr>
<td><strong>IPF Rule ID</strong></td>
<td>If the packet violated an IP Filter rule, this field will display the ID assigned to the rule.</td>
</tr>
<tr>
<td><strong>Action(s)</strong></td>
<td>Displays an icon (🗑️) you can click on to delete the entry from the list, if you want it to be removed prior to its automatic timed expiration.</td>
</tr>
</tbody>
</table>
18 Configuring IP Filters and Blocking Protocols

This chapter describes two Configuration Manager features that enable you to control the data passing through your network:

- The IP filter feature enables you to create rules to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN. Although IP filter rules provide a very flexible and powerful tool to enhance network security and control user activity, they can also be complex and generally require an advanced understanding of IP protocols.

- The blocked protocols feature enables you to simply select from a predefined list the protocol that you want to block. All data passed to the ADSL/Ethernet router using a blocked protocol will be discarded, without consideration of the source computer, destination computer, or the device interface on which it was received.

18.1 Configuring IP Filters

When you define an IP filter rule and enable the feature, you instruct the SAR110 to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, 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.

18.1.1 Viewing Your IP Filter Configuration

To view your current IP filter configuration, log into Configuration Manager, click the Services tab, and then click IP Filter in the task bar. The IP Filter page displays, as shown in Figure 50.
The IP Filter Configuration page displays global settings that you can modify, and the IP Filter rule table, which shows all currently established rules. See “Creating IP Filter Rules” for a description of the items that make up a rule. When rules are defined, you can use the icons that display in the Actions column to edit (✏️), delete (❌), and view details on (🔍) the corresponding rule.

### 18.1.2 Configuring IP Filter Global Settings

The IP Filter Configuration page enables you to configure several global IP Filter settings, and displays a table showing all existing IP Filter rules. The global settings that you can configure are:

- **Security Level**: This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when High is selected, only those rules that are assigned a security value of High will be in effect. The same is true for the Medium and Low settings. When None is selected, IP Filtering is disabled.

- **Private/Public/DMZ Default Action**: This setting specifies a default action to be taken (Accept or Deny) on private, public, or DMZ-type device interfaces when they receive packets that do not match any of the filtering rules. You can specify a different default action for each interface type. (You specify an interface’s type when you create the interface; see the PPP configuration page, for example.)

  - A public interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is Deny, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.
  
  - A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network.
Typically, the global setting for private interfaces is *Accept*, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection.

- The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface—a whether from a LAN or external source—are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to *Deny* so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

### 18.1.3 Creating IP Filter Rules

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule, and refer to the examples below for assistance:

1. On the main IP Filter page, click *Add*.
   
The IP Filter Rule – Add page displays, as shown in Figure 51.
## IP Filter Rule - Add

### Basic Information

- **Rule ID:** [Field]
- **Action:**
  - Accept
  - Deny
- **Direction:**
  - Incoming
  - Outgoing
- **Interface:** [Field]
- **In Interface:** [All]
- **Log Option:**
  - Enable
  - Disable
- **Security Level:**
  - High
  - Medium
  - Low
- **Blacklist Status:**
  - Enable
  - Disable
- **Log Tag:** [Field]
- **Start Time (HH MM SS):** [Field]
- **End Time (HH MM SS):** [Field]
- **Src IP Address:** [Field]
- **Dest IP Address:** [Field]

### Protocol

- **Protocol:** [Field]
- **Store State:**

### Source Port

- **Source Port:** [Field]

### Dest Port

- **Dest Port:** [Field]

### TCP Flags

- **TCP Flags:** [Field]

### ICMP Type

- **ICMP Type:** [Field]
- **ICMP Code:** [Field]

### IP Frag Pkt

- **IP Frag Pkt:**
  - Yes
  - No
  - Ignore
- **IP Option Pkt:**
  - Yes
  - No
  - Ignore

### Packet Size

- **Packet Size:** [Field]

### TCP Rule Status

- **TCP Rule Status:**
  - Enable
  - Disable

---

*Figure 51. IP Filter Rule – Add Page*
2. Enter or select data for each field that applies to your rule. The following table describes the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., 10, 20, 30) so that you leave enough room between them for inserting a new rule if necessary.</td>
</tr>
<tr>
<td>Action</td>
<td>The action that will be taken when a packet matches the rule criteria. The action can be Accept (forward to destination) or Deny (discard the packet).</td>
</tr>
</tbody>
</table>
| Direction     | Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. 

Incoming refers to packets coming from the LAN, and outgoing refers to packets going to the Internet.

You can use rules that specify the incoming direction to restrict external computers from accessing your LAN. |
<p>| Interface     | The interface on the SAR110 on which the rule will take effect. See the examples on below for suggestions on choosing the appropriate interface for various rule types. |
| In Interface  | The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction. |
| Log Option    | When Enabled is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring in the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to designated administrators. See Chapter 17, “Configuring Firewall Settings” for instructions. |
| Security Level| The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Black List Status</strong></td>
<td>Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the ADSL/Ethernet router from forwarding packets from that source for a specified period of time. See Chapter 17, “Configuring Firewall Settings” for instructions.</td>
</tr>
<tr>
<td><strong>Log Tag</strong></td>
<td>A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to Enable if you configure a Log Tag.</td>
</tr>
<tr>
<td><strong>Start/End Time</strong></td>
<td>The time range during which this rule is to be in effect, specified in military units.</td>
</tr>
</tbody>
</table>
| **Src IP Address**   | IP address criteria for the source computer(s) from which the packet originates. In the drop-down list, you can configure the rule to be invoked on packets containing:  
  - any: any source IP address.  
  - lt: any source IP address that is numerically less than the specified address.  
  - lteq: any source IP address that is numerically less than or equal to the specified address.  
  - gt: any source IP address that is numerically greater than the specified address.  
  - eq: any source IP address that is numerically equal to the specified address.  
  - neq: any source IP address that is not equal to the specified address.  
  - range: any source IP address that is within the specified range, inclusive.  
  - out of range: any source IP address that is outside the specified range.  
  - self: the IP address of the ADSL/Ethernet router interface on which this rule takes effect.                                                                 |
| **Dest IP Address**  | IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent).  
In addition to the options described for the Src IP Address field, the following option is available:  
  - bcast: Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed. |
### Field | Description
--- | ---
Protocol | The basic IP protocol criteria that must be met for rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (eq), that they must not contain the specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).
Store State | If this option is enabled, then stateful filtering is performed—the rule is also applied in the other direction on the given interface during an IP session.
Source Port | Port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) if you have not specified a protocol criteria. See the description of Src IP Address for the selection options.
Dest Port | Port number criteria for the destination computer(s) (i.e., the port number of the type of computer to which the packet is being sent). This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.
TCP Flag | Specifies whether the rule should apply only to TCP packets that contain the synchronous (SYN) flag, only to those that contain the non-synchronous (NOT-SYN) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.
ICMP Type | Specifies whether the value in the type field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICMP Code</strong></td>
<td>Specifies whether the value in the code field in ICMP packet headers will be used as criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) the specified value, or you can select any to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.</td>
</tr>
</tbody>
</table>
| **IP Frag Pkt**| Determines how the rule applies to IP packets that contain fragments. You can choose from the following options:  
  - **Yes**: The rule will be applied only to packets that contain fragments.  
  - **No**: The rule will be applied only to packets that do not contain fragments.  
  - **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria. |
| **IP Option Pkt**| Determines whether the rule should apply to IP packets that have options specified in their packet headers.  
  - **Yes**: The rule will be applied only to packets that contain header options.  
  - **No**: The rule will be applied only to packets that do not contain header options.  
  - **Ignore**: (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria. |
| **Packet Size**| Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criterion. (*lt* = less than, *gt* = greater than, *lteq* = less than or equal to, etc.) |
| **TOD Rule Status**| The Time of Day Rule Status determines how the Start Time/End Time settings are used.  
  - **Enable**: (Default) The rule is in effect for the specified time period.  
  - **Disable**: The rule is not in effect for the specified time period, but is effective at all other times. |
3. When you are done selecting criteria, ensure that the Enable radio button is selected at the top of the page, and then click Submit. After a confirmation page displays, the IP Filter Configuration page will redisplay with the new rule showing in the table.

If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different from the globally configured level.

4. Ensure that the Security Level and Private/Public/DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click Submit. A page displays to confirm your changes.

5. Click the Admin tab, and then click Commit & Reboot in the task bar.

6. Click Commit to save your changes to permanent memory.

### 18.1.4 IP filter rule examples

**Example 1.** Blocking a specific computer on your LAN from using accessing web servers on the Internet:

1. Add a new rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 for example).

2. Specify a source IP address of the computer you want to block.

3. Specify the Protocol = TCP and enable the Store State setting.

4. Specify a destination port = 80, which is the well-known port number for web servers.

5. Enable the rule by clicking the radio button at the top of the page.

6. Click Submit to create the rule.

7. On the IP Filter Configuration page, set the Security Level to the same level you chose for the rule, and set both the Private Default Action and the Public Default Action to Accept.
8. Click [Submit], and commit your changes.

Figure 51 above shows the configuration for this rule. The specified computer will not be able to access the Web, but will be able to access FTP Internet sites (and any others that use destination port numbers other than 80).

**Example 2.** Blocking Telnet accesses to the SAR110:

1. Add a new rule for packets incoming on the ppp-0 interface.

2. Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number used for the Telnet protocol.

3. Enable the rule by clicking the radio button at the top of the page.

4. Click [Submit] to create the rule, and commit your changes.

Figure 52 shows how this rule could be configured:
### IP Filter Rule - Add

#### Basic Information

<table>
<thead>
<tr>
<th>Rule ID: 18</th>
<th>Action:</th>
<th>Accept</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction:</td>
<td>Incoming</td>
<td>Outgoing</td>
<td></td>
</tr>
<tr>
<td>Interface:</td>
<td></td>
<td>ppp-0</td>
<td></td>
</tr>
<tr>
<td>In Interface:</td>
<td>All</td>
<td>Log Option:</td>
<td>Enable</td>
</tr>
<tr>
<td>Security Level:</td>
<td>High</td>
<td>Blocklist Status:</td>
<td>Enable</td>
</tr>
<tr>
<td>Src IP Address:</td>
<td>any</td>
<td>Dest IP Address:</td>
<td>any</td>
</tr>
<tr>
<td>Protocol:</td>
<td></td>
<td>Store State:</td>
<td></td>
</tr>
<tr>
<td>Source Port:</td>
<td>any</td>
<td>Dest Port:</td>
<td>any</td>
</tr>
<tr>
<td>TCP Flag:</td>
<td></td>
<td>ICMP Type:</td>
<td>any</td>
</tr>
<tr>
<td>ICMP Code:</td>
<td></td>
<td>IP Frag Pkt:</td>
<td></td>
</tr>
<tr>
<td>Packet Size:</td>
<td></td>
<td>TOD Rule Status:</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**Figure 52. IP Filter Rule Example 2**
18.1.5 Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Display the IP Filter Configuration page, and then click **Stats** in the row corresponding to the rule. The IP Filter Rule – Statistics page displays, as shown in Figure 53.

![IP Filter Rule – Statistics Page](image)

You can click **Clear** to reset the count to zero and **Refresh** to display newly accumulated data.

18.1.6 Managing Current IP Filter Sessions

When two computers communicate using the IP protocol, an IP session is created for the duration of the communication. The SAR110 allows a fixed number of concurrent IP sessions. You can view information about each current IP session and delete sessions (for security reasons, for example).

To view all current IP sessions, display the IP Filters Configuration page, and then click **Session**. Figure 136 shows an example of an IP Filter Sessions page.

![IP Filter Sessions Page](image)
The IP Filter Session table displays the following fields for each current IP session:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Index</td>
<td>The ID assigned by the system to the IP session (all sessions, whether or not they are affected by an IP filter rule, are assigned a session index).</td>
</tr>
<tr>
<td>Time to expire</td>
<td>The number of seconds in which the connection will automatically expire</td>
</tr>
<tr>
<td>Protocol</td>
<td>The underlying IP protocol used on the connection, such as TCP, UDP, IGMP, etc.</td>
</tr>
<tr>
<td>I/F</td>
<td>The interface on which the IP Filter rule is effective</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP addresses involved in the communication. The first one shown is the initiator of the communication.</td>
</tr>
<tr>
<td>Port</td>
<td>The hardware addresses of the ports involved in the communication</td>
</tr>
<tr>
<td>In/Out Rule Index</td>
<td>The number of the IP Filter rule that applies to this session (assigned when the rule was created)</td>
</tr>
<tr>
<td>In/Out Action</td>
<td>The action (accept, deny, or unknown), being taken on data coming into or going out on the interface. This action is specified in the rule definition.</td>
</tr>
<tr>
<td>Actions</td>
<td>Provides a icon you can click on to delete the IP session. When you delete a session, the communication between is discontinued.</td>
</tr>
</tbody>
</table>

You can click [Refresh] to display newly accumulated data.

18.2 Blocking Protocols

The Blocked Protocols feature enables you to prevent the ADSL/Ethernet router from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

To display the Blocked Protocols page, click the Services tab, and then click Blocked Protocols in the task bar. The Blocked Protocols page displays, as shown in Figure 55.
Chapter 18. Configuring IP Filters and Blocking Protocols

Figure 55. Blocked Protocols Page

WARNING

Blocking certain protocols may disrupt or disable your network communication or Internet access. If you are unfamiliar with how your network or Internet connection uses these protocols, contact your ISP before disabling.

The following list describes each of the available protocols.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE</td>
<td>Point-to-Point Protocol over Ethernet. Many DSL modems use PPPoE to establish and maintain a connection with a service provider. PPPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.</td>
</tr>
<tr>
<td>IP Multicast</td>
<td>IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.</td>
</tr>
<tr>
<td>RARP</td>
<td>Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.</td>
</tr>
<tr>
<td>AppleTalk®</td>
<td>A networking protocol used in Apple Macintosh® networks.</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI protocol provides the method by which computers identify themselves to and communicate with each other.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>IPX</strong></td>
<td>Internetwork Packet Exchange. A networking protocol used on Novell Netware®-based LANs.</td>
</tr>
<tr>
<td><strong>BPDU</strong></td>
<td>Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities, and costs, and are exchanged across bridges to detect and eliminate loops in a network.</td>
</tr>
<tr>
<td><strong>ARP</strong></td>
<td>Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.</td>
</tr>
<tr>
<td><strong>802.1Q</strong></td>
<td>This IEEE specification defines a protocol for virtual LANs on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.</td>
</tr>
</tbody>
</table>

To block a protocol, click the appropriate check box, and click **Submit**. After you have verified that the device continues to function as expected, click the Admin tab, click **Commit & Reboot** in the task bar, and then click **Commit** to save your changes to permanent memory.
19 Viewing DSL Parameters

To view configuration parameters and performance statistics for the SAR110’s DSL line, log into Configuration Manager, and then click the WAN tab. The DSL Status page displays by default, as shown in Figure 56.

The DSL Status page displays current information on the DSL line performance. The page refreshes according to the setting in the Refresh drop-down list, which you can configure. You can click \textbf{Clear} to reset all counters to zero, and \textbf{Refresh} to redisplay the page with newly accumulated values.

Although you generally will not need to view this data, it may be helpful when troubleshooting connection or performance problems with your ISP.

You can click \textbf{DSL Param} to display data about the configuration of the DSL line, as shown in Figure 57.
The DSL Parameters and Status table displays settings preconfigured by the product manufacturer or your ISP.

The Config Data table lists various types of error and defects measurements found on the DSL line. You cannot modify this data.

From the DSL Status page, you can click **Stats** to display DSL line performance statistics, as shown in Figure 58.
The DSL Statistics page reports error data relating to the last 15-minute interval, the current day, and the previous day.

At the bottom of the page, the Detailed Interval Statistic table displays links you can click on to display detailed data for each 15-minute interval in the past 24 hours. For example, when you click on 1-4, data displays for the 16 intervals (15-minutes each) that make up the previous 4 hours. Figure 59 shows an example.

<table>
<thead>
<tr>
<th>15-Min Interval No.</th>
<th>Errored Seconds</th>
<th>Severely Errored Seconds</th>
<th>Unavailable Seconds</th>
<th>Valid Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 59. DSL Interval Statistics Page
20. Administrative Tasks

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

- Viewing System Alarms
- Upgrading the Software
- Using Diagnostics
- Modifying Port Settings

You can access these tasks from the Admin tab task bar. The other Admin tasks listed in the Admin tab—Configuring User Logon and Committing and Rebooting—are described in Chapter 4, “Basic for Configuration using the Web Interface.”

20.1 Viewing System Alarms

You can use the Configuration Manager to view information about alarms that occur in the system. Alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the device. (Despite their name, not all alarms indicate problems in the functioning of the system.)

20.1.1 Viewing the Alarm Table

To display the Alarm page, log into the Configuration Manager, click the Admin tab, and then click **Alarm** in the task bar.

The Alarm page is shown in Figure 60.

![Figure 60. Alarm Page](image)

Each row in the table displays the time and date that an alarm occurred, the type of alarm, and a brief statement indicating its cause.

To remove all entries from the list, click **Clear**. New entries will begin accumulating and will display when you click **Refresh**.
20.1.2 Displaying the Alarm Monitor in a Separate Window

If you want to display an automatically updating Alarm table, you can click [Alarm Monitor] to display a separate Alarm Monitor window, as shown in Figure 61.

![Alarm Monitor Window](image)

Figure 61. Alarm Monitor Window

You can click on the Refresh Rate drop-down list to select a recurring time interval after which the page will redisplay with new data.

You can leave the Alarm Monitor window open and active even after closing the Configuration Manager.

20.2 Upgrading the Software

Your ISP may from time to time provide you with an upgrade to the software running on the ADSL/Ethernet router. All system software is contained in a single file, called an image. The image is composed of several distinct parts, each of which implements a different set of functions.

Configuration Manager provides an easy way to upload the new software image, or a specific part of the image) to the memory on the ADSL/Ethernet router. To upgrade the image, follow this procedure:

1. Log into Configuration Manager, click the Admin tab, and then click [Image Upgrade] in the task bar.

   The Image Upgrade window is shown in Figure 62.
2. In the Upgrade File text box, type the path and file name of the file as provided by your ISP. You can click \texttt{Browse...} to search for it on your hard drive.

3. Click \texttt{Upload}.

After a few seconds, a message like the following should display (the file name may differ):

File: TEImage.bin successfully saved to flash. Please reboot for the new image to take effect.

4. Turn power to the unit off, wait a few seconds, and turn it on again.

The new software will now be in effect.

\textbf{20.2.1 What if something goes wrong?}

Occasionally a software upload might go wrong 😔

Under these circumstances the firmware on the router may become corrupted or damaged. Under these circumstances you cannot access the router using the web management.

When this happens it’s useful to connect the serial cable to the console port of the router and talk to the router using a terminal programme. This way you can then check the text messages coming from the router to see if it is indicating corrupt firmware or configuration files (see How to… for details on connecting to the router using the serial/console port).

With the terminal programme running and the console port connected switch the router off, wait 5 seconds and then switch it back on again. You can then check to see if the router is indicating corrupt settings/firmware as it boots up. If it’s reporting problems with the firmware then you can use tftp to send the firmware to the router.
First of all check what the router says on boot up. If it is saying that it's waiting for tftp to 192.168.1.1 (this is the default IP address of the router when it has total firmware corruption) then you must use tftp to send the firmware to the address 192.168.1.1. BUT if the problem is corrupted configuration files then the router will have the default address 192.168.7.1. Check the console screen and see what it says…. You will then need to ensure that your computer is on the same subnet e.g. if router is on 192.168.1.1 then set computer to 192.168.1.2. If the router is on 192.168.7.1 then set you computer to 192.168.7.2 (for example).

Tftp is a native programme with Windows. To run the tftp programme you need to exit windows to a DOS/Command Prompt. The syntax for using tftp (tftp is a native programme in Windows/DOS) is

```
C:\>tftp /?
```

Transfers files to and from a remote computer running the TFTP service.

```
TFTP [-i] host [GET | PUT] source [destination]
```

- **-i** Specifies binary image transfer mode (also called octet). In binary image mode the file is moved literally, byte by byte. Use this mode when transferring binary files.

- **host** Specifies the local or remote host.

- **GET** Transfers the file destination on the remote host to the file source on the local host.

- **PUT** Transfers the file source on the local host to the file destination on the remote host.

- **source** Specifies the file to transfer.

- **destination** Specifies where to transfer the file.

```
C:\\>
```

So….. for example, if the router is on address 192.168.1.1, then the command would be

```
Tftp -i 192.168.1.1 PUT TELImage.bin
```

After you issue the command the LED's on the front of the router will flicker as the data is sent. There is no other indication that the data is being sent but DO NOT touch the computer or router until the file has been sent. This will take 2 or 3 minutes. When tftp has finished the tftp programme will report success. At this stage you can switch the router off and then back on to reboot with the new
firmware file (check the console/terminal screen to check it boots up okay).

20.3 Using Diagnostics

The diagnostics feature executes a series of tests of your system software and hardware connections. Use this feature when working with your ISP to troubleshoot problems.

Follow these instructions to begin the diagnostics program:

1. Log into Configuration Manager, click the Admin tab, and then click **Diagnostics** in the task bar.

   Figure 63 shows the Diagnostics page.
2. From the Virtual Circuits drop-down list, select the name of your ATM interface (see Configuring the ATM VCC for an explanation of ATM interfaces). Usually, this will be `atm-0`.

3. Click [Submit].

The diagnostics utility will run a series of tests to check whether the device's connections are up and working. This takes only a few seconds. The program reports whether the test passed or failed, as shown in Figure 64. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

![Figure 64. Diagnostics Page—After Execution](image)

You can click [Help] to display an explanation of each test. Work with your ISP to interpret the results of the diagnostic tests.

Please note, in the UK we use PPPoA NOT PPPoE. Therefore the diagnostics will show FAIL for the PPPoE tests – don’t worry 😊

### 20.4 Modifying Port Settings

#### 20.4.1 Overview of IP port numbers

The header information in an IP data packet specifies a destination port number. Routers use the port number along with the specified IP addresses to forward the packet to its intended recipient.
For example, all IP data packets that the ADSL/Ethernet router receives from the Internet specify the same IP address (your public IP address) as the destination. However, depending on the port number contained in a data packets, the ADSL/Ethernet router may pass the packet on to its embedded Web or Telnet servers, or to another computer on the network.

The Internet community has developed a list of common server types such as HTTP, Telnet, e-mail, and many others, and assigned a unique port number to each. These are not mandatory, but are useful in promoting communication between separately administered LANs.

20.4.2 Modifying the ADSL/Ethernet routers’ port numbers

In some cases, you may want to assign non-standard port numbers to the HTTP and Telnet servers that are embedded on the SAR110. The following scenario is one example of why changing the HTTP port number may be necessary:

You have an externally visible Web server on your LAN, with a NAT rule (rdr flavor) that redirects incoming HTTP packets to that Web server. When incoming packets contain a destination IP address of your public IP address (which is assigned to the ADSL/Ethernet router’s WAN port) and the standard Web server port number of 80, the NAT rule recognizes the port number and redirects the packets to your Web server’s local IP address.

Assume in this scenario that you also want to enable external access to the SAR110 Configuration Manager, so that your ISP can log in and manager your system, for example. Accessing Configuration Manager requires accessing the SAR110 own Web server (also called its HTTP server). In this case, you would want to use the Port Settings feature to assign a non-standard port number to the SAR110’s HTTP server. Without a non-standard port number, the NAT rule would redirect your ISP’s log in attempt to your LAN HTTP server rather than to the HTTP server on the SAR110.

Thereafter, when your ISP wants to log on to your Configuration Manager, they would type your IP address in their browser, followed by a colon and the non-standard port number, as shown in this example:

http://10.0.1.16:61000

Your ISP may also have special circumstances that require changing the HTTP or Telnet port numbers; contact them before making any changes here.
Follow these steps to modify port settings:

1. Log into Configuration Manager, click the Admin tab, and then click **Port Settings** in the task bar.

   The Port Settings page is shown in Figure 65.

   ![Port Settings Page](image)

   **Figure 65. Port Settings Page**

   2. Type the new port number(s) in the appropriate text box(es) and click **Submit**.

   - For the HTTP server, the default port number is 80; for the Telnet server, the default is port number is 23; for the FTP server, the default port number is 21.
   - You can enter a non-standard port number for either server type in the range 61000-62000.

3. Click **Commit & Reboot** in the task bar, and click **Commit** to save your changes to permanent memory.
21 Committing Your Changes and Rebooting the Device

21.1 Committing Your Changes

Whenever you use the Configuration Manager to change system settings, the changes are initially placed in temporary storage called random access memory or RAM. Your changes are made effective when you submit them, but can be lost if the device is reset or turned off.

You can commit changes to save them permanently to flash memory.

Submitting changes saves them only until the device is reset or powered down. Committing changes saves them permanently.

To commit changes, click the Admin tab, click Commit & Reboot in the task bar, and then click . Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.

The changes are saved to permanent storage. The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly, as described in the following section.

21.2 Rebooting the Device

To reboot the device from the Commit & Reboot page, select a reboot mode from the drop-down menu, and then click . You can select from the following three options when rebooting:

- Reboot from Last Configuration reboots the device using the current settings in permanent memory, including any changes you just committed.

- Reboot from Backup Configuration reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.

- Reboot from Default Configuration reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.
22 How to…

22.1 How to enter Command Line Interface mode

Although set-up options can be done via the web interfaces, some users may require to modify router configuration via the Command Line Interface (CLI) mode. To access the CLI mode you can use either Telnet via the LAN or use console programme via the serial port.

22.1.1 Telnet

To access the command line interface via Ethernet interface, you can use TELNET to log in the Router from the local Ethernet network using the Ethernet IP address that is assigned to your ADSL Router. The Ethernet IP of the ADSL Router is by default set to 192.168.7.1.

Select Start->Programs->MS-DOS Prompt.

Find the IP address of the Router’s Ethernet port. Then use TELNET to login the Router. For example, TELNET 192.168.7.1 (in the example below the IP of the router in our test was set to 192.168.0.11 – however you should use the correct IP address set for your router).

You will see that a telnet dialog pops up asking for your configuration Login name. By default this is ‘DSL’. Then you need the password which by default is also ‘DSL’. Then the $ prompt should be shown with a successful login.
Now you are ready to configure the Router by using command line interface (CLI) commands.

22.1.2 Using terminal program via serial console port

A terminal can be connected directly to the Serial console port. This requires the use of a terminal emulation software package such as Microsoft HyperTerminal. By default setting, the Router is configured to communicate at a baud rate of 38400. Any standard terminal that supports baud rate of 38400 can be connected to the Router’s console port. Please configure your serial port as:

- BPS: 38400
- Data bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Then do the following steps to log on to the Router via Microsoft HyperTerminal.

Select Start->Programs->Accessories->HyperTerminal

Enter a connection name and click OK

Select properly COM port and click OK
Enter the following parameters:

- Bits per second: 38400
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Then click OK

When the HyperTerminal window appears, you must press the enter key several times to get the command prompt for the Router's command line interface.
You should then see the $ prompt.

Now you are ready to configure the Router by using the command line interface (CLI) commands.

### 22.1.3 Basic CLI syntax

If you type ‘? <Enter>’ at the CLI prompt then the following instructions are given.
This shows the complete list of CLI commands.

To enter a command you just type the command in as simple text.
E.g. ‘modify ethernet intf ifname eth-0 ip 192.168.7.1’ modifies the
LAN IP address ...
Remember, after doing any changes in CLI mode you must enter the 'commit' command to store your settings. If you don’t do this then they may be lost after a power down or restart.

22.2 Common CLI Commands

This section helps to explain some of the more commonly used CLI commands. Generally we would advise using the web based interface for router configuration however, sometimes there may be a need to use CLI configuration via the console port (e.g. if you have changed the default IP address to an unknown value so you cannot access the web interface).

22.2.1 commit

Commit the active config to the flash
22.2.2 reboot < default | backup | last | clean | minimum>

Reboot the device:

Default
load factory defaults on restart
Backup
load backup settings on restart
Last
load last saved configuration on restart
Clean
load basic configuration with LAN settings on restart
Minimum
Load basic, minimum settings (no LAN or WAN defined) on restart

22.2.3 get ip <address | cfg | route | stats>

Display basic settings for the LAN port

address
IP Address Table
cfg
IP Configuration
route
IP Route Table
stats
IP Statistics

e.g.
$get ip address

<table>
<thead>
<tr>
<th>Ip Address</th>
<th>Mask</th>
<th>If Name</th>
<th>BCast Addr</th>
<th>MaxReasm</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>255.0.0.0</td>
<td>lo-0</td>
<td>1</td>
<td>65535</td>
</tr>
<tr>
<td>192.168.7.1</td>
<td>255.255.255.0</td>
<td>eth-0</td>
<td>1</td>
<td>65535</td>
</tr>
</tbody>
</table>

$ 

22.2.4 modify ethernet intf ifname <name> [ip,mask,usedhcp,speed,duplex]

Allows you to modify LAN port settings

Ifname <name>
Interface Name (see above to get interface name)

[ ip <ddd.ddd.ddd.ddd> ]
IP Address of the Ethernet Port

[ mask <ddd.ddd.ddd.ddd> ]
Network Mask

[ usedhcp local|remote|false ]
Dhcp local|remote|Do not use

[ speed auto|10BT|100BT ]
Line speed to be used by Ethernet intf

[ duplex auto|half|full ]
Duplex mode to be used by Ethernet intf

e.g.
$modify ethernet intf ifname eth-0 ip 192.168.7.1

Interface : eth-0
IP Filter Type : Private  Configured IP Address : 192.168.7.1
Mask : 255.255.255.0 UseDhcp : False
Physical Interface : -  Nat Direction : IN
Configured Duplex : Auto  Duplex : AutoNeg In Prog
22.2.5 modify nbsize maxipsess 'value'

'value'

Value for the maximum number of IP sessions allowed

e.g.

modify nbsize maxipsess 300

22.2.6 create user name <name> passwd <name> [root | user]

name <name> User Name
passwd <name> User Password
[ root | user ] User Privileges (root user can modify settings)
useserial Use Serial Number

e.g.

create user name fred passwd 1234

Entry Created

Privilege UserName

--------------------
user fred

$
22. How to… Solwise SAR110 ADSL Ethernet Router User’s Guide

Modify the IP Address and Subnet Mask to suite and then click on Submit. Finally save your configuration (Admin/Commit & Reboot/Commit) and then reboot (Admin/Commit & Reboot/Reboot).

Please note, if the router fails to login using this manually entered WAN address (for example you may have entered it wrong or it’s not correct) then the router will default to the WAN address as supplied to the router when it logs in.

22.4 eMule/eDonkey

22.4.1 What’s the problem?

Frequently people complain about lockup on their router when running file ‘sharing’ programmes like Emule or Edonkey. The
problem is the router gets overworked with the very high number of UDP sessions that these programmes create.

22.4.2 How do I fix it?

The 'fix' is three fold…

a) Lower the connection limits in your software; e.g. to 150.

b) On the router use the following CLI command to increase the maximum number of ip sessions that the router can cope with to 400;

modify nbsize maxipsess 400

c) On the router use the following CLI command to decrease the NAT UDP timeout value to 120 seconds (you can also do this via the web interface);

modify nat global udp timeout 120

22.5 Enabling ZIPB

22.5.1 What's ZIPB?

ZIPB means Zero IP Bridge. It’s the correct term for what is often incorrectly referred to as transparent bridging or half-bridged mode or sometimes as DHCP spoofing (which means something else). What this means is you can setup the router to simple act as an 'ethernet modem' and let all IP traffic thorough transparently but without the router using one of your internet IP addresses. A typical use for this configuration might be for if you want to use a Linux firewall box up to route all you IP traffic so you want the Linux box to take your single ISP assigned IP address. The other advantage of using ZIPB is there is no requirement for NAT, as the public IP address is passed directly to the PC on the LAN. This eliminates the need for extensive ALG support.

This is distinct from the situation where you have been given a block of fixed IP’s by your ISP. In this case you need to use an “IP Unnumbered PPP interface” as detailed below.

22.5.2 How it works

On boot-up, the LAN interface of the router will have a private IP address, for example 192.168.7.1.

Assuming the PPP user name and password are correctly configured (or after the user has configured these for the first time), the PPP link is established. Once the router has retrieved the public IP address via IPCP, the “zipb” process will create a spoofed IP address, and assign this address to the modem LAN interface. The LAN side

Now the DHCP server is updated to allow clients to obtain the public IP address and gateway addresses on their next DHCP lease renewal. By default, the "spoofed address" is created by manipulating the public IP address obtained via IPCP. The WAN side PPP link uses an “unnumbered” IP interface. Proxy ARP is
configured in the IP stack to allow the LAN PC to receive valid ARP replies for all requests on its local subnet. Additionally, ZIPB will add a virtual interface to the LAN side so that the web pages can be accessed via the LAN.

22.5.3 Here's how to do it

First of all set the IP address of your PC so that you can 'see' the router configuration

e.g. (assuming the router is on the default address 192.168.7.1)

Create a ppp-0 connection as detailed above but ensure that DNS is enabled (so that the DNS addresses will be passed along to your client)…
For example, below shows the ppp-0 details.

Now goto the web configuration screens for the router and goto
Services/NAT. Select ‘Disable’ NAT and then click on ‘Submit’:

Now goto LAN/DHCP Mode and select ‘DHCP Server’ and ‘Submit’:

Click on DHCP Server…

Now click on Add…
Enter the details for a server pool. E.g. as shown above (the actual values don't seem to matter 😊 It's just that the DHCP server mode doesn't work correctly unless you have a server pool defined).

Now goto Bridging and enable ZIPB and click on submit...

Now goto Services/NAT and disable NAT and click on Submit...
Now Goto Admin and Commit the changes…

That’s the router configured. Now you can go to the TCP settings for you computer and tell it to use DHCP for it’s IP settings:
Then Ok the settings.

22.5.4 Testing it's worked

Assuming the router has logged in okay to your ISP you can check that the ZIPB is working by checking to see if your PC has been assigned IP settings from the ISP.

e.g. Under W2K or XP go to a command DOS prompt and use 'ipconfig /all' to show you your LAN IP settings:
Notice how your LAN IP address is now an ISP assigned address. Also the DNS server addresses are those sent by your ISP.

You can also do a ping test to check that DNS resolution is working.

If you don’t have correct IP values then change your IP address back to the old IP address e.g. 192.168.7.2 and then go in and check your settings. Also check from the main status page that the router has logged into the ISP.

## 22.6 Operation with multiple IP’s

Imagine your ISP has given 5 fixed, public IP’s and you want to use the 110 as a simple router with the 110 consuming just one of these fixed IP’s and the remaining 4 IP’s being used by your LAN side PC’s. This is distinct from the situation where you have just one fixed IP address and you want this to be assigned to a single PC on the LAN side – in this case you need to use ZIPB as detailed above.

The technique used to configure your router to use a single, public address is called IP Unnumbered PPP interface.

### 22.6.1 IP Unnumbered PPP interface

The modem’s PPP interface is typically assigned a unique IP address from the ISP’s PPP server. This IP address must be in a
different subnet than the IP addresses assigned to the modem’s LAN interfaces, such as eth-0 and usb-0.

The IP Unnumbered feature provides an alternative configuration that enables the PPP interface to be created with an IP address that is the same as that assigned to the modem’s Ethernet interface, eth-0. Using this feature, the PPP interface does not need to obtain an IP address from the ISP.

The PPP interface borrows the IP address from eth-0 to facilitate routing. During IPCP negotiations with the ISP’s server, the PPP interface conveys this address to the other side as its own. If the ISP’s server is configured to allow IP Unnumbered connections, then it does not provide another IP address to the PPP interface, as it would in normal operation.

If the ISP’s PPP server is not configured to allow IP Unnumbered connections, then the server would respond with an IPCP negative acknowledgement (NAK) and instead assign a new IP address to the interface, as it would in normal operation.

The IP Unnumbered feature can be useful in environments in which conserving IP addresses is a priority.

It is assumed that the LAN hosts are configured with IP addresses that are visible to the ISP (i.e., not translated via NAT). In typical scenarios where the modem is configured with only one WAN interface (in this case, the IP Unnumbered PPP interface), users will not need to configure NAT in conjunction with this feature.

22.6.2 Configuration

To configure a PPP interface as IP Unnumbered interface, the PPP interface must be created without an IP address and must specify the interface from which to borrow an IP address (only eth-0 is supported). The stages necessary to do this are:

1. Configure the LAN address and subnet mask of router to the correct value as advised by your ISP.
2. Set IP address and subnet mask of your LAN PC’s to their correct public addresses from your provided block.
3. Go into CLI console mode using telnet or RS232/hyperterminal.
4. Use CLI to delete your current ppp interface

$delete ppp intf ifname ppp-0

If-Name : ppp-0 L2TP Call type : inlac
Interface Sec Type : Public Phy Interface : aal5-0
Configured IP Address : 0.0.0.0 NAT Direction : OUT
Init MRU : 1500 Magic : False
Encapsulation : PPPOE Service Name : -
UseDhcp : False UseDns : True
DRoute : True Status : Start
Gateway IP Address : 0.0.0.0 Associated Num If-Name: -
Use Gateway : remote
Entry Deleted

5. Use CLI to create a new ppp interface but tell the new ppp interface to borrow it’s IP address from the LAN/ethernet port settings.

$create ppp intf ifname ppp-0 ppoa lowif aal5-0 numif eth-0 droute true

Entry Created

    If-Name               : ppp-0          L2TP Call type        : inlac
    Interface Sec Type    : Public         Phy Interface         : aal5-0
    Configured IP Address : 0.0.0.0        NAT Direction         : OUT
    Init MRU              : 1500           Magic                 : False
    Encapsulation         : PPPOA          Service Name          : -
    UseDhcp               : False          UseDns                : False
    DRoute                : True           Status                : Start
    Gateway IP Address    : 0.0.0.0        Associated Num If-Name: eth-0
    Use Gateway           : remote

6. Commit changes and reboot.

$commit

Set Done

$reboot

7. Go back in via the web interface and...

   a) Set ppp settings with your correct ISP login name/password
   b) Make sure your VCI/VPI/VC/LLC settings are correct
   c) Disable NAT
   d) Commit changes and reboot

PPPoE interfaces can also be created in this manner. A gateway IP address can also be specified using the gwy parameter, or can be learned during the IPCP handshake. A specified gateway IP address will override any address learned via IPCP.

22.6.3 Limitations

The following limitations apply when implementing an IP Unnumbered interface:
• Only point-to-point interfaces can be IP Unnumbered e.f. PPPoA or PPPoE.
• The interface from which the PPP interface borrows the IP address must be the modem’s Ethernet interface, eth-0.
• The interface eth-0 cannot be configured to receive its IP address through DHCP, and the IP address cannot be modified during an active PPP connection.
• The ISP’s access server must be configured with an IP route that specifies the LAN’s network address as the destination and the interface associated with that user’s VPI/VCI as the gateway.

22.6.4 IP Unnumbered with NAT

The configuration details shown above require each LAN PC to have a public IP address (within a range given by the ISP) and does not make use of Network Address Translation (NAT). However, often you end up with having more clients than public IP addresses.

For example, you may obtain four public IP address from the ISP for use with servers on the LAN (web server, mail server, etc.), but may have 10 additional PCs that use private IP addresses in the subnet 192.168.1.x, mask 255.255.255.0.

The user can configure NAT to enable these 10 PCs to access the internet. This can be achieved by creating a virtual IP (VIP) LAN interface on the modem with private IP address (say, 192.168.1.1, mask 255.255.255.0). The user would then create a NAT rule (NAPT flavor) to translate the PCs’ local IP addresses to the VIP IP address. The following CLI commands create a rule of this type and enable the NAT service:

```
create nat rule entry ruleid 1 napt lcladdrfrom 192.168.1.2 lcladdrto 192.168.1.254 modify nat global enable
```

22.7 Blocking remote access to your SAR110 router

By default the ports 80, 21 and 23 are open on your 110 to allow remote connectivity. These ports are set this way to facilitate remote administration of your router. Most users will **NOT** want these ports open.

There are two ways to accomplish this:

22.7.1 Using IP Filters

One way is to create IP Filters which block incoming traffic on these three ports.

Goto Services, IP Filter…

Now click on Add to create a rule. Now create a rule to block port 21 use the following settings:
Next create similar rules for port 23...
And then for port 80...
Now you have the three new filter rules added you need to set the security level to Low and the Public Default Action to Accept (as shown below).
When you have finished the configuration click on Submit to store the configuration.

Remember to Commit the configuration after you’ve finished.

### 22.7.2 Using RDR forwarding rules

Another way to block these open ports is to add three RDR port forwarding rules which forward these ports to an unused LAN address (e.g., .254).

Goto Services, NAT Rule Entry and Add three new rules.

Add three rules similar to those shown below:
### NAT Rule - Detail

<table>
<thead>
<tr>
<th>NAT Rule Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID: 30</td>
</tr>
<tr>
<td>Rule Flavor: RDR</td>
</tr>
<tr>
<td>If Name: ALL</td>
</tr>
<tr>
<td>Protocol: TCP</td>
</tr>
<tr>
<td>Local Address From: 192.168.0.254</td>
</tr>
<tr>
<td>Local Address To: 192.168.0.254</td>
</tr>
<tr>
<td>Global Address From: 0.0.0.0</td>
</tr>
<tr>
<td>Global Address To: 0.0.0.0</td>
</tr>
<tr>
<td>Destination Port From: 80</td>
</tr>
<tr>
<td>Destination Port To: 80</td>
</tr>
<tr>
<td>Local Port: 80</td>
</tr>
</tbody>
</table>

[Button: Close]  [Button: Refresh]  [Button: Help]

### NAT Rule - Detail

<table>
<thead>
<tr>
<th>NAT Rule Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID: 31</td>
</tr>
<tr>
<td>Rule Flavor: RDR</td>
</tr>
<tr>
<td>If Name: ALL</td>
</tr>
<tr>
<td>Protocol: TCP</td>
</tr>
<tr>
<td>Local Address From: 192.168.0.254</td>
</tr>
<tr>
<td>Local Address To: 192.168.0.254</td>
</tr>
<tr>
<td>Global Address From: 0.0.0.0</td>
</tr>
<tr>
<td>Global Address To: 0.0.0.0</td>
</tr>
<tr>
<td>Destination Port From: 23</td>
</tr>
<tr>
<td>Destination Port To: 23</td>
</tr>
<tr>
<td>Local Port: 23</td>
</tr>
</tbody>
</table>

[Button: Close]  [Button: Refresh]  [Button: Help]
## NAT Rule – Detail

<table>
<thead>
<tr>
<th>NAT Rule Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID:</td>
<td>32</td>
</tr>
<tr>
<td>Rule Flavor:</td>
<td>RDR</td>
</tr>
<tr>
<td>IF Name:</td>
<td>ALL</td>
</tr>
<tr>
<td>Protocol:</td>
<td>TCP</td>
</tr>
<tr>
<td>Local Address From:</td>
<td>192.168.0.154</td>
</tr>
<tr>
<td>Local Address To:</td>
<td>192.168.0.154</td>
</tr>
<tr>
<td>Global Address From:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Global Address To:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Destination Port From:</td>
<td>21</td>
</tr>
<tr>
<td>Destination Port To:</td>
<td>21</td>
</tr>
<tr>
<td>Local Port:</td>
<td>21</td>
</tr>
</tbody>
</table>
23 DNS Addresses

Below shows the current name server (DNS) addresses as used by the most popular ISP’s. Please note that this should not be taken as a definitive list and it might be that the address for a listed provider might have changed. You are therefore advised to check with your ISP:

<table>
<thead>
<tr>
<th>ISP</th>
<th>DNS</th>
</tr>
</thead>
</table>
| Pipex | 158.43.240.4  
| | 158.43.240.3 |
| BT_test (as used by bt_test@startup_domain) | 194.72.7.57  
| | 194.73.82.242 |
| PlusNet | 212.159.11.150  
| | 212.159.13.150 |
| Nildram | 195.112.4.4  
| | 195.112.4.7 |
| Demon | 158.152.1.58  
| | 158.152.1.43 |
| BT Openworld | 213.120.62.97-104 |
| KC | 212.50.160.28  
| | 212.50.160.100 |
| Freedom-2-Surf | 194.106.56.6  
| | 194.106.33.42 |
| Eclipse | 212.104.130.9  
| | 212.104.130.65 |
| Breath-pro | 212.159.11.129  
| | 212.159.13.130 |
| Claranet | 195.8.69.7  
| | 195.8.69.12 |
| Freeserve | 195.92.195.94  
| | 195.92.195.95 |
| Mailbox | 195.82.96.40  
| | 195.82.96.6 |
| Onetel | 212.38.173.189  
| | 212.38.173.190 |
| Onyx | 194.176.65.5  
| | 194.176.68.30 |
| Virgin | 194.168.4.100  
<p>| | 194.168.8.100 |</p>
<table>
<thead>
<tr>
<th></th>
<th>DNS Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT Broadband</td>
<td>194.168.8.100</td>
</tr>
<tr>
<td></td>
<td>193.113.212.38</td>
</tr>
<tr>
<td></td>
<td>194.72.6.57</td>
</tr>
</tbody>
</table>
24 Appendix A IP Addresses, Network Masks, and Subnets

24.1 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. For details on this subject, see Appendix 24.

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."

24.1.1 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 2 shows the structure of an IP address.

<table>
<thead>
<tr>
<th></th>
<th>Field1</th>
<th>Field2</th>
<th>Field3</th>
<th>Field4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>Network ID</td>
<td>Host ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class B</td>
<td>Network ID</td>
<td></td>
<td>Host ID</td>
<td></td>
</tr>
<tr>
<td>Class C</td>
<td>Network ID</td>
<td></td>
<td></td>
<td>Host ID</td>
</tr>
</tbody>
</table>

Here are some examples of valid IP addresses:
24.1.2 Network classes

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

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

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

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

Some important notes regarding IP addresses:

- The class can be determined easily from field1:
  - field1 = 1-126: Class A
  - field1 = 128-191: Class B
  - field1 = 192-223: Class C
  (field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

24.2 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 field 1 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 field 4 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 field 4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field 4 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.
25 Appendix B Binary Numbers

25.1 Binary Numbers

In everyday life, we use the decimal system of numbers. In decimal, numbers are written using the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. Computers, however, do not use decimal. Instead, they use binary.

**Definition**

Binary numbers are numbers written using only the two digits 0 and 1, e.g., 110100.

**Hint**

Does "base ten" sound familiar? (Think grade school.) Base ten is just another name for decimal. Similarly, base two is binary.

Just as each digit in a decimal number represents a multiple of 10 (1, 10, 100, 1000, 10,000, etc.), each digit in a binary number represents a multiple of 2 (1, 2, 4, 8, 16, etc.). For example:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000's</td>
<td>-</td>
</tr>
<tr>
<td>100's</td>
<td>-</td>
</tr>
<tr>
<td>10's</td>
<td>1</td>
</tr>
<tr>
<td>1's</td>
<td>3</td>
</tr>
</tbody>
</table>

- 1 3 = 1 1 0 1

Also, since binary uses only two digits to represent all numbers, a binary number has more digits than the same number in decimal. In the example above, you can see that the decimal number 13 is the same as the binary number 1101 (8 + 4 + 1 = 13).

25.1.1 Bits and bytes

Computers handle binary numbers by grouping them into units of distinct sizes. The smallest unit is called a bit, and the most commonly used unit is called a byte.

**Definition**

A bit is a single binary digit, i.e., 0 or 1.

A byte is a group of eight consecutive bits (the number of bits can vary with computers, but is almost always eight), e.g., 11011001. The value of a byte ranges from 0 (00000000) to 255 (11111111).

The following shows the values of the eight digits in a byte along with a sample value:

<table>
<thead>
<tr>
<th>128's</th>
<th>64's</th>
<th>32's</th>
<th>16's</th>
<th>8's</th>
<th>4's</th>
<th>2's</th>
<th>1's</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
The decimal value of this byte is 173 \((128 + 32 + 8 + 4 + 1 = 173)\).
26 Appendix C Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the SAR110, and provides instructions for using several IP utilities to diagnose problems.

26.1 Basic Connectivity

First of all check the status LED’s on the front of the router to ensure basic connectivity is okay:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Troubleshooting Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEDs</strong></td>
<td></td>
</tr>
<tr>
<td>Power LED does not illuminate after product is turned on.</td>
<td>Verify that you are using the power cable provided with the device and that it is securely connected to the SAR110 and a wall socket/power strip.</td>
</tr>
<tr>
<td>ADSL LED does not illuminate after phone cable is attached.</td>
<td>Verify that a standard telephone cable like the one provided is securely connected to the ADSL port and your wall phone jack. Wait 30 seconds to allow the device to negotiate a connection with your ISP.</td>
</tr>
<tr>
<td>PC LED does not illuminate after Ethernet cable is attached.</td>
<td>Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the SAR110. Make sure the PC and/or hub is turned on. Verify that you are using a straight-through type Ethernet cable to the uplink port on a hub or to a stand-alone PC. If you connected the device to an ordinary hub port (not Uplink), you must use a cross-over cable. (Hold the connectors at each end of the cable side-by-side in the same position. If the order of their color-coded wire pairs is the same, it is a straight-through type.) Contact Customer Support if your cable is not the correct type. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.</td>
</tr>
<tr>
<td>DIAG LED stays illuminated after turning the device on.</td>
<td>The DIAG LED should turn off after about 10-15 seconds. If it does not, turn off the SAR110, wait 10 seconds, and then turn it back on.</td>
</tr>
</tbody>
</table>

26.2 Logging in with the ISP

Now goto the Status page for the web configuration manager for the router:
Check that the DSL/Operational Status shows ‘Showtime/Data’ and the ‘LED’ is green. This indicates that you have a valid ADSL signal on the line. If it shows red or yellow then there is a problem with the ADSL signal. In which case check your phone line/ADSL cable. Also try the router plugged into the main, master phone socket. Also try disconnecting all other phone devices from the line.

Once there is an ADSL signal there you should next check the WAN Interfaces. Check the status for the ppp-0 interface. Where it says ‘IP Address’ there should be a valid IP address shown. Also the Status ‘LED’ at the end of the line should be green. These things indicate that there is a valid login with your ISP. If you haven’t got an IP address shown (and the Status LED is NOT green) then the reason is the router is failing to login into your ISP. This might be for the simple reason that you have not correctly typed in your login name/password. So, first of all you need to check that your user name/password are correct. Click on the ‘ppp-0’ link on the ppp-0 Wan Interface line:
Click on the pencil symbol on the end of the line so you can reenter your login details:

Reenter your details and then click on Submit. Then go back to the Status page to see if it now shows a valid WAN IP address.

If not then the next thing to try is the BT test account (sorry, you cannot do this in the Hull/KC area because KC don’t have a test account).

To do this go to the Edit ppp-0 screen again and this time use the Login Name: `bt_test@startup_domain`. The Password doesn’t matter; you can leave that alone. Submit the changes and again check the WAN status. Do you now have a valid IP Address? If so then the problem is with your account: Contact your ISP and tell...
them you’ve tried the BT test account and got a successful login but you can’t get your ISP account to work. If you still get no login even with the bt_test account then there might be something wrong with your line.

26.3 PC cannot access the Internet

So, your status screen shows you are logged into the ISP but you still haven’t got internet access.

26.3.1 Pinging the WAN side of the router

First of all let’s do some basic ‘ping’ tests. Ping is a basic IP programme that allows you to test connectivity to IP’s. The next section explains how to use the ping command. First of all, goto the ‘ppp-0’ status from the front page of the router Status and note down the WAN IP address.

Now try and ‘ping’ that WAN address. You should get a reply. If you don’t then first of all ensure that you have remembered to enable NAT (we are assuming here that you are using NAT routing of course). Goto the Services/NAT screen and ensure that NAT is showing Enabled:

Next ensure that you have set Default Route to Enable. Goto WAN on the management screens:
Then click on the magnifying glass to examine the ppp settings...

Check that the ‘Default Route’ is set to ‘Enable’.
If not then click on the Pencil to goto the ppp edit screen and change the settings.
Hopefully you should now be able to ping the WAN side of the router.

### 26.3.2 Pinging the internet

The next stage is to try and ping a site on the internet. The easiest way to test this is to do a test ping to the DNS address of your ISP. If you remember, back in Part 2 of Chapter 3, one of the things you needed to know was the DNS address of your ISP. As mentioned, this is information you need to get from your ISP OR, if you can’t get this information from your ISP then you could check the table of popular DNS values given above (see Contents for the correct chapter). Or, failing that, you can use the DNS address from our ISP which is 212.50.160.100 but this is not guaranteed.

Anyway, assuming that you have a valid DNS address try pinging it. Do you get a reply? If not then I would check the DNS address you are using ☺

### 26.4 Connecting to a web site

So, you have an ADSL connection, you are logging in with the ISP okay and you can ping your ISP’s DNS but you still can’t get to a web site in your browser. Check the IP settings for your computer. Ensure that your computer has a default gateway entry which is the address of the router. Also ensure that your computer IP settings show the correct DNS value. If still no joy check the DNS address with the ISP; perhaps even try a different DNS value.

You might also have a problem with the MTU setting on your computer. Check this setting as detailed below.

### 26.5 Diagnosing Problem using IP Utilities

#### 26.5.1 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 192.168.7.1
```

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

If the target computer receives the message, a Command Prompt window displays like that shown in Figure 66.
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 SAR110 is working (using the preconfigured default LAN IP address 192.168.7.1) 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.

26.5.2 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 in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

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

\texttt{nslookup}

Click \texttt{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.microsoft.com.

The window will display the associate IP address, if known, as shown in Figure 67.
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.

### 26.6 MTU value. What is it and why does having the correct value matter?

**26.6.1 What are the symptoms of having a wrong MTU value?**

Typical symptoms of having an incorrect MTU value are:

- Very slow web access
- Inability to connect to some web sites
- Can’t send large emails or emails with attachments
- PC crashes trying to send large emails or emails with attachments or to multiple recipients

**26.6.2 So what is it?**

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can’t handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled. Most computer operating systems provide a default MTU value that is suitable for most users.

**26.6.3 Why is it important?**

The main reason one would be concerned with changing a default MTU value is the problem of IP fragmentation. IP fragmentation occurs when you pass through a router with an MTU less than the MTU you are using. If your TCP/IP stack is set to a MTU of 1500 and you hit a router with a MTU set to 576. The router will fragment your packets down to 576. When you finally reach your destination, those datagrams will have to be re-assembled and this will slow down your throughput, e.g., download time.

You can check on fragmentation and other errors by using the `netstat -s` (use `netstat -s | more` to stop the scroll and `netstat -x` to see the options available to you) command and checking the IP statistics. For example, note the Datagram is the MTU.

**IP Statistics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Received</td>
<td>152113</td>
</tr>
<tr>
<td>Received Header Errors</td>
<td>0</td>
</tr>
<tr>
<td>Received Address Errors</td>
<td>0</td>
</tr>
<tr>
<td>Datagrams Forwarded</td>
<td>0</td>
</tr>
<tr>
<td>Unknown Protocols Received</td>
<td>0</td>
</tr>
</tbody>
</table>
Received Packets Discarded = 0
Received Packets Delivered = 152113
Output Requests = 122510
Routing Discards = 0
Discarded Output Packets = 0
Output Packet No Route = 0
Reassembly Required = 0
Reassembly Successful = 0
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0

Another problem to check out is whether or not you are having excessive retransmissions. The lower your retransmit rate (Segments Sent/Segments Retransmitted) the better. If you have a retransmit rate in Windows, check Microsoft there are some patches can fix this type of problem. In this example (using netstat -s), the rate is about 1.5%. Note the Segment is the MSS.

TCP Statistics

Active Opens = 476
Passive Opens = 22
Failed Connection Attempts = 27
Reset Connections = 219
Current Connections = 10
Segments Received = 149817
Segments Sent = 117832
Segments Retransmitted = 1820

26.6.4 So how do I set the MTU value on my Windows PC?

In order to alter the MTU value on a Windows systems involves modifying the registry. Personally I use an MTU value of 1200 decimal (hex 4B0). You might get away with a higher value but I find that 1200 always works.

The easiest way to modify the MTU value in your Windows registry is to use the DrTCP utility. A copy of this utility is included on the manuals/drivers CD supplied with your router. Alternatively it can be downloaded at

http://www.dslreports.com/front/drtc.html

Run DrTCP and a screen similar to this…. Is shown:
To alter the MTU value make sure you have selected the correct LAN adapter under Adapter Settings. Then enter the MTU value you want to use (as in the example above).

26.6.5 Problems with ‘SpyWare’

Sometimes you might experience router problems when using spyware software like Overnet or e-Mule. This is because the router could get more IP sessions trying to go through than it can cope with.

To solve this you can use a CLI command (see CLI commands above) to increase the maximum number of IP sessions allowed. The command is

```
modify nbsize maxipsess 'value'
```

See the section on CLI commands for details on this command.
## Appendix D Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10BASE-T</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>100BASE-T</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>ADSL</strong></td>
<td>Asymmetric Digital Subscriber Line. The most commonly deployed &quot;flavor&quot; of DSL for home users. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.</td>
</tr>
<tr>
<td><strong>analog</strong></td>
<td>Of data, having a form is analogous to the data's original waveform. The voice component in DSL is an analog signal. See also digital.</td>
</tr>
<tr>
<td><strong>ATM</strong></td>
<td>Asynchronous Transfer Mode. A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See also data rate.</td>
</tr>
<tr>
<td><strong>authenticate</strong></td>
<td>To verify a user's identity, such as by prompting for a password.</td>
</tr>
<tr>
<td><strong>binary</strong></td>
<td>The &quot;base two&quot; system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See also bit, IP address, network mask.</td>
</tr>
<tr>
<td><strong>bit</strong></td>
<td>Short for &quot;binary digit,&quot; a bit is a number that can have two values, 0 or 1. See also binary.</td>
</tr>
<tr>
<td><strong>bps</strong></td>
<td>bits per second</td>
</tr>
<tr>
<td><strong>bridging</strong></td>
<td>Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The SAR110 can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See also routing.</td>
</tr>
<tr>
<td><strong>broadband</strong></td>
<td>A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.</td>
</tr>
<tr>
<td><strong>broadcast</strong></td>
<td>To send data to all computers on a network.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Dynamic Host Configuration Protocol. DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address.</td>
</tr>
</tbody>
</table>
from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.

**DHCP relay**
Dynamic Host Configuration Protocol relay
A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the SAR110’s interfaces can be configured as a DHCP relay. See DHCP.

**DHCP server**
Dynamic Host Configuration Protocol server
A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.

digital
Of data, having a form based on discrete values expressed as binary numbers (0’s and 1’s). The data component in DSL is a digital signal. See also analog.

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

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

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

**DSL**
Digital Subscriber Line
A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.

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

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

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

firewall
Any method of protecting a computer or LAN connected to the Internet from intrusion or attack from the outside. Some firewall protection can be provided by packet filtering and Network Address Translation services.
FTP
File Transfer Protocol
A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

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

Gbps
Abbreviation for Gigabits ("GIG-uh-bits") per second, or one billion bits per second. Internet data rates are often expressed in Gbps.

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

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

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

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

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

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

in-line filter
See microfilter.

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

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

IP
See TCP/IP.

IP address
Internet Protocol address
The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See also domain name, network mask.
ISP
Internet Service Provider
A company that provides Internet access to its customers, usually for a fee.

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

LED
Light Emitting Diode
An electronic light-emitting device. The indicator lights on the front of the SAR110 are LEDs.

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

mask
See network mask.

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

microfilter
In splitterless deployments, a microfilter is a device that removes the data frequencies in the DSL signal, so that telephone users do not experience interference (noise) from the data signals. Microfilter types include in-line (installs between phone and jack) and wall-mount (telephone jack with built-in microfilter). See also splitterless.

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

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

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

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

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

packet
Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
ping
Packet Internet (or Inter-Network) Groper
A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

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

POTS
Plain Old Telephone Service
Traditional analog telephone service using copper telephone lines. Pronounced "pots." See also PSTN.

POTS splitter
See splitter.

PPP
Point-to-Point Protocol
A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the SAR110 uses two forms of PPP called PPPoA and PPPoE. See also PPPoA, PPPoE.

PPPoA
Point-to-Point Protocol over ATM
One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.

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

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

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

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

RJ-11
Registered Jack Standard-11
The standard plug used to connect telephones, fax machines, modems, etc. to a telephone jack. It is a 6-pin connector usually containing four wires.

RJ-45
Registered Jack Standard-45
The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

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

rule
See filtering rule, NAT rule.

SDNS
Secondary Domain Name System (server)
A DNS server that can be used if the primary DNS server is not available. See DNS.
SNMP
Simple Network Management Protocol
The TCP/IP protocol used for network management.

splitter
A device that splits off the voice component of the DSL signal to a separate line, so that data and telephone service each have their own wiring and jacks. The splitter is installed by your telephone company where the DSL line enters your home. The CO also contains splitters that separate the voice and data signals, sending voice to the PSTN and data on high-speed lines to the Internet. See also CO, PSTN, splitterless, microfilter.

splitterless
A type of DSL installation where no splitter is installed, saving the cost of a service call by the telephone company. Instead, each jack in the home carries both voice and data, requiring a microfilter for each telephone to prevent interference from the data signal. ADSL is usually splitterless; if you are unsure if your installation has a splitter, ask your DSL provider. See also splitter, microfilter.

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

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

TCP
See TCP/IP.

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

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

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

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

twisted pair
The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category
5 (CAT 5) is used for 100BASE-T networks. See also 10BASE-T, 100BASE-T, Ethernet.

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

**VC**  
Virtual Circuit  
A connection from your ADSL router to your ISP.

**VCI**  
Virtual Circuit Identifier  
Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See also VC.

**VPI**  
Virtual Path Identifier  
Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See also VC.

**WAN**  
Wide Area Network  
Any network spread over a large geographical area, such as a country or continent. With respect to the SAR110, WAN refers to the Internet.

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

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

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

**WWW**  
World Wide Web  
Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.
Appendix E ALG’s

Below shows the list of Application Layer Gateways (ALG’s) that are automatically supported by the SAR110. ALG’s are programmes for which the router knows which ports to open up for outgoing traffic:

<table>
<thead>
<tr>
<th>Port Num</th>
<th>Protocol</th>
<th>ALG Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>TCP</td>
<td>FTP</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>LDAP</td>
</tr>
<tr>
<td>407</td>
<td>UDP</td>
<td>TIMBUKTU</td>
</tr>
<tr>
<td>554</td>
<td>TCP</td>
<td>RTSP</td>
</tr>
<tr>
<td>1002</td>
<td>TCP</td>
<td>LDAP</td>
</tr>
<tr>
<td>1701</td>
<td>UDP</td>
<td>L2TP</td>
</tr>
<tr>
<td>1719</td>
<td>UDP</td>
<td>H323_RAS</td>
</tr>
<tr>
<td>1720</td>
<td>TCP</td>
<td>H323_Q931</td>
</tr>
<tr>
<td>1723</td>
<td>TCP</td>
<td>PPTP</td>
</tr>
<tr>
<td>1863</td>
<td>TCP</td>
<td>MSN_MSGR</td>
</tr>
<tr>
<td>6301</td>
<td>UDP</td>
<td>SGICompCore</td>
</tr>
<tr>
<td>6661</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6662</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6663</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6664</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6665</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6666</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6667</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6668</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>6669</td>
<td>TCP</td>
<td>MIRC</td>
</tr>
<tr>
<td>7070</td>
<td>TCP</td>
<td>REAL AUDIO</td>
</tr>
<tr>
<td>7648</td>
<td>TCP</td>
<td>CUSEEME</td>
</tr>
</tbody>
</table>
Index

100BASE-T .................................................. 199
10BASE-T .................................................... 199
ADSL ............................................................ 199
ADSL cable .................................................... 18
ADSL port ...................................................... 18
Alarm Monitor window .................................. 146
Alarm page ................................................... 145
Alarms .......................................................... 145
ALG .............................................................. 206
Analog .......................................................... 199
Asynchronous Transfer Mode ........ See ATM
ATM .............................................................. 199
defined .......................................................... 95
viewing configuration ................................ 95
ATM VCC – Add page ....................................... 96, 98
ATM VCC Configuration page ......................... 95
Attacks ......................................................... 121
BASIC NAT flavor .......................................... 75
BIMAP NAT flavor ......................................... 79
Binary numbers ............................................. 187, 199
Bits ...................................................... 187, 199
Black List ...................................................... 121
managing ........................................................ 122
Blocked Protocols page .................................. 138
Bridge Configuration page .............................. 117
Bridge forwarding table .................................. 115
Bridges vs routers ........................................... 116
Bridging ......................................................... 199
defined .......................................................... 115
defining interfaces ....................................... 117
with IP-enabled interfaces .............................. 118
Broadband .................................................... 199
Broadcast ..................................................... 199
Bytes ............................................................ 187
Commit & Reboot page ................................. 43
Computers
configuring IP information ............................. 19
Configuration Manager
overview ..................................................... 37
Connectors
rear panel .................................................... 15
Data packet .................................................... 63
Date and time, changing ................................. 40
Default configuration ..................................... 36
Default gateway ............................................ 86
De-militarized zones ...................................... 126
Denial of Service .......................................... 121
DHCP
defined .......................................................... 53, 199
device modes .................................................. 54
setting operating mode ................................. 61
DHCP Address Table page .............................. 59
DHCP client
configuring device as .................................... 47
defined .......................................................... 53
DHCP Configuration page .............................. 55, 61
DHCP relay ...................................................... 200
configuring device as .................................... 54, 60
DHCP Relay Configuration page ....................... 60
DHCP server ..................................................... 200
configuring the device as ............................... 55
defined .......................................................... 53
modifying, viewing pools ................................ 58
pools ............................................................. 53
using a LAN device as .................................... 54
using existing on LAN .................................... 45, 47
using ISP
as ................................................................. 54
using the device as ........................................54
viewing assigned addresses ..........................59
DHCP Server Pool—Add page .......................56
Diagnostics ..............................................150
Diagnostics page .........................................150
Digital ................................................................200
DNS ................................................................57, 81, 200
defined ..........................................................81
relay .............................................................82
DNS Configuration page ..................................83
Domain name ..................................................57, 200
Domain Name System .................................. See DNS
download .....................................................200
DrTCP ..........................................................197
DSL ..............................................................200
defined ..........................................................200
DSL interface ..................................................49
DSL Interval Statistics page .........................143
DSL Parameters page ....................................142
DSL Statistics page .......................................142
DSL Status page ...........................................141
Dynamically assigned IP addresses ..................53
e-Mule ..........................................................198
EOA ..............................................................106
defined ..........................................................107
settings ..........................................................107
EOA interface .................................................49
EOA Interface – Add page .............................109
EOA page .......................................................107
Eth-0 interface ..............................................36
defined ..........................................................36
Ethernet ........................................................200
defined ..........................................................200
Ethernet cable ................................................18
straight-through vs crossover ........................189
Features .......................................................11
FILTER NAT flavor ...........................................77
Filtering rule ...................................................200
Firewall .........................................................200
settings ........................................................121
Firewall Blacklisted Hosts page ....................122
Firewall Configuration page .........................119
Front panel .....................................................14
FTP ..............................................................201
Gateways .........................................................57
in DHCP pools ...............................................57
Gateway ........................................................86
defined ..........................................................86
Gigabit .........................................................201
Hardware connections ..................................17, 18
Home Tab ....................................................39
Hop ..............................................................201
defined ..........................................................201
Hop count ......................................................92, 201
Host ............................................................201
Host ID ........................................................183
HTTP ..........................................................201
HTTP port, modifying address ........................150
Image Upgrade page .......................................147
In-line filter .................................................. See Microfilter
Internet .........................................................201
Intranet ........................................................201
IP address ......................................................87
in device’s routing table .................................87
IP address pools ...............................................59
excluding addresses ....................................59
modifying ....................................................59
IP Address Table page ....................................49
IP addresses ..................................................201
explained ......................................................183
viewing device’s ............................................49
IP configuration .............................................201
Windows 2000 ..............................................20
Windows 95/98 ....................................22, 25
Windows Me ........................................21
Windows NT 4.0 ..................................24

IP Configuration
Windows XP ......................................19
IP data packet ......................................63
IP Filter Configuration page ....................126
IP Filter Rule – Statistics page ..................136
IP Filter Rule – Add Page ........................128
IP filter rules
adding ..................................................127
examples .............................................133
settings ...............................................129
IP filter sessions ....................................136
IP Filter Sessions page ............................136
IP filters
viewing statistics ...................................136
IP Global Statistics page .........................50

IP information
configuring on LAN computers.................19
IP Route – Add page ................................89
IP Route Table page ................................87
IP routes
adding ..................................................88
manually configuring ...............................86
type ....................................................88
IP Routes
defined ...............................................85

IPoA
defined .............................................111
IPoA Interface – Add page .......................113
IPoA page ...........................................111
ISP ....................................................202
LAN ..................................................202
LAN Configuration page ........................46
LAN interface .......................................60
configuring multiple .........................50, 50
LAN IP address ....................................45, 47
configuring ..........................................45
specifying ...........................................45
viewing ..............................................49

LAN network mask ...............................47

LEDs ..................................................14, 202
troubleshooting ....................................189

Login
to Configuration Manager ......................37

Loopback IP address ................................49

MAC addresses ....................................202
in DHCP Address Table ..........................59
in DHCP pools ......................................57
Mask ..............................................See Network mask

Mbps ...................................................202
Microfilter .........................................202
MTU ...................................................196

NAPT (NAT flavor) ................................70

NAT ..................................................202
adding rules ........................................70
BASIC flavor .......................................75
BIMAP flavor .......................................79
default configuration .........................64, 64
defined ...............................................63
FILTER flavor .......................................77
global settings ....................................64
napt flavor ..........................................70
PASS flavor ........................................80
RDR flavor .........................................72
viewing performance statistics ..............67

NAT Configuration page .......................64

NAT Rule Configuration page .................67
NAT Rule Global Statistics page ..............67
NAT Rule Statistics page ......................67
NAT Rule—Add page - basic ....................76
NAT Rule—Add page - bimap ....................79
NAT Rule—Add page - filter ....................77
<table>
<thead>
<tr>
<th>Index</th>
<th>Solwise SAR110 ADSL Ethernet Router User's Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Rule—Add page - napt ........................................ 71</td>
<td>DNS Configuration .................................. 83</td>
</tr>
<tr>
<td>NAT Rule—Add page - pass ........................................... 80</td>
<td>DSL Interval Statistics ......................... 143</td>
</tr>
<tr>
<td>NAT Rule—Add page - rdr ........................................... 73</td>
<td>DSL Parameters ........................................ 142</td>
</tr>
<tr>
<td>NAT Translation – Details page ...................................... 69</td>
<td>DSL Statistics ........................................ 142</td>
</tr>
<tr>
<td>NAT Translations page ............................................. 68</td>
<td>DSL Status ............................................. 141</td>
</tr>
<tr>
<td>Navigating ..................................................................... 38</td>
<td>EOA ................................................................ 107</td>
</tr>
<tr>
<td>Netmask ................................................................ 202</td>
<td>EOA Interface - Add .................................... 109</td>
</tr>
<tr>
<td>Network ......................................................................... 202</td>
<td>Firewall Blacklisted Hosts .......................... 122</td>
</tr>
<tr>
<td>Network Address Translation ........................................ 202</td>
<td>Firewall Configuration ................................ 119</td>
</tr>
<tr>
<td>Network classes ........................................................ 184</td>
<td>Image Upgrade ............................................. 147</td>
</tr>
<tr>
<td>Network ID ............................................................... 183</td>
<td>IP Address Table ........................................ 49</td>
</tr>
<tr>
<td>Network interface card ................................................ 11</td>
<td>IP Filter Configuration ................................ 126</td>
</tr>
<tr>
<td>Network mask ............................................................. 202</td>
<td>IP Filter Rule - Add .................................... 128</td>
</tr>
<tr>
<td>Network mask ............................................................. 184</td>
<td>IP Filter Rule - Statistics ......................... 136</td>
</tr>
<tr>
<td>NIC ................................................................................. 202</td>
<td>IP Filter Sessions ...................................... 136</td>
</tr>
<tr>
<td>Node on network defined ................................................ 45</td>
<td>IP Global Statistics ...................................... 50</td>
</tr>
<tr>
<td>Notational conventions .................................................. 12</td>
<td>IP Route - Add ............................................ 89</td>
</tr>
<tr>
<td>nslookup ........................................................................ 195</td>
<td>IP Route Table ............................................ 87</td>
</tr>
<tr>
<td>Overnet .......................................................................... 198</td>
<td>IPoA ............................................................. 111</td>
</tr>
<tr>
<td>Packet ............................................................................. 202</td>
<td>IPoA Interface .............................................. 113</td>
</tr>
<tr>
<td>Packets .......................................................................... 202</td>
<td>LAN Configuration .......................................... 46</td>
</tr>
<tr>
<td>Packets filtering .......................................................... 125</td>
<td>NAT Configuration ........................................ 64</td>
</tr>
<tr>
<td>Pages .............................................................................. 202</td>
<td>NAT Rule Add - basic ..................................... 76</td>
</tr>
<tr>
<td>Alarm ............................................................................. 145</td>
<td>NAT Rule Add - bimap .................................. 79</td>
</tr>
<tr>
<td>Alarm Monitor window .................................................... 146</td>
<td>NAT Rule Add - filter ................................... 77</td>
</tr>
<tr>
<td>ATM VCC - Add ............................................................... 96, 98</td>
<td>NAT Rule Add - napt .................................... 71</td>
</tr>
<tr>
<td>ATM VCC Configuration .................................................. 95</td>
<td>NAT Rule Add - pass ..................................... 80</td>
</tr>
<tr>
<td>blocked Protocols .......................................................... 138</td>
<td>NAT Rule Add - rdr ...................................... 73</td>
</tr>
<tr>
<td>Bridge Configuration ..................................................... 117</td>
<td>NAT Rule Configuration ................................... 67</td>
</tr>
<tr>
<td>Commit &amp; Reboot ............................................................ 43</td>
<td>NAT Rule Global Statistics ............................... 67</td>
</tr>
<tr>
<td>DHCP Address Table ....................................................... 59</td>
<td>NAT Rule Statistics ....................................... 67</td>
</tr>
<tr>
<td>DHCP Configuration ....................................................... 55, 61</td>
<td>NAT Translations ........................................... 68</td>
</tr>
<tr>
<td>DHCP Relay Configuration .............................................. 60</td>
<td>NAT Translations - Details ............................... 69</td>
</tr>
<tr>
<td>DHCP Server Pool - Add .................................................. 56</td>
<td>Port Settings ................................................. 152</td>
</tr>
<tr>
<td>Diagnostics ................................................................. 150</td>
<td>PPP - Detail .................................................. 102</td>
</tr>
<tr>
<td>DST ................................................................................. 104</td>
<td>PPP Configuration .......................................... 99</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Upgrading software</td>
<td>146</td>
</tr>
<tr>
<td>Upstream</td>
<td>205</td>
</tr>
<tr>
<td>User Password Configuration page</td>
<td>42</td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>27, 38</td>
</tr>
<tr>
<td>VC</td>
<td>205</td>
</tr>
<tr>
<td>VCI</td>
<td>205</td>
</tr>
<tr>
<td>VPI</td>
<td>205</td>
</tr>
<tr>
<td>WAN</td>
<td>205</td>
</tr>
<tr>
<td>WAN interface</td>
<td></td>
</tr>
<tr>
<td>configuring multiple</td>
<td>50</td>
</tr>
<tr>
<td>IP address</td>
<td>49</td>
</tr>
<tr>
<td>Web browser</td>
<td>205</td>
</tr>
<tr>
<td>requirements</td>
<td>11</td>
</tr>
<tr>
<td>version requirements</td>
<td>37</td>
</tr>
<tr>
<td>Web browsers</td>
<td></td>
</tr>
<tr>
<td>compatible versions</td>
<td>37</td>
</tr>
<tr>
<td>Web page</td>
<td>205</td>
</tr>
<tr>
<td>Web site</td>
<td>205</td>
</tr>
<tr>
<td>Windows NT</td>
<td></td>
</tr>
<tr>
<td>configuring IP information</td>
<td>24</td>
</tr>
<tr>
<td>World Wide Web</td>
<td>205</td>
</tr>
</tbody>
</table>