



Sarian Systems 2000 Series Reference Guide

© 2002-2003 Sarian Systems Limited. All rights reserved. No part of this document covered by copyright may be reproduced or copied in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems without written permission of Sarian Systems Ltd.

Sarian Systems reserve the right to modify or revise all or part of this document, its contents, and any products described herein at any time without prior notification and shall not be responsible for any loss, cost, or damage, including consequential damage, caused by reliance on these materials.

Issue 1.7, 9th June 2003. Part # 6222-0001

CONTENTS

PREFACE	5
1 INTRODUCTION	6
1.1 Unpacking The Unit	6
1.2 Front Panel Features	7
1.3 Rear Panel Features	8
1.4 GPRS SIM Card Installation	9
2 USING THE WEB INTERFACE	12
2.1 Installing The Driver File	12
2.2 Creating A New Connection	14
2.3 Configuring A New Connection	16
2.4 Initiating A Connection	18
3 THE COMMAND LINE INTERFACE	20
3.1 The “AT” Command Prefix	20
3.2 The Escape Sequence	21
3.3 Result Codes	21
3.4 “S” Registers	21
3.5 Application Commands	22
3.6 The Active Port	22
3.7 Establishing A Remote Connection	23
4 CONFIGURING YOUR UNIT	24
4.1 Logging In	24
4.2 The Configuration Pages	25
4.3 Configure ► ADAPT	26
4.4 Configure ► Analyser	28
4.5 Configure ► ASY Ports	33
4.6 Configure ► Backup IP addresses	35
4.7 Configure ► Calling Numbers	36
4.8 Configure ► Command Mappings	37
4.9 Configure ► DHCP Server	37
4.10 Configure ► DNS Update	39
4.11 Configure ► Ethernet	41
4.12 Configure ► Event Handler	44
4.13 Configure ► Firewall	46
4.14 Configure ► Firewall Timers	48
4.15 Configure ► FTP Relay Agents	49
4.16 Configure ► General	51
4.17 Configure ► GPRS Module	56
4.18 Configure ► ISDN LAPB	59
4.19 Configure ► ISDN LAPD	62

4.20	Configure ▶ IP Routes	64
4.21	Configure ▶ IPSEC	67
4.22	Configure ▶ IPsec ▶ Eroutes	70
4.23	Configure ▶ IPsec ▶ Default Eroute	74
4.24	Configure ▶ NUI Mappings	75
4.25	Configure ▶ PPP	76
4.26	Configure ▶ Protocol Bindings	94
4.27	Configure ▶ SMS Edit	95
4.28	Configure ▶ SMTP	95
4.29	Configure ▶ SNTP	97
4.30	Configure ▶ Static NAT Mappings	98
4.31	Configure ▶ SYNC Ports	99
4.32	Configure ▶ Time	100
4.33	Configure ▶ Time Bands	100
4.34	Configure ▶ TPAD	102
4.35	Configure ▶ Users	109
4.36	Configure ▶ X.25 Macros	110
4.37	Configure ▶ X.25 PADS	112
4.38	Configure ▶ X.25 PADS ▶ Parameters	115
4.39	Configure ▶ X.25 Switch	120
4.40	Saving configuration settings.	125
5	STATISTICS PAGES	127
5.1	Statistics ▶ Adapt	127
5.2	Statistics ▶ ASY Ports	127
5.3	Statistics ▶ DNS Update	128
5.4	Statistics ▶ Ethernet	128
5.5	Statistics ▶ IP	128
5.6	Statistics ▶ IPsec ▶ Dynamic Eroutes	129
5.7	Statistics ▶ IPsec ▶ IKE SAs	129
5.8	Statistics ▶ IPsec ▶ IPsec SAs	129
5.9	Statistics ▶ PPP	130
5.10	Statistics ▶ SYNC Channels	130
5.11	Statistics ▶ TPAD	131
5.12	Statistics ▶ X.25 PAD	132
6	STATUS PAGES	134
6.1	Status ▶ Analyser Trace	134
6.2	Status ▶ DHCP Server	134
6.3	Status ▶ Event Log	135
6.4	Status ▶ File Directory	135
6.5	Status ▶ Firmware Versions	135
6.6	Status ▶ GPRS Module	135
6.7	Status ▶ IGMP Groups	136
6.8	Status ▶ ISDN BRI	136
6.9	Status ▶ Web Directory	136

6.10	Status ► Web Server	137
6.11	Status ► X.25 Sessions	137
7	THE FILING SYSTEM	138
7.1	System Files	138
7.2	Filing System Commands	138
8	USING V.120	141
8.1	Initial Set Up	141
8.2	Initiating A V.120 Call	141
8.3	Answering V.120 Calls	141
9	X.25 PACKET SWITCHING	143
9.1	Introduction.	143
9.2	X.28 Commands	143
10	PPP OVER ETHERNET	150
11	IPSEC AND VPN'S.	151
11.1	What is IPsec ?	151
11.2	Data Encryption methods.	151
12	FIREWALL SCRIPTS	155
12.1	Firewall script syntax.	155
12.2	Filtering on port numbers.	160
12.3	Filtering on TCP flags.	161
12.4	Filtering on ICMP codes.	162
12.5	Stateful inspection.	163
12.6	The fwlog.txt File.	166
12.7	Debugging a Firewall	168
13	REMOTE MANAGEMENT	170
13.1	Remote Management Using V.120	170
13.2	Remote Management Using Telnet	170
13.3	Remote Management Using FTP	170
13.4	Remote Management Using X.25	171
14	THE EVENT LOG	172
14.1	What Is The Event Log?	172
14.2	The logcodes.txt File	173
15	AT COMMANDS	175
15.1	D Dial	175
15.2	H Hang-up	175
15.3	Z Reset	175
15.4	&C DCD Control	175
15.5	&F Load Factory Settings	176
15.6	&V View Profiles	176
15.7	&W Write sregs.dat	176

15.8 &Y Set Default Profile	176
15.9 &Z Store phone number	177
15.10\LS Lock Speed	177
15.11\PORT Set Active Port	177
15.12\at Ignore invalid AT commands	178
16 "S" REGISTERS	179
16.1 S0 V.120 Answer Enable	179
16.2 S2 Escape Character	179
16.3 S23 Parity	180
16.4 S15 Data forwarding timer	180
16.5 S31 ASY Interface Speed	180
16.6 S33 DTR dialling	181
16.7 S45 DTR Loss De-bounce	181
17 GENERAL SYSTEM COMMANDS	182
17.1 CONFIG Show/Save Configuration	182
17.2 REBOOT Reboot Unit	182
18 ASY PORT CONNECTORS	183
19 LOGCODES.TXT	184
20 EMAIL TEMPLATES	190
20.1 Template Structure	190

PREFACE

Sarian Systems 2000 series products are extremely versatile and may be used in a wide variety of applications. It would not be possible to describe in detail all such applications in a single guide. Consequently, this guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

Throughout this manual certain typographical conventions are used as follows:

Text Type	Meaning
Text like this ...	is standard text.
Text like this...	indicates points that are of particular importance.
<i>Text like this ...</i>	indicates commands entered by the user.
Text like this ...	indicates responses from the unit to commands you enter at the command line.
Configure ► Save	is a reference to the Windows or the unit's menu system.

Requests for corrections or amendments to this guide are welcome and should be addressed to:

Sarian Systems Ltd.
Riverside Business Park
Leeds Road, Ilkley
West Yorkshire
LS29 8JZ

Safety and operational notices.

1. With respect to European EMC requirements, Sarian 2000 series are Class A products. In a domestic environment, these products may cause radio interference in which case the user may be required to take adequate measures.
2. For office and domestic operation Sarian 2000 series products are designed for use only with the approved mains power transformer supplied by Sarian Systems Ltd.
3. Ports that are capable of connecting to other apparatus are defined as SELV ports. To ensure conformity with EN60950 ensure that these ports are only connected to ports of the same type on other apparatus.
4. Do not attempt to repair the products. They contain no electronic components that can be serviced or replaced by the user. Any attempt to service or repair the unit by the user will void the product warranty.
5. Sarian 2000 series products are designed for indoor use only and should be used in an environment that is suitable for computers and other electronic equipment.
6. Users of models incorporating GSM/GPRS capability should ensure that the unit (when used with the supplied aerial) is positioned at least 1 metre away from themselves.

1 Introduction

Thank you for purchasing a Sarian 2000 series product. There are number of models in the 2000 series which at the time of writing include:

Model	Description
IR2140	ISDN router, 4 serial ports
IM2040	ISDN multiplexer, 4 serial ports
GR2130	GPRS / ISDN router, 3 serial ports
IR2420	ISDN router / 3-port hub, 2 serial ports
GR2410	GPRS / ISDN router / 3-port hub, 1 serial port

This guide describes the operation of all of the standard features available across the range at the time of writing. Consequently, some of the features described in this guide may only be available on certain models or must be purchased as “feature packs”. You should refer to the specification of the particular model you have purchased to ascertain which features are supported as standard.

In addition to a comprehensive range of communications capabilities, Sarian 2000 series products provide a combination of powerful, yet easy to use, configuration, management and diagnostic tools. The LAN interfaces supports 10/100-mode operation with auto-detect and, depending upon the model, up to four asynchronous serial devices may be connected to share a single WAN interface (e.g. ISDN).

In many applications, the serial ports will be configured to appear as if they were standard “AT” modems and behave accordingly. However, many other standard protocols are supported (e.g. B and D-channel X.25, PPP, V.120, TPAD etc). This makes it simple and cost-effective to migrate existing terminal equipment, which uses the analogue telephone network, to faster, more reliable and cost-effective digital services.

All major features of the unit can be configured using a standard Internet Web browser. This can be done locally (via a serial port or LAN port) or remotely (via the WAN connection). A built-in Web-server and flexible FLASH-memory based filing system mean that the unit can also be customised to provide application specific functions, statistics and diagnostic information.

Sarian 2000 series products are ideal for applications such as general IP routing, on-line authorisation of credit card transactions or terminal serving. They are able to emulate most of the standard industry protocols, such as TPAD, and can carry out both APACS 30 and APACS 50 transactions with remote hosts much faster than with traditional analogue modems, whilst requiring no changes either to the host or to the terminal software.

Your 2000 series unit also supports up to four Switched Virtual Circuits (SVC’s) over the ISDN D-channel (where this service is available from your network supplier), simultaneously with two 64Kb/s B channel circuits, thus enabling you to gain the maximum benefit from your investment in ISDN lines.

An optional advanced feature allows the encapsulation of TCP/IP data in X.25 packets allowing the unit to be used to carry “always on” traffic between two LANs without using the ISDN B channels.

1.1 Unpacking The Unit

Open the box and carefully take out all of the items. These should include a packing list that details the full contents of the package.

Check each item on the packing list against the package contents. If any item is missing or damaged, please contact your supplier. You should also make a record of any damage that may have occurred during shipping and report it to the carrier.

1.2 Front Panel Features

The front panel of each product incorporates a number of LED indicators that will illuminate steady or flashing when the unit is in use. The precise number and function of the LED's will depend upon the model you have purchased. The illustration below is of the IR2140.



The following descriptions cover all the different types of indicator that are used on 2000 series products:

ON (all models)

The **ON** indicator will illuminate steady red when power is applied.

LAN (router and hub models only)

The **LAN** indicator(s) will illuminate steady when there is a connection to the associated LAN port or flash when data is transmitted or received on that port.

D, B1, B2 (ISDN models only)

The **D**, **B1** and **B2** indicators reflect the status of the ISDN BRI connection as follows:

- ◆ The **D** indicator will illuminate steady when the ISDN LAPD link is established. It will flash slowly when a D-channel X.25 link has been raised. When the D-channel X.25 link is passing data, it will flash quickly.
- ◆ The **B1** and **B2** indicators will illuminate steady when the respective B-channel is active. If data is being transmitted or received over any of these channels, the appropriate indicator will flash. The **B2** indicator will also flash when the unit is first powered up to indicate that the unit is performing a self-test. When it stops flashing the unit is ready to use.

DTE

The **DTE** indicators (up to four) will illuminate steady if a terminal is connected to the corresponding port and the DTR signal is on. If data is being transmitted via a particular port the corresponding indicator will flash.

NET, SIM, DAT (GPRS models only)

These indicators relate to GPRS operation and operate as follows:

- ◆ The **NET** indicator illuminates steady when a GPRS network has been detected. It is also **used** to indicate the GSM signal strength when no separate signal strength indicators are available. When signal strength is low it will flash slowly. A stronger signal will result in a faster flash rate.
- ◆ The **SIM** indicator illuminates steady when a valid SIM card is installed in the unit.
- ◆ The **DAT** indicator flashes to indicate that data is being transferred over GPRS.

note

On models with both ISDN and GPRS the D, B1 and B2 indicators are shared with the NET, SIM and DAT indicators so that their function depends on how the unit is configured.

1.3 Rear Panel Features

The rear panels of the 2000 series products incorporate the power supply connector, serial port connectors and, if applicable connectors for LAN cables and GPRS aerials. Some models also include a “user” switch that is normally used to reset the unit. The following illustration shows the rear panel of the IR2140.



The following descriptions cover all the different types of connector that are used on 2000 series products.

1.3.1 The power connector

Sockets marked **12V DC** or **DC IN** are used to connect the mains power adapter. To connect the power supply push the plug from the mains adapter firmly into the socket on the rear of the unit before connecting the power supply to the mains AC outlet.

note:

You must not use any power supply adapter other than that supplied by Sarian Systems. Doing so may damage the product and will invalidate the warranty.

When you first apply power to the unit, the **ON** indicator will illuminate and after about 10 seconds, the unit will initiate a series of diagnostic self-tests. During this process one or more of the other indicators (depending on the model), will flash to show that the unit is busy. When the flashing stops, the unit is ready to use.

1.3.2 LAN connectors

Connectors labelled **LAN (or 10/100 LAN)** are used to connect the unit to a 10/100-BaseT LAN.

On models with a single LAN port (e.g. IR2140), the router may be connected to your LAN (directly or via a suitable hub), using the CAT5 cable supplied.

On models with integral hub capability (e.g. IR2410), the operation of the individual ports will depend upon the configuration of the unit i.e. they may be configured to act as hub ports (so as to provide access to a LAN for other connected terminal devices) or they may appear as individual LAN segments with their own Ethernet MAC/IP addresses.

note:

The LAN ports on the IR2420 and GR2410 are auto-sensing for both speed and direction i.e. standard or crossover cables may be used interchangeably.

1.3.3 ISDN BRI connector

The connector labelled **ISDN BRI** is used to connect the unit to the ISDN network using the cable supplied. One end of the cable should be fitted into this connector (with the retaining clip at the bottom) before the other end is connected to the wall mounted ISDN outlet socket.

note:

You should not use any cable other than the one supplied or a purpose designed ISDN cable. Doing so may damage the product and invalidate the warranty.

1.3.4 Serial port connectors

Serial port connectors are labelled **PORT** or **DTE** and the number will vary depending upon the model you have purchased. The type of connector used may be a standard 25-way D socket or an 8-way/8-contact RJ45 socket. Where RJ45 sockets are used the unit will be supplied with the appropriate number of RJ45 to 9-way D adapters. Details of the pin designations for the ports are given under the heading ASY Port Connectors. In general, 25-way D sockets support RS232 synchronous and asynchronous operation, though some models can be provided with X.21/RS485 capability. Ports using RJ45 connectors provide RS232 asynchronous operation only.

1.3.5 User switch

If present, the small, recessed switch labelled **USER** normally acts as a reset switch. Pressing this while the unit is powered up will cause a hardware reset (similar to removing and re-applying power).

1.3.6 Aerial (or GPRS Aerial)

Models that incorporate a GPRS (General Packet Radio System) module, will feature a TNC connector on the rear panel labelled **AERIAL** or **GPRS AERIAL**.

These models are capable of working at GSM 900 and DCS 1800 frequencies and a dual-band GSM900/DCS1800 aerial is normally supplied with the unit. This should be screwed onto the AERIAL connector prior to operation. For desktop operation, the unit is also supplied with a detachable 90° “elbow” adapter. Using the aerial without this adapter allows it to be mounted on a wall or other vertical surface using the keyhole slots provided in the base.

In cases where signal reception is weak, it is permissible to use an external antenna and Sarian Systems can supply a range of specialist antennas.

1.4 GPRS SIM Card Installation

Models such as the GR2130 and GR2420 incorporate a wireless GPRS module, which is capable of transmitting and receiving data at rates up to 33,000bps.

note:

Before you can use the router in this mode, you must have a subscription with a suitable GSM network operator that provides GPRS coverage in your area.

If, when you ordered the router, you also took out a subscription to a mobile GPRS service through Sarian Systems, the SIM card required to activate the service will already be installed in your unit. In this case the installation procedure described below will not apply.

If you have NOT ordered your GPRS service subscription from Sarian Systems, your operator will provide you with a “SIM” (Subscriber Identity Module) card. This card must be installed in the router before use.

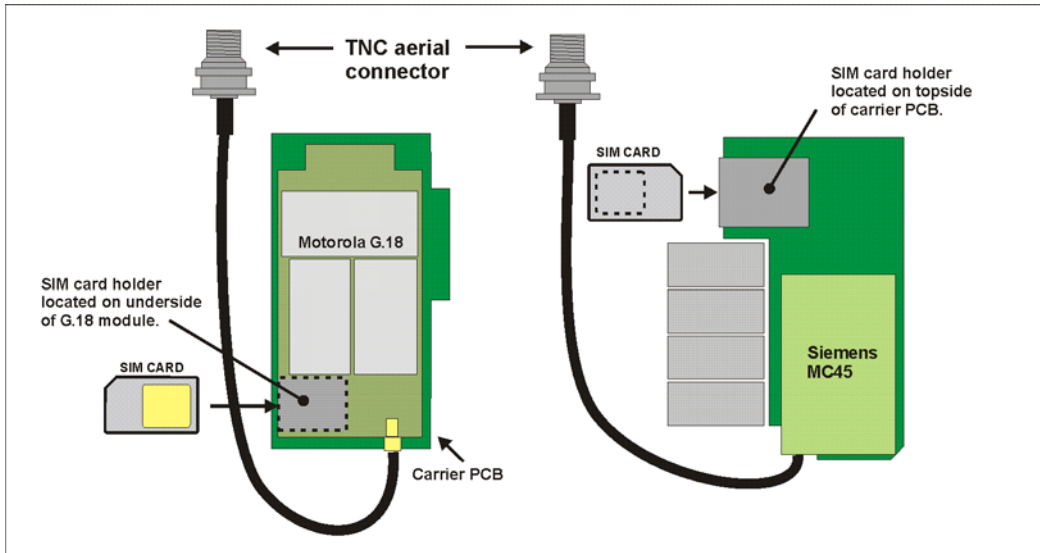
1.4.1 GR2130 and GR2410

The GPRS module (which incorporates the SIM-card holder), on these models is located inside the unit and cannot be accessed without removing the lid. To do this you will require a small crosshead screwdriver.

First make sure that the unit is disconnected from the mains power supply and then proceed as follows:

- a) Remove the aerial (if fitted).
- b) Turn the unit onto its lid and remove the 2 fixing screws from the base (two additional screws for re-assembling the case are provided separately with the unit).

- c) Place the unit the correct way up and carefully lift the lid free noting that it will only fit correctly one way round.
- d) Locate the SIM-card holder. Your unit may contain one of two alternative GPRS modules (Motorola G.18 or Siemens MC45). The following illustration shows the location of the SIM-card holder for both types of module:



- e) Make sure the SIM card is correctly oriented according to the module type and then insert it into the holder in the direction of the arrow and push it firmly into place.
- f) Replace the lid (making sure of the orientation) and fix with the four screws.
- g) Screw the GPRS aerial (with or without the elbow adapter as necessary) to the TNC connector on the rear panel.

You should now refer to the section entitled Configuring/Testing GPRS Models before attempting to use the unit.

1.4.2 Configuring/Testing GPRS Models

Refer to the **Configure ► GPRS Module** section of this guide to configure your router for the correct APN and PIN code (if any).

You can now power up your unit and test connection to the GPRS network. If you have correctly configured everything, the **SIM** indicator on the front panel should illuminate green to show that a GPRS enabled SIM card is present. The unit will now attempt to log on to the specified GPRS network and if it is able to do so, the **GPRS** indicator will illuminate steady. Data passing to and from the network will be reflected by the status of the **DAT** indicator, which will flash alternatively red and green. If you are unable to connect to the network, go to the **Status ► GPRS Module** web page and press the **Refresh** button. The page should appear similar to the following:

Results of Last Modem Status Poll:
Outcome: Got modem status OK:

SIM status	READY
Signal strength	>= -51 dBm
Manufacturer	"Motorola"
Network	000,000,"Orange"
GPRS Attachment Status	Attached
Network Registration	Registered, home network

Click the refresh button to get the current status. Note that this will disconnect the modem.

Refresh

note:

The signal strength is shown in “negative dB”, which means that the stronger the signal, the lower the number. As a guide -30dB would be a very strong signal, only normally obtained very close to a cell site. -120dB represents a very weak signal on the limits of operation. If your unit reports -120dB or less, try re-orienting the antenna or consider adding an external antenna.

2 Using The Web Interface

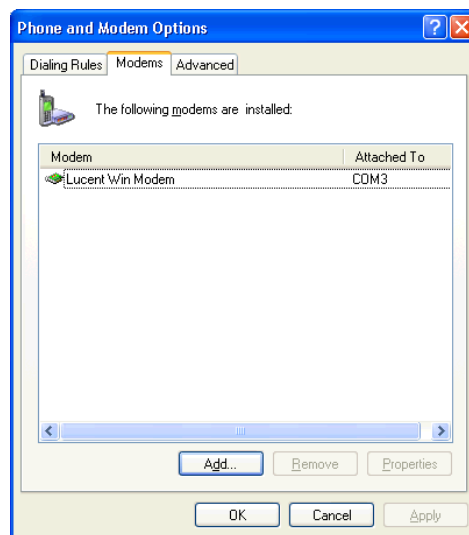
To access the built-in web pages using a web browser (e.g. Internet Explorer), you will need to install the **sarian2k.inf** driver file and create a PPP Dial-up Networking connection (DUN) for the unit as described below. It is assumed that you already have a basic knowledge of Windows networking concepts and terminology.

note:

To use Dial-up Networking you must have the **TCP/IP ► Dial-up adapter** installed in the Network Configuration for Windows. Check this by selecting **Settings ► Control Panel ► Network ► Configuration**.

2.1 Installing The Driver File

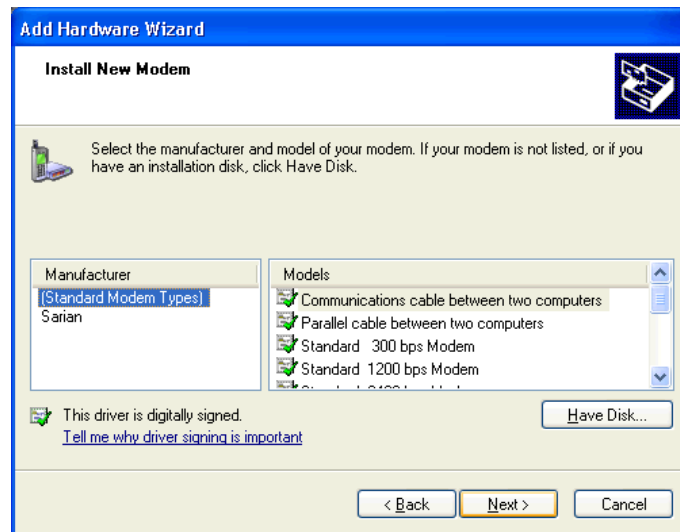
The precise procedure for installing the **.inf** driver file for the unit will vary slightly between different versions of Windows. The following description applies to Windows XP. Start by selecting **Start ► Control Panel ► Phone and Modem Options**. Select the **Modems** tab and you will see a dialog similar to the following:



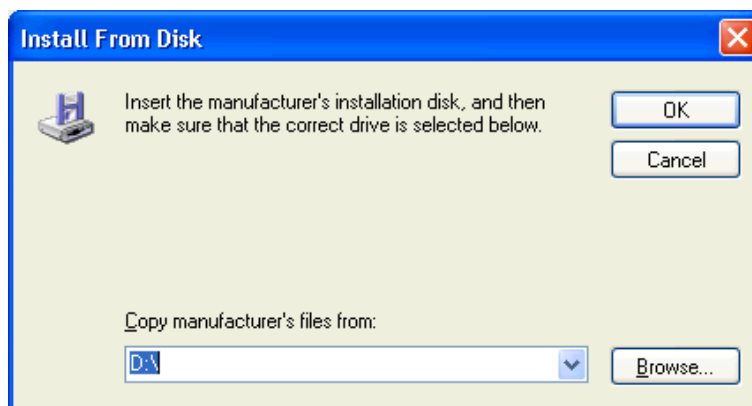
Click on **Add...** to move to install a new modem driver:



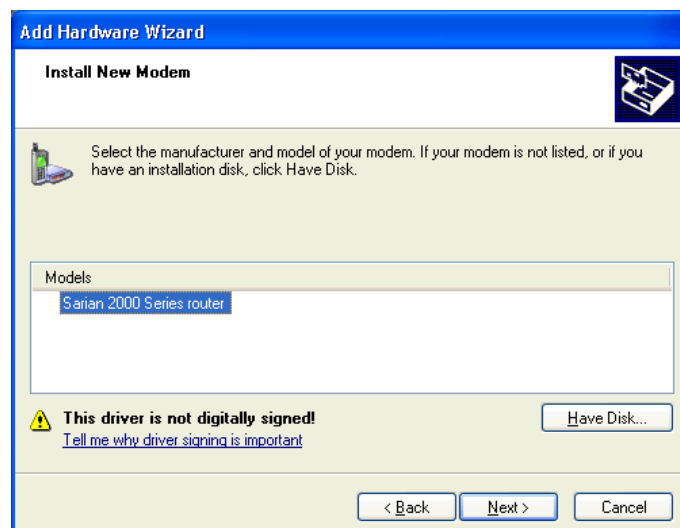
Check the **Don't detect my modem, I will select it from a list** option before clicking **Next** > to display the following dialog screen:



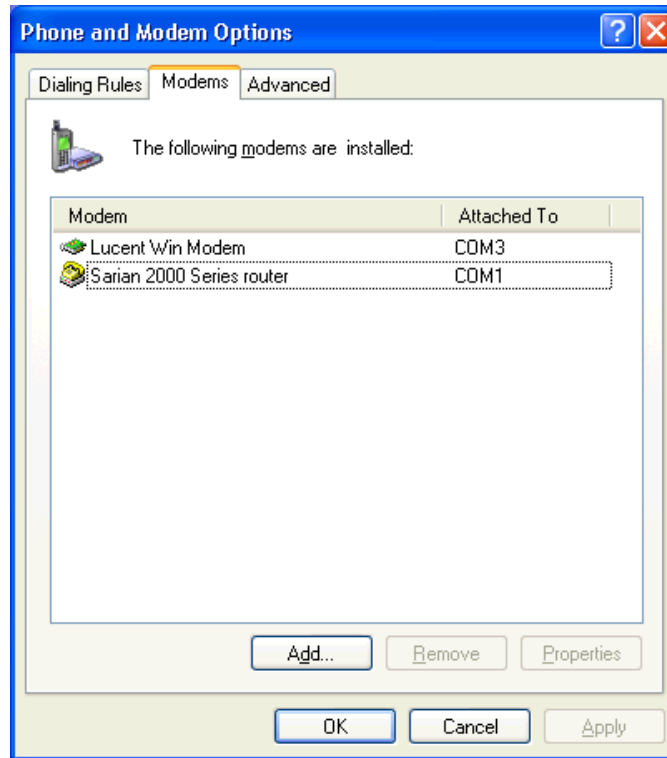
This screen lists the manufacturers and models of modem currently available on your system. Insert the CD supplied into the CD drive and click on **Have Disk**....



Use the **Browse** button to locate the **sarian2k.inf** file on the drive CD supplied with your unit. This will be in the appropriate Windows version sub-directory of the drives folder e.g. win95-98. The name and description of the Sarian unit will appear in the **Models** list:



Click **Next >** and you will be asked to select which COM port the unit is to be connected to. Select an appropriate port, click **Next >** and Windows will install the driver. Once installation is complete click **Finish** to return to the **Phone and Modem Options** dialog:



Click on the **OK** button if you are satisfied with the installation.

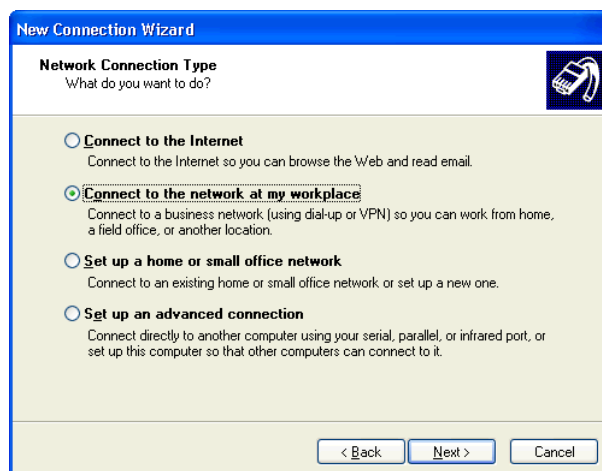
2.2 Creating A New Connection

You now need to create a new network connection through which you can access your unit.

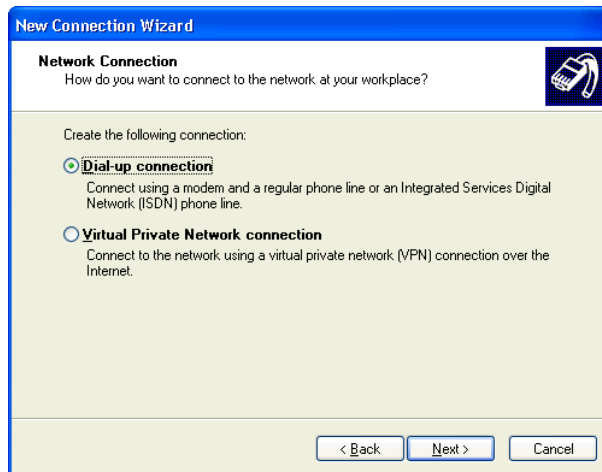
If you are planning to connect the unit directly to your PC for configuration purposes, connect it to the appropriate COM port now using a suitable serial cable.

If you wish to configure a remote unit, make sure it is connected to a suitable ISDN line and make a note of the ISDN number.

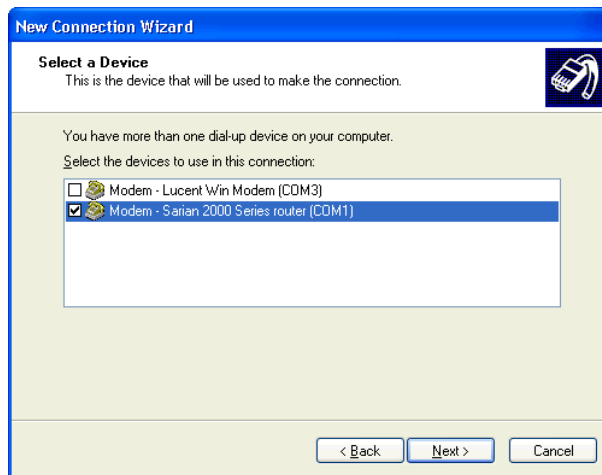
From the Windows **Start** menu, select **All Programs > Accessories > Communications > New Connection Wizard**. You will be presented with the New Connection Wizard introduction screen. Click on **Next** to proceed to the Network Connection Type dialog:



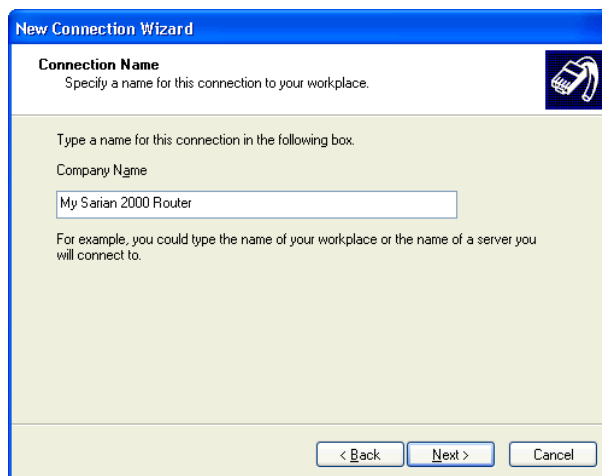
Select the **Connect to the network at my workplace** radio-button then click on **Next >**:



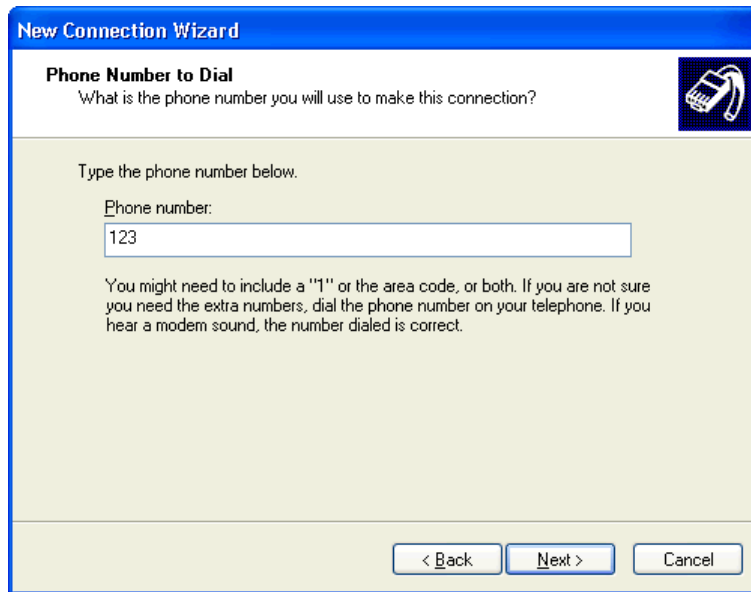
Select the **Dial-up connection** radio-button then click on **Next >**:



From the **Select a Device** dialog, select the Sarian device you have just installed and make sure that any other devices in the list are unchecked. Click **Next >**.



You must now enter a name for the connection. It is helpful to choose a name that you will easily remember such as "My Local Sarian" or "IR2140 - Bristol Office". Click **Next >**.



The next dialog allows you to fill in the phone number for the connection.

If the connection is being created for direct local access using a COM port, you should set the phone number to 123. This number will be intercepted by the unit and recognised as an attempt to connect locally.

If the connection is being created for remote access, enter the correct ISDN telephone number (including the area code), for the remote unit.

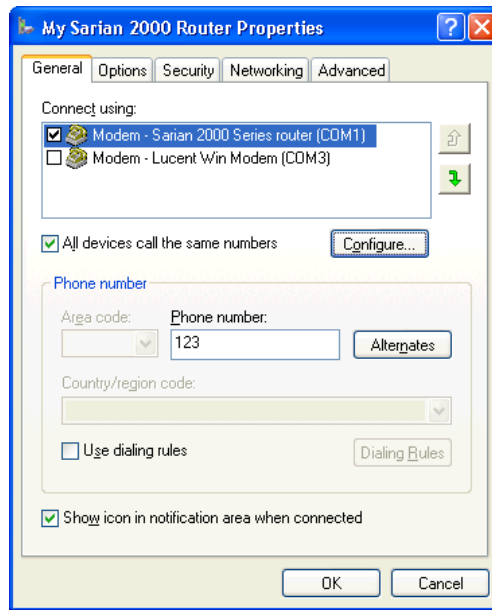
When you have done this click **Next >**. The final dialog screen will confirm that the connection has been created and includes a check box to allow you to create a shortcut on your desktop if necessary. Click on **Finish** to complete the task.

2.3 Configuring A New Connection

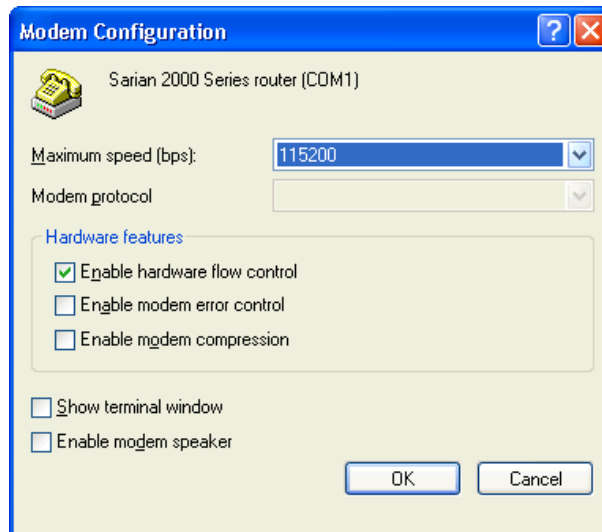
The new Network Connection that you have just created may now be used to connect to the unit but before you do this, you will need to check some of the configuration properties. Click on the Start button and select **Connect To ► My Sarian 2000 Router** (substituting the connection name you chose).



Click on the **Properties** button to display the properties dialog for the connection:



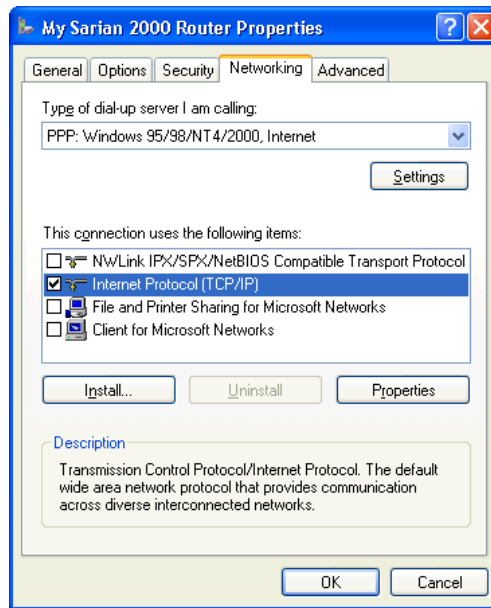
On the General tab, click **Configure** to display the Modem Configuration dialog:



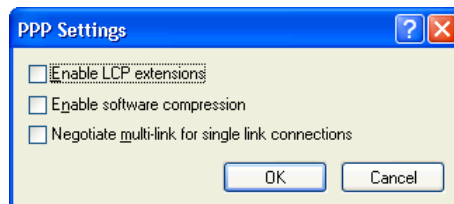
Make sure that the Maximum speed (bps) is set to 115200 and that the Enable hardware flow control box is checked.

Click **OK** when you have finished to return to the main properties dialog.

Now select the **Networking** tab:



Make sure that the **Type of dial-up server I am calling** is set to **PPP: Windows 95/98/NT/2000, Internet** and click on **Settings**:



Make sure that all three options are unchecked before clicking **OK** to return to the **Networking tab**.

In the **This connection uses the following items** list, Internet Protocol (TCP/IP) should be the only item that is checked. Make sure that this is the case and then click **OK** to return to the main dialog. You are now ready to initiate a connection.

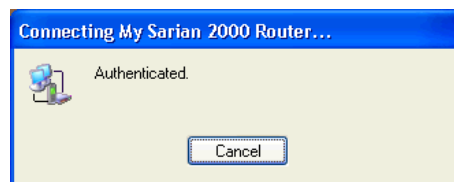
2.4 Initiating A Connection

In the main dialog, you are asked to enter a username and password. The default settings for your unit are “**username**” and “**password**” respectively but you should change as soon as possible in order to prevent unauthorised access to your unit (refer to the section entitled **Configure ► Users** for instructions on how to do this). The username is not case sensitive, but the password is.

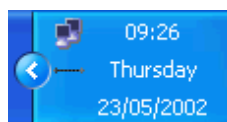
**note:**

When you type the password it will appear as a series of dots to ensure privacy.

Once you have entered these, initiate a connection to your unit by clicking the **Dial** button. During the dialling and connection process, you may see a series of status dialogs and, if the connection is successful, the final dialog will indicate that the PPP login has been authenticated:



After a short delay, this dialog will minimise to a “linked computers icon in the Windows taskbar:



You should now be ready to access the built-in web pages using your Web browser. The default “web address” for the unit is **1.2.3.4**. By default, this is also mapped to the hostname **ss.2000r**.

You will need a valid username and password to access the web interface. Once again, the factory default settings are **username** and **password** respectively. If these values do not allow access, you should contact your system administrator.

3 The Command Line Interface

Using a Web browser to modify text box or table values in the configuration pages is the simplest way to configure the unit and this process is described in the next chapter. However, if you do not have access to a Web browser, the unit can be configured using text commands entered via one of the serial ports. To do this you will need a PC and some communications software such as HyperTerm (supplied with Windows) or TeraTerm™. The same commands may also be used to configure the unit remotely via Telnet, X.25 or V.120.

There several types of text command:

AT commands & S registers (similar to those used in modems)

AT commands (pronounced “ay tee”), are supported in order to maintain compatibility with modems when the unit is used as a modem replacement.

Sarian Systems application commands

Application commands are specific to Sarian Systems products and are used to control most features of the unit when not using the Web interface.

X.3 commands

These are standard X.3 commands which are used only in X.25 PAD mode

TPAD commands

These are used only in TPAD mode.

3.1 The “AT” Command Prefix

The “**at**” command prefix is used for those commands that are common to modems. To configure the unit using **AT** commands you must first connect it to a suitable asynchronous terminal.

If you are using a terminal connected to **ASY0**, the unit will automatically detect the interface speed and data format that you are using.

If you are using **ASY1**, **ASY2** or **ASY3** you will first need to set the interface speed/data format for your terminal to 115,200bps, 8 data bits, no parity and 1 stop bit (these settings can be changed later if necessary).

When your terminal is correctly configured, apply power and wait for the **B1** indicator to stop flashing. Unless you have previously configured the unit to automatically connect to a remote system on power-up, it will now be ready to respond to commands from an attached terminal and is in “command mode”.

Now type “**at**” (in upper or lower case), and press [Enter]. The unit should respond with the message **OK**. This message is issued after successful completion of each command line. If an invalid command is entered, the unit will respond with the message **ERROR**.

note:

For consistency AT commands are shown in bold, lower case throughout this guide.

If there is no response, check that the serial cable is properly connected and that your terminal or PC communications software is correctly configured before trying again.

If you have local character echo enabled on your terminal, you may see the AT command displayed as **aatt**. If this happens you may use the **ate0** command to prevent the unit from providing character echo.

The **at** command prefix and the commands that follow it can be entered in upper or lower case. After the prefix, you may enter one or more commands on the same line of up to 40 characters. When the line is entered, the unit will execute each command in turn.

3.2 The Escape Sequence

If you enter a command such as **atd**, which results in the unit establishing a connection to a remote system, it will issue a **CONNECT** result code and switch from command mode to on-line mode. This means that it will no longer accept commands from the terminal. Instead, data will be passed transparently through the unit to the remote system. In the same way, data from the remote system will pass straight through to your terminal.

The unit will automatically return to command mode if the connection to the remote system is terminated. To return to command mode manually, you must enter a special sequence of characters called the “escape: sequence”. This consists of three occurrences of the “escape character”, a pause (user configurable) and then **at**. The default escape character is “+” so the default escape sequence is:

```
+++ {pause} AT
```

Entering this sequence when the unit is on-line will cause it to return to command mode but it will NOT disconnect from the remote system unless you specifically instruct it to do so (using **ath** or another method of disconnecting). If you have not disconnected the call, the **ato** command may be used to go back on-line.

3.3 Result Codes

Each time an AT command line is executed, the unit responds with a result code to indicate whether the command was successful. If all commands entered on the line are valid, the **OK** result code will be issued. If any command on the line is invalid, the **ERROR** result code will be issued.

Result codes may take the form of an English word or phrase (verbose code) or an equivalent number (numeric code), depending on the setting of the **atv** command. Verbose codes are used by default. The **atv0** command can be used to select numeric codes if required. A full list of the Result codes is provided in the following table:

Numeric Code	Verbose Code	Meaning
0	OK	Command line executed correctly
1	CONNECT	ISDN connection established
2	RING	Incoming ring signal detected
3	NO CARRIER	X.25 service not available
4	ERROR	Error in command line
6	NO DIALTONE	ISDN service not available
7	BUSY	B-channel(s) in use
8	NO ANSWER	No response from remote

3.4 “S” Registers

“S” registers are “special” registers in the unit that are used to store certain types of configuration information. They are essentially a “legacy” feature included to provide compatibility with software that was originally designed to interact with modems. A full list of the registers is provided under the section heading “S registers”.

3.5 Application Commands

The unit also supports numerous text-based “application” commands that are specific to Sarian Systems products and do not require the **at** prefix. Some of these are generic i.e. they are related to the general operation of the unit; others are application or protocol specific.

Before you can use application commands from ASY0 or ASY1 you must lock the interface speed to the same as that of your terminal. To do this first ensure that the unit is responding to **at** commands correctly and then enter the command:

```
at\ls
```

This will lock the interface speed to the same speed as the terminal. The speed will remain locked until the unit goes on-line and then off-line again, the power is removed or the unit is reset.

Once the port speed has been locked, **at** commands will still work but you may also use the application commands.

If you change the terminal speed after entering **atls** you will not be able to use the application commands. However, AT commands will still operate and you may unlock the port speed again (by setting **s31** to 0) or lock it to a different speed by setting register **s31** to the appropriate value. For example, to lock the speed at 19,200bps enter the command:

```
ats31=6
```

then change your terminal settings to match.

note:

Speed locking is not necessary for ASY 2 or 3 or when you use the text commands via a Telnet session.

Sarian application commands (referred to just as text commands throughout the remainder of this guide), can be entered in upper or lower case but unlike **at** commands, only one command may be entered on a line. After each successful command, the **OK** result code will be issued. An invalid command will cause the **ERROR** result code to be issued.

The general syntax for an application commands is:

```
<cmd_name> <instance> <param_name> <value>
```

where:

<cmd_name> is the name of the command

<instance> is the instance number for the entity that you are configuring.

<param_name> is the name of the parameter that you wish to configure.

<value> is the new value for the specified parameter.

For example, to set the window size for X.25 PAD instance 1 to 5 you would enter:

```
pad 1 window 5
```

Even if there is only once instance of particular entity, you should only enter 0 for the instance number.

3.6 The Active Port

When entering AT or application commands it is important to understand that in most cases, the command only affects the settings for the “active” port. This is usually the port to which you are

physically connected but you may, if necessary, set the active port to another port of your choice using the **at\port=n** command where **n** is 0-3.

3.7 Establishing A Remote Connection

Once you have finished configuring the unit, there are several ways of establishing a link to a remote system:

- ◆ An outgoing V.120 call may be made using the `atd` command
- ◆ You can initiate a DUN session to establish a dial-up PPP connection.
- ◆ An outgoing X.25 call may be made using the `atd` command followed by the `X.28 CALL` command.

An outgoing TPAD call may be made by using the `a` (address) command followed by the appropriate NUA (this is normally only carried out under software control).

Similarly, incoming calls will be handled according to which protocols have been bound to the ASY ports and whether or not answering is enabled for each protocol.

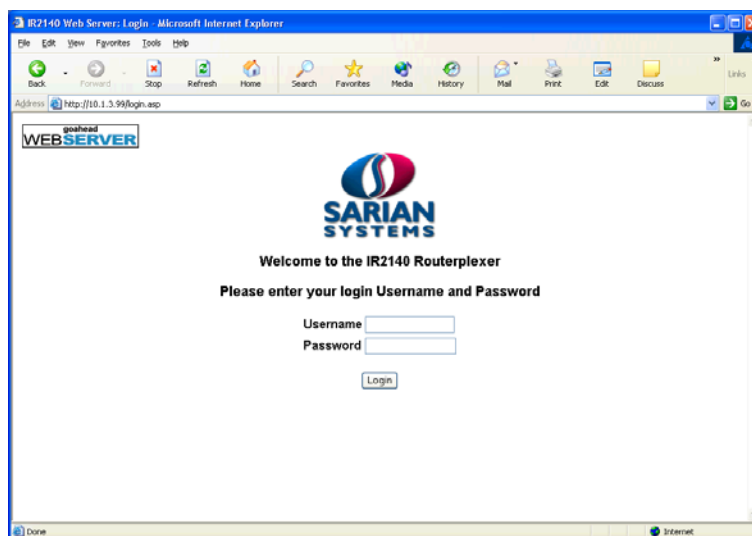
4 Configuring Your Unit

This section describes the various configuration parameters for the unit and how to set or change them using the built-in web pages or the text commands.

Generally, configuration using the Web pages is achieved by entering the required values into text boxes or tables on the page, or by turning features on or off using checkboxes. The same results can be achieved entering the appropriate text commands via one of the serial ports.

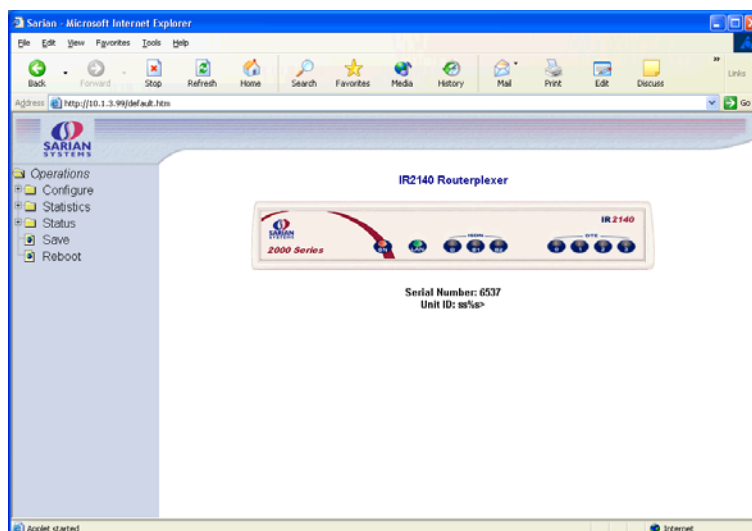
4.1 Logging In

To configure the unit via the Web interface, establish a DUN connection to it and then run your web browser and enter **1.2.3.4** for the web address. You will be presented with a logon page similar to the following:



The default Username and Password are **“username”** and **“password”** respectively. Enter these and click the **Login** button to access the configuration pages. The password will be displayed as a series of dots for security purposes.

Correct entry of the user name and password will display the main operations page similar to that shown below.



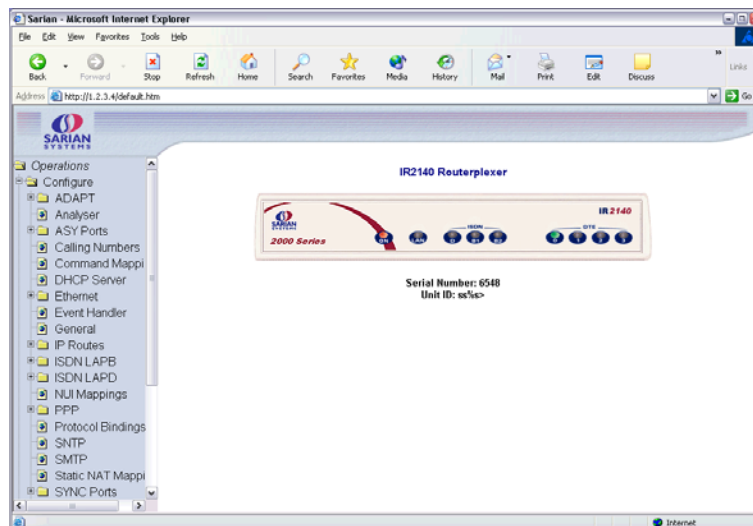
In the main frame there is a representation of the front panel of your unit that will be updated every few seconds to show the actual status of the LED indicators. The model number of your unit will be shown at the top of the screen. The unit's serial number and ID are shown below the front panel representation.

Down the left side of the page you will see a directory tree listing the various folders and pages that are available.

Each folder may be preceded by a small "+" symbol and a closed folder icon indicating that it can be expanded to reveal sub-pages or folders. To do this, click anywhere on the appropriate line. The closed folder icon will change to an open folder icon and the "+" symbol will change to "-". Clicking on the line again will hide the sub-options. Where there are no sub-pages, a web-page icon is shown next to the page title. Clicking on this will display the associated web page. The following sections describe how to use these pages to configure and monitor the operation of your unit.

4.2 The Configuration Pages

Click on the **Configure** closed folder icon. The folder will open to show its contents as illustrated below:



You will see a list of web pages and sub-folders containing further web pages. Each page allows you to configure parameters that are related to a particular function or protocol. For example, the **Ethernet** page allows you to set up the unit's IP address, DNS server address etc.

A page will contain a mixture of text-boxes, check boxes and/or list-boxes. To configure a particular item simply select the appropriate value from a list, type in into a text-box the appropriate value from a series of checkboxes.

When you have finished making changes on a particular page, click on the **OK** button to accept the changes or **CANCEL** to revert to the existing values.

note:

Pressing **OK** will save the changes you have made for the current session only i.e. they will be lost if the unit when the power is removed. If you wish to save the changes more permanent, make sure that you save them to non-volatile memory as described in **Saving Configuration Changes**.

The following sections describe each of the configuration pages in detail. They first explain each of the parameters or options shown on the web page. This is followed by a description of the equivalent text commands.

4.3 Configure ► ADAPT

The unit incorporates two **Adapt** (rate adaptation protocol) instances. Each instance allows you to select and configure a protocol that is to be used for providing rate adaptation over ISDN B channel. The supported protocols are V.110, V.120 and X.75. Depending on which protocol is selected, there may be an associated LAPB instance (distinct from the two general purpose LAPB instances). LAPB would be used, for example, by V.120 when operating in error corrected (Multi-frame) mode.

Using the web page:

V120 mode:

When the **V mode** parameter has been set to V120, the **V120 mode** parameter allows you to select Unacknowledged, Multi-frame or Multi-frame/Fallback mode for V.120 operation.

Unacknowledged mode is the simplest mode and does not provide error control.

Multi-frame mode provides error control but may only be used if the remote system also supports this mode.

In Multi-frame/Fallback mode, the unit will attempt to establish a multi-frame error controlled link but will allow a connection in Unacknowledged mode if the remote unit does not support error control.

MSN:

The **MSN** parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with answering enabled, it will cause the unit to answer only incoming calls to telephone numbers where the trailing digits match that value. For example setting MSN to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

If answering is disabled the MSN parameter is ignored.

Sub-address:

The **Sub-address** parameter provides the filter for the ISDN sub-address facility. It is blank by default but when set to an appropriate value with answering enabled, it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match that value. For example, setting the **Sub-address** parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

If answering is disabled i.e. S0 is set to 0, the **Sub-address** parameter is ignored.

V mode:

The **V mode** parameter allows you to specify which rate adaptation protocol to use. This can be one of the following:

Option	Description
V.120 Mode	This allows one B-channel to carry multiple sub-rate channels in a succession of statistically multiplexed (variable-length) frames. These frames support error detection and correction procedures if selected under V120 mode (above).
V110 Mode	V.110 is a fixed-frame based rate adaptation standard that subdivides the ISDN B-channel capacity so that it can carry one lower speed (sub-rate) data channel.
V110/V120 Detect	This mode detects which protocol (V.110 or V.120) the remote host is using.
X75 Transparent	This selects bit transparent X.75 mode of operation.
X75 T.70 NL	This option generates T.70 NL telematic prefixes that are required

	by some ISDN terminal adapters.
--	---------------------------------

V110 user rate:

The **V110 user rate** parameter allows you to specify the data rate to be used on ISDN when operating in V.110 mode.

V110 fixed rate:

Setting this parameter to Yes prevents the V.110 protocol from changing the data rate.

LAPB Configuration:

The following parameters are only used if a V.120 connection is established in Multi-frame mode:

N400 counter:

This is the standard LAPB/LAPD re-try counter. The default value is 3 and it should not normally be necessary to change this.

RR timer (ms):

This is a standard LAPB/LAPD "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 timer (ms):

This is a standard LAPB/LAPD timer. The default value is 1000 milliseconds and under normal circumstances, it should not be necessary to change it.

T200 timer (ms):

This is a standard LAPB/LAPD re-transmit timer. The default value is 1000 milliseconds and under normal circumstances, it should not be necessary to change it.

Using text commands:

To configure rate adaptation parameters via the command line use the **adapt** command.

To display current settings for **adapt 0** enter the command:

```
adapt 0 ?
```

To change the value of a parameter use the command in the format:

```
adapt <instance> <parameter> <value>
```

where *<instance>* is 0 or 1.

The parameters and values are:

Parameter	Values	Equivalent web parameter
fixed_rate	on, off	V110 fixed rate
msn	number	MSN
msnv110	Number	MSN for V.110
multi	0,1,2	Mode: 0=unacknowledged, 1=multi-frame, 2=multi-frame/fallback
sub	number	Sub-address
user_rate	5,6,7,8,9,10,11	V110 User Rate: 5=38400, 6=19200, 7=9600, 8=4800,

		9=2400, 10=1200, 11=600
vmode	0,1,2,3,4	V Mode: 0=V120 mode, 1=V110 mode, 2=V110/V120 detect, 3=X75 Transparent, 4=X75 T.70 NL

To change the values of the LAPB parameters for rate adaptation, use the **lapb** command. **LAPB2** is used for **adapt 0** and **LAPB3** is used for **adapt 1**.

4.4 Configure ► Analyser

Your unit can be configured to maintain a trace of activity taking place at the various ports and of the layer 2 and 3 protocols. Trace information is stored in a circular buffer in memory. When the buffer is full, the storage of new trace data starts at the beginning of the buffer again (overwriting the oldest data). This buffer appears in the file directory as a pseudo-file called **ana.txt**.

The following is a typical trace showing activity on the D-channel:

```

----- 4-5-2002 13:11:50.260 -----
L2 DCHAN SABME from NT to TE: COMMAND POLL SAPI=10, TEI=01,
                                42,03,7F,

-----
----- 4-5-2002 13:11:50.260 -----
L2 DCHAN UA from TE to NT: RESPONSE FINAL SAPI=10, TEI=01,
                                42,03,73,

-----
----- 4-5-2002 13:11:50.330 -----
L2 DCHAN I FRAME from NT to TE: COMMAND SAPI=10, TEI=01, NS=00,
NR=00,
                                42,03,00,00,

X25 RESTART from DCE to DTE:
LCG=0 LCN=0 PTI
10, 00, FB,
07 00 ..

-----
----- 4-5-2002 13:11:50.330 -----
L2 DCHAN I FRAME from TE to NT: COMMAND SAPI=10, TEI=01, NS=00,
NR=01,
                                40,03,00,02,

X25 RESTART CONFIRMATION from DTE to DCE:
LCG=0 LCN=0 PTI
10, 00, FF,

-----

```

Both B and D-channel analysis can be enabled simultaneously if necessary and you can select which LAPB and LAPD sources you wish to include in the trace by checking the appropriate boxes.

Using the web-page:

The **Configure ► Analyser** Web page allows you to turn the analyser On or Off and to determine what information is included in the trace using the following parameters:

Analyser:

To turn the analyser on, select the On option from the selection box labelled **Analyser** at the top of the page. Selecting Off will turn the analyser off again.

Protocol layers:

The check boxes shown under this heading are used to specify which protocol layers are included in the trace. You can choose to generate a trace of the physical layer (Layer 1), the Link Layer (Layer 2) protocol, the Network Layer (Layer 3) protocol or any combination, by checking or clearing the appropriate check-boxes. In addition, you may select XOT (X.25 over TCP/IP) tracing if this feature is included in your product.

IKE:

This checkbox is used to enable or disable the inclusion of IKE packets in the analyser trace when using IPSec.

ISDN sources:

The group of check boxes shown under this heading are used to select the ISDN channels (B1, B2 and D) that will be included in the trace. To include or exclude a specific LAPB or LAPD instance from the trace ensure that the appropriate checkbox is checked or cleared respectively.

ASY sources:

The group of checkboxes shown under this heading is used to select the ASY ports that will be included in the trace. To include a trace of commands issued to and responses from a particular port, ensure that the appropriate box is checked. The list of available ports will include the physical ASY ports and some virtual ASY ports that are used internally.

note:

On models fitted with a GPRS module, one of the ASY ports (usually ASY1), is replaced by the GPRS port.

Raw sync sources:

The group of checkboxes shown under this heading are is to select the synchronous sources to be included in the trace. These include the ISDN channels D, B1 and B2 and any other synchronous ports/protocols that your unit may include (e.g. physical port 1, 2 etc). This feature is especially useful for monitoring data transferred over ISDN when the higher layer protocol does not record data in the trace (e.g.V.120).

Max I-PAK size:

The text-box labelled Max I-PAK Size allows you to specify the maximum number of bytes from each X.25 Information Frame that will be included in the trace. Frames that are larger than this value are truncated. The larger this value, the quicker the **ana.txt** pseudo-file (in which the trace output is stored), will fill so that the effective length of the trace is reduced. The default value of 128 should be suitable in most cases.

At the bottom of the page, the **OK** and **Cancel** buttons may be used to save or cancel any changes respectively.

PPP sources:

The group of checkboxes shown under this heading may be used to select the PPP sources to be included in the trace.

IP sources:

The group of checkboxes shown under this heading may be used to select the IP sources to be included in the trace. These sources include the PPP and ETH instances.

IP filters:

This text box is used to prevent the tracing of packets to or from specific TCP or UDP ports. The format of this text box is a comma-separated list of port numbers. For example, you may wish to exclude tracing of HTTP traffic that would otherwise swamp the data of interest. This can be done by entering “80” in the IP Filters box.

Using text commands:

From the command line, the **ana** command can be used to configure the protocol analyser.

To display the current settings for the analyser enter the command:

```
ana <instance> ?
```

where <instance> is 0 (there is only one instance of the Analyser).

To change the value of a parameter use the same command in the format:

```
ana 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
anon	on, off	Analyser
asyon	1-15	ASY sources
ikeon	on, off	IKE
ipfilt	number list	IP filters
ipon	0-255	IP sources
l1on	on, off	Protocol layers - layer 1
l2on	on, off	Protocol layers - layer 2
l3on	on, off	Protocol layers - layer 3
lapbon	1-3	ISDN sources - LAPB
lapdon	1-7	ISDN sources - LAPD
maxdata	number	Max I-PAK size
pppon	0-31	PPP sources
syon	1-15	Raw sync sources
xoton	on, off	Protocol layers - XOT

For example, to turn the analyser on, enter:

```
ana 0 anon on
```

To clear the existing contents of the analyser trace prior to starting a new trace session, use the following command:

```
ana 0 anaclr
```

To include or exclude trace information from the various possible sources, use the appropriate command from the above table in conjunction with the required value from the following tables:

ASY sources:

Value	ASY 3	ASY 2	ASY 1 (or GPRS)	ASY 0
-------	-------	-------	--------------------	-------

0	OFF	OFF	OFF	OFF
1	OFF	OFF	OFF	ON
2	OFF	OFF	ON	OFF
3	OFF	OFF	ON	ON
4	OFF	ON	OFF	OFF
5	OFF	ON	OFF	ON
6	OFF	ON	ON	OFF
7	OFF	ON	ON	ON
8	ON	OFF	OFF	OFF
9	ON	OFF	OFF	ON
10	ON	OFF	ON	OFF
11	ON	OFF	ON	ON
12	ON	ON	OFF	OFF
13	ON	ON	OFF	ON
14	ON	ON	ON	OFF
15	ON	ON	ON	ON

IP or PPP sources:

Value	PPP 4	PPP 3	PPP 2	PPP 1	PPP 0
0	OFF	OFF	OFF	OFF	OFF
1	OFF	OFF	OFF	OFF	ON
2	OFF	OFF	OFF	ON	OFF
3	OFF	OFF	OFF	ON	ON
4	OFF	OFF	ON	OFF	OFF
5	OFF	OFF	ON	OFF	ON
6	OFF	OFF	ON	ON	OFF
7	OFF	OFF	ON	ON	ON
8	OFF	ON	OFF	OFF	OFF
9	OFF	ON	OFF	OFF	ON
10	OFF	ON	OFF	ON	OFF
11	OFF	ON	OFF	ON	ON
12	OFF	ON	ON	OFF	OFF
13	OFF	ON	ON	OFF	ON
14	OFF	ON	ON	ON	OFF
15	OFF	ON	ON	ON	ON
16	ON	OFF	OFF	OFF	OFF
17	ON	OFF	OFF	OFF	ON
18	ON	OFF	OFF	ON	OFF
19	ON	OFF	OFF	ON	ON
20	ON	OFF	ON	OFF	OFF
21	ON	OFF	ON	OFF	ON
22	ON	OFF	ON	ON	OFF
23	ON	OFF	ON	ON	ON
24	ON	ON	OFF	OFF	OFF
25	ON	ON	OFF	OFF	ON
26	ON	ON	OFF	ON	OFF
27	ON	ON	OFF	ON	ON
28	ON	ON	ON	OFF	OFF
29	ON	ON	ON	OFF	ON
30	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON

To include ETH as an IP source add 128 to the values from the above table. For example, to turn on tracing for ETH0 and PPP0 only, enter the command:

ipon 129

LAPB sources:

Value	LAPB 1	LAPB 0
0	OFF	OFF
1	OFF	ON
2	ON	OFF
3	ON	ON

LAPD sources:

Value	LAPD 2	LAPD 1	LAPD 0
0	OFF	OFF	OFF
1	OFF	OFF	ON
2	OFF	ON	OFF
3	OFF	ON	ON
4	ON	OFF	OFF
5	ON	OFF	ON
6	ON	ON	OFF
7	ON	ON	ON

Raw Sync sources:

Value	Physical Port 1	Physical Port 0	ISDN B2	ISDN B1	ISDN D
0	OFF	OFF	OFF	OFF	OFF
1	OFF	OFF	OFF	OFF	ON
2	OFF	OFF	OFF	ON	OFF
3	OFF	OFF	OFF	ON	ON
4	OFF	OFF	ON	OFF	OFF
5	OFF	OFF	ON	OFF	ON
6	OFF	OFF	ON	ON	OFF
7	OFF	OFF	ON	ON	ON
8	OFF	ON	OFF	OFF	OFF
9	OFF	ON	OFF	OFF	ON
10	OFF	ON	OFF	ON	OFF
11	OFF	ON	OFF	ON	ON
12	OFF	ON	ON	OFF	OFF
13	OFF	ON	ON	OFF	ON
14	OFF	ON	ON	ON	OFF
15	OFF	ON	ON	ON	ON
16	ON	OFF	OFF	OFF	OFF
17	ON	OFF	OFF	OFF	ON
18	ON	OFF	OFF	ON	OFF
19	ON	OFF	OFF	ON	ON
20	ON	OFF	ON	OFF	OFF
21	ON	OFF	ON	OFF	ON
22	ON	OFF	ON	ON	OFF
23	ON	OFF	ON	ON	ON
24	ON	ON	OFF	OFF	OFF

25	ON	ON	OFF	OFF	ON
26	ON	ON	OFF	ON	OFF
27	ON	ON	OFF	ON	ON
28	ON	ON	ON	OFF	OFF
29	ON	ON	ON	OFF	ON
30	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON

4.5 Configure ► ASY Ports

Each ASY port can be independently configured for interface speed, parity setting, character echo etc. These parameters can be set via the appropriate **Configure ► ASY Port** web page or from the command line using AT commands and S registers.

Using the web-page:

The **Configure ► ASY Ports** folder icon opens to list a page for each of the asynchronous serial ports (usually ASY0, 1, 2 & 3). On models fitted with GPRS there will also be a **GPRS Port** page. Each page allows you to configure the following port parameters:

Answer ring count (s0):

This parameter controls the answering of incoming V.120 calls. When set to zero, V.120 answering is disabled, otherwise V.120 answering is enabled on this port. The actual value used for this parameter sets the number of rings the unit will wait before answering. This is equivalent to setting the value of the S0 register for the relevant ASY port.

DCD:

The **DCD** parameter is used to configure the way in which the unit controls the DCD signal to the terminal.

Setting **DCD** to Auto configures the unit so that it will only turn the DCD signal on when an ISDN connection has been established (this is equivalent to **at&c1**).

Setting **DCD** to On configures the unit so that the DCD signal is always on when the unit is powered-up (this is equivalent to **at&c0**).

Setting **DCD** to Off configures the unit so that the DCD signal is normally on but goes off for the length of time specified by S10 after a call is disconnected (this is equivalent to **at&c2**).

DTR control:

The **DTR control** parameter is used to configure the way in which the unit responds to the DTR signal from the terminal.

Setting **DTR control** to None configures the unit so that the DTR signal from the attached terminal is ignored (this is equivalent to **at&d0**).

Setting **DTR control** to Drop Call configures the unit so that it will disconnect the current call and return to AT command mode when the DTR signal from the terminal goes from On to Off (this is equivalent to **at&d1**).

Setting **DTR control** to Drop Line & Call configures the unit so that it will disconnect the current call, drop the line and return to AT command mode when the DTR signal from the terminal goes from On to Off (this is equivalent to **at&d2**).

DTR de-bounce time (x20ms):

The value of this parameter determines the length of time (in multiples of 20ms), for which the DTR signal from the terminal must go Off before the unit acts upon any options that are

set to trigger on loss of DTR. Increasing or decreasing this value makes the unit less or more sensitive to “bouncing” of the DTR signal respectively.

Echo:

This parameter can be used to turn character echo On or Off when using the text command interface. Turn character echo Off if your terminal provides local character echo.

Escape character:

This parameter determines which character is used in the escape sequence. The value of this parameter is the decimal ASCII code for the character, normally 43 (“+” symbol). Changing this parameter has the same effect as changing the **s2** register.

Escape delay (x20 ms):

This parameter defines the required minimum length of the pause (in multiples of 20ms), in the escape sequence between entering three escape characters and then entering “**at**”.

Flow control:

The unit supports software flow control using XON/XOFF characters and hardware flow control using the RS232 RTS and CTS signals. Use this drop-down list to select Software, Hardware or a combination of Both. To disable flow control select the None option.

Interface speed:

This parameter allows you to select the interface speed from a drop down list. Select the required speed (from 300bps to 115,200bps), or for **ASY 0** or **ASY 1** only you may select the Auto option to allow automatic speed detection from the AT commands entered at the port.

Result codes:

This parameter is used to select Numeric, Verbose or no result codes (None) when using the text command interface.

Parity:

This parameter is used to set the ASY port parity to Even, Odd or None as required.

Power-up profile:

This parameter can be set to 0 or 1 to determine which of the two stored profiles is loaded when the unit is first powered up.

The two buttons at the bottom of the page are used to save and load the **config.da0** and **config.da1** profiles as required.

Load Profile

Clicking the **Load Profile** button loads the profile specified in the list box to the right.

Save Profile

Clicking the **Save Profile** button will store the current settings to the profile specified in the list box to the right. You may create two stored profiles for each port containing the settings detailed on this page. All profiles are stored in the **sregs.dat** file.

note:

On the GR2130 GPRS router, the configuration page for one of the ASY ports (usually **ASY 1**), is replaced by a page entitled **GPRS Port**.

Using text commands:

ASY ports are configured from the command line using AT commands and S- registers:

Cmd/S-reg.	Description
E	Echo
V	Verbose mode
Z	Load profile
&C	DCD control
&D	DTR response
&K	Flow control
&W	Store profile
&Y	Power up profile
S0	Answer Ring count
S2	Escape character
S12	Escape delay
S23	Parity
S31	ASY port speed
S45	DTR de-bounce time (x20ms)

To save any changes you have made to the profiles in command mode, use the **at&w** command.

4.6 Configure ► Backup IP addresses

This page contains a table that is used to specify alternative addresses to use when the unit fails in an attempt to open a socket. These addresses are used only for socket connections that originate from the unit and are typically used to provide backup for XOT connections, email transmissions, TANS (TPAD answering) connections or any application in which the unit is making outgoing socket connections.

When a back-up address is in use, the original IP address that failed to open is tested at intervals to see check if it has become available again. Additionally, at the end of a session, the unit will remember when an IP address has failed and use the back-up IP address immediately for future connections. When the original IP address eventually becomes available again, the unit will automatically detect this and revert to using it.

Using the Web page:

The web page contains a table with four columns headed:

IP Address:

In this column you should enter the original IP address to which the backup address relates.

Backup IP Address:

This is the backup address to try when the unit fails to open a connection to **IP Address**.

Retry Time (s):

The is the length of time seconds that the unit will wait between checks to see if a connection can yet be made to **IP address**.

Try Next:

Setting the value in the **Try Next** column to Yes allows you “chain” backup addresses so that more than one backup address can be specified for one original address. To do this, enter the **Backup IP address** from one entry in the table as the **IP address** for the next entry and then specify a third address as the **Backup IP address** in that entry.

For example, in the following table, address 10.1.2.17 is used as the first backup address for 10.1.2.16. If the unit fails to open a connection to 10.1.2.16 it will then try to open 10.1.2.17. If this also fails the unit will then try 133.16.16.2.

IP Address	Backup IP Address	Retry Time	Try Next
10.1.2.16	10.1.2.17	120	Yes
10.1.2.17	133.16.16.2	120	No

In this example, the address 133.16.16.2 could be specified to use a PPP dial-up connection in the routing table.

If the **Try Next** parameter is set to No, the unit will not attempt to connect to any further addresses.

4.7 Configure ► Calling Numbers

note:

This feature is for use by experienced personnel for network testing and fault diagnosis. It should not be required in normal use. To use this feature, your ISDN circuit must support Calling Line Identity (CLI) facility. If CLI is available, incoming calls from specified numbers may be answered normally or alternatively, rejected with an optional reject code.

Using the web-page:

The **Configure ► Calling Numbers** page contains a table that allows you to enter a series of telephone numbers each of which has an associated Answer or Reject parameter, and in the case of Reject numbers, a reason code. For each number that you enter and set to Reject, the unit will reject incoming calls from that number using the reject reason code specified. The reason code is simply a numeric value that may be selected to suit your particular application. If any one of the entries is set to Answer the unit will only answer incoming calls from that number and will reject calls from other numbers using a standard ISDN reject code.

Using text commands:

To configure calling numbers from the command line use the **rejlst** command. To display an entry in the calling numbers list enter the command:

```
rejlst <entry> ?
```

where <entry> is 0-9. For example, to display entry number 5 enter the command:

```
rejlst 5 ?
```

Up to three separate commands are needed to set up an entry. These take the form:

```
rejlst <entry> NUM <number>
rejlst <entry> ANS <mode>
rejlst <entry> CODE <code>
```

where:

<entry> is the required entry number in the calling numbers table in each case

<number> is the telephone number

<mode> is either Off to reject calls from the corresponding number (the default), or On to accept calls.

<code> is the reject reason code.

For example:

```
rejlst 0 NUM 1234567
rejlst 0 ANS OFF
rejlst 0 CODE 42
```

4.8 Configure ► Command Mappings

It is possible to specify a small number of command “aliases” on your unit. This allows you to specify substitute strings for text commands entered at the command line.

Using the web-page:

The **Configure ► Command Mappings** page contains a table that allows you to specify up to four aliases for commands entered as the command prompt. Each table entry has the following fields:

Command to Map:

This column specifies the command that you want substituted.

Command Mapping:

This column specifies the corresponding replacement command.

Using text commands:

From the command line, use the **cmd** command to configure or display the command mappings. To display the current command mappings enter the following commands:

```
cmd <n> cmdmapo ?
cmd <n> cmdmapi ?
```

Where *n* is the table entry number, i.e. 0 to 3. The *cmdmapi* parameter shows the command to be substituted, and the *cmdmapo* parameter shows the replacement command.

To change a command mapping use the following commands:

```
cmd <n> cmdmapo <string>
cmd <n> cmdmapi <string>
```

note:

If either string contains blank characters you must enclose it with double quotes. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

For example, to substitute the command “type ana.txt” with “tana”, use the commands:

```
cmd 0 cmdmapo "type ana.txt"
cmd 0 cmdmapi tana
```

After you have done this, typing “tana” at the command line will have the same effect as typing “type ana.txt”.

4.9 Configure ► DHCP Server

The unit incorporates a Dynamic Host Configuration Protocol (DHCP) server. DHCP is a standard Internet protocol that allows a DHCP server to dynamically distribute IP addressing and configuration information to network clients.

Using the web-page:

The **Configure ► DHCP Server** page allows you to set up the parameters for the DHCP server. The parameters are as follows.

Minimum assigned IP address:

This parameter specifies the lowest IP address that the DHCP server will assign to a client. Clearing this parameter will disable the DHCP server. This may be necessary if another device on the LAN provides a DHCP server.

IP address range:

This parameter is used to specify the number of different IP addresses that the DHCP server will assign. A value of 10 would assign 10 addresses starting with the address set for the **Minimum assigned IP address** parameter.

DNS server address:

This parameter specifies the IP address of a DNS server to be used by clients on the LAN. This will usually be the IP address of the unit itself (as configured by the **Configure ► Ethernet ► IP address** parameter). Alternatively, you may set this to the address of an alternative DNS server.

Gateway address:

A “gateway” is required in order to route data to IP addresses that are not on the local subnet. This parameter specifies the IP address of the gateway (which is usually the IP address of the router itself as configured by the **Configure ► Ethernet ► IP address** parameter). Alternatively, you may set this to the address of another router on the LAN.

Mask:

This parameter specifies the subnet mask used on the network to which the unit is connected. For example, for a Class A network this would be 255.255.255.0.

Lease time (mins):

This parameter specifies how long a DHCP client can use an assigned IP address before it must renew its configuration with the DHCP server. The lease time parameter is specified in minutes, the minimum being one minute.

Using text commands:

From the command line, use the **dhcp** command to configure or display the DHCP server settings. To display current settings for the DHCP server enter the following command:

```
DHCP <instance> ?
```

where <instance> is 0. At present there can only be one **dhcp** instance i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
dhcp 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
dns	IP address	DNS server address
gateway	IP address	Gateway address
ipmin	IP address	Minimum assigned IP address

iprange	number	IP address range
lease	number	Lease time (mins)
mask	IP Netmask	Mask

For example, to set the IP Address range to 30, enter:

```
dhcp 0 iprange 30
```

4.10 Configure ► DNS Update

Sarian 2000 series routers support “Dynamic DNS” in accordance with RFC2136 and RFC2485. This allows them to update specified DNS servers with their IP addresses when they first connect to the Internet and at regular intervals thereafter. The **Configure ► DNS Update** page allows you to configure the dynamic DNS Update feature to operate as required.

Using the Web page:

The web page includes the following parameters:

DNS server IP address:

This parameter is used to specify the IP address of the DNS Server that you wish to use. This server must support “DNS Update messages”. Dynamic DNS is generally offered as a subscription based service by ISP’s but it may be appropriate for you to establish your own DNS Server if you have a large number of deployed units.

Zone to update:

When using Dynamic DNS it will be necessary for you to select or “purchase” a domain name e.g. “mycompany.co.uk”. This parameter should be set match this domain name.

Name to update:

This parameter specifies an identifier that is used in conjunction with the **Zone to update** parameter to uniquely identify the unit e.g. epos33. The **Name to update** in conjunction with the **Zone to update** specifies the full address of the unit e.g. *epos33.mycompany.co.uk*.

Update interval (s):

This parameter specifies the interval (in seconds), at which the unit will issue update messages to the DNS server.

Username:

This parameter is used to store the username that has been allocated to you by the Dynamic DNS service Provider.

Password:

This parameter is used to store the password that has been allocated to you by the Dynamic DNS service Provider.

Confirm password:

Enter the password again in this field to confirm it.

Password is Base64 encoded:

Some Dynamic DNS servers issue passwords that are Base64 encoded e.g. Linux base servers. If this is the case turn this option on so that the unit correctly decodes the password before transmission. Note that the password is not actually transmitted as part of the message but is used to create a “signature” that is appended to the message. If the

password is issued to you as a hexadecimal string instead of text, you must prefix the parameter with 0x.

Interface:

This parameter defines which interface type is configured for Internet connections (usually PPP).

Interface #:

This parameter defines which **Interface** instance is configured for Internet connections.

Local time offset from GMT (hrs):

As part of the authentication process the DNS update message must include a time-stamp that is referenced to GMT. If you live in a non-GMT time zone ensure that you select the correct time offset.

Auto-detect time offset:

If no time offset is specified the unit can be configured automatically correct for time zone differences by setting this parameter to Yes.

Required time accuracy (s)

This parameter specifies the permitted variance between the unit's time and that of the DNS server.

Time to live (s):

This parameter specifies the "time to live" in seconds i.e. how long a unit that resolved the address is allowed to cache the address for after resolving it.

Always delete previous records:

When set to Yes, this parameter causes the DNS server to delete all records of previous addresses served to the unit.

Using text commands:

From the command line, use the **dnsupd** command to configure or display DNS Update settings.

To display current settings enter the command:

```
dnsupd 0 ?
```

To change the value of a parameter use the command in the format:

```
dnsupd 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
autotzone	on, off	Auto-detect time offset
b64pw	on, off	Password is Base64 encoded
delprevrr	on, off	Always delete previous records
ifadd	0,1,2	Interface #
ifent	none, ppp,eth	Interface
name	text	Name to update
password	text	Password
server	IP address	DNS server IP address
ttl	number	Time to live (s)
tzone	0-24	Local time offset from GMT (hrs)

upd_int	number	Update interval (s)
username	text	Username
zone	text	Zone to update

For example, to set the username to “david24” you would enter the command:

```
dnsupd 0 username david24
```

4.11 Configure ► Ethernet

The **Configure ► Ethernet** folder opens to list configuration pages for each of the available **ETH** ports on the unit. On router models such as the IR2140, there will only be one such page; on hub models such as the IR2420, there will be several. Each page allows you to configure parameters such as the IP address, address mask etc.

Using the web-page:

IP Analysis:

This parameter is used to include or exclude IP data from this Ethernet port from the analyser trace and is equivalent to checking or un-checking the equivalent IP sources checkbox on the **Configure ► Analyser** page.

DHCP client:

This parameter is used to enable or disable the DHCP client for this Ethernet port.

IP address:

This parameter specifies the IP address of this Ethernet port on your LAN.

Mask:

This parameter specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port. Typically, this would be 255.255.255.0 for a Class A network.

Max rate (kbps):

On models with multiple LAN ports, this parameter may be used to specify a maximum data rate in kbps that the unit will receive on this port. This may be useful in applications where separate LAN ports are allocated to separate LAN's and it is necessary to prioritise traffic from one LAN over another.

Group:

On units with a built-in hub such as the IR2420, the **Group** parameter for each port is normally set to 0. This means that all ports “belong” to the same hub. If required however, the **Group** parameter may be used to isolate specific ports to create separate hubs. For example, if ETH 0 and ETH 1 have their **Group** parameter set to 0 whilst ETH 2 and ETH 3 have their **Group** parameter set to 1, the unit will in effect be configured as two 2-port hubs instead of one 4-port hub. This means that traffic on ETH 0 and 1 will not be visible to traffic on ETH 2 and 3 (and vice versa).

DNS server:

This parameter specifies the IP address of a DNS server to be used by the unit for resolving IP hostnames.

Gateway:

This parameter specifies the IP address of a gateway to be used by the unit. IP packets whose destination IP addresses are not on the LAN to which the unit is connected will be forwarded to this gateway.

NAT:

This parameter enables or disables IP Network Address Translation (NAT) at the Ethernet interface. When network address translation is enabled, all inbound IP traffic appears to originate from the **IP address** assigned to the Ethernet interface.

Speed:

The **Speed** parameter is used to select 10Base-T, 100Base-T or auto-detect mode. The currently selected mode will be shown in brackets after the parameter name.

Firewall:

This parameter is used to enable or disable firewall operation for this **ETH** instance.

IGMP:

This parameter is used to enable or disable the Internet Group Management Protocol for this **eth** instance.

IPSec:

This parameter is used to enable or disable IPSec security features for this **ETH** instance.

GRE:

This parameter enables GRE (Generic Routing Encapsulation) for this **ETH** instance. GRE is a simple tunnelling protocol. For further details refer to RFC2784.

Remote management:

When set to Enabled, this parameter allows other users on this **ETH** instance (i.e. the LAN to which the **ETH** instance is connected), to access the unit's Telnet, FTP and Web services for the purpose of managing the unit. To prevent users from this type of access, set the parameter to Disabled.

RIP version:

RIP (Routing Information Protocol), is used by routers to determine the best route to any destination. There are several different versions that can be enabled or disabled using this parameter. When **RIP version** is set to Off, RIP is disabled and no RIP packets transmitted out this interface. When **RIP version** is set to V1 or V2, the unit will transmit RIP version 1 or 2 packets respectively (version 2 packets are sent to the "all routers" multicast address. (224.0.0.9). When RIP Version is set to V1 Compat, the unit will transmit RIP version 2 packets to the subnet broadcast address. This allows V1 capable routers to act upon these packets.

When RIP is enabled, RIP packets are transmitted when the **ETH** instance first becomes active, and at intervals specified by the **RIP interval** parameter on the **Configure ► General** page.

RIP destination IP:

RIP packets are normally sent out on a broadcast basis or to a multi-cast address. This parameter may be used to force RIP packets to be sent to a specified IP address. It is particularly useful if you need to route the packets via a VPN tunnel.

PING request interval (s)

If this parameter is set to a non-zero value the unit will generate a “ping” (ICMP echo request) to the address specified by the **PING IP address** parameter (generally for debug/test purposes). Setting the value to 0 disables the ping facility.

PING IP address

This parameter specifies the address to which ICMP echo requests will be sent if the **PING request interval** is greater than 0.

No PING response out of service delay (s)

This parameter is used to specify the length of time (in seconds), before a route will be designated as being out of service if no response has been received after three PING attempts.

Out of service time (s)

This parameter is used to specify the length of time (in seconds) for which any routes using this **ETH** interface will be designated as being out of service after the above parameter has been effected.

note:

The 2000 series routers currently only transmit RIP packets; they do not act upon any received RIP packets.

Using text commands:

From the command line, use the **eth** command to configure or display the Ethernet interface settings. To display current settings for the Ethernet interface enter the following command:

```
eth <instance> ?
```

At present there can only be one **ETH** instance i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
eth 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
dhcpccli	on, off	DHCP client
dnsserver	IP address	DNS server
do_nat	on, off	NAT
firewall	on, off	Firewall
gateway	IP address	Gateway
gre	on, off	GRE
group	0-3, 255	Group
igmp	on, off	IGMP
ipaddr	IP address	IP address
ipanon	on, off	IP analysis
ipsec	on, off	IPSec
mask	IP netmask	Mask
maxkbps	number	Max rate
nocfg	on, off	Remote management
oossecs	number	Out of service time (s)

pingint	number	PING request interval (s)
pingip	IP address	PING IP address
pingoos	number	No PING response out of service delay (s)
rip	0-3	RIP version
ripip	IP address	RIP destination IP
speed	auto, 10, 100	Speed

For example, to set the unit's IP Address to 1.2.3.4, enter:

```
eth 0 ipaddr 1.2.3.4
```

4.12 Configure ► Event Handler

The unit maintains a log of certain types of event in the **eventlog.txt** pseudo file. When an event of a specified level (or higher) occurs, it can be configured to automatically generate and send an email message, or on GPRS models an SMS message, to a pre-defined address. The **Configure ► Event Handler** option is used to set-up the email or SMS related options for this feature.

Using the web page:

To use the automatic email alarm facility, you must first ensure that a valid **Dial-out number**, **Username** and **Password** have been specified on the **Configure ► PPP** (standard parameters) page, and that the SMTP parameters have been set correctly on the **Configure ► SMTP** page.

To use the automatic SMS alarm facility you must first ensure that a valid **SMS Message Centre** number has been specified on the **Configure ► GPRS** page.

Then set the following parameters as required:

4.12.1 Email parameters:

Emails today:

This read-only value maintains a count of how many emails have been sent during the last 24-hour period.

Max emails/day:

The value in this field is the maximum number of email messages that the unit will generate per day. This is intended to prevent messages being repeated frequently when you have set the event trigger level to a low value i.e. a value that results in many events generating an automated email alarm.

Email template:

This field contains the name of the template file that will be used to form the basis of any email messages generated by the event logger. The default template is a text file called **event.eml** that is stored within the compressed **.web** file.

You may create alternative templates but you must use the **.eml** file extension and store the files in the normal file directory. If you create a new template with the name **event.eml**, this will take precedence over the pre-defined **event.eml** template.

Email trigger priority:

This is the lowest priority event code that will generate an email alarm message. For example, if this value is set to 6, only events with a priority of 6 or higher will trigger an automated email alarm. To disable email alarms set this value to 0.

Email To:

This parameter is used to specify the email address for the recipient of email messages generated by the event logger.

Email From:

This parameter is used to specify the email address for the unit. You will need to set up an email account with your Internet Service Provider.

Email Subject:

This field should contain a brief description of the email content.

Traps today:

This read-only value maintains a count of how many SNMP trap messages have been sent during the current day.

Max traps/day:

The value in this field is the maximum number of SNMP trap messages that the unit can generate per day. This is intended to prevent messages being repeated frequently when you have set the trap trigger level to a low value i.e. a value that results in many traps occurring in one day.

Trap trigger priority:

This is the lowest event priority code that will generate an SNMP trap message. For example, if this value is set to 6, only events with a priority of 6 or higher will trigger an automated SNMP trap message.

4.12.2 SMS Parameters:**note:**

The following parameters apply only to models with GPRS capability.

SMS messages today:

This read-only value maintains a count of how many SMS messages have been sent during the last 24-hour period.

Max SMS/day:

The value in this field is the maximum number of SMS messages that the unit will generate per day. This is intended to prevent messages being repeated frequently when you have set the event trigger level to a low value i.e. a value that results in many events generating an automated SMS alarm.

SMS trigger priority:

This is the lowest priority event code that will generate an SMS alarm message. For example, if this value is set to 6, only events with a priority of 6 or higher will trigger an automated SMS alarm. To disable SMS alarms set this value to 0.

SMS template:

This field contains the name of the template file that will be used to form the basis of any SMS alarm messages generated by the event logger. The default template is a text file called **event.sms** that is stored within the compressed **.web** file.

You may create alternative templates but you must use the **.sms** file extension and store the files in the normal file directory. If you create a new template with the name **event.sms**, this will take precedence over the pre-defined **event.sms** template.

SMS destination:

This is the destination phone number for SMS alarm messages including the international dialling code but no “+” prefix or leading 0’s.

Using text commands:

From the command line, the **event** command may be used to configure the email options for the event logger.

To display the current email settings for the event logger enter the command:

```
event <instance> ?
```

where <instance> is 0. At present there is only one event log i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the command in the format:

```
event 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
emax	number	Max emails/day
etemp	filename	Email template
etrig	0-9	Email trigger level
from	email address	Email From
sms_temp	filename	SMS Email template
sms_to	phone number	SMS destination number
sms_trig	0-9	SMS trigger level
subject	text	Email Subject
to	email address	Email To
trap_max	number	Max traps/day
trap_trig	0-9	Trap trigger level

For example, to set the maximum number of emails that may be sent in one day to 3, enter:

```
event 0 emax 3
```

4.13 Configure ► Firewall

Some models in the Sarian 2000 series incorporate a comprehensive “firewall” facility. A firewall is a security system that is used to restrict the type of traffic that the router will transmit or receive, based on a combination of IP address, service type, protocol type, IP flags etc. Firewalls are used to minimise the risk of unauthorised access to your local network resources by external users or to restrict the range of external resources to which local users have access. A more detailed description of how firewalls operate on the 2000 series is given under the heading “Firewall Scripts”. If you intend to implement a firewall you should refer to that section first.

On the 2000 series, the rules governing the operation of the firewall are contained in a pseudo-file called **fw.txt**. This file can be created either by using the controls on the **Configure ► Firewall** web page, or by using a text editor on your PC and then loading the resulting file into the unit (using FTP or XMODEM).

Using the web page:

If you have not yet created a file called **fw.txt** on the unit, the **Configure ► Firewall** page will initially contain a blank script with a button labelled **Insert** to the right. If you have created the file it will be displayed in the top section of the screen with line numbers at the left and a series of buttons at the right that allow you to delete, edit or insert lines.

At the bottom of the screen are three more buttons labelled **Reset**, **Save** and **Restore**.

To create a new rule directly on the web page click on the **Insert** button at the right of the screen. If there are already one or more lines in the file, there will be two **Insert** buttons, one next to the line (which inserts a new line above the current line) and one on the line below (which inserts a new line below the current line).

In either case a new text box will be created into which you can type the new rule. When you have finished typing the rule press the **OK** button to add it to the file or **Cancel** to abandon the changes. The unit will validate the rule and if it is valid it will add it to the file. If errors are detected it will display a warning message with an indication of the error and you may then choose to edit the line or delete it.

To edit an existing rule click on the **Edit** button to the right of the rule and then on **OK** or **Cancel** when you have completed the changes.

To delete an existing line press the delete button to the right of it.

When you have completed your editing session, click on the **Save** button at the bottom of the screen to copy it back to the **fw.txt** pseudo-file. If you do not save the file any changes you have made will be lost when the power is removed or the unit is rebooted.

If you wish to cancel all changes you have made during an editing session and you have not yet saved them, you may click on the Restore button. This will copy the **fw.txt** file to the screen.

The third button at the bottom of the screen labelled Reset Hit Counters allows you to zero the rule hit counters shown at the left of each rule.

Using text commands:

If your firewall script is particularly complex, you may wish to create it on your PC using the text editor of your choice and then load it onto the PC when it is complete. To do this simply create the file and save it as **fw.txt**. You may then load the file onto the unit using XMODEM as follows:

- 1) Connect the router to your PC using ASY0 and apply power.
- 2) Load your terminal program, select the correct COM port.
- 3) Type **at** and press Enter; the unit should respond with **OK**. If the command is not echoed turn echo on by entering **ate1**.
- 4) Type **atlls**; the unit should respond with **OK**.
- 5) Type **xmodem fw.txt** and press Enter and the unit will wait for the file transfer to start.
- 6) Select the File transfer > XMODEM > Send option in your terminal software and when prompted for a filename select the **fw.txt** file you created.
- 7) When the file transfer is complete the unit will display the **OK** message.

Refer to the section entitled “*FTP under Windows*” for instructions on how to access the unit for the purpose of carrying out FTP file transfers.

Once the file **fw.txt** has been successfully loaded onto the unit the router will automatically “compile” it and generate a file called **fwstat.txt**. If there are any errors in the **fw.txt** file these will be identified in **fwstat.txt**.

4.14 Configure ► Firewall Timers

This page contains the timer parameters that are used by the Firewall stateful inspection module. This module establishes temporary firewall rules that last for the duration of a single connection only. Typically, the first packet of a TCP connection (a SYN packet), is used to create a stateful inspection rule that only allows subsequent packets for that TCP connection through the firewall. The timers described below are used to set limits on how long such rules may persist.

Using the Web page:

The web page includes the following parameters:

TCP opening (secs):

This specifies the length of time following receipt of a TCP packet that causes a stateful inspection rule to be created before a TCP connection must be established. If a TCP connection is not established within this period, the associated stateful inspection rule will be removed.

TCP open (secs):

This parameter specifies the length of time that an established TCP connection may remain idle before the stateful inspection rule created for it is removed. The timer is restarted each time a packet is processed by the associated stateful inspection rule.

TCP closing (secs):

This parameter specifies the length of time that is allowed for a TCP socket to close once the first FIN packet has been received. If the timer elapses before the socket has completed closing the associated stateful inspection rule is removed.

TCP closed (secs):

This parameter specifies the length of time that a stateful inspection rule will remain in place after a TCP connection has closed.

UDP (secs):

This parameter specifies the length of time that a stateful inspection rule will remain in place following the receipt of a UDP packet. The timer is restarted each time packets matching the rule pass in each direction. As a consequence, rules based on UDP should only be used if it is anticipated that packets will travel in both directions.

ICMP (secs):

Some ICMP packets, such as ECHO requests, will generate responses. This parameter specifies the length of time that a stateful inspection rule created in respect of an ICMP packet will remain in place before being removed if a response packet has not been received. Such a rule will also be removed immediately following the receipt of a response.

Other protocol (secs):

If a stateful inspection rule is created from a packet type other than TCP, UDP or ICMP, this parameter specifies the length of time for which the rule will persist. The timer is restarted each time a packet is processed by the rule.

Using text commands:

From the command line, use the **fwall** command to configure or display firewall timer settings.

To display current settings enter the command:

```
fwall <instance> ?
```

where `<instance>` is 0. At present there is only one firewall instance i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the command in the format:

```
fwall 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
closed	number	TCP closed
closing	number	TCP closing
icmp	number	ICMP
open	number	TCP open
opening	number	TCP opening
other	number	Other protocol
udp	number	UDP

For example, to set the firewall TCP closing timer to 15 seconds you would enter the command:

```
fwall 0 closing 15
```

4.15 Configure ► FTP Relay Agents

The **FTP Relay agents** allow any files transferred onto the unit by a specified user (using File Transfer Protocol), to be temporarily stored in memory and then relayed to a specified FTP host. This is useful when the unit is being used to collect data files from a locally attached device such as a webcam, which must then be relayed to a host system over a slower data connection such as GPRS. In effect, the router acts as a temporary data buffer for the files.

The **FTP Relay Agent** can also be configured to email (as an attachment) any files that it was unable to transfer to the FTP Server. To facilitate this you should set the **Email Template, To, From** and **Subject** parameters as appropriate and also configure the SMTP Client (see **Configure ► SMTP**).

Using the Web page:

The web page includes the following parameters:

Local username:

This parameter should be set to match one of the user names programmed in the **Configure ► Users** page. This name is then used as the FTP login "username" when the local device needs to relay a file.

Server hostname:

This is the name of the FTP host to which files from the locally attached device are to be relayed.

Server username:

This is the user name required for login to the specified FTP host.

Server password:

This is the password to be used for logging into the FTP host.

Server confirm password:

Enter the password again in this field to confirm it.

Remote directory:

This is the full name of the directory on the FTP host to which the file is to be saved.

Client timeout (s):

This parameter specifies the length of time in seconds that the unit will maintain a connection to an FTP host after transferring a file.

Client retry count:

This parameter specifies the number of times the unit will try to connect to the specified FTP host.

Client retry interval (s):

This parameter specifies the interval in seconds between successive retries.

Transfer failure mode:

If the unit cannot establish a connection to the specified FTP host after the number of retries specified above, it will either retain the file in memory or delete it depending upon the setting of this parameter. If the file is retained, manual intervention will be required to recover it at a later stage.

note:

The file will be lost if the power is removed from the unit.

Rename local file:

When this parameter is set to Yes, the unit will store uploaded files internally with a filename in the form "relnnnn" where nnnn is a sequential number. For each new file received the number is incremented. When the file is relayed to the FTP host the original filename is used.

When the parameter is set to No, the file is stored internally under its original filename.

Email template:

This field contains the name of the template file that will be used to form the basis of any email messages generated by the **FTP Relay Agent**. This would normally be the standard **event.eml** template provided with the unit but you may create alternative templates if necessary (see EMAIL TEMPLATES).

Email To:

This parameter is used to specify the email address for the recipient of email messages generated by the **FTP Relay Agent**.

Email From:

This parameter is used to specify the email address for the unit. You will need to set up an email account with your Internet Service Provider.

Email Subject:

This field should contain a brief description of the email content.

Using text commands:

From the command line, use the **frelay** command to configure or display **FTP Relay Agent** settings.

To display current settings enter the command:

```
frelay <instance> ?
```

where <instance> is the instance number of the agent .To change the value of a parameter use the command in the format:

```
frelay 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
ftpd	text	Server directory
ftphost	IP address	Server hostname
ftppwd	text	Server password
ftpuser	text	Server username
locuser	text	Local username
norename	off, on	Rename local file
retries	number	Client retry count
retryint	number	Client retry interval (s)
savemode	off, on	Transfer failure mode
smtp_from	email address	Email From
smtp_subject	text	Email Subject
smtp_temp	filename	Email template
smtp_to	email address	Email To
timeout	number	Client timeout (s)

For example, to set the FTP directory for **FTP Relay Agent 1** to “images” you would enter the command:

```
frelay 1 ftpdir images
```

4.16 Configure ► General

The **Configure ► General** page is used to set up a variety of features that relate to the basic operation of the unit.

Using the web page:

Power-up config:

This specifies which of the two configuration files is loaded when the unit is powered up or re-booted. This is equivalent to the **config n powerup** text command.

Serial number:

This read-only field displays the unit’s serial number.

Unit identity:

The unit identity is a string of up to 20 characters that can be used to identify the unit in emails generated by the event logger. It is also displayed as a prompt when logging on remotely. The character sequence “%s” may be used as part of the string. This is substituted by the unit’s serial number when the unit identity is displayed. For example, if the unit serial number is 005555, entering the string “MyRouter_%s>” would show the prompt **MyRouter_005555>** during a remote login.

Auto start macro:

The **Auto start macro** is a command that will be executed automatically when the unit is first powered up. This command will be issued to **ASY 0**. If it is necessary to issue a command to

another ASY port then the command line interface must be used. For example, to issue a command to ASY port 3 you would use:

```
cmd 3 autocmd <command>
```

where <command> is the command to be issued to **ASY 3** on power-up.

System hostname:

The **System hostname** field can be used to allocate a synonym for the local IP address of the unit. For example, the default local IP address is 1.2.3.4. The unit will respond to this address when you enter it into your Web browser. The default **System hostname** that maps to this address is **ss.2000r**.

note:

To work correctly with Windows 98 the System Hostname must include at least one full stop.

Secondary hostname:

This allows a second hostname to be assigned to a unit. This is associated with the secondary IP address (see below).

Secondary IP address:

This is used to set up a second IP address for the unit, allowing different routes to be set up to the unit. This might be useful if you want to remotely access a unit via D-channel or B-channel. For example, you could use SNMP to IP address 1.2.3.6 on D-channel but use FTP to address 1.2.3.4 on B-channel.

Remote command timeout (s):

This specifies the maximum period of inactivity (in seconds), that may occur before a remote command session is terminated. The default value is 90 seconds.

X25 remote command address:

This parameter is used to allow remote access to the unit via an X.25 channel. If the address specified, (up to 15 digits), matches the trailing digits of an incoming X.25 call, the calling user will be prompted to enter their user name and password. Correct entry of these will allow the calling user to control the unit remotely. The range of functions they will be able to access will depend upon their user access level.

GPRS LED mode:

On models fitted with GPRS, this parameter is used to select whether the dual-function status indicators on the front panel reflect the status of the GPRS module or the ISDN connection and may be set to GPRS or ISDN respectively.

ASY LED mode:

This parameter determines what causes the ASY port LED's to illuminate.

When set to Connection, the LED for an ASY port illuminates when the protocol bound to that port is connected.

When set to DTR status, the LED for an ASY port illuminates when the terminal connected to that port raises the DTR signal.

When set to GPRS Signal Strength the four LED's that normally indicate activity on the ASY ports function instead as a signal strength indicator. If only one LED is illuminated the signal is weak, if all four are illuminated the signal is at full strength.

ASY <port> name:

These parameters allow a name to be associated with each of the physical and logical ASY ports. Once you have allocated a name it will appear in the heading of the **Config ► ASY** port page for that port. It will also be displayed when using the **at\port=** command.

GPRS port name:

On models fitted with GPRS this parameter allows you assign a name to the port occupied by the GPRS module, usually ASY 1. Once you have allocated a name it will appear in the heading of the **Config ► ASY Ports ► GPRS Port** page. It will also be displayed when using the **at\port=** command.

ASY <port> Telnet mode:

This parameter is used to select the Telnet mode when a remote entity is connected to an ASY port via TCP/IP (i.e. connected to TCP port 4000 to 4003 for ASY ports 0 – 3 respectively).

When set to Raw Mode no byte stuffing is used.

When set to Telnet Mode standard Telnet byte stuffing is used.

When set to Telnet No Null Stuffing Telnet byte stuffing without null stuffing is used.

GPRS port Telnet mode:

On models fitted with GPRS, this parameter is used to select the Telnet mode when a remote entity is connected to the GPRS port via TCP/IP. The three available options are the same as those for **ASY <port> Telnet** mode described above.

TCP socket inactivity timer (s):

This specifies the maximum period of inactivity (in seconds) that may occur before an open TCP/IP socket is closed. The default value is 300 seconds (5 minutes) and should not normally require altering.

TCP socket keep-alive (s):

This specifies the amount of time (in seconds) between sending “keep-alive” messages over open TCP connections. The purpose of these messages is to prevent a connection from closing even when no data is being transmitted or received. The default value of this parameter is zero, which disables keep-alive messages.

TCP socket connect timeout (s):

This parameter is used to specify the amount of time after which a TCP socket may remain idle before being closed. If the value is set to 0 the socket may remain open indefinitely.

SNMP enterprise number:

This parameter specifies the value of the Object Identifier component following “enterprises” to be used by SNMP managers when accessing the MIB on the unit. Object Identifiers of objects in the unit’s SNMP MIB have the prefix { enterprises n ir2140 } where n is the SNMP enterprise number.

SNMP enterprise name:

This specifies the name corresponding to the SNMP enterprise number above.

SNMP community string:

This specifies the required SNMP Community String to be used by SNMP managers in order to access the unit’s MIB.

SNMP trap destination address:

This is the IP address (or host name) of the destination for SNMP trap messages.

GP sockets use IP from interface:

This parameter allows general-purpose TCP sockets to use a source IP address other than that of the interface on which the socket connection is created.

The unit creates general-purpose sockets automatically when your application requires them e.g. when TPAD calls are made over IP or XOT. Normally, the source address used by the socket will be that of the outgoing interface (usually PPP). However, for some applications such as when setting up a VPN, it may be necessary to specify that the socket use a different source address such as that of the local Ethernet port. This parameter is used to specify from which interface the source address should be derived and may be set to None (default), ETH or PPP.

GP sockets use IP from interface #:

This parameter is used in conjunction with the **GP sockets use IP from interface** parameter above to select which interface instance is used to derive a source address.

DNS resolve only:

Entering a host and/or domain name in this field e.g. "www.sarian.co.uk" prevents the unit from performing a DNS lookup on any other host/domain name.

Additional FTP NAT port:

FTP control channels normally use TCP port 21 to carry the FTP commands. Consequently, when NAT is enabled the unit monitors the FTP commands on this port number and checks for the two FTP commands "PORT" and "PASV". These commands contain information relating to IP addresses which may need modifying during the NAT process. Such modifications may result in different sized packets being generated that then require that the TCP sequence numbers be modified to allow for the changes.

This parameter may be used to specify an additional port number (other than 21), which the unit should monitor and is useful where FTP servers are known to be listening on non-standard control channels.

RIP interval (s):

If this parameter is set to a non-zero value then RIP (Routing Information Protocol) packets will be transmitted at the specified interval (in seconds). These packets contain the unit's current routes (e.g. any active ppp instance routes), static routes and the default route.

IP route out of service time (s):

This specifies the time in (seconds), for which an IP route is flagged as "out of service" when the route cannot be activated (i.e. the metric for the route is set to 16). This means the unit will subsequently attempt to route packets through other routes with matching net masks that are not out of service.

Alternative route delay (s):

This parameter is normally set to 0 and should not be changed without reference to Sarian technical support.

Always-on route return-to-service delay (s):

An "always-on" route is either a route with the interface set to Ethernet or a route with the interface set to a PPP instance that has the AODI mode parameter set to On. If such a route goes out of service for some reason and then becomes available again some time later the

unit will automatically bring the route back up. This parameter is used to set the delay in seconds between the service becoming available again and the unit starting to use it.

User task filename:

This specifies the name of a file containing a “user task” file. A user task is a software module that may be loaded into the unit to provide support for a new protocol or application.

The **Configure: Auto-Configure Email Fields** section is used to set up parameters for use in communicating with a configuration server via email. The following parameters may be set:

To:

This parameter is used to specify the email address field for auto-configuration request emails. This should be set to the email address of the auto-configuration server.

From:

This parameter is used to specify email address of the unit for the auto-configuration request emails.

Subject:

This field should contain a brief description of the email content for auto-configuration emails.

Using text commands:

From the command line, the general settings are configured using the **cmd** command.

To display current general settings enter the command:

```
cmd <instance> ?
```

where <instance> is 0, 1, 2 or 3.

note:

The instance number should be 0 in all cases EXCEPT when using the **ASY name** or **Telnet mode** parameters, in which cases the instance number should match the required port number.

To change the value of a parameter use the command in the format:

```
cmd <instance> <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
asyled_mode	number	ASY LED mode
asyname	text	ASY <port> name
autocmd	text	Auto start macro
cmdnua	number	X.25 remote command address
comm_str	text	SNMP community string
dnsname	text	DNS resolve only
ent_name	text	SNMP enterprise name
ent_nb	number	SNMP enterprise number
from	text	Auto-configure Email: From
ftpnatport	number	Additional FTP NAT port
gprsled_mode	0,1	GPRS LED mode
hostname	text	System hostname
ipadd	0,1,2	GP Sockets use IP from interface #
ipent	“, ETH, PPP	GP Sockets use IP from interface

rip	number	RIP interval (s)
route_dly	number	Alternative route delay (s)
route_dwn	number	IP Route out of service time (s)
routeup_dly	number	'Always-on' route return-to-service delay (s)
sec_hostname	text	Secondary hostname
sec_ip	text	Secondary IP address
sock_connto	number	TCP socket connect timeout (s)
sock_inact	number	TCP socket inactivity timer (s)
sock_keeptact	number	TCP socket keep-alive interval (s)
subject	text	Auto configure Email: Subject
telnet_mode	number	ASY <port> Telnet mode
to	text	Auto configure Email: To
trap_ip	text	SNMP trap destination address
tremto	number	Remote command timeout (s)
unitid	text	Unit identity
usertask	filename	User task filename

For example, to set the System hostname to “my.router” enter the command:

```
cmd 0 hostname my.router
```

4.17 Configure ► GPRS Module

GPRS functionality is only available on models such as the GR2130 that are fitted with an internal GPRS module. This module replaces one of the ASY ports (normally ASY1) and provides wireless data connectivity over the GSM network at speeds of up to 33Kbps. This means that the unit can be used in situations where no ISDN service connection is available. In addition, GPRS models can be configured to send or receive SMS messages. These may be used as an alternative to emails for issuing remote alarms or for automating remote configuration of deployed units.

Before attempting to connect to a GPRS service, you need to set a few parameters specific to your GSM operator. It will be useful to have the following information to hand:

- ◆ Your assigned APN (Access Point Name)
- ◆ PIN Number for your SIM card (if any)

Using the web page:

APN:

When using a GPRS router, you must inform the GPRS network which remote host you wish to connect to. You do this by specifying an Access Point Name (APN). Your network provider or your system administrator will provide this information if you have a private APN.

Often this will look like an Internet address such as “isp.vodafone.ie”, but can also be a simple text string such as “orangeinternet” or “mainhost”. Be sure to enter this correctly otherwise you will be unable to make a connection to the network.

Use backup APN:

This parameter is used to turn the **Backup APN** facility On or Off.

Backup APN:

This parameter may be used to specify an alternative service APN for use in the event that the unit cannot connect using the primary APN specified by the **APN** parameter. The unit will only use this APN if the primary APN fails and the **Use backup APN** parameter is enabled.

Retry APN time (mins):

If the **Use backup APN** parameter is enabled, this parameter is used to define how long the unit will use the backup APN before attempting to revert to the primary APN.

PIN:

Some SIM cards are locked with a Personal Identification Number (PIN) code to prevent misuse if they are lost or stolen. Your GSM operator should be able to tell you if your SIM has a PIN code as supplied.

If you enter a PIN code in this field, the unit will try to unlock the SIM before attempting to connect to the network.

note:

The PIN code is not shown for security reasons and it is essential that you enter this correctly as three incorrect attempts will usually block the SIM card from use. In this event, you will need to remove the SIM card from the unit and insert it into a mobile phone then enter the Personal Unblocking Key (PUK), which can be obtained from the network operator.

Initialisation string <n>:

These parameters (**Initialisation string 1**, **Initialisation string 2** etc.) allow you to specify a number of initialisation strings that are sent to the GPRS module each time a GPRS connection is attempted. These can be used to set non-standard GPRS operating modes.

Each string is prefixed with the characters "AT" before being sent to the GPRS module and they are sent to the GPRS module in the order specified until an empty string is encountered. For example, **Initialisation string 3** will not be sent unless **Initialisation string 1** and **Initialisation string 2** are both specified. Initialisation strings are not normally required for most applications as the unit will normally be pre-configured for correct operation with most networks.

Hang-up string:

This parameter allows you to specify a text string that is sent to the GPRS module when disconnecting a call. The unit will automatically insert the AT command prefix before it issues the command to the GPRS module so you do not need to include it in the string. Note that the unit will also use the standard **ath** hang-up so it is not normally necessary to specify an alternative string.

Link retries:

Sarian GPRS routers normally make multiple attempts to connect to the GPRS network in the event that the signal is lost. In some cases, this can result in a "lock-up" situation where the GSM network is unable to attach the GPRS device due to the multiple attempts. The **Link retries** parameter specifies the number of attempts at connection that the unit should make before internally resetting the link. Leave the parameter set at its default value of 0 for normal operation.

SMS message centre:

This is the number of the SMS message centre (sometimes referred to as the Service Centre Address), to be used to relay SMS messages or alarms. This number must include the international dialling code e.g. 44 for the UK, but not "+" prefix or leading 0's e.g. 44802000332. SMS alarms are generated when the **SMS trigger priority** is greater than 0 and an event of this priority or higher occurs. SMS messages may be edited and sent using the **SMS Edit** page.

If no number is specified it is possible that the unit will operate using the default message centre for the GSM service to which you have subscribed.

SMS command separator:

This parameter specifies the character to be used to separate multiple command lines when a remote SMS sender is controlling the unit. The default separator is <CR><LF> but some SMS capable devices are not equipped with <CR> and <LF> keys so an additional means of separating multiple lines is required.

SMS polling interval (mins):

This specifies the interval in minutes that the unit will wait in between checks for incoming SMS messages. Setting this interval to 0 turns off checking.

SMS command caller ID:

This parameter specifies a number that is compared with the trailing digits of the SMS sender's phone number. If the numbers match, then the SMS text is treated as if it were a text command being entered via one of the serial ports. If the parameter is left blank, SMS messages are logged in the event log but are not treated as commands.

Enable Mux / Disable Mux:

The two buttons at the bottom of the page labelled **Enable Mux** and **Disable Mux** are used to enable or disable 0710 multiplex mode for the GPRS module. When this mode is enabled (which it is by default), several additional parameters become effective on the **Configure ► ISDN LAPB** page under the heading **Async Mux 0710 Parameters**. Refer to the description of this page for further information.

Using text commands:

From the command line, the **modemcc** command can be used to configure the GPRS module.

To display the current settings for the GPRS module enter the command:

```
modemcc <instance> ?
```

where <instance> is 0.

To change the value of a parameter use the same command in the format:

```
modemcc 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
apn	text	APN
bupapn	text	Backup APN
hang_str	text	Hang-up string
init_str	text	Init string 1
init_str1	text	Init string 2
init_str2	text	Init string 3
link_retries	number	Link retries
pin	number	PIN
retry_apntim	number	Retry APN time (mins)
sca	phone number	SMS message centre (Service Centre Address)
sms_callerid	number	SMS command caller ID
sms_cmd_sep	character	SMS command separator
sms_interval	number	SMS polling interval (s)
usebuapn	on, off	Use backup APN

For example, to set the first initialisation string, enter:

```
modemcc 0 init_str +cgdcont=1,"ip","isp.vodafone.ie",,0,0
```

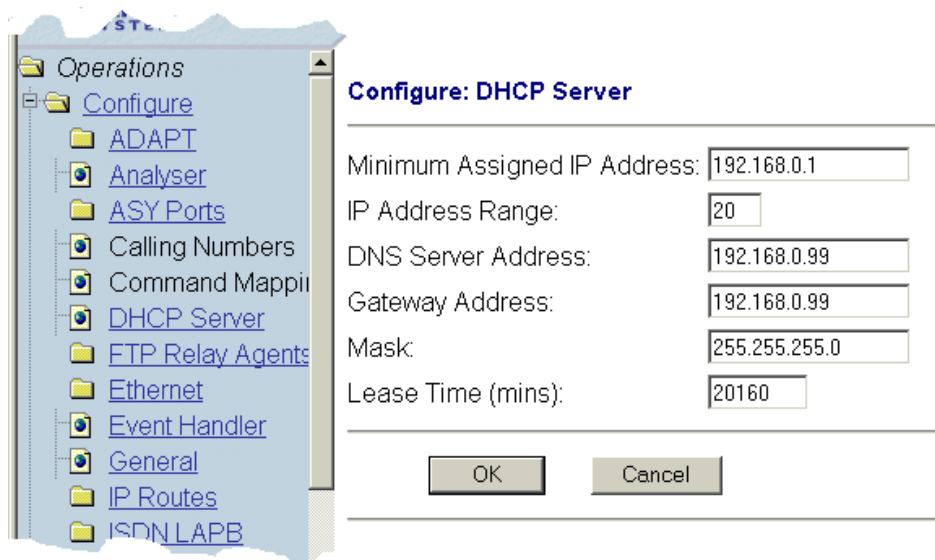
note:

If your initialisation strings contains blanks, then you must enclose the entire string with double quotation marks.

4.17.1 Additional configuration for GPRS

If you are intending to use your GPRS router to connect a local PC or laptop to remote services via GPRS, you will need to ensure that both the PC and the router share a common TCP/IP subnet.

To ensure that this is the case, use the units DHCP server to give your PC an IP address in the correct range. To do this, navigate to **Configure ► DHCP Server**, the following page will be displayed:



Fill in the six sections appropriately, then click **OK**, not forgetting to save the configuration later. In the above example, the unit has an IP address (set in **Configure ► Ethernet ► ETH0**) of 192.168.0.99 and the first PC to connect to it will be given an address of 192.168.0.1 enabling communication on the same subnet.

If you have correctly configured the unit, you should now be able to connect the LAN port to a PC or Laptop (using an Ethernet hub or a crossover cable), for the purpose of accessing host services such as Internet pages or email.

4.18 Configure ► ISDN LAPB

LAPB (Link Access Procedure Balanced) is a standard subset of the High-Level Data Link Control (HDLC) protocol. It is a bit-oriented, synchronous, link-layer protocol that provides data framing, flow control and error detection and correction. LAPB is the link layer used by X.25 applications.

Using the web page:

The **Configure ► ISDN LAPB** option expands to list separate pages for the LAPB 0 and LAPB 1 instances that allow you to set the following parameters.

Layer 1 interface:

This parameter determines which physical interface is to be used for carrying LAPB data. This can be set to either ISDN or PORT. If ISDN is selected then LAPB data is carried over

the ISDN BRI physical interface. By selecting PORT, LABP data can be routed to either ASY 0 or ASY 1 (operating in synchronous mode), as selected by the Sync Port parameter below.

To configure ASY 0 or ASY 1 for synchronous operation see **Configure ► Sync Ports**.

Sync port:

This parameter is only relevant if the Layer 1 Interface option above has been set to Port (as opposed to ISDN). It is used to select ASY0 or ASY1 as the layer 1 interface for LAPB data.

Answering:

If the LAPB **Answering** parameter is set to On, the unit will answer incoming calls on the relevant LAPB session. To prevent the unit from answering incoming calls on this LAPB session set the option to Off.

DTE/DCE mode:

When the **DTE/DCE mode** parameter is set to DTE, the unit will behave as Data Terminal Equipment with respect to the ISDN network. This is the default value and should not be changed for normal operation across the ISDN network. If your application involves using two units back-to-back, one of the units should have the **DTE/DCE mode** value set to DCE so that it acts as Data Communications Equipment.

MSN:

The **MSN** parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with LAPB Answering On it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the **MSN** value. For example setting the **MSN** parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

If LAPB **Answering** is Off this parameter is not used.

Sub-address:

The **Sub-address** parameter provides the filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value with answering enabled it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the **Sub-address** value. For example setting the **Sub-address** parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

If LAPB **Answering** is Off this parameter is not used.

RR timer (ms):

This is a standard LAPB/LAPD "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

Inactivity timer (s):

This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled.

T1 timer:

This is a standard LAPB/LAPD timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 timer:

This is the standard LAPB/LAPD re-transmit timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

N400 counter:

This is the standard LAPB/LAPD re-try counter. The default value is 3 and it should not normally be necessary to change this.

Window size:

This parameter is used to set the X.25 window size. The value range is from 1 to 7 with the default being 7.

Restart when activate:

This parameter can be set to No or Immediate. When set to Immediate, the LAPB instance will send an X.25 restart packet immediately on receipt of a SABM. If the parameter is set to No, then no X.25 restart is sent.

Passive timer (ms):

This parameter sets the length of time (in milliseconds), that the LAPB instance will wait from an ISDN B-channel becoming active before attempting to establish a LAPB connection i.e. the length of time for which the LAPB instance stays passive. The default is 0 as most ISDN networks allow CPE devices to initiate a LAPB link. If your ISDN network does not permit CPE devices to initiate the LAPB link you should set this parameter to a value that allows the network sufficient time to establish the LAPB link.

Async Mux 0710 Parameters**note:**

The parameters listed under this heading are intended for use in providing technical support only and should not be adjusted in normal operation.

Using text commands:

From the command line, use the **lapb** command to configure or display LAPB settings.

To display current settings for a LAPB instance enter the command:

```
lapb <instance> ?
```

where <instance> is 0 or 1.

To change the value of a parameter use the command in the format:

```
lapb <instance> <parameter> <value>
```

where <instance> is 0 or 1.

The parameters and values are:

Parameter	Values	Equivalent web parameter
ans	on, off	Answering
dtemode	0,1	DCE/DTE mode
l1iface	isdn, port	Layer 1 interface
l1nb	0,1	Sync port
msn	number	MSN
n400	1-255	N400 counter
pstime	number	Passive timer (ms)
restartact	0,1	Restart when activate
sub	number	Sub-address filter
t1time	number	T1 timer (ms)
t200	number	T200 timer (ms)

tinact	number	Inactivity timer (s)
tnoact	number	Activity timer (ms)
window	1-7	Window size

For example, to enable answering on LAPB 0 you would enter the command:

```
lapb 0 ans on
```

4.19 Configure ► ISDN LAPD

Link Access Protocol D (LAPD) is the protocol used for ISDN D-channel signalling and call set up.

Using the web page:

The **Configure ► ISDN LAPD** option expands to list separate pages for the LAPD 0, LAPD 1 and LAPD 2 instances. LAPD2 is normally reserved for ISDN call control. LAPD0 and LAPD1 can be used as required for SAPI16 traffic i.e. D-channel X.25. The configuration pages allow you to set the following parameters for each instance.

Enabled:

Setting this parameter to No will disable the LAPD instance. This may be necessary if you have an installation where two or more units are connected to the same ISDN “S” bus. In this case, only one of the units may be configured for D-channel X.25 on TEI1, SAPI16. On each of the other units you must disable any LAPD instance for which the TEI is set to 1 in order to prevent it from responding to X.25 traffic on that TEI that is actually destined for another unit.

DTE/DCE mode:

When the **DTE/DCE mode** parameter is set to DTE, the unit will behave as a DTE. This is the default value and should not be changed for normal operation across the ISDN network. If your application involves using two units back-to-back, one of the units should have the **DTE mode** value set to DCE.

Keep active:

When the **Keep active** parameter is set to Yes, the unit will try to re-activate a D-channel connection after disconnection by the network by transmitting SABME frames. If it is unable to reactivate the connection after re-trying the number of times specified by the N400 counter, it will wait for 1 minute before repeating the re-try sequence.

If the **Keep active** parameter is set to No, the unit will not attempt to reactivate a D-channel link following deactivation by the network.

N400 counter:

This is the standard LAPB/LAPD retry counter. The default value is 3 and it should not normally be necessary to change this.

RR timer (ms):

This is a standard LAPB/LAPD “Receiver Ready” timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

Deactivation:

This parameter can be set to Active or Passive. When set to Passive, the unit will not deactivate a LAPD session when an X.25 PAD session is terminated using the **log** command. To enable automatic deactivation of a LAPD session the option should be set to Active.

T1 timer (ms):

This is the standard LAPB/LAPD timer. The default value is 1000 milliseconds (1 second) and it should not normally be necessary to change this.

T200 timer (ms):

This is the standard LAPB/LAPD re-transmit timer in milliseconds. The default value is 1000 milliseconds (1 second) and it should not normally be necessary to change this.

TEI:

Each ISDN terminal device connected to your ISDN basic rate outlet must be assigned a unique Terminal Endpoint Identifier (TEI). In most cases, this is negotiated automatically. In some cases however, it may be necessary to assign a fixed TEI.

When **TEI** is set to 0, the TEI is negotiated with the ISDN network. To use a fixed TEI set the **TEI** parameter to the appropriate value as specified by your service provider.

Window size:

This specifies the transmit window size when using D-channel X.25. The default is 7.

Tx throughput (bps):

The **Tx Throughput** parameter is used in conjunction with the **Rx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.

If this parameter is set to 0, the unit will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.

When set to a value greater than 0, the unit will limit the rate at which data is transmitted over the LAPD link

Note that if multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Rx throughput (bps):

The **Rx Throughput** parameter is used in conjunction with the **Tx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.

If this parameter is set to 0, the unit will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.

When set to a value greater than 0, the unit will limit the rate at which data can be received over the LAPD link when it detects that receive throughput exceeds the specified rate.

Note that if multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

D64S mode:

D64S mode is a mode in which ISDN B-channel(s) may be used without the need to use any D-channel protocol. It is sometimes referred to as “nailed up” ISDN. To enable this mode for this LAPD instance, set the **D64S mode** parameter to On and ensure that the **TEI** parameter is set to 255. This means that for any application that uses ISDN (e.g. PPP) then it will use D64S mode.

note:

You may only use this mode if it is supported by your ISDN service provider.

First D64 B-channel:

When using D64S mode there is no dialling protocol to negotiate which B-channel to use. This must therefore be specified using this parameter. To use B1 set the parameter to 1, or select 2 to use B2 (if another channel is requested from an application then it will use the other unused B-channel).

Using text commands:

From the command line, use the **lapd** command to configure or display LAPD settings.

To display current settings for a LAPD instance enter the command:

```
lapd <instance> ?
```

where <instance> is 0, 1 or 2.

To change the value of a parameter use the command in the format:

```
lapd <instance> <parameter> <value>
```

where instance is 0, 1 or 2.

The parameters and values are:

Parameter	Values	Equivalent web parameter
dtemode	on, off	DTE/DCE mode
keepact	on, off	Keep active
n400	1-255	N400 counter
nodeact	on, off	Deactivation
rthruput	0-9600	RX throughput (bps)
t1time	number	T1 timer (ms)
t200	number	T200 timer (ms)
tei	0-255	TEI
tnoact	number	Activity timer (ms)
tthruput	0-9600	TX throughput (bps)
window	1-7	Window size

For example, to select DCE mode for LAPD 2 you would enter:

```
lapd 2 dtemode off
```

4.20 Configure ► IP Routes

The **Configure ► IP Routes** page allows you to set up static IP routes for particular IP subnets, networks or addresses, or a default route. This page expands to list separate pages for **Route 0**, **Route 1**, etc, and **Default Route 0**, **Default Route 1** etc which, when populated with the appropriate information define the static routing table used by the unit.

Each **Route <n>** page contains parameters used to configure a static IP route. The **Default Route <n>** page contains parameters used to configure a default route that will be used to route all non-local IP addresses not specified in a static IP route.

Using the web pages:

4.20.1 IP Route parameters

IP address / Mask:

These parameters are used in conjunction with each other to specify the destination subnet, network or IP address for packets that will match this route i.e. if the unit receives a packet with a destination IP address that matches the specified **IP address / Mask** combination, it will route that packet through the interface specified by the **Interface / Interface #** parameters.

Source address / Source mask:

If necessary you may use the **Source address** and **Source mask** parameters to further qualify the way in which the unit will route packets. If these parameters are specified, the source address of the packet being routed must match these parameters before the packet will be routed through the specified interface.

Interface:

Specifies the interface through which to route packets with match the **IP address / Mask** or **IP address / Mask** plus **Source address / Source Mask** combination. Either PPP or Ethernet may be selected.

Interface #:

Specifies the instance of the above interface (e.g. PPP instance 1).

Interface sub-config:

Specifies that the parameter settings in the appropriate PPP sub configuration (**Configure ► PPP ► SubConfigs**) that will override the parameters in the PPP instance specified in **Interface / Interface #** above.

Connected metric / Disconnected metric

A “metric” is a value between 1 and 15 that is used to select which route will be used when the subnet for a packet matches more than one of the IP route entries.

Each route can be assigned a “connected metric” and a “disconnected metric”. The **Connected metric** parameter is used to specify the metric for a route whose interface is up. The **Disconnected metric** parameter is used to specify the metric for a route whose interface is down. Normally both values should be the same but in some advanced routing scenarios it may be necessary to use different values.

If a particular route fails it will automatically have its metric set to 16, which means that it is temporarily deemed as being “out of service”. The default out of service period is set by the **IP route out of service time** parameter on the **Configure ► General** web page. Note however, that this default period may be overridden in certain situations such as when a firewall stateful inspection rule specifies a different period. When a route is out of service, any alternative routes (with matching subnets), will be used first.

Redial delay (s):

The delay in seconds to wait before re-initiating a connection after it has been dropped whilst still required.

4.20.2 Default Route Parameters

Source address / Source mask:

Default routes are used to route all packets that do not match one of the defined static routes. If these parameters are specified, the source address of the packet being routed must match these parameters before the packet will be routed through the specified default interface.

Interface / Interface #:

These parameters are used to specify the interface through which the unit will route packets to IP addresses that do not match one of the static routes.

Interface sub-config:

Specifies that the parameter settings in the appropriate PPP sub configuration (**Configure ► PPP ► SubConfigs**) that will override the parameters in the PPP instance specified in Interface and Interface # above.

Connected metric / Disconnected metric

These parameters are used to set-up the connected and disconnected metric values for this IP route. For a full explanation refer to the **Connected metric** and **Disconnected metric** parameter descriptions in the **Configure ► IP Routers ► Static IP Route parameters** page above.

Redial delay:

The delay in seconds to wait before reinitiating a connection after it has been dropped whilst still required.

Using text commands:

From the command line, use the **route** command to configure a static IP route, or the **def_route** command to configure the default IP route. To display the current settings for a particular IP route, enter the following command:

```
route <instance> ?
```

To set up parameters for a static IP route, enter the command in the format:

```
route <instance> <parameter> <value>
```

for example:

```
route 0 ipaddr 1.2.3.4
```

The parameter options and values are:

Parameter	Values	Equivalent web parameter
dial_int	0-255	Redial delay (s)
ipaddr	IP address	IP address
ll_add	number	Interface #
ll_cfg	number	Interface sub-config
ll_ent	“, PPP, or ETH	Interface
mask	IP netmask	Mask
metric	1-16	Disconnected metric
srcip	IP address	Source address
srcmask	IP netmask	Source mask
upmetric	1-16	Connected metric

To display the current settings for the default route, enter the following command:

```
def_route <instance> ?
```

where <instance> is always 0 (zero), as there is only one default IP route.

To set up parameters for a default IP route, enter the command in the format:

```
def_route 0 <parameter> <value>
```

For example:

```
def_route 0 ll_ent ppp
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
dial_int	0-255	Redial Delay (s)
ipaddr	IP address	IP address
ll_add	number	Interface #
ll_cfg	number	Interface sub-config
ll_ent	“, PPP, or ETH	Interface
metric	number	Connected metric
srcip	IP address	Source address
srcmask	IP netmask	Source mask
upmetric	number	Disconnected metric

4.21 Configure ► IPSEC

IPSEC refers to a group of protocols and standards that may be used to protect data during transmission over the Internet (which is not inherently secure). Various levels of support for IPSEC can be provided on 2000 series products depending upon which model you have purchased. The web pages located under the heading **Configure ► IPSEC** are used to set the various parameters and options that are available. You should note however that this is a complex area and you should have a good understanding of user authentication and data encryption techniques before you commence. For further information refer to “IPSec and VPN’s”.

IPSec ► IKE

The first stage in establishing a secure link between two endpoints on an IP network is for those two points to securely exchange a little information about each other. This enables the endpoint responding to the request to decide whether it wishes to enter a secure dialogue with the endpoint requesting it. To achieve this, the two endpoints commonly identify themselves and verify the identity of the other party. They must do this in a secure manner so that the process cannot be “listened in to” by any third party. The IKE protocol is used to perform this “checking” and if everything matches up it creates a Security Association between the two endpoints, normally one for data being sent TO the remote end and one for data being received FROM it.

Once this initial association exists the two devices can “talk” securely about and exchange information on what kind of security protocols they would like to use to establish a secure data link, i.e. what sort of encryption and/or authentication they can use and what sources/destinations they will accept. When this second stage is complete (and provided that both systems have agreed what they will do), IPSec will have set up it’s own Security Associations which it uses to test incoming and outgoing data packets for eligibility and perform security operations on before passing them down or relaying them from the “tunnel”.

Using the Web pages:

The **Configure ► IKE** page lists the various IKE parameters:

Encryption algorithm:

This parameter selects the encryption algorithm to be used for IKE exchanges over the IP connection. You can select DES, 3DES or leave the option blank (in which case key exchanges will not be encrypted).

Authentication algorithm:

This parameter selects the algorithm used to verify that the contents of data packets have not been changed in transit since they were sent. You may select none (i.e. blank), MD5 or SHA-1.

Duration (s):

This parameter determines how long (in seconds) the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA. Enter a value between 1 and 28800 seconds (8 hours).

Aggressive mode:

Historically, fixed IP addresses have been used in setting up IPSec tunnels. Today it is more common, particularly with Internet ISPs, to dynamically allocate the user a temporary IP address as part of the process of connecting to the Internet. In this case, the source IP address of the party trying to initiate the tunnel is variable and cannot be pre-configured.

In main mode (i.e. non-aggressive), the source IP address must be known i.e. this mode can only be used over the Internet if the ISP provides a fixed IP address to the user or you are using X.509 certificates.

Aggressive mode was developed to allow the host to identify a remote unit (initiator) from an ID string rather than from its IP address. This means that it can be used over the Internet via an ISP that dynamically allocates IP addresses. It also has two other noticeable differences from main mode. Firstly, it uses fewer messages to complete the phase 1 exchange (3 compared to 5) and so will execute a little more quickly, particularly on networks with large turn-around delays such as GPRS. Secondly, as more information is sent unencrypted during the exchange, it is potentially less secure than a normal mode exchange.

This parameter is used to select main mode (Off) or aggressive mode (On).

note:

Main mode can be used without knowing the remote unit's IP address when using certificates. This is because the ID of the remote unit (its public key) can be retrieved from the certificate file.

IKE MODP group:

This parameter allows you to set the key length used in the IKE Diffie-Hellman exchange to 768 bits (group 1) or 1024 bits (group 2). Normally this option is set to group 1 and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting group 2 to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

IPSec MODP group:

This parameter allows the user to set the width of the numeric field used in the calculations for phase 2 of the security exchange.

With No PFS (Perfect Forwarding Security) selected, the data transferred during phase 1 can be re-used to generate the keys for the phase 2 SA's (hence speeding up connections). However, in doing this it is possible (though very unlikely), that if the phase 1 keys were compromised (i.e. discovered by a third party), the phase 2 keys might be more easily compromised.

Enabling group 1 or 2 IPsec MODP forces the key calculation for phase 2 to use new data that has no relationship to the phase 1 data and initiates a second Diffie-Hellman exchange. This provides an even greater level of security but of course can take longer to complete (see comments on group 1/ group 2 calculation times under **IKE MODP group**).

Act as initiator only:

Setting this parameter to Yes prevents the unit from responding to any remote IKE requests. When set to No the unit will both initiate an IPsec IKE exchange if required to do so and respond to any incoming IKE requests.

RSA private key file:

This parameter specifies the name of a file for the X.509 certificate holding the unit's private part of the public/private key pair used in certificate exchanges. See *X.509 certificates* for further explanation.

Maximum re-transmits:

This parameter specifies the maximum number of times that IKE will retransmit a negotiation frame as part of the exchange before failing.

Re-transmit interval (s):

This parameter specifies the amount of time in seconds that IKE will wait for a response from the remote system before retransmitting the negotiation frame.

Inactivity timeout (s):

This parameter specifies the period of time in seconds after which when no response to a negotiation packet has been received from the remote IKE will give up.

NAT traversal enabled:

When set to On, this parameter enables support for NAT traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is being performed.

The version of NAT traversal supported is that described in the IETF draft "draft-ietf-ipsec-nat-t-ike-03.txt".

NAT traversal keep-alive interval (s)

This parameter may be used to set a timer (in seconds), such that the unit will send regular packets to a NAT device in order to prevent the NAT table from expiring.

Debug:

When set to On this parameter provides additional tracing of IKE exchanges in the IP Analyser log. See the section on the protocol analyser for more details of general analyser capabilities.

Using text commands:

From the command line, use the **ike** command to configure or display IKE settings.

To display current settings for IKE instance enter the command:

```
ike <instance> ?
```

where <instance> is 0.

To change the value of a parameter use the command in the format:

```
ike <instance> <parameter> <value>
```

where <instance> is 0.

The parameters and values are:

Parameter	Values	Equivalent web parameter
aggressive	on, off	IKE aggressive mode
authalg	md5, sha1	IKE authentication algorithm
debug	on, off	IKE debug trace
encalg	des, 3des	IKE encryption algorithm
ikegroup	1, 2, !	IKE MODP group
inactto	0-255	IKE inactivity timeout (s)
ipsecgroup	1, 2, !	IPSec MODP group
ltime	1-28800	IKE session duration
natt	on, off	NAT Traversal on, off
noresp	on, off	IKE initiate only mode on, off
natkaint	number	NAT traversal keep-alive interval (s)
privrsakey	filename	IKE X.509 certificate file
retran	0-9	IKE max. re-transmits
retranint	0-255	IKE re-transmit interval (s)

note:

Using ! for a parameter in a text command means blank.

For example, to turn aggressive mode on you would enter:

```
ike 0 aggressive on
```

4.22 Configure ► IPSec ► Eroutes

Once the IKE parameters have been set-up, the next stage is to define the characteristics of the encrypted routes, or tunnels (“*Eroutes*”). This includes items such as what source/destination addresses will be connected by the tunnel and what type of encryption/authentication procedures will be applied to the packets traversing it. For obvious reasons it is essential that parameters such as encryption and authentication are the same at each end of the tunnel. If they are not, then the two systems will not be able to agree on what set of rules or “policy” to adopt for the encrypted route and communication cannot take place.

Using the web pages:

The **Configure ► IPSec ► Eroutes** page contains a number of sub-pages for *Eroutes* 0-9, 10-19 etc.

note:

The number of *Eroutes* available depends on how many licenses you have purchased. *Eroute* licenses may be purchased in groups of 10 up to a maximum of 30).

The parameters listed on each *Eroute* page are as follows:

Peer IP/hostname:

This is the IP address of the remote unit to which you wish to connect.

Peer ID:

In normal mode (i.e. when **Aggressive mode** is Off) this must be the IP address of the peer. When **Aggressive mode** is On, this parameter is a string of up to 20 characters that is used in to identify the remote system and should contain the same text as the **Our ID** field in the corresponding remote unit's *Eroute* configuration.

Our ID:

When **Aggressive mode** is On, this parameter is a string of up to 20 characters sent to the remote system to identify the initiator. When certificates are used this field should contain, the "Alname" field in a valid certificate held on the unit.

Send our ID as FQDN:

When set to Yes, this parameter indicates to the remote peer that the ID is in Fully Qualified Domain Name format e.g. "bill.smith@anycompany.com". When set to No, the ID is indicated as being of simple Key ID type e.g. billsmith. The default is No and it should only be necessary to select Yes where interoperability problems are encountered with other manufacturer's VPN equipment.

Local subnet IP address:

This is the IP address of the local sub-net. This will usually be the IP address of the local router's Ethernet interface or that of a specific device on the local sub-net (such as a PC running a client or host application).

Local subnet mask:

When connecting two sub-nets it will often be desirable to allow any device on one sub-net to connect to any other device on the remote sub-net. This mask sets the range of addresses that will be allowed to use the *Eroute*.

Remote subnet IP address:

This is the IP address of the remote sub-net. It will usually be the IP address of the remote router's Ethernet interface or that of a specific device on the remote sub-net (such as a PC running a client or host application).

Remote subnet mask:

When connecting two sub-nets it will often be desirable to allow any device on one sub-net to connect to any other device on the remote sub-net. This mask sets the range of addresses that can be addressed on the remote sub-net via the *Eroute*.

Mode:

This parameter can be set to Tunnel or Transport. In normal use this will be set to Tunnel i.e. both the data payload and the packet headers/routing information will be encrypted.

AH authentication algorithm:

This parameter selects the algorithm used to verify that the packet contents have not been changed in transit since they were sent. You may select None, MD5 or SHA-1.

Normally it is preferable to use ESP authentication and turn AH authentication off (as ESP provides better protection) but for compatibility with some older systems it may necessary. There is little point in using AH and ESP Authentication together but this is also possible.

ESP authentication algorithm:

This parameter selects the algorithm used to verify that packet contents have not been changed. You may select None, MD5 or SHA-1.

ESP encryption algorithm:

This parameter specifies the cryptographic algorithm to be used when securing the packet payload. You may select None, DES, 3-DES or RIJN (AES).

IPCOMP algorithm:

This parameter determines whether data compression is used.

When LZJH is selected, sophisticated data compression is applied to the data being carried. The effectiveness of data compression will vary with the type of data but a typical ratio achieved for a mix of data, for instance Web pages, spreadsheets, databases, text files, GIFs etc would be between 2 and 3:1. This has the effect of increasing the connection throughput. If the data is traversing a network where charges are based on the amount of data passed (such as many GPRS networks), it may also offer significant cost savings. Note however that if the data is already compressed, such as .zip or .jpg files, then the system will detect that the data cannot be compressed further and send it un-compressed.

When set to NONE, data is not compressed.

note:

Data compression is an optional feature that may not appear on your product unless you have purchased it as a separate feature pack.

IP protocol:

This parameter acts as a filter. When set to UDP the unit will allow only UDP packets to cross the *Eroute*. When set to TCP only TCP packets will pass and when set to Off, all packet types may pass.

Destination port:

This parameter specifies a port number in the range 1-32767. When set to 0, data to any port can be transmitted. When set to a value in the above range, only data destined for that port will be transmitted.

Duration (s):

This parameter specifies the length of time in seconds (from 0 to 28800) for which a phase 2 *Eroute* SA can remain valid. When this period has expired the unit will initiate a new phase 2 key exchange to re-validate the other end of the connection. A value of 0 means that the SA's will not time-out (unless the duration has been set in kilobytes using the **Duration (kb)** parameter).

Duration (kb):

As an alternative to negotiating new keys based on duration of connection, the "lifetime" of a session may be set based on the amount of data transferred. This parameter is used to specify the validity of an SA in terms of the maximum amount of data (in kb) that may be transmitted before a new phase 2 key exchange will be initiated. A value of 0 means that SA's will not time-out (unless the duration has been set in seconds using the **Duration (s)** parameter).

No SA action:

This parameter determines how the router will respond if it receives a request to route a packet that matches an *Eroute* definition (i.e. source address, destination address, protocol

etc match) but for which no SA's exist. When set to Use IKE, it will try to initiate an IKE session to establish SA's. When set to Drop Packet it will discard the packet. When set to Pass Packet it will allow the packet through without authentication or encryption.

Create SA's automatically:

When this parameter is set to Yes, the Eroute will automatically attempt to create an IPSec SA (VPN Tunnel) regardless of whether the unit needs to route any packets to the remote subnet or not. This effectively creates an "always on" Eroute.

Authentication method:

This parameter specifies the "key" used between VPN endpoints to encrypt and de-crypt data.

The Pre-shared keys option requires that both the remote and host system (initiator and responder) share a secret key, or password, that can be matched by the responder to the initiator calling in.

Selecting the RSA signatures option invokes the use of X.509 certificates (see "X.509 Certificates" for more information). To configure users and their passwords or pre-shared secrets on the 2000 Series, you must populate the User table with details of the remote system's ID (IP address in Normal mode and ID string when **Aggressive mode** is On), and the password to use (see **Configure ► Users**).

note:

As IKE has a single configuration for **Aggressive Mode** being On or Off, the user table will either contain a series of *IP addresses* and passwords when **Aggressive mode** is Off or a series of remote *ID strings* and passwords if **Aggressive mode** is On.

The User table serves a dual purpose in that it may contain a series of entries for normal login access (i.e. for dial-in HTTP, FTP or Telnet access) and entries for IPSec look-up. In the screen-shot below entries 1-3 are for normal login access, entry 6 is the routers own ID and password (for aggressive mode IPSec connections) and entries 7 and 8 define two remote units that may wish to initiate an IPSec aggressive mode connection into this system.

It is important to remember that each system needs to look up it's own secret password against it's ID in the table as well. So if the IKE responder ID is set to "mysystemhost" the user table must have a corresponding entry for this ID.

GRE:

This parameter enables GRE (Generic Routing Encapsulation) for this **Eroute** instance. GRE is a simple tunnelling protocol that *does not provide encryption or authentication*. For further details refer to RFC2784.

NAT traversal keep-alive interval (s)

This parameter may be used to set a timer (in seconds), such that the unit will send regular packets to a NAT device in order to prevent the NAT table from expiring.

Using text commands:

From the command line, use the **Eroute** command to configure or display *Eroute* settings. To display current settings for a specific *Eroute*, enter the command:

```
ike <eroute> ?
```

where <eroute> is the number of the *Eroute* .

To change the value of a parameter use the command in the format:

```
ike <eroute> <parameter> <value>
```

where <eroute> is the number of the *Eroute*. The parameters and values are:

Parameter	Values	Equivalent web parameter
ahauth	none, md5, sha1	AH authentication algorithm
authmeth	preshared, rsa	Authentication method
autosasa	yes, no	Create SA's automatically
dstport	number	Destination port
espauth	none, md5, sha1	ESP authentication algorithm
espcnc	none, des, 3des, aes	ESP encryption algorithm
gre	on, off	GRE
idisfqdn	yes, no	Send our ID as FQDN
ipcompalg	none, lzjh	Compression algorithm
lkbytes	number	SA duration (kb)
locip	IP address	IP address of local subnet
locmsk	subnet mask	IP address mask for local subnet
ltime	0-28800	SA duration (s)
mode	tunnel, transport	Operational mode
natkaint	number	NAT keep alive interval (s)
nosa	drop, pass, try	No SA action
ourid	text	Aggressive mode ID
peerip	IP address	IP address of remote unit
proto	off, tcp, udp	IP protocol
remip	IP address	IP address of remote subnet
remmsk	subnet mask	IP address mask for remote subnet

e.g. to set the IP address of the remote unit for *Eroute* 2 to 192.168.100.1 you would enter:

```
eroute 2 peerip 192.168.100.1
```

4.23 Configure ► IPSec ► Default Eroute

Like normal IP routing set-up, IPSec “Eroutes” have a default configuration that is applied if no specific route can be found. This is useful when, for instance, you wish to have a number of remote users connect via a secure channel (perhaps to access company financial information) but also still allow general remote access to other specific servers on your network.

Using the web page:

The default action for what to do when a packet is to be routed but no secure *Eroute* exists is specified on the **Configure ► IPSec Eroutes ► Default Eroute** page. The parameters are as follows:

No inbound SA action:

This parameter determines how the router will respond if a packet is received when there is no SA. If Drop Packet is selected then only packets that match a specified *Eroute* will be routed, all other data will be discarded. This has the effect of enforcing a secure connection to all devices behind the router.

If Pass Packet is selected then data that matches an *Eroute* definition will be decrypted and authenticated (depending on the *Eroute* options selected) but data that does not match will also be allowed to pass.

No outbound SA action:

This parameter determines how the router will respond if a packet is transmitted when there is no SA. If Drop Packet is selected then only packets that match a specified *Eroute* will be routed, all other data will be discarded. If Pass Packet is selected then data that matches an *Eroute* definition will be encrypted and authenticated (depending on the *Eroute* options selected) but data that does not match will also be allowed to pass.

Using text commands:

From the command line, use the **def_eroute** command to configure or display default *Eroute* settings.

To display current settings enter the command:

```
def_eroute <instance> ?
```

where <instance> is 0.

To change the value of a parameter use the command in the format:

```
def_eroute <instance> <parameter> <value>
```

where <instance> is 0.

The parameters and values are:

Parameter	Values	Equivalent web parameter
nosain	drop, pass	IP address of remote unit
nosaout	drop, pass	Use UDP header

4.24 Configure ► NUI Mappings

NUI mappings allow the user to configure the unit so that NUI strings received on incoming X.25 calls can be automatically mapped to the appropriate NUA's.

Using the web page:

To create a series of mappings fill in the NUI's in the left column of the table and the appropriate NUA in the right hand column.

Using text commands:

To configure NUI mappings from the command line use the **nuimap** command.

To display a current mapping enter the command:

```
nuimap <entry> ?
```

where <entry> is 0-19. For example, to display current mapping number 5 enter the command:

```
nuimap 5 ?
```

Two separate commands are needed to set up a mapping. These take the form:

```
nuimap <entry> NUI <NUI>
nuimap <entry> NUA <NUA>
```

where:

<entry> is the required entry number in the mapping table in each case

<NUA> is the X.25 NUA value

<NUI> is the X.25 NUI value.

For example:

```
nuimap 0 NUI my_host01
nuimap 0 NUA 23421234567890
```

4.25 Configure ► PPP

PPP is a standard protocol for transporting data from IP networks across point-to-point links and is essential for dial-up Internet access. As data is transferred across IP networks in synchronous format, your unit supports asynchronous to synchronous PPP conversion. This allows asynchronous terminals connected to the unit to communicate with remote synchronous PPP devices. Normally this is carried out using a single B-channel so that data can be transferred at speeds up to 64kbps.

note:

In order to use PPP your terminal must also support the PPP protocol (Windows dial-up networking supports PPP).

The unit also supports Multi-link PPP (MLPPP). MLPPP uses both ISDN B-channels simultaneously (and two PPP instances), to provide data transfer speeds up to 128Kbps for applications such as email transmission and retrieval, high speed internet access (your ISP must also support MLPPP) or establishing a high speed point to point connection between two Sarian units.

Using the web pages:

The **Configure ► PPP** folder contains a number of sub-folders and sub-pages for configuring variations aspects of PPP operation. These pages are described in the following sections.

4.25.1 Configure ► PPP ► MLPPP

Desired local ACCM:

For advanced users only - default value is 0x00000000.

Desired remote ACCM:

For advanced users only - default value is 0xffffffff.

Request remote CHAP authentication:

Set this parameter to Yes if it is required that the unit authenticate itself with the remote system using CHAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter should be set to No.

Password:

This is the password used for authenticating with the remote system when multi-link PPP is used. This password is used for both B-channel PPP connections.

Confirm password:

If altering the password, the new password must also be entered here. The unit will check that both fields are identical before changing the parameter value.

Short sequence numbers:

MLPPP data packet sequence numbers are usually stored in 16 bits. This parameter may be set to On to select 12-bit sequence numbers if necessary.

Username:

This is the user name for logging on to the remote system when multi-link PPP is used.

Connections parameters:

The parameters in this section are used to specify when the secondary ISDN B channel should be activated.

1B->2B rate (bytes/s)

This is the transfer rate (in bytes/sec) that will trigger the unit to activate the secondary B-channel. If this parameter is set to 0 the secondary B-channel will not be used. The default is 2000 bytes/s.

1B->2B delay (s)

This is the time (in seconds) for which the **1B->2B rate** must be sustained before the secondary B-channel is activated. If this parameter is set to 0, the secondary B-channel will not be used. The default is 10 seconds.

2B->1B rate (bytes/s)

This is the value (in bytes/sec) below which the data transfer rate must fall before the secondary B-channel will be deactivated. If this parameter is greater than the **1B->2B rate** then the secondary B-channel connection will not be dropped until the connection is terminated. The default is 1000 bytes/s.

2B->1B delay (s)

This is the time (in seconds) for which the transfer rate must fall below **2B->1B rate** before the secondary B-channel will be deactivated. The default is 60 seconds.

note:

The following four parameters are only available if you have purchased the AODI software option. To use AODI you will also have to enable the Always on mode parameter on the Configure>General page and

D->1B up rate (bytes/s)

When **Always on mode** is On, this is the value (in bytes/s) above which the data transfer rate must remain for **D->1B up delay (s)** before the unit will activate a B-channel

D->1B up delay (s)

When **Always on mode** is On, this is the time (in seconds) for which the data transfer rate must remain above the specified **D->1B rate** before the unit will activate a B-channel.

1B->D down rate (bytes/s)

When **AODI always on** is On, this is the value (in bytes/s) below which the data transfer rate must remain for **1B->1D down delay (s)** before the unit will deactivate the B-channel

1B->D down delay (s)

When **Always on mode** is On, this is the time (in seconds) for which the data transfer rate must remain below the specified **1B->D rate** before the unit will deactivate a B-channel.

Using text commands:

From the command line use the **mlppp** command to set or display MLPPP parameter settings. To display current settings for MLPPP enter the following command:

```
mlppp <instance> ?
```

where *<instance>* is currently always 0.

To set the value for a parameter enter the command in the format:

```
mlppp <instance> <parameter> <value>
```

For example:

```
mlppp 0 username fred
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
l_accm	hex number	Desired local ACCM
l_shortseq	on, off	Short sequence numbers
password	text	Password
r_chap	on, off	Request remote CHAP authentication
r_accm	hex number	Desired remote ACCM
username	text	Username
Connections parameters		
ddown_delay	number	1B->D down delay
ddown_rate	number	1B->D down rate
down_delay	number	2B->1B down delay
down_rate	number	2B-> 1B down rate
dup_delay	number	D->1B up delay
dup_rate	number	D->1B up rate
up_delay	number	1B -> 2B delay
up_rate	number	1B -> 2B rate

4.25.2 Configure ► PPP ► External Modems**Using the web-page:**

In circumstances where it is necessary to communicate with the router remotely via a normal analogue modem (perhaps because no ISDN line is available), this page may be used to set up the various parameters associated with controlling the modem.

ASY port

This parameter is used to specify the ASY port to which the external modem is connected. The default value is 255, which means that no external modem is available.

Modem init string n

Up to three initialisation strings may be defined which are issued in sequence to the modem each time a dial-out call is made.

Hang-up string

This parameter is used to define the hang-up string to be used when call is to be terminated (usually **ath**).

Using text commands:

From the command line, use the **modemcc** command to configure or display the DHCP server settings. To display current settings for the DHCP server enter the following command:

```
modemcc <instance> ?
```

where <instance> is 0. At present there can only be one **modemcc** instance i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
modemcc 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
asy_add	0-3, 255	ASY port
init_str	string	Modem init string 1
init_str1	string	Modem init string 2
init_str2	string	Modem init string 3
hang_str	string	Hang-up string

For example, to set the ASY port number to 1, enter:

```
modemcc 0 asy_add 1
```

4.25.3 Configure ► PPP ► QOS

The QOS (Quality Of Service) support now included on some models provides the means to prioritise different types of IP traffic. It is generally used to ensure that low priority applications do not “hog” the available bandwidth to the detriment of those with a higher priority. For example, this might mean that EPOS transactions carried over XOT will be prioritised at a higher level than HTTP type traffic used for Internet access. Without some form of QOS all IP packets are treated as being equal so there is no discrimination between applications.

The IP packet Type Of Service (TOS) field is used to indicate how a packet should be prioritised. Using the top 6 bits of the TOS field, a router that supports QOS will assign a DSCP (Differentiated Services Code Point) value to the packet. This may take place within the router when it receives the packet or another router closer to the packet source may have already assigned it. Based on the DSCP value, the router will assign the packet to a priority queue. There are currently four such queues for each PPP instance within Sarian 2000 series routers and each queue can be configured to behave in a particular way so that packets in that queue are prioritised for routing according to predefined rules.

There are two principle ways in which prioritisation may be effected:

A priority queue can be configured to allow packets to be routed at a specified data rate (providing that queues of higher priority are not already using the available bandwidth).

Weighted Random Early Dropping (WRED) of packets may be used as queues become busy in an attempt to get the TCP socket generating the packets to “back-off” it's transmit timers thus preventing the queue overflow (which would result in all subsequent packets being dropped).

QOS is a complex subject and can have a significant impact on the performance of your router. For detailed background information on QOS refer to RFC2474 (Definition of the Differential Services Field).

Basic operation.

In Sarian 2000 series routers the classification of incoming IP packets for the purposes of QOS takes place within the firewall. The firewall allows the system administrator to assign a DSCP value to a packet with any combination of source/destination IP address/port and protocol. Details on how this is done are given below in the chapter on Firewall scripts.

When the routing code within the unit receives an incoming packet, it directs it to the interface applicable to that packet at the time (this is the case whether or not QOS is being applied). Just before the packet is sent to the interface, the QOS code intercepts the packet, and assigns it to one of the available priority queues (currently 10 per PPP instance), based on it's DSCP value.

Each priority queue has a profile assigned to it. This profile specifies parameters such as the minimum transmit rate to attempt, maximum queue length, and WRED parameters.

The packet is then processed by the queue management code and either dropped, or placed in the queue for later transmission.

There are a number of configuration pages associated with QOS operation which are described in the following sections.

4.25.4 Configure ► PPP ► QOS ► DSCP Mappings

Each DSCP value must be mapped to a queue. These mappings are set-up using the **DSCP Mappings** configuration page. The **Default** parameter at the top of the page is used to set-up a default queue, which may be set to a value from **Q0** to **Q9**. Below this is a list of valid DSCP codes, each of which may also be set to a value from **Q0** to **Q9** or **Default**.

When you change the **Default** DSCP queue setting, any DSCP codes that are set to **Default** will have their queue number changed.

Using text commands:

From the command line, use the **dscp** command to configure or display the DSCP mappings. To display a DSCP mapping enter the following command:

```
dscp <code> ?
```

where <code> is a valid DSCP code from 0 to 63, or 64 (see note below).

To change the value of a parameter use the following command:

```
dscp <code> q <value>
```

where <code> is a valid DSCP code and <value> is 0 to 9.

To set the default mapping value enter the command:

```
dscp 64 q <value>
```

where <value> is the default queue number required between 0 and 9.

note:

The **dscp** value of 64 is actually an invalid code and is only used to set up the default priority.

4.25.5 Configure ► PPP ► QOS ► Q Profiles

You may define up to 12 distinct "queue profiles" that may then be assigned to the QOS queues as required. The queue profile determines how QOS queues with that profile assigned to them will behave.

Using the web page:

Each of the **Queue Profile** pages lists the following parameters:

Minimum Kbps:

This parameter is used to set the minimum data transfer rate in kilobits/sec that the unit will try to attain for this queue.

Maximum Kbps:

This parameter is used to set the maximum data transfer rate in kilobits/sec that the unit will try to attain for this queue. This means that if the unit determines that bandwidth is available to send more packets from a queue that has reached its **Minimum Kbps** setting, it will send more packets from that queue until the **Maximum Kbps** setting is reached.

Note that if you do not want this queue to provide more bandwidth than specified by the **Minimum Kbps** setting, this setting should be set to a value the same as or lower than the **Minimum Kbps** setting.

Maximum packet Q length:

This parameter specifies the maximum length of a queue (in terms of the number of packets in the queue). Any packets received that would cause the maximum length to be exceeded are dropped.

WRED minimum threshold:

This parameter specifies the minimum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value the WRED algorithm may cause packets to be dropped.

WRED maximum threshold:

This parameter specifies the maximum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value the WRED algorithm will cause all packets to be dropped.

WRED maximum drop probability (%)

This parameter is used to set the maximum % probability used by the WRED algorithm to determine whether or not a packet should be dropped when the queue length is approaching the **WRED maximum threshold** value.

note:

If the length of a queue is less than the **WRED minimum threshold** value, there is 0% chance that a packet will be dropped. When the queue length is between the WRED minimum and maximum values, the % chance of a packet being dropped increases linearly up to the **WRED maximum drop probability %**.

WRED Q length weight factor

This parameter specifies a weighting factor to be used in the WRED algorithm when calculating the weighted queue length. The weighted queue length is based upon the previous queue length and has a weighting factor that may be adjusted to provide different transmit characteristics. The actual formula used is:

$$\text{new_length} = (\text{old_length} * (1 - 1/2^{\text{wfact}})) + (\text{cur_length} * 1/2^{\text{wfact}})$$

Small weighting factor values result in a weighted queue length that moves quickly, and more closely matches the actual queue length. Larger weighting factor values result in a queue length that adjusts more slowly. If a weighted queue length moves too quickly (small

weighting factor), it may result in dropped packets if the transmit rate rises quickly, but will also recover quickly after the transmit rate dies off.

If a weighted queue length moves too slowly (large weighting factor), it will allow a burst of traffic through without dropping packets, but may result in dropped packets for some time after the actual transmit rate drops off.

The weighting factor used should therefore be selected carefully to suit the type of traffic using the queue.

Using text commands:

From the command line, use the **qprof** command to configure or display the queue profiles. To display a queue profile enter the following command:

```
qprof <instance> ?
```

where <instance> is the number of the queue profile to be displayed.

To change the value of a parameter use the following command:

```
qprof <instance> <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
maxkbps	number	Maximum Kbps
maxth	number	WRED Maximum Threshold
minkbps	number	Minimum Kbps
minth	number	WRED Minimum Threshold
mprob	0-100	WRED Maximum Drop Probability (%)
qlen	number	Maximum Packet Q Length
wfact	number	WRED Q Length Weight Factor

For example, to set the maximum throughput for queue profile 5 to 10kbps enter the command:

```
qprof 5 maxkbps 10
```

4.25.6 Configure ► PPP ► QOS ► QOS n

In addition to the QOS parameter on the PPP standard parameters page (which is used to enable QOS for that PPP instance), each PPP instance has 10 associated QOS queues into which packets may be placed when using QOS. Each of these queues must be assigned a queue profile (from the twelve available profiles) and a priority value.

Using the web page:

Each of the **PPP QOS** pages includes the **Link speed** parameter at the top followed by a list of queues with drop-down selection boxes that are used to assign a profile and a priority to each queue.

Link speed (Kbps):

This parameter should be set to the maximum data rate that this PPP link is capable of sustaining. It is used when calculating whether or not the data rate from a queue may exceed its **Minimum Kbps** setting (as determined by the profile assigned to it) and send at a higher rate (up to the **Maximum Kbps** setting).

Queue priorities

Below this heading is a list of the queues from 0 to 9 alongside each of which are drop down selection lists for assigning profile numbers (from 0 to 11) and queue priorities. The priority may be set to Very High, High, Medium, Low or Very Low.

Using text commands:

From the command line, use the **qos** command to assign profiles and priorities to each of the queues relating to a PPP instance. To display a list of the profiles assigned to the queues belonging to a QOS instance, enter the following command:

```
qos <instance> ?
```

To assign a profile to a queue for a QOS instance, use the command in the format:

```
qos <instance> parameter <value>
```

where <instance> is the QOS instance number. The parameters and values are:

Parameter	Values	Equivalent web parameter
linkkbps	number	Link speed (Kbps)
q0prof	0-11	Queue 0 Profile
q0prio	0-4	Queue 0 Priority
q1prof	0-11	Queue 1 Profile
q1prio	0-4	Queue 1 Priority
q2prof	0-11	Queue 2 Profile
q2prio	0-4	Queue 2 Priority
q3prof	0-11	Queue 3 Profile
q3prio	0-4	Queue 3 Priority
q4prof	0-11	Queue 4 Profile
q4prio	0-4	Queue 4 Priority
q5prof	0-11	Queue 5 Profile
q5prio	0-4	Queue 5 Priority
q6prof	0-11	Queue 6 Profile
q6prio	0-4	Queue 6 Priority
q7prof	0-11	Queue 7 Profile
q7prio	0-4	Queue 7 Priority
q8prof	0-11	Queue 8 Profile
q8prio	0-4	Queue 8 Priority
q9prof	0-11	Queue 9 Profile
q9prio	0-4	Queue 9 Priority

The queue priority values are mapped as follows:

Value	Priority
0	Very High
1	High
2	Medium
3	Low
4	Very Low

4.25.7 Configure ► PPP ► Sub-Configs

These pages must be used in conjunction with the **Configure ► IPRoutes** pages. Sub-configurations can be used as an alternative to using an entire PPP instance if only a few

parameter changes from an existing ppp instance are required. (This saves on memory usage in the unit.)

If the normal route for a particular sub-net is down, the alternate route (with a higher metric) may specify that the same ppp instance is used but with a different sub configuration. The sub configuration may contain an alternative phone number for example. Currently, the only parameter that can be used in a sub configuration is the phone number but other parameters may be included in the future.

Using text commands:

From the command line, use the **pppcfg** command to set or display PPP sub-configurations. To display current settings for a given sub-configuration enter the following command:

```
pppcfg <instance> ?
```

where <instance> is between 1 and 10.

To set the value for a parameter enter the command in the format:

```
pppcfg <1...10> <parameter> <value>
```

For example:

```
pppcfg 1 phonenum 08457654321
```

Phonenum is currently the only parameter.

4.25.8 Configure ► PPP ► PPP n ► Standard

The following parameters are those that you are most likely to need to customise PPP for your application. More advanced settings are covered in the next section.

IP analysis:

This parameter is used to include or exclude IP data from this PPP instance from the analyser trace and is equivalent to checking or un-checking the equivalent IP sources checkbox on the **Configure ► Analyser** page.

PPP analysis:

This parameter is used to include or exclude PPP data from this PPP instance from the analyser trace and is equivalent to checking or un-checking the equivalent IP sources checkbox on the **Configure ► Analyser** page.

Answering:

If the PPP **Answering** parameter is On, the unit will answer incoming calls on the relevant PPP channel. To prevent the unit from answering incoming calls on this PPP channel set the option to Off. If PPP **Answering** is set to Callin, the unit requires the remote peer authenticate itself, *but only if the remote peer has dialled in*.

Calling number:

This parameter is used to restrict the range of numbers from which PPP will answer incoming calls i.e. PPP will only answer a call if the trailing digits of the calling number match what is specified by this parameter. For example, if **Calling Number** was set to **3**, incoming calls from 1234563 would be answered but calls from 1234567 would not.

MSN:

If PPP Answering is Off this parameter is not used.

This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with PPP **Answering** On it will cause the unit to answer incoming calls to only telephone numbers where the trailing digits match the value selected. For example setting MSN to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

Sub-address:

If PPP Answering is Off this parameter is not used.

The **Sub-address** parameter provides the filter for the ISDN sub-address facility. It is blank by default but when set to an appropriate value with PPP **Answering** On it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the **Sub-address** value. For example setting the **Sub-address** parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

Remote management:

When set to Enabled, the **Remote Management** parameter allows other users on this **PPP** instance (i.e. the LAN to which the **PPP** instance is connected), to access the unit's Telnet, FTP and Web services for the purpose of managing the unit. To prevent users from this type of access, set the parameter to Disabled.

Dial-out prefix:

When making outgoing PPP calls, the value specified by the **Dial-out Prefix** parameter is inserted at the start of the actual number being called. This is normally used to access an outside line. For example, when using AODI or BACP, the remote peer may provide a number to be used for raising an additional B-channel to increase bandwidth. However, such a number will not normally include the digits needed to connect to an outside line via a PABX.

Dial-out number:

To allow the unit to automatically make outgoing PPP calls you must enter the ISDN number of your Internet Service Provider (ISP) in the **Dial-out Number** field. The Event Log, in conjunction with the SMTP client, uses this feature to send email messages.

Use GPRS/external modem:

On models fitted with a GPRS module the PPP instance can be configured to use either GPRS or an external modem (connected via one of the ASY ports).

Username:

This is the username that should be used when authenticating with the remote system and is usually only required for outgoing PPP calls.

Password:

This is the password that should be used when authenticating with the remote system and is usually only required for outgoing PPP calls.

Confirm password:

If altering the password, the new password must also be entered here. The unit will check that both fields are identical before changing the parameter value.

AODI NUA:

This parameter is used to specify the NUA (Network User Address) required to connect to your AODI (Always On Dynamic ISDN) access service provider and is only available if you have purchased the AODI software option.

Always on mode:

This parameter is used to configure the PPP instance so that in the event that it is disconnected the unit will try to re-connect again after approximately 10 seconds. It should be set to On when using AODI or when using GPRS.

DNS server:

This field should be used to enter the address of the DNS server that should be used to resolve IP addresses. If this field is left blank, PPP will attempt to negotiate this address during the network negotiation phase.

Multi-link:

This configures the PPP instance to operate in multi-link mode (MLPPP).

Inactivity timeout (s):

PPP will close the connection if the link is inactive for the length of time specified by this parameter (in seconds).

Minimum link up-time (s):

If this parameter is set to a non-zero value, then PPP will not close the connection for the specified period (in seconds), even if the link is inactive.

Firewall:

The Firewall parameter is used to turn Firewall script processing On or Off for this interface.

IGMP:

This **IGMP** parameter is used to enable or disable the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

IPSec:

The IPSec parameter is used to enable or disable IPSec processing on this interface. If set to On, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.

GRE:

This parameter enables GRE (Generic Routing Encapsulation) for this **ppp** instance. GRE is a simple tunnelling protocol. For further details refer to RFC2784.

RIP version:

RIP (Routing Information Protocol), is used by routers to determine the best route to any destination. There are several different versions that can be enabled or disabled using this parameter. When **RIP Version** is set to Off, RIP is disabled and no RIP packets transmitted out this interface. When **RIP Version** is set to V1 or V2, the unit will transmit RIP version 1 or 2 packets respectively (version 2 packets are sent to the "ALL ROUTERS" multicast address. (224.0.0.9). When RIP Version is set to V1 Compat, the unit will transmit RIP version 2 packets to the subnet broadcast address. This allows V1 capable routers to act upon these packets.

When RIP is enabled, RIP packets are transmitted when the eth instance first becomes active, and at intervals specified by the **RIP Interval** parameter on the **Configure ► General** page.

RIP destination IP:

RIP packets are normally sent out on a broadcast basis or to a multi-cast address. This parameter may be used to force RIP packets to be sent to a specified IP address. It is particularly useful if you need to route the packets via a VPN tunnel.

Time band:

This parameter specifies the **Time Band** number to use for this PPP instance. See **Configure ► Time Bands**.

Log event up-time (mins):

The unit logs the amount of time that a PPP instance remains connected during each 24-hour period (continuously or otherwise). This parameter may be used to specify the length of time in minutes that the instance may remain connected before the unit generates an eventlog entry.

Local IP address:

This is the IP address of the unit. When making outgoing PPP connections, this field is generally left blank, and the remote end of the connection will supply the IP address. If receiving incoming calls, set this field to the desired IP address for the unit.

Remote IP address pool minimum:

PPP has a list of IP addresses to supply to incoming connections. This is the first address supplied to the incoming caller. The **Request IPCP remote address option** parameter should also be set. This parameter may require alteration if the default value "10.10.10.0" does not suit the remote network configuration.

Remote IP address pool range:

This specifies the range of IP addresses that the PPP instance can provide to the remote unit. This will only be required if the **Remote IP address pool minimum** IP address is already in use. For example, if **Remote IP pool minimum parameter** is set to 10.10.10.1 and the **Remote IP address Pool range** is set to 9, this PPP instance would be authorised to assign IP address in the range of 10.10.10.1 to 10.10.10.10. In practice, 10.10.10.1 would always be assigned unless it is in use by another PPP instance.

Remote network address:

This specifies the unit's IP network address. This is only used when the network address is not remotely assigned.

Remote network mask:

This specifies the IP netmask for the **Remote network address** parameter (see above).

NAT:

This parameter enables or disables IP Network Address Translation (NAT). NAT allows a number of users to share a single server-assigned IP address. From the wide area network side of the unit, all inbound and outbound IP traffic appears to originate from this one IP address.

NAT source IP address:

If specified, and **NAT** is On for this interface, then the source address of packets being sent out this interface is changed to this address, rather than the interface address.

Using text commands:

From the command line, use the PPP command to set or display PPP parameter settings. To display current settings for a PPP instance enter the following command:

```
ppp <instance> ?
```

To set the value for a parameter enter the command in the format:

```
ppp <instance> <parameter> <value>
```

For example:

```
ppp 0 ans 1
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
ans	0 (off), 1 (on), 2 (callin)	Answering
aodion	on, off	AODI mode
aodinua	number	AODI NUA
cingnb	phone number	Calling number
dnserver	IP address	DNS server
do_nat	on, off	NAT
firewall	on, off	Firewall
gre	on, off	GRE
igmp	on, off	IGMP
ipaddr	IP address	Local IP address
ipmin	IP address	Remote IP address pool minimum
iprange	number	Remote IP address pool range
ipsec	on, off	IPSec
mask	IP address mask	Remote network mask
minup	number	Minimum link up-time (s)
msn	number	MSN
multilink	on, off	Multi-link
hrtbeatint	number	Heartbeat interval (s)
hrtbeatip	IP address	Heartbeat destination IP address
natip	IP address	NAT source IP address
netip	IP address	Remote network address
nocfg	on, off	Remote management
password	text	Password
phonenum	phone number	Dial-out number
prefix	number	Dial-out prefix
rip	0 (off), 1 (V1), 2 (V2), 3 (V1 compat)	RIP version
ripip	IP address	RIP destination IP
sub	number	Sub-address
tband	0-3	Time band
timeout	number	Inactivity timeout
uplogmins	number	Log event up-time (mins)
username	text	Username

4.25.9 Configure ► PPP ► PPP n ► Advanced

The parameters listed in the following table are unlikely to require alteration. They are initial values used during negotiation of the PPP link and will be acceptable for most applications. You should not alter these values unless you are familiar with the operation of the PPP protocol.

Parameter	Default value
Desired Local ACCM	0x00000000
Desired Local MRU	1500
Desired Remote ACCM	0xFFFFFFFF
Desired Remote MRU	1500
Request Local ACFC	yes
Request Local Compression	yes
Request Local PFC	yes
Request Remote ACFC	no
Request Remote Compression	no
Request Remote PFC	no

DNS server port:

This parameter specifies the TCP port the unit will use to access the DNS server specified in the **DNS server** PPP Standard Parameter. The default value for this parameter is 53.

Request BACP:

Set this parameter if you wish the unit to use BACP (Bandwidth Allocation and Control Protocol) to determine the ISDN number to dial for the second or third multi-link connection.

Request callback:

Set this parameter to Yes if you wish the unit to request a call back when it dials into another Sarian unit. Note that the answering PPP instance of the remote unit must also be configured with the phone number of the calling unit and a suitable username and password.

Allow remote to request callback:

This parameter when set to Yes this parameter allows the unit to respond to incoming callback requests.

Request IPCP local address option:

Set this parameter if you wish the unit to negotiate its IP address. This parameter should normally be set to Yes.

Request local PAP authentication:

Set this parameter for connections where the remote system should use the PAP authentication procedure before allowing a connection to be made. Generally, this parameter is set for incoming connections, and cleared for outgoing connections.

Request local CHAP authentication:

Set this parameter for connections where the remote system should use the CHAP authentication procedure before allowing a connection to be made. Generally, this parameter is set for incoming connections, and cleared for outgoing connections.

Request local compression:

Setting this parameter to On causes the unit to request the use of VJ Header Compression, which compresses TCP/IP headers to about 3 bytes rather than the standard 40 bytes. It is generally only used to improve efficiency on slow speed links such as GPRS.

Request local PFC:

Setting this parameter to On causes the unit to request Protocol Field Compression, which compresses PPP protocol fields from 2 to 1 bytes.

Request remote ACFC:

Setting this parameter to On causes the unit to get the remote to request Address Control Field Compression. When negotiated, the address/control fields are removed from the start of the PPP header.

Request IPCP remote address option:

Set this parameter if it is required that the remote system have an address supplied. An attempt to negotiate an IP address from the IP address pool will be made. Generally, this parameter is set for incoming connections, and cleared for outgoing connections.

Request remote PAP authentication:

Set this parameter if it is required that the unit authenticate itself with the remote system using PAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter should be off.

Request remote CHAP authentication:

Set this parameter to Yes if it is required that the unit authenticate itself with the remote system using CHAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter should be set to No.

Request remote compression:

Setting this parameter to On causes the unit to get the remote to request the use of VJ compression.

Request remote PFC:

Setting this parameter to On causes the unit to get the remote to request Protocol Field Compression.

LCP echo request interval (s):

Setting this parameter to a non-zero value causes PPP to issue Link Control Protocol (LCP) Echo Request packets to the remote peer at the specified intervals. This would be used to keep a link active, for example when using GPRS.

PING Request interval (s)

If this parameter is set to a non-zero value the unit will generate a "ping" (ICMP echo request) to the address specified by the **PING IP address** parameter (generally for debug/test purposes). Setting the value to 0 disables the ping facility.

PING IP address

This parameter specifies the address to which ICMP echo requests will be sent if the **PING request interval** is greater than 0.

No PING response deact delay (s)

This parameter is primarily used where IP traffic is being carried over a GPRS network. It specifies an amount of time after which if no response has been received to three pings, the unit will deactivate the interface in an attempt to re-establish communications.

Use ETH0 for PING source IP:

Setting this parameter to Yes causes the unit to use the IP address of ETH0 (instead of the current IP address of the PPP interface), as the source address for the auto PING packets.

Heartbeat interval (s):

If this parameter is set to a non-zero value, the unit will transmit “heartbeat” packets at the interval specified. Heartbeat packets are UDP packets that contain status information about the unit that may be used for diagnostic purposes.

Heartbeat destination:

This parameter specifies the destination IP address for heartbeat packets.

Layer 1 interface:

This parameter can be set to Default, Port or Eth and determines whether PPP frames are carried over ISDN, X.25 call, local DUN (Default option) or over one of the serial ports operating in synchronous mode (Port option) or over an Ethernet interface (Eth option).

Layer 1 interface #:

When the layer 1 interface is set to Port, then this field specifies which synchronous port to use.

Data limit warning level (kb):

On GPRS networks (where charging is based on the amount of data transferred as opposed to time spent on-line), this parameter may be used to specify a data limit after which the unit will create an entry in the event log to indicate that this amount of data has been transferred. For example, if your monthly tariff includes up to 5Mb of data before you are charged an “excess”, you might set the **Data limit warning level** to 4000. This would cause the unit to place a warning entry in the event log once you had transferred 4Mb.

Data limit stop level (kb):

This parameter is used to set the maximum amount of data that may be transferred before the unit will “lock” the interface and prevent further transfer. As with the **Data Limit Warning Level** parameter it is used on networks where the tariff is based on the amount of data transferred to help prevent excess charges being incurred.

Once the interface has been locked, it may be unlocked manually by clicking on the **Clear Total Data Transferred** button on the appropriate **Statistics ► PPP** page or automatically at the start of the next billing period by setting the **Data Limit Reset Day of Month** appropriately.

Data limit reset day of month:

If you wish to automatically unlock a locked interface at the start of a new billing period, this parameter should be set to the appropriate day of the month (from 1 to 28). When this date is reached the unit will unlock the interface and data transfer may resume. If the parameter is set to 0, automatic unlocking will not occur and manual unlocking will be necessary (by clicking on the **Clear Total Data Transferred** button on the appropriate **Statistics ► PPP** page.

Using text commands:

From the command line the advanced PPP parameters are set using the same **ppp** command as for the standard parameters. The advanced parameters and values are:

Parameter	Values	Equivalent web parameter
dnsport	number	DNS server port
echo	number	LCP echo request interval (s)
l_accm	hex number	Desired local ACCM
l_acfc	on, off	Request local ACFC
l_addr	on, off	Request IPCP local address option

l_bacp	phone number	Request BACP
l_callb	on, off	Request call-back
l_chap	on, off	Request local CHAP authentication
l_comp	on, off	Request local compression
l_mru		Desired local MRU
l_pap	on, off	Request local PAP authentication
l_pfc	on, off	Request local PFC
l1iface	0 (default), 1 (port), 2 (eth)	Layer 1 interface
l1nb	number	Layer 1 interface #
pinfreth0	on, off	Use ETH0 for PING source IP
ping_deact	number	No PING response deact delay (s)
pingint	number	PING request interval (s)
pingip	IP address	PING IP address
r_accm	hex number	Desired remote ACCM
r_acfc	on, off	Request remote ACFC
r_addr	on, off	Request IPCP remote address option
r_callb	on, off	Allow remote to request call-back
r_chap	on, off	Request remote CHAP authentication
r_comp	on, off	Request remote compression
r_mru		Desired remote MRU
r_pap	on, off	Request remote PAP authentication
r_pfc	on, off	Request remote PFC

4.25.10 Configure ► PPP ► PPP n ► PPP/IP over X.25

The Sarian 2000 series can optionally support transmission of TCP/IP packets encapsulated in X.25. This feature allows the ISDN D-channel to be used as an “always on” connection providing a permanent, low speed Internet Protocol pipe between two Local Area Networks.

These parameters are used when configuring PPP or IP over X.25. The parameters are as follows:

Calling NUA:

This specifies the calling X.25 address to be used when using PPP or IP over X.25.

Default packet size:

This specifies the default X.25 packet size to use.

IP over X25 mode:

When set to On, this causes the unit to route IP data over X.25. Otherwise, PPP over X.25 is used.

Layer 2 interface:

This parameter is used to select whether the PPP instance will use B or D-channel X.25. If None is specified, then PPP/IP over X.25 mode is disabled.

Layer 2 interface #:

This parameter specifies which LAPB or LAPD instance to use for the relevant PPP instance.

LCN:

The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

LCN direction:

This parameter determines whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is Down and LCNs are decremented i.e. if the first CALL uses 1024, the next will use 1023 etc. Setting the parameter to Up will cause the LCN to be incremented from the start value.

Restart delay (ms):

When the **Restarts** parameter is set to On the value specified in the **Restart delay** dialog box determines the length of time in milliseconds that the unit will wait before issuing a Restart packet. The default value is 2000 giving a delay of 2 seconds.

Restarts:

It is normally possible to make X.28 CALLs immediately following the initial SABM, UA exchange. In some cases however, the X.25 network may require an X.25 RESTART before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe.

The default value is On. This means that the unit will issue X.25 RESTART packets. To prevent the unit from issuing RESTART packets set this parameter to Off.

Backup X25 Interface parameters:

These parameters are used to specify details of a backup interface to be used if the link layer interface used by PPP is lost. The parameters are as follows:

Calling NUA:

This specifies the calling X.25 address to be used when making outgoing X.25 calls on the backup interface.

Called number:

This specifies the X.25 call string to be used to make outgoing calls on the backup interface.

Layer 2 interface:

This specifies which layer 2 interface (LAPB or LAPD) is to be used.

Layer 2 interface #:

This parameter specifies which LAPB or LAPD instance to use for the relevant PPP instance.

LCN:

The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

LCN direction:

This parameter determines whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is DOWN and LCNs are decremented i.e. if the first CALL uses 1024, the next will use 1023 etc. Setting the parameter to UP will cause the LCN to be incremented from the start value.

Using text commands:

From the command line the PPP over X25 parameters are set using the same **ppp** command as for the standard parameters. The PPP over X25 parameters and values are:

Parameter	Values	Equivalent web parameter
cingnua		Calling NUA
defpack		Default packet size
dorest	on, off	Restarts
ipmode	on, off	IP over X.25 mode
l2iface		Layer 2 interface
l2nb		Layer 2 interface #
lcn	number	LCN
lcnup		LCN direction
restdel		Restart delay (s)
Backup X25 Interface parameters		
bakcingnua		Calling NUA
bakl2iface		Layer 2 interface
bakl2nb		Layer 2 interface #
baklcn		LCN
baklcnup		LCN direction
baknum		Called number

4.26 Configure ► Protocol Bindings

Sarian 2000 series products are soft configurable to allow different protocols to be used on different ports. The process of selecting which protocol will be used on which port is referred to as “binding”.

Using the web page:

The **Configure ► Protocol Bindings** page allows you to define which protocols will be used on each of the ASY ports.

For example, you may wish to use ASY 0 for a B-channel X.25 application. In this case, you would need to bind **ASY0** to an X.25 PAD, say **PAD0**. You would then associate the PAD with a LAPB instance using the appropriate **Configure ► X.25 PAD** page.

By default, if no specific protocol has been bound to an ASY port the unit will automatically associate a PPP instance with that port i.e. PPP is treated as the default protocol.

To change a binding or add a new one, select the required protocol from the drop down list on the left and select the correct ASY port or REM from the list on the right. Once you have selected the appropriate values click the **Add** button. Each time you do this the new binding will appear in the list at the top of the page along with a **Remove** button. Clicking the **Remove** button will remove the binding and re-associate PPP with the appropriate port.

If you add a binding to an ASY port that already has a binding, the new binding will replace the old one.

The REM option listed with the ASY ports is the name for the Remote virtual ASY port. This port may be used to allow a remote X.25 or V.120 user to take control of the unit for management purposes.

Using text commands:

To display a list of current bindings from the command line enter the command:

```
bind ?
```

To bind protocols to ports via the command line, use the **bind** command in the format:

```
bind <protocol> <instance> <asy <number>|rem>
```

For example, to assign the PAD 0 to ASY 1 you would enter:


```
bind pad 0 asy 1
```

To use the unit in V.120 mode you would use the **bind** command to bind a V.120 instance to the required serial port. For example:

```
bind v120 0 asy 0
```

Similarly, to access the internet using PPP via a terminal connected to ASY 2 you would enter the command:

```
bind ppp 1 asy 2
```

4.27 **Configure ► SMS Edit**

Sarian 2000 series models with GPRS capability such as the GR2130, are capable of sending SMS alarms and messages. The SMS related parameters on the **Configure ► Event Handler** and **Configure ► GPRS module** pages are used to configure the unit to send such alarms but the **SMS Edit** page allows you to edit and send an SMS message manually.

Using the web page:

The **Configure ► SMS Edit** page contains two text boxes and two buttons which operate as follows:

To:

The **To** text box is used to enter the destination number for the SMS message.

Message:

Enter the message text that you want to send in the **Message** text box.

Send:

Click on the **Send** button to transmit the message.

Cancel:

Click on the **Cancel** button to clear the message

Using text commands:

There is no text command equivalent of the **SMS Edit** page.

4.28 **Configure ► SMTP**

The Simple Mail Transfer Protocol (SMTP) is widely used for the transmission of electronic mail. The unit incorporates a software module known as an SMTP Client. This sends emails by establishing a connection to a remote computer that is running an SMTP server and then transmits emails using the SMTP protocol.

Using the web page:

The **Configure ► SMTP** page allows you to set up the parameters for the SMTP (Simple Mail Transfer Protocol) client. This is used by the Event Logger when it has been configured to automatically generate email messages for events of a specified priority or higher.

Default reply address:

This address will be inserted into the email header if it is found that no reply address exists in the appropriate email template. If the email template contains an address in the **Reply to:** field it will override the Default Reply Address.

Interface:

The **Interface** field is used to specify the type of interface to use. Either PPP or Ethernet may be selected.

Interface #:

The **Interface #** field is used to specify which instance of PPP to use for SMTP (normally PPP1).

Mail from address:

This parameter specifies the text to be inserted between the MAIL FROM braces command issued to the SMTP server. Most SMTP servers will accept an empty string, but some require that an address should be entered in this field. Consult your SMTP service provider for information on whether it is necessary to enter an address in this field.

Retry delay (s):

If the first attempt at sending an automatic email fails then the unit will wait the specified amount of time (in seconds) before making another attempt. If this parameter is set to 0 then the unit will not make any further attempts to transmit the email.

Server address:

In order to allow the unit to send email messages, you will need to insert the address of your SMTP mail server for outgoing mail into the **Server Address** field e.g. **smtp.myisp.co.uk**. You will also need to use the **Configure ► PPP** pages to set the PPP dialout number to the correct number for your ISP.

Server port:

This is the TCP port number that the SMTP server listens on. It should not normally be necessary to change the default value of 25.

Using text commands:

From the command line, use the **smtp** command to configure or display SMTP settings. To display current settings for an SMTP instance enter the following command:

```
SMTP <instance> ?
```

where <instance> is 0. At present there can only be one instance of SMTP i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
smtp 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
ll_add	0,1	Interface #
ll_ent	PPP	Interface
mail_from	email address	Mail From address
port	number	Server port
reply_to	email address	Default reply address
retry_dly	number	Email retry delay
server	text	Server address

For example, to set the server address to **smtp.myisp.net.uk**, enter:

```
smtp 0 server smtp.myisp.net.uk
```

4.29 Configure ► SNTP

The unit supports the Simple Network Time Protocol (SNTP). This protocol is used to synchronise the unit's internal clock with the time and date information provided by a remote computer. The remote computer must be running an SNTP server in order to obtain this information.

Using the web page:

The **Configure ► SNTP** page allows you to set up the parameters for the SNTP (Simple Network Time Protocol) client. The SNTP client can be used to update the unit's real time clock when it is configured to connect to the Internet (or a private IP network with an NTP server).

NTP server:

This is the IP address or host name of the NTP server you wish to use.

Interval (hrs):

This is the interval (in hours) at which the SNTP client will attempt to update the real time clock.

Offset from GMT (hrs):

This parameter should be set to + or – the number of hours the unit's time should be ahead or behind Greenwich Mean Time.

Check on power-up:

Specifies whether the unit will attempt to connect to the NTP server every time the unit is booted.

Using text commands:

From the command line, use the **sntp** command to configure or display SNTP settings. To display current settings for an SNTP instance enter the following command:

```
sntp <instance> ?
```

where <instance> is 0. At present there can only be one instance of SNTP i.e. 0, but the instance parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
sntp 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
interval	0-1000	Interval (hrs)
offset	-12 - 13	Offset from GMT (hrs)
pwrchk	yes, no	Check on power-up
server	text	NTP server

For example, to set the server address to **ntp.myisp.net.uk**, enter:

```
sntp 0 server ntp.myisp.net.uk
```

4.30 Configure ► Static NAT Mappings

The unit supports Network Address Translation (NAT), which may be enabled on a particular interface such as a PPP instance. When operating with NAT enabled, this interface has a single externally visible IP address. When sending IP packets, the local IP addresses (for example on a local area network) are replaced by the single IP address of the interface. The unit keeps track of the local IP addresses and port numbers so that if a matching reply packet is received it is directed to the correct local IP address. With only one externally visible IP address, NAT effectively prevents external computers from addressing specific local hosts, thus providing a form of “firewall” security.

Static NAT mappings allow received packets destined for particular ports to be directed to specific local IP addresses. For example if you wanted to run a server on a local area network and make it externally accessible you would need to set up a static NAT mapping using the local IP address of the server and the port number used to access the required service.

Using the web page:

The **Configure ► Static NAT Mappings** page displays a table that allows you to set the following values for each mapping:

Min Port

This parameter is used to specify the lowest port number to be re-directed.

Max Port

This parameter is used to specify the highest port number to be re-directed.

Map to IP address

Enter an IP address to which packets containing the specified destination port number are to be redirected.

Using text commands:

From the command line use the **nat** command to configure settings for the static NAT mappings.

To display current settings for a particular mapping enter the command:

```
nat <entry> ?
```

This lists the port number and the mapped IP address.

To change the value of a parameter use the command in the format:

```
nat <entry> <parameter> <value>
```

where *<entry>* is 0-5, corresponding to the table entry number.

The parameters and values are:

Parameter	Values	Equivalent web parameter
ipaddr	IP address	Map to IP address
minport	number	Minimum port number
maxport	number	Maximum port number
port	0 – 65535	Port number

For example, to set the IP address for entry 0 in the table to 10.1.2.10 enter the command:

```
nat 0 ipaddr 10.1.2.10
```

4.31 Configure ► SYNC Ports

The DTE ports on your unit will usually be configured for asynchronous operation. This is the most common mode of serial communication. However, some applications will require synchronous serial communications using a protocol such as HDLC. This section describes the various parameters that may require setting up correctly for such an application.

note:

The number of synchronous serial ports available will vary depending on the model you have purchased. Check the model specification to determine how many, if any, are fitted.

Using the web page:

The **Configure ► SYNC Ports** page allows you to set up the parameters that control the operation of one or more serial ports when used in synchronous mode. To enable synchronous mode, a protocol such as LAPB must be configured to use a synchronous port as its lower layer interface. The parameters for a synchronous port are described below:

Clock source:

This specifies whether the clock is provided by the unit (Internal) or by the device connected to the unit (External).

Speed:

If **Clock Source** is **Internal**, this specifies the clock speed (in Hz) to be used on the synchronous interface. Otherwise, this parameter is ignored.

Mode:

This specifies the type of physical interface to be used. Currently only RS232 mode may be specified.

Duplex:

This parameter specifies whether the synchronous interface is to operate in full or half duplex mode. This should normally be set to full duplex (the default).

Invert RX clock:

This parameter specifies whether or not an inverted clock should be used for receive data. This should normally be Off.

Invert TX clock:

This parameter specifies whether or not an inverted clock should be used for transmit data. This should normally be Off.

Using text commands:

From the command line, use the **sy** command to configure or display SYNC port settings. To display current settings for a SYNC port enter the following command:

```
sy <port> ?
```

At present there is only one SYNC port, i.e. 0, but the port parameter has been included to allow for future expansion.

To change the value of a parameter use the following command:

```
sy 0 <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
clksrc	int/ext	Clock source
duplex	full/half	Duplex
mode	rs232	Mode
rxclkinv	on, off	Invert RX clock
speed	numeric	Speed
txclkinv	on, off	Invert TX clock

For example, to set the synchronous port speed to 64000 bits/sec, enter:

4.32 Configure ► Time

The unit incorporates a battery-backed real-time clock/calendar. This is used for time/date stamping internal files and statistics. Normally, once the time and date has been set, the unit will keep the time accurate to +/- 5 seconds/day while power is applied. However you may also configure it to automatically obtain the correct time at regular intervals using the SNTP option.

Using the web page:

This page allows you to set the date and time by filling in the appropriate dialog boxes.

Using text commands:

To set the time and date from the command line use the **time** command.

To display the time/date as currently set on the unit, enter the command without a parameter:

```
Time
12:23:58, 10 Mar 2000
OK
```

To set the time/date, enter the command in the format:

```
time <hh> <mm> <ss> <dd> <mm> <yyyy>
```

The 24-hour clock system is used. For example:

```
time 22 16 00 12 03 2002
22:16:00, 12 Mar 2002
OK
```

will set the time/date to 10:16pm on 12th March 2002.

4.33 Configure ► Time Bands

2000 series routers support “time bands” which are used to determine periods of time during which routing is allowed or prevented. For example, an office router could be configured so routing is only allowed on weekdays. At present, time bands may only be applied to PPP instances.

Time Bands are specified by a series of “transition” times. At each of these times routing is either enabled or disabled. The default state for a Time Band is On which means that PPP instances that are associated with un-configured Time Bands will operate normally.

note:

An entry is made in the Event Log whenever a Time Band transition occurs.

Using the web page:

There are four **Time Band** instances and each page contains a table that allows you to enter up to ten "transition" times.

Days of the week are entered in the format "Mon", "Tue", "Wed", "Thu", "Fri", "Sat" and "Sun". To specify multiple days, separate them by a comma. Alternatively, the working days from Monday to Friday inclusive may be entered as "MF". Similarly, the entire week may be specified as "ALL".

Times of the day are specified as hours and minutes in 24-hour clock format. Valid formats are:

H
 HH
 H:M
 H:MM
 HH:M
 HH:MM

For example, to set up the router to allow PPP routing only on weekdays between 9:00am and 5:30pm you would set up the table for **Time Band 0** as follows:

Days	Transition Time	State
MF	9:00	On
MF	17:30	Off

Now, at 9:00am on weekdays the state is switched to **On** so that routing is allowed on that **Time Band** during the day. At 5:30 each evening the state is set to **Off** and routing is disabled until 9:00am the following morning (or the following Monday morning after a Friday).

To activate this **Time Band** for a PPP instance you must now set **Time band** parameter for that instance to the appropriate value in the **Configure ► PPP (Standard parameters)** web page.

Using text commands:

To set the time and date from the command line use the **tband** command.

To display current time band settings, enter the command in the format:

```
TBAND <instance> ?
```

To set-up a transition you will need to enter three commands (one each to specify the days of the week, the time and the transition state):

```
tband <instance> <days#> <days>
tband <instance> <time#> <time>
tband <instance> <state#> <on|off>
```

Where:

<instance> is the Time Band instance number
<day#> is the day entry number
<time#> is the time entry number
<state#> is the state entry number
<days> specifies the days on which the transition occurs
<time> specifies the time at which the transition occurs
<state> specifies the type of transition (**on** or **off**)

Valid days of the week are "Mon", "Tue", "Wed", "Thu", "Fri", "Sat" and "Sun". To specify multiple days, separate them by a comma. Alternatively, the working days from Monday to Friday inclusive may be entered as "MF". Similarly, the entire week may be specified as "ALL".

Times of the day are specified as hours and minutes in 24-hour clock format. Valid formats are:

H
 HH
 H:M
 H:MM
 HH:M
 HH:MM

For example, to set up the router to allow PPP routing only on weekdays between 9:00am and 5:30pm you would enter the following commands:

```
tband 0 days0 mf
tband 0 time0 9
tband 0 state0 on
tband 0 days1 mf
tband 0 time1 5:30
tband 0 state1 off
```

4.34 Configure ► TPAD

TPAD is a simplified version of X.25 PAD that is commonly used for carrying out credit-card clearance transactions. Your unit supports the use of TPAD over the ISDN B and D-channels with automatic fall-back from one to the other in the event of service failure.

Using the web-page:

The **Configure ► TPAD** option expands to list separate pages for each of the available TPAD instances. Each page is split into two sections. The first section includes general TPAD parameters (many of which are common to X.25). The second includes parameters relating to the backup interface.

General parameters:

B-channel #:

This parameter may be used to specify an ISDN number. This is used in cases where no ISDN number is provided with the **atd** command when making an outgoing call.

Prefix #:

This parameter is used to specify a dialling code that the unit will place in front of the telephone number that is issued by the terminal in the **atd** command. For example, if the **Prefix #** was set to 0808 and the number specified by the terminal in the **atd** command was 111222, the actual number dialled by the unit would be 0808111222.

Prefix removal #:

This parameter is used to specify a dialling prefix that is normally inserted by the terminal in the **atd** command that is removed by the unit before dialling takes place. For example, if the **Prefix removal #** was set to 0808 and the terminal issued a **atd** command containing 0808111222 then the actual number dialled by the unit would be 111222.

note:

Prefix # and **Prefix removal #** are usually used in conjunction with each other to substitute the dialling code issued by the terminal for an alternative code.

NUA:

This parameter specifies the X.25 Network User Address to be used for outgoing X.25 calls if no NUA is specified in the call string.

NUI:

This specifies the X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string.

Call user data:

This specifies a text string that will be placed in the Call User Data field of an outgoing X.25 call request packet. Whether or not this information is required will depend on the X.25 host that you are connecting to. In most cases the information is not required.

Forward mode time (ms):

If not framed with STX ETX can still have data formatted after this period.

Clearing time (direct mode) (ms):

This parameter defines the clearing time in milliseconds that an X.25 call will be left "open" after receiving a response from the host. Each response from the host resets this timer.

Terminal ID:

The **Terminal ID** parameter can be used to insert or replace a Terminal ID in the APACS 30 string.

Terminal ID translation:

If this parameter is set to On, any Terminal ID provided by a connected terminal will be replaced by the ID set in the Terminal ID field above.

APACS 50 terminal ID:

This parameter specifies the terminal ID for use with incoming APACS 50 polling calls.

Connect string:

This parameter specifies a string to be sent to the user's terminal when an outgoing TPAD call has been connected, instead of the normal ENQ character. For example, this might be used to make a TPAD connection look like a PAD connection by specifying "CON COM" as the connect string.

Use connect string:

This parameter enables or disables use of the **Connect string** parameter.

Message numbering:

When this parameter is On, the unit will override the message numbering of the local equipment and substitute its own message numbering. This is useful when the locally connected equipment does not automatically increment the APACS 30 message number.

In same call:

If this parameter is set to Off only one transaction is allowed per call.

When set to Transaction, and **Message Numbering** is On, then multiple transactions are allowed per X.25 call but not until a response has been received from the host. When multiple transactions are sent message numbers are incremented for each transaction.

When set to Clear, multiple transactions per X.25 call are allowed irrespective of whether a response has been received from the host. Again, transaction numbers are incremented by the unit automatically.

Delimiter char:

This parameter specifies the character used to separate a main NUA from a backup NUA, and a main NUI from a backup NUI in an **atd** call string. The default value is the ASCII “!” character (decimal 33).

Poll chars:

This parameter is a string that specifies the set of characters to be treated as polling characters. The unit will respond to any of these characters using ACK. This parameter should normally be blank.

Merchant #:

This parameter can be used to insert a merchant number into the APACS 30 string when the locally connected equipment does not transmit a merchant number.

Calling NUA:

This is the NUA that the unit will report to the X.25 network as its own NUA. Often the X.25 network will override this NUA.

Layer 2 deactivation timer (s):

Once a TPAD X.25 call has been cleared, the unit will keep a LAPB instance active for the length of time set by this parameter. This is to allow further TPAD transactions to take place without having to make another ISDN call. The default value of 10 seconds should be acceptable for most applications.

If you select LAPD as the TPAD layer-2 interface, this value will automatically be set to 0 to disable layer-2 deactivation. You may still override the 0 setting by entering a new value but note that most network service providers prefer that LAPD connections are not repeatedly deactivated.

Default packet size:

This parameter specifies the default X.25 packet size to be used for TPAD transactions.

Layer 2 interface:

This parameter is used to select whether the TPAD instance will use B-channel X.25, D-channel X.25 or TCP as the transport protocol. For D-channel operation, ensure that the LAPD option is selected. For B-channel operation, select LAPB.

Layer 2 interface #:

This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select 0 or 1 for LAPB. Select 0, 1 or 2 for LAPD.

Remote IP address:

When the unit is configured for XOT or TCP socket mode, this parameter is used to specify the IP address of the host to which the XOT call is made. Note that the layer 2 interface must be set to TCP.

IP mode:

This parameter is used to select XOT or IP socket mode when the **Layer 2 interface** has been set to TCP.

IP port (TCP socket mode):

When making a TCP socket connection (i.e. the **Layer 2 interface** has been set to TCP), this parameter must be used to specify the TCP port number to use).

IP length header:

When making a TCP socket connection (i.e. the **Layer 2 interface** has been set to TCP), this parameter must be used to specify the TCP port number to use, this parameter may be used to specify the length of transaction data in a header packet.

LCN:

The unit supports up to eight logical X.25/TPAD channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).

Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

For incoming calls, the unit accepts the LCN specified by the caller.

LCN direction:

This parameter determines whether the X.25 LCN used for outgoing TPAD calls is incremented or decremented from the starting value when multiple TPAD instances share one layer 2 (LAPB or LAPD), connection. The default is DOWN and LCNs are decremented i.e. if the first CALL uses 1024, the next will use 1023 etc. Setting the parameter to UP will cause the LCN to be incremented from the start value.

Response timeout (s):

This is the length of time in seconds that the unit will wait for a response to a TPAD transaction request before clearing the TPAD call.

Excessive transaction time (s):

Setting this parameter to a non-zero value causes the unit to generate an "Excessive Transaction Time" event (code 56) each time a TPAD transaction takes longer than the specified number of seconds. This could be used in conjunction with an appropriate **Event Handler** configuration to generate email alerts or SNMP traps when TPAD transactions take longer than expected. See **logcodes.txt** for a complete list of events.

TID timeout (s):

This specifies the time in seconds before the **Terminal ID** is considered inactive.

Restart delay (ms):

When the **Restarts** parameter is set to On the, **Restart delay** value determines how long (in milliseconds) that the unit will wait before issuing a Restart packet. The default value is 2000 giving a delay of 2 seconds.

Restarts:

The **Restarts** parameter is only used in D-channel X.25 mode i.e. when the specified TPAD instance has been bound to a LAPD instance.

It is normally possible to make X.28 CALLs immediately following the initial SABM, UA exchange. In some cases however, the X.25 network may require an X.25 RESTART before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe.

The default value is On. This means that the unit will issue X.25 RESTART packets. To prevent the unit from issuing RESTART packets set this parameter to Off.

Include LRC:

The LRC (Longitudinal Redundancy Check) is a form of error checking that may be required by some TPAD terminals. When the **Include LRC** option is set to YES the unit will check the LRC.

Force parity ASY:

When this parameter is set to Yes, the unit will always use Even parity when relaying data from a remote host to a locally connected TPAD terminal. To allow data to pass through without the parity being changed, set this option to Off.

Force parity line:

When this parameter is set to Yes the unit will always use EVEN parity when relaying data from the locally connected TPAD terminal to the remote host. To allow data to pass through without the parity being changed, set this option to Off.

ACK data:

This parameter causes the unit to acknowledge TPAD data packets from the terminal. This parameter should normally be set to the default value of Yes. Note that this parameter is only used if no **Poll Chars** are defined.

DTE re-transmit:

Setting this parameter to Yes will cause the unit to retransmit the APACS 30 string if an error is detected.

Delete STX/ETX:

Setting this parameter to Yes will cause the unit to strip off the STX and ETX characters that normally surround the APACS 30 string.

Boot to direct mode:

Direct mode is a mode of operation whereby the unit automatically routes APACS 30 packets to their destination without the terminal having to perform any call control. If this parameter is set to Yes, then the next time the unit is rebooted it will operate in direct mode. For direct mode to work you must set up the appropriate addressing information (B channel, NUA or NUI). If this parameter is set to No, the unit will still try to use direct mode if it detects that it is required (due to the absence of call control information). This parameter can be used in certain cases where for some reason the unit cannot automatically determine whether or not to use direct mode. See also **Disable Direct Mode** below.

Disable direct mode:

Setting this parameter to Yes will prevent the unit from automatically using direct mode (see above) when it receives an APACS 30 packet without any call set-up.

Unable to authorise acquirer response:

This parameter only applies when the unit is operating in direct mode. In cases where the unit is unable to send the APACS 30 packet to the remote host, it replies to the terminal with an "unable to authorise" message. By default, this message contains a response code 05 which means declined. Entering a number for this parameter causes the unit to use that number in place of the default response code. A value of zero for this parameter prevents the unit from replying.

Transaction delay (ms):

Setting this parameter will cause the unit to pause for the specified number of milliseconds in between successfully connecting to the remote X.25 host and transmitting the APACS 30 string.

Data trigger:

This parameter can be used to generate a “Data Trigger” event (code 47) when the reply from the X.25 host contains the string specified in this parameter. It is possible to configure the unit to generate an automatic email when this event occurs. See **logcodes.txt** for a complete list of events.

Dialling context:

This parameter is for advanced users only. It enables TPAD transactions to be carried out using the V.120 protocol. The parameter is used in conjunction with the Polling Answering Service (PANS), and identifies which PANS instance is to be used for an outgoing V.120 call. For this to work, the PANS instance must be bound to a V.120 instance.

Backup Parameters:**Layer 2 deactivation timer (s):**

This parameter is functionally equivalent to the **Layer 2 Deactivation Timer** parameter in the general parameters section above but only applies to the backup service.

Layer 2 interface:

The **Layer 2 Interface** parameter specifies whether the backup service uses LAPB, LAPD or NONE.

Layer 2 interface #:

This parameter specifies which LAPB or LAPD instance to use for the backup interface. Select 0 or 1 for LAPB, select 0, 1 or 2 for LAPD.

LCN:

The **LCN** parameter is used to set the first LCN that will be used for the backup interface.

LCN direction:

This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

Using text commands:

From the command line, use the **tpad** command to configure or display TPAD settings.

To display current settings for a TPAD instance enter the command:

```
tpad <instance> ?
```

To change the value of a parameter use the command in the format:

```
tpad <instance> <parameter> <value>
```

The parameters and values are:

Parameter	Values	Equivalent web parameter
ackdat	on, off	ACK data
bdir	on, off	Boot to direct mode

bnumber	0, 1	B-channel #
cingnua	text	Calling NUA
clear_dirtime	number	Clearing time (direct mode) (ms)
constr	text	Connect string
cud	text	Call user data
defpak	number	Default packet size
delimchar	decimal ASCII	Delimiter character
delstx	on, off	Delete STX/ETX
dialctx	number	Dialling context
disdir	on, off	Disable direct mode
domsgnb	on, off	Message numbering
dorest	on, off	Restarts
dotermid	on, off	Terminal ID translation
fpar	on, off	Force parity ASY
ftime	number	Forward mode time (s)
inclrc	on, off	Include LRC
ipaddr	IP address	Remote IP address
iphdr	on, off	IP length header
ipmode	0 (XOT), 1 (TCP socket mode)	IP mode
ipport	number	IP port (TCP socket mode)
l2iface	lapb, lapd	Layer 2 interface
l2nb	0-1 (lapb), 0-2 (lapd)	Layer 2 interface #
lcn	number	LCN
lcnup	on, off	LCN direction
lpar	on, off	Force Parity Line
merchnum	text	Merchant #
nua	text	NUA
nui	text	NUI
pollchars	text	Poll characters
prefix	number	Prefix #
prefix_rem	number	Prefix removal #
restdel	number	Restart delay (ms)
samecall	0 (off), 1 (transaction), 2 (clear)	In same call
dteretran	on, off	DTE retransmit
termed	text	Terminal ID
termid50	number	APACS 50 terminal ID
texcess	number	Excessive transaction time (s)
tidtime	number	TID timeout (s)
tl2deact	number	Layer 2 deactivation timer (s)
trandel	0-5000	Transaction delay (ms)
tresp	number	Response timeout (s)
trig_str	text	Data trigger
uaarc	number	Unable to authorise acquirer response
useconstr	on, off	Use connect string
Backup parameters		
bakl2deact	number	Layer 2 deactivation timer (s)
bakl2iface	lapb, lapd	Layer 2 interface
bakl2nb	0,1,2 or 3	Layer 2 interface #
baklcn	number	LCN
baklcnup	up, down	LCN Direction

For example, to set up TPAD 0 to use LAPD 0 you would enter the commands:

```
tpad 0 l2iface lapd
tpad 0 l2nb 0
```

4.35 Configure ► Users

The unit allows you to define up to 40 authorised users (numbered 0 to 39). Each user has a password and an access level that determines what facilities the user has access to.

Using the web page:

The **Configure ► Users** page option displays a table that allows you to set the following parameters for each user:

Name:

Enter a user name of up to 14 characters.

Password:

Enter a password for the user of up to 14 characters.

Confirm Password:

Re-enter the Password in this field to confirm it.

Access Level:

Select the access level for the User. Level "SUPER" allows full access to all facilities.

Level "HIGH" allows users to change some settings such as the time & date and to reconfigure the general operation of the unit. However, a HIGH level user cannot change User settings.

Level MEDIUM allows read-only access i.e. the user will not be able to alter any of the configuration settings.

IP address

In the event that multiple PPP instances are enabled for answering and that multiple remote routers can dial into the Sarian, static routes cannot always be used to ensure that packets which should be routed to the remote network are sent through the correct PPP interface. This parameter can be used in conjunction with the IP mask parameter to associate a network address with a user.

When a remote router "dials in" and authenticates with the Sarian, the Sarian will create a dynamic route (that will override any static routes) for the duration of the PPP session. The interface for the dynamic route will be the PPP interface that answered the call. The network address for the dynamic route will be taken from the entry in the user table that matches the username that the remote router used during the PPP authentication.

IP mask

The IP mask parameter is used in conjunction with the **IP address** parameter above to fully qualify the network address for the user.

Dialback number

This parameter is used to specify a telephone number for the user in the event that "dial-back" is required.

Using text commands:

From the command line use the **user** command to configure settings for the authorised users.

To display current settings for a particular user enter the command:

```
user <user> ?
```

This lists the user name, password, the encrypted form of the password and the user access level. To change the value of a parameter use the command in the format:

```
user <number> <parameter> <value>
```

where <number> is 0-9. The parameters and values are:

Parameter	Values	Equivalent web parameter
access	0-4	User access code (0 = Super, 1=High, 2=Medium, 3=Low, 4=None)
ipaddr	IP address	IP address
mask	IP address mask	IP mask
name	up to 14 characters	User name
password	up to 14 characters	Password
phonenum	number	Dialback number

For example, to set the user name for User 2 to “James” enter the command:

```
user 2 name James
```

4.36 Configure ► X.25 Macros

The **Configure ► X.25 Macros** page allows you to define up to 10 X.25 CALL “macros” that can be used to initiate ISDN and/or X.25 layer 3 calls. These simple English-like names are mapped to full command strings. For example, the call string:

```
0800123456=789012Dtest data
```

could be given the name “X25test” and then executed simply by entering:

```
CALL X25test
```

Using the web page:

To create a macro, enter a name for the macro in the left column of the **Configure ► X.25 Macros** table and in the right column enter the appropriate command string (excluding the **atd** which is inserted automatically).

Using text commands:

From the command line the **macro** command may be used to define CALL macros.

To set up a new macro, two commands are required in the form:

```
macro <n> name <name>
```

```
macro <n> cmd <cmd>
```

The first command assigns the name <name> to macro number <n> where n is 0..9. The second assigns the command string <cmd> to macro number <n>.

For example:

```
macro 5 name X25test
```

```
macro 5 cmd 0800123456=789012Dtest data
```


To display the current values for a particular macro use the macro command in the following format:

macro <n> ?

4.37 Configure ► X.25 PADS

There are two main elements to the configuration procedure for accessing X.25 networks:

General and service related parameters

PAD parameters (X.3)

Each PAD configuration page also includes a sub-page detailing the X.3 PAD parameters. Collectively this set of values is known as a PAD profile. Your unit contains four pre-defined standard profiles numbered 50, 51, 90 and 91. You may also create up to four custom PAD profiles numbered 1 to 4 for each PAD instance.

Using the Web page:

Each PAD configuration page is split into two sections. The first section includes general PAD parameters; the second includes parameters relating to the backup interface. The parameters are as follows:

4.37.1 General Parameters

Answering NUA:

This is the NUA that the unit responds to for incoming X.25 calls.

Calling NUA:

This NUA will be used as the calling NUA when an outgoing X.25 call is made.

Auto macro:

This parameter specifies the name of an X.25 call macro that is used when an **atd** command is received by the unit. The **atd** command is ignored, and a PAD **CALL** command using the macro replaces it. The purpose of this feature is to allow non-PAD terminals to use an X.25 PAD network connection. X.25 call macros are set up in the **Configure ► X25 Macros** web page, or by using the macro text command.

Default packet size:

This parameter determines the default X.25 packet size. This may be set to 16, 32, 64, 128, 256, 512 or 1024 but the actual values permitted will normally be constrained by your service provider.

Layer 2 interface:

This parameter for each PAD is used to select whether it will be used for B or D-channel X.25 operation. For D-channel operation, ensure that the LAPD option is selected from the drop-down menu. For X.25 over an ISDN B-channel, select LAPB.

Layer 2 interface #:

The **Layer 2 Interface Number** is used to specify which Layer 2 instance will be used for this PAD (0 or 1 for LAPB, 0, 1 or 2 for LAPD).

LCN:

The unit supports up to eight logical X.25 channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).

Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

For incoming calls, the unit accepts the LCN specified by the caller.

LCN direction:

This parameter determines whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is Down and LCNs are decremented i.e. if the first CALL uses 1024, the next will use 1023 etc. Setting the parameter to Up will cause the LCN to be incremented from the start value.

NUI/NUA selection:

If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request. This can be extremely useful in backup scenarios.

Consider the following example; the unit is configured to do online authorisations via the ISDN D-channel and to fall back to B-channel (if the D-channel host did not respond for any reason). Using this parameter in conjunction with the backup equivalent, it is possible to configure the unit to use the supplied NUA to connect over D-channel and the supplied NUI to connect over B channel (for backup).

PAD profile #:

The **PAD profile #** allows you to select the PAD profile to use for this PAD instance. There are four pre-defined profiles numbered 50, 51, 90 and 91. In addition to the pre-defined profiles you can also create up to four user-defined profiles numbered 1, 2, 3 and 4.

To assign a particular profile to the PAD select the appropriate number from the list.

PAD prompt:

This parameter allows you to redefine the standard "PAD>" prompt. To change the prompt enter a new string of up to 15 characters into the text box.

Restart Delay (ms):

When the **Restarts** parameter is On the **Restart Delay** value determines the length of time in milliseconds that the unit will wait before issuing a Restart packet. The default value is 2000 giving a delay of 2 seconds.

Restarts:

It is normally possible to make X.25 CALLs immediately following the initial SABM, UA exchange. In some cases however, the X.25 network may require an X.25 Restart before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe.

The default value is On. This means that the unit WILL issue X.25 Restart packets. To prevent the unit from issuing Restart packets set this parameter to Off.

Inactivity timeout:

This parameter specifies the length of time in seconds after which the PAD will terminate an X.25 call if there has been no data transmission.

No Call L2 Timeout (s):

This parameter specifies the length of time in seconds after which the unit will disconnect a layer 2 link if there are no layer 3 calls in progress. For LAPB sessions this will also terminate the ISDN call.

PAD mode:

The **PAD Mode** parameter can be set to Normal or Prompt Always On.

In Prompt Always On mode the ASY port attached to the PAD behaves as if it were permanently connected at layer 2 i.e. it always displays a PAD> prompt. AT commands may still be entered but the normal result codes are suppressed.

To disable this mode set the parameter to Normal.

STX/ETX mode:

When the **STX/ETX mode** parameter is On the PAD instance will ignore data that is not encapsulated between the ASCII characters STX (Ctrl+B) and ETX (Ctrl+C). To disable this feature select the Off option.

Data trigger:

This parameter specifies a string, which if it appears in the received data causes a “Data Trigger” (47) event to be generated and recorded in the event log.

4.37.2 Backup Interface Parameters

Layer 2 interface:

This parameter specifies whether the backup service uses LAPB, LAPD or NONE.

Layer 2 interface #:

This parameter specifies which LAPB or LAPD instance to use for the backup interface. Select 0 or 1 for LAPB, select 0, 1 or 2 for LAPD.

LCN:

The **LCN** parameter is used to set the first LCN that will be used for the backup interface.

LCN direction:

This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

NUI/NUA selection:

If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request.

Using text commands:

To configure PAD parameters from the command line use the **PAD** command. To display the settings for the specified PAD instance use the command in the form:

```
pad <instance> ?
```

To change the value of a parameter use the command in the form:

```
pad <instance> <parameter> <value>
```

where **instance** is in the range 0-4.

The parameters and values are:

Parameter	Values	Equivalent web parameter
amacro	text	Auto macro
ansnua	NUA	Answering NUA
cingnua	NUA	Calling NUA
defpak	number	Default packet size

dorest	on, off	Restarts
inacttim	number	Inactivity timer (s)
l2iface	lapb, lapd	Layer 2 interface
l2nb	0,1,2	Layer 2 interface number
lcn	number	LCN
lcnup	on, off	LCN direction
nocalltim	number	No Layer 2 call timeout (s)
nuaimode	0,1,2	NUA or NUI only mode
padmode	0,1	PAD mode
profile	1-4, 50, 51,90,91	PAD profile
prompt	text	PAD prompt
restdel	number	Restart delay (ms)
stxmode	0,1	STX ETX mode
trig_str	text	Data trigger
Backup parameters		
bakl2iface	lapb, lapd	Layer 2 Interface
bakl2nb	0,1,2	Layer 2 Interface Number
baklcn	number	LCN
baklcnup	0,1	LCN direction
baknuaimode	0,1,2	NUA/NUI selection

For example, to configure PAD 1 to use LAPD enter the command:

```
pad 1 l2iface lapd
```

4.38 Configure ► X.25 PADS ► Parameters

Each PAD configuration page has an attached sub-page that allows you to edit the X.3 PAD parameters. These pages allow you to load one of the standard profiles or edit the individual parameters to suit your application requirements and save the resulting customised “user” profile to non-volatile memory.

1 PAD recall character

This parameter determines whether PAD recall is enabled. When this facility is enabled, typing the PAD recall character temporarily interrupts the call and returns you to the **PAD>** prompt where you may enter normal PAD commands as required. To resume the interrupted call, use the **CALL** command without a parameter.

The default PAD recall character is **[Ctrl-P]**. This may be changed to any ASCII value in the range 32-125 or disabled by setting it to 0.

When a call is in progress and you need to actually transmit the character that is currently defined as the PAD recall character, simply enter it twice. The first instance returns you to the **PAD>** prompt; the second resumes the call and transmits the character to the remote system.

Option	Description
0	Disabled
1	PAD recall character is CTRL-P (ASCII 16, DEL)
32-126	PAD recall character is user defined as specified

2 Echo

This parameter enables or disables local echo of data transmitted during a call. When echo is enabled, X.3 parameter 20 may be used to inhibit the echo of certain characters.

Option	Description
--------	-------------

0	Echo off
1	Echo on

3 Data forwarding characters

This parameter defines which characters cause data to be assembled into a packet and forwarded to the network.

Option	Description
0	No data forwarding character
1	Alphanumeric characters (A-Z, a-z, 0-9)
2	CR
4	ESC, BEL, ENQ, ACK
8	DEL, CAN, DC2
16	EXT, EOT
32	HT, LF, VT, FF
64	Characters of decimal value less than 32

Combinations of the above sets of characters are possible by adding the respective values together. For example, to define CR, EXT and EOT as data forwarding characters, set this parameter to $2+16 = 18$.

If no forwarding characters are defined the Idle timer delay (parameter 4) should be set to a suitable value, typically 0.2 seconds.

4 Idle timer delay

This parameter defines a time-out period after which data received from the DTE is assembled into a packet and forwarded to the network. If the forwarding time-out is disabled, one or more characters should be selected as "data forwarding characters" using parameter 3.

Option	Description
0	No data forwarding time-out
1	Data forwarding time-out in 20ths of a second.

5 Ancillary device control

This parameter determines method of flow control used by the PAD to temporarily halt and re-start the flow of data from the DTE during a call.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

6 Suppression of PAD service signals

This parameter determines whether or not the *PAD*> prompt and/or Service/Command signals are issued to the DTE.

Option	Description
0	PAD prompt and signals disabled
1	PAD prompt disabled, signals enabled
4	PAD prompt enabled, signals disabled
5	PAD prompt and signals enabled

7 Action on break (from DTE)

This parameter determines the action taken by the PAD on receipt of a break signal from the DTE.

Option	Description
0	No action
1	Send an X.25 interrupt packet
2	Send an X.25 reset packet to the remote system
4	Send an X.29 indication of break
8	Escape to PAD command state
16	Set PAD parameter 8 to 1 to discard output

Multiple actions on receipt of break are possible by setting this parameter to the sum of the appropriate values for each action required.

For example, when parameter 7 is set to 21 (16+4+1), an X.25 interrupt packet is sent followed by an X.29 indication of break and then parameter 8 is set to 1.

You should NOT set this parameter to 16 because the remote system would receive no indication that a break had been issued and output to the DTE would therefore remain permanently discarded. If you need to use the discard output option, use it in conjunction with the X.29 break option so that on receipt of the X.29 break the remote system can re-enable output to your DTE using parameter 8.

8 Discard output

This parameter determines whether data received during a call is passed to the DTE or discarded. It can only be directly set by the remote system and may be used in a variety of circumstances when the remote DTE is not able to handle a continuous flow of data at high speed.

Option	Description
0	Normal data delivery to DTE
1	Output to DTE discarded

9 Padding after Carriage Return

Slower terminal devices, such as printers, may require a delay after each Carriage Return before they can continue to process data. This parameter controls the number of pad characters (NUL - ASCII 0) that are sent after each CR to create such a delay.

Option	Description
0	No padding characters after CR
1-255	Number of padding characters (NUL) sent after CR

10 Line folding

Controls the automatic generation of a [CR],[LF] sequence after a certain line width has been reached.

Option	Description
0	No line folding
1-255	Width of line before the PAD generates [CR],[LF]

11 Port speed

This is a "read only" parameter, set automatically by the PAD and accessed by the remote system.

Option	Description
15	19,200 bps
14	9,600 bps
12	2,400 bps
3	1,200 bps

12 Flow control of PAD by DTE

Determines the flow control setting of the PAD by the DTE in the on-line data state.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS flow control (not a standard X.3 parameter)

13 Line Feed insertion after Carriage Return

Controls the automatic generation of a Line Feed by the PAD.

Option	Description
0	No line feed insertion
1	Line Feeds inserted in data passed TO the DTE
2	Line Feeds inserted in data received FROM the DTE
4	Line Feeds inserted after CRs echoed to DTE

The line feed values can be added together to select Line Feed insertion to any desired combination.

14 Line Feed padding

Some terminal devices such as printers require a delay after each Line Feed before they can continue to process data. This parameter controls the number of padding characters (NUL - ASCII 0) that are sent after each [LF] to create such a delay.

Option	Description
0	No line feed padding.
1-255	Number of NUL characters inserted after LF

15 Editing

Enables (1) or disables (0) local editing of data input fields by the PAD before data is sent. The three basic editing functions provided are character delete, line delete and line re-display.

The editing characters are defined by parameters 16, 17 and 18. In addition, parameter 19 determines which messages are issued to the DTE during editing.

When editing is enabled, the idle timer delay (parameter 4) is disabled and parameter 3 must be used to select the desired data forwarding condition.

16 Character delete character

This parameter defines the edit mode delete character (ASCII 0-127). The factory default is backspace (ASCII 08).

17 Line delete character

This parameter defines the edit mode line buffer delete character (ASCII 0-127). The factory default is CTRL-X (ASCII 24).

18 Line redisplay character

Specifies the character that re-displays the current input field when in editing mode (ASCII 0-127). The factory default is CTRL-R (ASCII 18).

19 Editing PAD service signals

Specifies the type of service signal sent to the DTE when editing input fields.

Option	Description
0	No editing PAD service signals
1	PAD editing service signals for printers
2	PAD editing service signals for terminals

20 Echo mask

This parameter defines characters that are NOT echoed when echo mode has been enabled using parameter 2.

Option	Description
0	No echo mask (all characters are echoed)
1	CR
2	LF
4	VT, HT or FF
8	BEL, BS
16	ESC, ENQ
32	ACK, NAK, STX, SOH, EOT, ETB, ETX
64	No echo of characters set by parameters 16, 17 & 18
128	No echo of characters 0-32 decimal

Combinations of the above sets of characters are possible by adding the respective values together.

21 Parity treatment

This parameter determines whether parity generation/checking is used.

Option	Description
0	No parity generation or checking
1	Parity checking on
2	Parity generation on
3	Parity checking and generation on

22 Page wait

This parameter determines how many line feeds are sent to the terminal before output is halted on a page wait condition. In other words, it defines the page length for paged mode output. A page wait condition is cleared when the PAD receives a character from the terminal.

Option	Description
0	Page wait feature disabled
1	Number of line feeds sent before halting output

Using text commands:

The X.3 PAD parameters can be edited from the command line using the **SET** command described under the X.28 Commands section.

Loading and Saving PAD profiles.

To create your own profiles, edit the appropriate parameters and then select user profile 1, 2, 3 or 4 as required from the list and click the **Save Profile** button.

Each PAD profile page includes two list boxes that allow you to load and save PAD profiles. To load a particular profile, select the profile from the list and click the **Load Profile** button. The parameter table will be updated with the values from the selected profile.

4.39 Configure ► X.25 Switch

The X25 Switch software available on some models provides X25 call switching between the following interfaces:

ISDN LAPD (using the D channel X.25 packet service)

LAPB, either on ISDN or a serial port operating in synchronous mode

X25 Over TCP/IP (XOT)

When this optional feature is included, the unit may be configured to pass X.25 calls received via one of these interfaces to another interface. In addition, it is possible to specify a backup interface so that if an outgoing call on one interface fails, then the backup interface is automatically tried. The physical interfaces used by the LAPB instances are specified in the appropriate **Configure-►LAPB** pages, and may either be ISDN or one of ASY 0 or ASY 1 operating in synchronous mode.

Using the Web page:

The **Configure ► X.25 Switch** page is used to configure the X.25 Switch entity. The parameters are described below.

Switch from XOT to:

This parameter controls the switching of incoming X.25 calls received via XOT. LAPD, LAPB 0 or LAPB 1 may be chosen. Calls received via XOT will be passed on to the specified interface.

Switch from LAPD to:

This parameter controls the switching of incoming X.25 calls received via ISDN LAPD. LAPB 0, LAPB 1 or XOT may be chosen. Calls received via LAPD will be passed on to the specified interface.

Switch from LAPB 0 to:

This parameter controls the switching of incoming X.25 calls received via LAPB 0. LAPD, LAPB 1 or XOT may be chosen. Calls received via LAPB 0 will be passed on to the specified interface.

Switch from LAPB 1 to:

This parameter controls the switching of incoming X.25 calls received via LAPB 1. LAPD, LAPB 0 or XOT may be chosen. Calls received via LAPB 1 will be passed on to the specified interface.

Backup from XOT to:

This parameter may be used to specify a backup interface in the case where an X.25 call originating from XOT cannot be switched to the interface chosen under the **Switch from XOT to** parameter (above). LAPD, LAPB 0, LAPB 1 or none may be chosen. If none is chosen, then no backup call will be attempted.

Backup from LAPD to:

This parameter may be used to specify a backup interface in the case where an X.25 call originating from LAPD cannot be switched to the interface chosen under the **Switch from LAPD to** parameter (above). LAPB 0, LAPB 1, XOT or none may be chosen. If none is chosen, then no backup call will be attempted.

Backup from LAPB 0 to:

This parameter may be used to specify a backup interface in the case where an X.25 call originating from LAPB 0 cannot be switched to the interface chosen under the **Switch from LAPB 0 to** parameter (above). LAPD, LAPB 1, XOT or none may be chosen. If none is chosen, then no backup call will be attempted.

Backup from LAPB 1 to:

This parameter may be used to specify a backup interface in the case where an X.25 call originating from LAPB 0 cannot be switched to the interface chosen under the **Switch from LAPB 1 to** parameter (above). LAPD, LAPB 0, XOT or none may be chosen. If none is chosen, then no backup call will be attempted.

Call prefix:

This parameter specifies the call prefix to inserted in front of the NUA in calls being switched to LAPD. For example, if the called NUA in the call being received by the LAPB 0 interface is 56565 and the call prefix is 0242 then the call placed on the LAPD interface is to NUA 024256565. Also, for calls in the reverse direction, if the prefix in the calling NUA matches this parameter then it is removed from the calling NUA field.

D-channel NUA:

The D Channel NUA is used as the calling NUA in calls being switched in the LAPD direction. If a calling NUA is not required then this field can be left blank.

TE NUA:

For calls being switched in the LAPB 0 direction this is the called NUA to use.

TE NUA (LAPB 1):

For calls being switched in the LAPB 1 direction this is the called NUA to use.

B-channel LCN:

This is the value of the first LCN (logical channel number) that will be assigned for outgoing X25 calls on LAPB 0 or LAPB 1.

B-channel LCN Direction:

This parameter determines whether the LCN used for outgoing X.25 calls on LAPB 0 or LAPB 1 is incremented or decremented from the starting value.

B-channel #:

This parameter specifies an ISDN number to be used for calls being switched in the direction of LAPB 0 or LAPB 1.

D-channel LCN:

This is the value of the first LCN that will be assigned for outgoing X25 calls on LAPD.

D-channel LCN direction:

This parameter determines whether the LCN used for outgoing X.25 calls on LAPD is incremented or decremented from the starting value.

LAPB 0 NUA:

This parameter specifies an X.25 NUA to be used as the called NUA in calls being switched in the direction of LAPB 0.

LAPB 1 NUA:

This parameter specifies an X.25 NUA to be used as the called NUA in calls being switched in the direction of LAPB 1.

LAPD default packet size:

This is the default packet size for X.25 calls being switched onto LAPD. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPD default window size:

This is the default window size for calls being switched onto LAPD. The default window size is 2, the valid range is 1 to 7.

LAPB0 default packet size:

This is the default packet size for calls being switched onto LAPB 0. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB0 default window size:

This is the default window size for calls being switched onto LAPB 0. The default window size is 2, the valid range is 1 to 7.

LAPB1 default packet size:

This is the default packet size for calls being switched onto LAPB 1. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB1 default window size:

This is the default window size for calls being switched onto LAPB 1. The default window size is 2, the valid range is 1 to 7.

XOT remote IP address:

For calls being switched in the direction of XOT, this parameter specifies the destination IP address to be used for the outgoing XOT call.

XOT source IP address interface:

The default value for this parameter is Auto, which means that the source IP address of an outgoing XOT connection on an un-NATed GPRS link is the address of the PPP interface assigned to GPRS. This is because the XOT connection is initiated (automatically), within the router and so does not originate from the local subnet (LAN segment to which the unit is attached via the Ethernet interface).

However, this means that if you are routing traffic from the local subnet across a VPN tunnel you would have to set up two Eroutes; one to match the local subnet address and one to

match the XOT source address (i.e. the address of the PPP interface associated with to the GPRS network).

By setting this parameter to Ethernet the unit will use the IP address of the Ethernet port instead of that of the PPP interface so that you need only set up on Eroute.

XOT source IP address interface #:

This is the number of the interface selected by the **XOT source IP address interface** parameter.

Notes on PAD Answering.

Because the other interfaces can operate as normal, even when the switch is operating, special care needs to be taken with regard to answering NUAs programmed on active PADs. For example when a call is being received on a LAPD or LAPB interface, a PAD instance (or remote configuration session) is capable of answering and terminating the call in preference to the call being switched. This means that the PAD's "Answering NUA" parameters should be left blank to ensure that the unit's PADs are not answering calls that need to be switched. If you do want a PAD instance to answer a call then program the "Answering NUA" field with as many digits as you can to ensure it only answers calls destined for that PAD. The same precautions apply to the **Configure ► General ► X25 Remote Command addr** parameter.

Using text commands:

To configure the X.25 switch parameters via the command line use the **x25sw** command.

To display current settings for the X.25 switch enter the following command:

```
X25sw 0 ?
```

To change the value of a parameter use the command in the format:

```
X25sw <instance> <parameter> <value>
```

where instance is 0. The parameter options and values are:

Parameter	Values	Equivalent web parameter
blcn	Number	B-channel LCN
blcnup	on, off	B-channel LCN direction
bnumber	ISDN number	B-channel #
bufrlapb0	0,1,3,4 (see note)	Backup from LAPB 0 to
bufrlapb1	0,1,2,4 (see note)	Backup from LAPB 1 to
bufrlapd	0,2,3,4 (see note)	Backup from LAPD to
bufrxot	0,1,2,3 (see note)	Backup from XOT to
callprefix	NUA	Call prefix
dchannua	NUA	D-channel NUA
dlcn	Number	D-channel LCN
dlcnup	on, off	D-channel LCN direction
ipaddr	IP Address	XOT remote IP address
lapb0nua	NUA	LAPB 0 NUA
lapb0ppar	7 (128), 8 (256), 9 (512), 10 (1024)	LAPB 0 default packet size
lapb0wpar	1-7	LAPB 0 default window size
lapb1nua	NUA	LAPB 1 NUA
lapb1ppar	7 (128), 8 (256), 9 (512), 10 (1024)	LAPB 1 default packet size
lapb1wpar	1-7	LAPB 1 default window size

lapdppar	7 (128), 8 (256), 9 (512), 10 (1024)	LAPD default packet size
lapdwpar	1-7	LAPD default window size
srcipadd	Auto, Eth	XOT remote IP address interface
srcipent	0, 1	XOT remote IP address interface #
swfrlapb0	1,3,4 (see note)	Switch from LAPB 0 to
swfrlapb1	1,2,4 (see note)	Switch from LAPB 1 to
swfrlapd	2,3,4 (see note)	Switch from LAPD to
swfrxot	1,2,3 (see note)	Switch from XOT to
te1nua	NUA	TE NUA (LAPB 1)
tenua	NUA	TE NUA

note:

Interfaces are coded as follows: 0 = none, 1 = LAPD, 2 = LAPB 0, 3 = LAPB 1, 4 = XOT

4.39.1 Configure ► X.25 Switch ► Mappings

X.25 switch mappings allow you to re-direct specified NUA's to alternative NUA's for switched X.25 calls. Up to twenty "NUA In" to "NUA Out" mappings are available. These mappings alter the called NUA field in any X.25 call. The comparison uses "tail" matching, so that only the rightmost digits in the NUA are compared with the table entry.

Using the Web pages.

The X.25 Switch ► Mappings web page displays a table with two columns in which you can specify the **NUA In** values and corresponding **NUA Out** values. For example, if the called NUA is 123456789345 and there is an **NUA In** table entry of 9345, then this will match, and the entire called NUA will be replaced with the corresponding **NUA Out** entry.

Using text commands.

To configure the X.25 switch NUA mappings via the command line use the **x25map** command.

To display a current X.25 switch NUA mapping enter the command:

```
X25map <entry> ?
```

where <entry> is a number in the range 0 to 19.

Two separate commands are needed to set up a mapping. These take the form:

```
X25map <entry> nuafrom <NUA>
X25map <entry> nuato <NUA>
```

where:

<entry> is the required entry number in the mapping table in each case

<NUA> is the appropriate NUA value

For example:

```
x25map 13 nuafrom 9345
X25map 13 nuato 23421234567890
```

4.39.2 X.25 Switch ► NUA to XOT IP address

Using the Web page:

This page displays a table with two columns in which you may specify up to 10 XOT NUA's and the IP addresses to which they should be switched.

Text commands:

To configure the NUA to XOT IP address mappings via the command line use the **nuaip** command.

To display a current NUA to XOT IP address mapping enter the command:

```
nuaip <entry> ?
```

where <entry> is a number in the range 0 to 9.

Two separate commands are needed to set up a mapping. These take the form:

```
nuaip <entry> nua <NUA>  
nuaip <entry> ipaddr <IP address>
```

where:

<entry> is the required entry number in the mapping table in each case

<NUA> is the incoming X.25 NUA to be matched (**NUA**)

<IP address> is the IP address to which the NUA should be mapped (**IP address**).

For example:

```
nuaip 5 nua 9345  
nuaip 5 ipaddr 192.168.20.30
```

4.40 Saving configuration settings.

Once you have configured the unit, your chosen settings must be saved to non-volatile memory to avoid losing them when the power is removed. Configuration information is stored in two types of file: *config* files and *profiles*.

4.40.1 Config files

All configuration information except AT command and S register settings, is stored in one of two files called **config.da0** and **config.da1**. This allows two different sets of configuration information to be stored using the **Save** option in the directory tree at the left of the web interface, or by using the **config** command from the command line.

You may select which of the two config files is loaded when the unit is powered-up or re-booted by setting the value of the **Power Up Config** option on the **Configure ► General** web page as required (or by using the **config** text command).

The config files only contain details of settings that have been changed from the default values.

4.40.2 Profiles

AT command and S register settings are stored as “profiles” contained in a file called **sregs.dat**. Two profiles (0 and 1) may be stored for each ASY port using the **Save Profile** button on the relevant **Configure ► ASY port** web page, or by using the **at&w** command.

It is important to remember that saving the settings for one ASY port does not save the settings for the other ports: the settings for each port must be saved individually.

For each ASY port, the profile to be loaded at reboot or power-up is specified in the **Power-up Profile** setting on the relevant **Configure ► ASY port** web page (or by using **at&y** command).

A profile for a particular ASY port may also be loaded to take immediate effect by using the **Load Profile** button on the ASY port's web page, or by using the **atz** text command.

5 Statistics Pages

Your 2000 series product maintains a wide range of statistics relating to each of the different protocol instances that may be used. These statistics are collected and maintained in non-volatile memory and may be displayed via the Statistics web pages.

Clicking on the **Statistics** branch of the directory tree will reveal options to display statistics for X.25 PAD, PPP, TPAD and V.120 instances, ASY ports or synchronous data channels.

To display the statistics for a particular port or protocol instance click on the appropriate “+” symbol to expand the required branch and then select the specific instance you require. For example, to display the statistics for X.25 PAD 0, click on the “+” symbol next to the X.25 PADS statistics label and then click on the PAD 0 hyperlink. On this page you can examine all statistics relating to the operation of PAD instance 0. This includes items such as the number of incoming calls, outgoing calls, number of bytes received etc.

Clearing Statistics

At the bottom of each page of statistics (you may need to use the scroll bar), is a button that allows you to clear all of the statistics counters for that page. Clicking the button once will clear all values on that page to 0.

The tables in the following sections list the statistics that are available on each of the statistics pages and provide a brief description of each item.

5.1 Statistics ► Adapt

Abbreviation	Description
TX Octets	Bytes transmitted
TX Errors	Transmit errors detected
RX Octets	Bytes received
RX Errors	Receive errors detected
General Errors	Other errors

5.2 Statistics ► ASY Ports

Abbreviation	Description
Rx Bytes	The number of bytes successfully received
Rx Overruns	The number of receiver overrun errors. An overrun occurs when the serial port overwrites valid, unread data in the receive data register or receive FIFO, resulting in loss of data.
Rx Aborts	The number of frames received with the Address Bit (AB bit) set.
Rx Breaks	The number of break characters received. A break character is defined as a constant low signal on the receive data line for one frame time or greater.
Rx Framing Errors	The number of framing errors detected on receive. A framing error is the detection of low signal during the stop bit time.
Rx Parity Errors	The number of parity errors detected.
Buffer Shortages	The number of frames discarded due to lack of system buffer space.
Message Shortages	The number of frames discarded due to lack of system message buffers.
Tx Bytes	The number of bytes successfully transmitted

Tx Underruns	The number of transmit underrun errors
--------------	--

5.3 Statistics ► DNS Update

Abbreviation	Description
Bad Key	Number of replies indicating that the Username is unknown or incorrect for the specified zone.
Bad Signatures	Number of replies indicating that the signature supplied in the update message was invalid (may indicate that the password field is incorrect).
Bad Time	Number of replies indicating that the time specified in the update message is outside the allowed window.
Not Authorised	Number of replies indicating that the server is not authoritative for this zone (may indicate that the zone field is incorrect).
Not Zone	Number of replies indicating that the username is not valid within the specified zone.
Other Errors	Number of non-specific error messages received from server.
Refusals	Number of rejected DNS Update messages
Successful Updates	Number of replies indicating that the update message was successful.
Updates sent	Total Number of DNS Update messages sent.

5.4 Statistics ► Ethernet

Abbreviation	Description
Rx Packets	Received Ethernet packets
Rx Bytes	Received Ethernet data bytes
Tx Packets	Transmitted Ethernet packets
Tx Bytes	Transmitted Ethernet data bytes
Rx Overruns	Receive overruns
Collisions	Collisions detected
Other Errors	Other errors detected

5.5 Statistics ► IP

Abbreviation	Description
Rx Packets	The number of packets correctly received.
Rx Bytes	The number of data bytes received (incl. IP headers).
Tx Packets	The number of packets correctly transmitted.
Tx Bytes	The number of data bytes transmitted (incl. IP headers).
Checksum Errors	The number of checksum errors detected.
TCP Retransmits	The number of TCP packets retransmitted.
Discards	The number of received packets discarded.
Routed Packets	The number of transmitted packets routed.
Routed Bytes	The number of transmitted data bytes (incl. IP headers).
NATed Packets	The number of packets that have undergone Network Address Translation.
NATed Bytes	The number of data bytes that have undergone Network Address Translation.
Packet Timeouts	The number of packets dropped because hopcount (TTL) reached 0.
NAT Shortages	The number of the NAT translation table became full.

No Route	The number of packets received for which no route to the destination could be found.
Filtered Packets	The number of routed packets that have been filtered out.
Tx Multicast	The number of multicast packets transmitted.
Rx Multicast	The number of multicast packets received.

5.6 Statistics ► IPSec ► Dynamic Eroutes

This page displays a list of all the dynamic Eroutes. Eroutes are created after a successful IKE negotiation. Each entry indicates the negotiated encryption/authentication/compression algorithms and the subnets to which they apply.

Abbreviation	Description
Peer ID	The ID of the remote peer. This will either be an IP address or a text description. It is supplied by the remote peer and is used in deciding which protocols/algorithms may be used.
AH	The negotiated AH algorithm (MD5 or SHA-1), or N/A if none negotiated.
ESP Auth	The negotiated ESP authentication algorithm (MD5 or SHA-1), or N/A if none negotiated.
ESP Enc	The negotiated ESP encryption algorithm (DES, 3DES, AES or NULL), or N/A if none negotiated.
IPCOMP	The negotiated compression algorithm (LZJH) or N/A if none negotiated.
SRC IP	Together with the SRC Mask indicates the source (local) subnet to which the Eroute applies.
DST IP	Together with the DST Mask indicates the destination (remote) subnet to which the Eroute applies.

5.7 Statistics ► IPSec ► IKE SAs

This page displays a list of IKE Phase 1 SAs. These may be used to generate new phase 2 sessions with the remote peer identified by the **Remote IP** entry. It also displays a list of incomplete Phase 2 negotiations though because the negotiations are generally very rapid, such entries will not remain in the table for long and may not be visible at all.

Abbreviation	Description
Remote IP	The IP address of the remote peer with which the Phase 1 SA has been established.
Session ID	For phase 1 SAs this value is 0. For phase 2 SAs the value will be non-zero with each phase 2 negotiation using a different session ID.
Time Left	The amount of time in seconds that the SA has left to live. Once they have expired they are removed from the table and another Phase 1 SA must be created before further phase 2 negotiations may be performed.

5.8 Statistics ► IPSec ► IPSec SAs

This page displays a list of all inbound and outbound IPSec SAs. These SAs are used in conjunction with the Eroutes to provide the required encryption etc. for the specified source and destination addresses.

Abbreviation	Description
SPI	Each IPSec has an associated SPI (Security Parameters

	Index). For all but IPComp SAs this value will be a random number between 0x100 and 0xFFFFFFFF. IPComp SAs use an SPI that indicates the algorithm being used.
IP	The remote IP address to which the SA applies.
AH	The negotiated AH algorithm (MD5 or SHA-1), or N/A if none negotiated.
ESP Auth	The negotiated ESP authentication algorithm (DES, 3DES, AES or NULL), or N/A if none negotiated.
IPCOMP	The negotiated compression algorithm (LZJH) or N/A if none negotiated.
Bytes Delivered	The number of bytes that have been processed by this SA
Bytes Left	The number of bytes that this SA is allowed to process before being removed. It is decremented each time a packet is processed.

Alongside each table entry a **Remove** button is provided so that an SA may be remove manually if necessary.

When IP compression has been negotiated, the page will also provide an indication of the effective compression ratio.

5.9 Statistics ► PPP

Abbreviation	Description
Total Data Transferred	The total number of bytes transferred.
Tx Octets	Transmitted PPP data octets.
Tx LCP Packets	Transmitted Link Control Protocol packets.
Tx PAP Packets	Transmitted Password Authentication Protocol packets.
Tx IPCP Packets	Transmitted PPP IP Control Protocol packets.
Tx BACP Packets	Transmitted Bandwidth Allocation Control Protocol packets.
Tx BAP Packets	Transmitted BAP Packets.
Tx Errors	Transmission errors.
Rx Octets	Received PPP data octets.
Rx LCP Packets	Received Link Control Protocol packets.
Rx PAP Packets	Received Password Authentication Protocol packets.
Rx IPCP Packets	Received PPP IP Control Protocol packets.
Rx BACP Packets	Received Bandwidth Allocation Control Protocol packets.
Rx BAP Packets	Received BAP Packets.
Rx Unknown Packets	Received unrecognised packets.
Rx CRC Errors	Received packets containing CRC errors.
Rx Framing Errors	Received Framing errors.
Rx Errors	Other receive errors.

note:

At the bottom of the PPP Statistics page there is an addition button labelled **Clear Total Data Transferred**. This is used to allow data transfer to recommence after the **Data Limit Stop Level** has been reached (See **Configure ► PPP ► Advanced** parameters).

5.10 Statistics ► SYNC Channels

Abbreviation	Description
Rx Frames	Received HDLC frames
Rx Bytes	Successfully received data bytes

Rx Giants	Received frames exceeding maximum frame length
Rx Runts	Received frames shorter than the minimum frame length
Rx CRC Errors	Received Cyclic Redundancy Check errors
Rx Overruns	Receive FIFO overflows
Rx Aborts	Received abort sequences detected
Buf Short	Frames discarded due to lack of system buffer space
Msg Short	Frames discarded due to lack of system message buffers
Tx Frames	Transmitted HDLC frames
Tx Bytes	Successfully transmitted data bytes
Tx Underruns	Transmit FIFO underruns

5.11 Statistics ► TPAD

Layer 3 X.25 Statistics

Abbreviation	Description
Tx Calls	X.25 call attempts
Rx Calls	Received X.25 calls
Rx Paks	Received X.25 packets
Rx Bytes	Received X.25 data bytes
Tx Restarts	Transmitted X.25 Restart Request packets
Rx Restarts	Received X.25 Restart Indication packets
Tx Paks	Transmitted X.25 packets
Tx Bytes	Transmitted X.25 data bytes

Layer 2 LAPD Statistics

Abbreviation	Description
TEI	Current Terminal Endpoint Identifier
Rx Frames	Received I-frames
Rx Bytes	Received I-frame data bytes
Rx Rejs	Received reject frames
Tx Rejs	Transmitted reject frames
Tx Frames	Transmitted I-frames
Tx Bytes	Transmitted I-frame data bytes
Rx Sabmes	Received SABME frames
Tx Sabmes	Transmitted SABME frames
Retrans	I-frame re-transmissions
State	Current link status - "up" or "down"
UnSolResp	Received unsolicited responses (Rej or RR)
TeiRem	TEI removals

D-channel Statistics

Abbreviation	Description
Frame Loss	Framing loss events
Sync Loss	INFO-2 events
Collisions	D-channel collisions
Ph Acts	Physical layer activations

Layer 1 D-channel Sync Statistics

Abbreviation	Description
Rx Giants	Received frames exceeding maximum frame length
Rx Runts	Received frames shorter than minimum frame length
Rx Frames	Received HDLC frames
Rx Bytes	Successfully received data bytes
Rx Crcerr	Received Cyclic Redundancy Check errors
Rx Overrun	Receive FIFO overflows
Rx Abort	Received Abort sequences detected
Rx NonOct	Received framing errors.
Msg Short	Frames discarded due to lack of system message buffers
Buf Short	Frames discarded due to lack of system buffer space
Tx Frames	Transmitted HDLC frames
Tx Bytes	Successfully transmitted data bytes
Tx Und	Transmit FIFO underruns

5.12 Statistics ► X.25 PAD

Layer 3 X.25 Statistics

Abbreviation	Description
Tx Calls	X.25 call attempts
Rx Calls	Received X.25 calls
Rx Paks	Received X.25 packets
Rx Bytes	Received X.25 data bytes
Tx Restarts	Transmitted X.25 Restart Request packets
Rx Restarts	Received X.25 Restart Indication packets
Tx Paks	Transmitted X.25 packets
Tx Bytes	Transmitted X.25 data bytes

Layer 2 LAPD Stats

Abbreviation	Description
TEI	Current Terminal Endpoint Identifier
Rx Frames	Received I-frames
Rx Bytes	Received I-frame data bytes
Rx Rejs	Received reject frames
Tx Rejs	Transmitted reject frames
Tx Frames	Transmitted I-frames
Tx Bytes	Transmitted I-frame data bytes
Rx Sabmes	Received SABME frames
Tx Sabmes	Transmitted SABME frames
Retrans	Retransmitted I-frames
State	Current link status - "up" or "down"
UnSolResp	Received unsolicited responses (Rej or RR)
TeiRem	TEI removals

D Channel Stats

Abbreviation	Description
Frame Loss	Framing loss events
Sync Loss	INFO-2 events
Collisions	D-channel collisions
Ph Acts	Physical layer activations

Layer 1 D Sync Stats

Abbreviation	Description
Rx Giants	Received frames exceeding maximum frame length
Rx Runts	Received frames shorter than minimum frame length
Rx Frames	Received HDLC frames
Rx Bytes	Successfully received data bytes
Rx Crcerr	Received Cyclic Redundancy Check errors
Rx Overrun	Receive FIFO overflows
Rx Abort	Received Abort sequences
Rx NonOct	Received framing errors
Msg Short	Frames discarded due to lack of system message buffers
Buf Short	Frames discarded due to lack of system buffer space
Tx Frames	Transmitted HDLC frames
Tx Bytes	Successfully transmitted data bytes
Tx Und	Transmit FIFO underruns

6 Status Pages

The next sub-heading on the directory tree is **Status**. Clicking on the “+” symbol at the left of the **Status** folder expands the sub-tree to list a number of pages which contain various status information about the unit:

Under the **Status** folder there are hyperlinks for pages that display the analyser log, event log, file directory etc. Click on the appropriate hyperlink to view the status screen for the item you require.

6.1 Status ► Analyser Trace

If the protocol analyser has been enabled, the contents of the analyser log can be viewed on the **Status ► Analyser Trace** page. The amount of detail provided in the log depends upon which analyser options have been turned on. Use the scroll bar at the right of the screen to navigate up/down stored trace information. The most recent data will appear at the top of the screen.

Using text commands:

To view the analyser trace from the command line, use the **type** command to list the **ana.txt** pseudo file:

```
type ana.txt
```

6.2 Status ► DHCP Server

The **Status ► DHCP Server** page displays a table of IP addresses leased by the DHCP server. Each table entry consists of the following:

IP address:

This is the IP address assigned to the client

Hostname:

This is the IP Hostname of the client to which the IP address was assigned

Lease time left (mins):

This is the time remaining in minutes before the client must renew its configuration with the DHCP server

Using text commands:

From the command line you may view the DHCP server status by using the **dhcp** command as follows:

```
dhcp 0 status
```

For example:

```
dhcp 0 status
Entry: IP [10.1.2.13], hostname [Server], expiry 46 (mins)
Entry: IP [10.1.2.12], hostname [Tim], expiry 53 (mins)
Entry: IP [10.1.2.11], hostname [Alan], expiry 50 (mins)
Entry: IP [10.1.2.15], hostname [Colin], expiry 59 (mins)
Entry: IP [10.1.2.91], hostname [Phil], expiry 37 (mins)
Entry: IP [10.1.2.16], hostname [Reception], expiry 41 (mins)
Entry: IP [10.1.2.10], hostname [X25], expiry 44 (mins)
```



```
Entry: IP [10.1.2.17], hostname [Robin], expiry 49 (mins)
Entry: IP [10.1.2.14], hostname [Alistair], expiry 59 (mins)
OK
```

6.3 Status ► Event Log

The **Status ► Event Log** page allows you to display the contents of the **eventlog.txt** pseudo-file with the most recent events listed at the top of the log. Each event log entry consists of the time and date of the event followed by a brief description. The information can be very useful in tracing and diagnosing fault conditions.

Using text commands:

From the command line you may view the contents of the event log by using the **TYPE** command to list the **eventlog.txt** pseudo file:

```
type eventlog.txt
```

6.4 Status ► File Directory

The **Status ► File Directory** page provides a list of files currently stored in the filing system. The listing includes the filename, size in bytes, read/write status and creation date/time.

Using text commands:

From the command line the file directory may be listed using the **dir** command.

6.5 Status ► Firmware Versions

The **Status ► Firmware Versions** page shows the model information and serial number for your unit and a list of the various firmware modules that are loaded along with the version number for each module.

Using text commands:

From the command line the firmware versions can be listed using either **ati5** or **id?**

6.6 Status ► GPRS Module

The **Status ► GPRS Module** page displays information about the current status of the GPRS module on those models that incorporate one. This includes:

SIM status:

This identifies whether or not a valid SIM card has been installed in the module. If no SIM installed the status will display as **ERROR**. If a valid SIM is installed but a required PIN has not been correctly entered, the status will display as **CPIN** (PIN number required) or **PUK** (SIM blocked, unblocking code required).

Signal strength:

This shows the GPRS signal strength in dBm being received by the module. The range is –113dBm (min.) to –51dBm (max.)

Manufacturer:

This entry shows the manufacturer of the GPRS module.

Network:

This entry shows the name of the GSM network to which the GPRS module is currently connected or **ERROR** if no network is available.

GPRS Attachment Status:

This field displays the current status of the module with respect to the GPRS service. It may be one of the following:

- ◆ **Not attached** – the unit has not connected to a GRPS service.
- ◆ **Attached** – the unit has connected to a GPRS service.
- ◆ **Unknown** – unknown response from GPRS module.

Network Registration Status:

This field indicates the status of the GPRS module with respect to the GSM network. It may be one of the following:

- ◆ Not registered, not searching
- ◆ Registered, home network
- ◆ Not registered, searching
- ◆ Registration denied
- ◆ Registered, roaming
- ◆ Unknown

6.7 Status ► IGMP Groups

The **Status ► IGMP Groups** lists statistics relating to the Internet Group Management Protocol (IGMP). This protocol is used for the management of IP multicast group membership. The statistics are described in the following table:

Abbreviation	Description
Free Groups	Number of available multicast group entries
Min Free Groups	Lowest value of Free Groups since power up
RX Total	Total number of IGMP packets received
RX Reports	Number of host membership report packets received
RX Queries	Number of host membership query packets received
TX General Queries	Number of general group membership query packets transmitted
TX Group Queries	Number of group specific membership query packets transmitted
Too Short	Number of IGMP packets received with an incorrect length
Bad Checksum	Number of IGMP packets received with an incorrect checksum
RX Bad Queries	Number of bad query packets received
RX Bad Reports	Number of bad report packets received

6.8 Status ► ISDN BRI

The **Status ► ISDN BRI** page shown below lists the status of the ISDN B and D-channels. If no ISDN connection is present, all three entries will be listed as Off. If the unit is connected to an ISDN line and the D-channel is functioning correctly, the D-channel entry will be shown as On. If one or two B-channels are in use, the appropriate B-channel entries will be shown as On.

6.9 Status ► Web Directory

The **Status ► Web Directory** page displays a list of all the files that are currently stored in the **ir2140.web** file. The listing shows the filenames and their sizes in bytes and at the bottom of the page gives totals for the number of files and space used.

6.10 Status ► Web Server

The **Status ► Web Server** page displays memory usage statistics for the built-in Web server.

6.11 Status ► X.25 Sessions

The **Status ► X.25 Sessions** page lists the available pool of X.25 sessions (8 in total). For each session it lists the current state (FREE or ENGAGED) and for each busy session it also shows the User, Link, Mode and NUA.

The User is the PAD or TPAD instance that is using the session.

The Link identifies the layer 2 protocol, either LAPB or LAPD.

The Mode identifies whether the call is outgoing (OUT) or incoming (IN).

Using the text commands:

From the command line the **statx** command can be used to display X.25 session status information. For example:

```
statx
  X25_SESSION  STATE      USER      LINK      MODE      NUA
  0             Free
  1             Engaged   PAD  0     LAPB  0     OUT    45
  2             Free
  3             Free
  4             Free
  5             Free
  6             Free
  7             Free
OK
```

7 The Filing System

The unit has its own FLASH memory filing system that uses DOS-like filenames of up to 12 characters long (8 characters followed by the “.” separator and a 3-character extension). The filing system is used to store the system software, Web pages, configuration information and statistics in a single root directory.

Sub-directories are not supported and a maximum of 22 files can be stored providing there is sufficient memory remaining. New files can be downloaded into the unit from a local terminal or from a remote system over the ISDN connection. Existing files can be renamed or deleted using DOS-like commands.

Although the filing system will only store up to 22 files, all those associated with the built-in website are stored in a single file with the .WEB extension and extracted as required.

7.1 System Files

The **dir** command described below is used to display a list of the currently stored files. A typical file directory will include the following files:

Filename	Description
ana.txt	Pseudo file for Protocol Analyser output
config.da0	Data file containing Config. 0 settings
direct	File directory
eventlog.txt	Pseudo file for Event Log output
fw.txt	Firewall script file
fwstat.txt	Firewall script status file
image	Main system image
*.web	File containing compressed Web pages for your model
logcodes.txt	Text file containing Event Log config. info.
sbios	Sarian BIOS and bootloader
sregs.dat	Data file containing AT command & S register settings
x3prof	X.25 PAD profile parameters

7.2 Filing System Commands

7.2.1 COPY Copy file

The **copy** command is used to make a copy of a file. The format is:

```
copy <filename> <newfilename>
```

where *<filename>* is the name of an existing file and *<newfilename>* is the name of the new copy that will be created.

7.2.2 DEL Delete file

The **del** command is used to delete files from the filing system. The format is:

```
del <filename>
```

where *<filename>* is the name of an existing file.

7.2.3 DIR List file directory

The **dir** command is used to display the file directory. For example:

```
dir
      direct      3360 ro  07:25:07, 03 Jan 2000
      sbios       65536 ro  07:25:07, 03 Jan 2000
      image      257508 rw  09:53:46, 20 Jan 2000
      sregs.dat   400 rw  09:56:05, 20 Jan 2000
      config.da0  76 rw  07:19:39, 21 Jan 2000
      IR2140.web  80256 rw  22:13:25, 19 Jan 2000
OK
```

Each line shows the file name and extension (if any), the file size (in bytes), the read/write status (ro = read only, rw = read/write) and the time/date of creation.

note:

File write operations are carried out as a background task and can be relatively slow due to the constraints of FLASH memory. As a result, the file directory may only be updated several seconds after a particular file operation has been carried out.

7.2.4 MOVE Move file

The move command is used to replace one file with another whilst retaining the original filename. The format is:

```
move <fromfile> <tofile>
```

For example, the command:

```
move new.web IR2140.web
```

will delete the file called **IR2140.web** and then rename the file called **new.web** as **IR2140.web**.

7.2.5 REN Rename file

The **ren** command is used to rename files in the filing system. The format is:

```
ren <oldfilename> <newfilename>
```

7.2.6 SCAN Scan file system

The scan command performs a diagnostic check on the file system and reports any errors that are found. For example:

```
scan
      direct ....ok
      sbios ....ok
      sregs.dat ....ok
      config.da0 ....ok
      ir2140.web ....ok
      image ....ok, data ok
```

The scanning process may take several seconds so you should not enter any other commands until the results are listed.

7.2.7 TYPE Display text file

The **type** command is used to display the contents of a text file. The format is:

```
type <filename>
```

For example:

```
type config.da0
bind PAD 0 ASY 0
pad 0 l2iface LAPB
cmd 0 username sarian
cmd 0 epassword Oz57X0kd
cmd 0 hostname ss.2000r
OK
```

7.2.8 XMODEM File transfer

The **xmodem** command is used to initiate an XMODEM file upload from the port at which the command is entered. The format is:

```
xmodem <filename>
```

where *<filename>* is the name under which the file will be saved when the upload is complete.

After entering the **xmodem** command the unit will wait for your terminal program to start transmitting the file. When the upload is complete and the file has been saved, the unit will respond with the **OK** result code.

A remote XMODEM upload can also be initiated by establishing a Telnet session over ISDN, and then issuing the **xmodem** command from the remote terminal.

8 Using V.120

V.120 is a protocol designed to provide high-speed point-to-point communication over ISDN. It provides rate adaptation and can optionally provide error control. Both the calling and called units must be configured to use V.120 before data can be transferred. Similarly, if one unit is configured to use the error control facility, the other must be configured in the same way.

8.1 Initial Set Up

Before using V.120 you must first bind one of the two available V.120 instances to the required ASY port using the **Configure ► Protocol Bindings** page or by using the **bind** command from the command line. For example:

```
bind v120 0 asy 0
```

You should also select the appropriate method of flow control for the ASY port using the **Configure ► ASY port** page or by using the **at&k** command from the command line. Other ASY port options such as character echo, result code format etc. should also be configured as necessary.

8.2 Initiating A V.120 Call

Once the initial configuration is complete, V.120 calls may be initiated using the appropriate **atd** command. For example:

```
atd01234567890
```

A successful connection will be indicated by a CONNECT result code being issued to the ASY port and the unit will switch into on-line mode. In this mode, all data from the terminal attached to the bound ASY port will be passed transparently through the unit across the ISDN network to the remote system. Similarly, all data from the remote system will be passed directly to the terminal attached to the bound ASY port.

If a V.120 call fails the unit will issue the NO ANSWER or NO CARRIER result code to the ASY port and remain in command mode.

The **atd** command may also be used to route a call to an ISDN sub-address by following the telephone number with the letter **s** and the required sub-address value.

For example:

```
atd01234567890s003
```

In this case, the remote system will only answer the call if it has been configured to accept incoming calls on the specified sub-address.

8.3 Answering V.120 Calls

V.120 answering can be enabled from the command interface by setting register S0 for the appropriate ASY port to a non-zero value. For example:

```
ats0=1
```

You should ensure that you have set **s0** for the correct ASY port by either entering it directly on that port or by using the **at\port=** command to select the correct port first.

The actual value used for the parameter sets the number of rings the unit will wait before answering.

Finally, you must ensure that there are no conflicts with other protocols configured to answer on other ASY ports. This can be done by disabling answering for the other ports/protocols or by using the MSN and/or Sub-address parameters to selectively answer calls to different telephone numbers using different protocols.

For example, if you have subscribed to the ISDN MSN facility, you may have been allocated say four telephone numbers ending in 4, 5, 6 and 7. You could then set the MSN parameter for the appropriate V.120 instance to 4 to configure V.120 to answer only incoming calls to the MSN number ending in 4.

You should check that if PPP answering is enabled you have NOT selected the same MSN and Sub-address values for PPP. If they are the same, V.120 will answer the call ONLY if S0 is set to 1. Otherwise, PPP will take priority and answer the call.

9 X.25 Packet switching

9.1 Introduction.

X.25 is a data communications protocol that is used throughout the world for wide area networking across Packet Switched Data Networks (PSDNs). The X.25 standard defines the way in which terminal equipment establishes, maintains and clears “switched virtual circuits” (SVC’s), across X.25 networks to other devices operating in packet mode on these networks.

The protocols used in X.25 operate at the lower three layers of the ISO model. At the lowest level the Physical layer defines the electrical and physical interfaces between the DTE and DCE. Layer 2 is the Data Link Layer that defines the unit of data transfer as a “frame” and includes the error control and flow control mechanisms. Layer 3 is the Network layer. This defines the data and control packet structure and the procedures used to access services that are available on PSDN’s.

A further standard, X.31 defines the procedures used to access X.25 networks via the ISDN B and D-channels.

Your Sarian unit includes support for allowing connected terminals to access X.25 over ISDN B channels, the ISDN D-channel or over TCP. It can also be configured so that if there is a network failure it will automatically switch to using an alternative service. The Packet Assembler/Disassembler (PAD) interface conforms to the X.3, X.28 and X.29 standards.

Up to six PAD instances (from an available pool of 8), can be created and dynamically assigned to the asynchronous serial ports or the **REM** pseudo-port.

Each application that uses the unit to access an X.25 network will have its own particular configuration requirements. For example, you may need to program your Network User Address (NUA) and specify which Logical Channel Numbers (LCN’s) should be used on your X.25 service. This information will be available from your X.25 service provider. You will also need to decide whether your application will use B or D-channel X.25.

Once you have this information, the PAD configuration pages can be used to set up the appropriate parameters.

B-channel X.25

The unit can transfer data to/from X.25 networks over either of the ISDN B-channels.

Once the unit has been configured appropriately, the ISDN call to the X.25 network can be made using an **atd** command or by executing a pre-defined macro. The format of the **atd** command allows you to combine the ISDN call and the subsequent X.25 call in a single command. Alternatively, the X.25 call may be made separately from the **PAD>** prompt once the ISDN connection to the X.25 network has been established.

D-channel X.25

The unit can transfer data to/from X.25 networks over the ISDN D-channel *if your ISDN service provider supports this facility*. The speed at which data can be transferred varies depending on the service provider but is generally 9600bps or less.

9.2 X.28 Commands

Once an X.25 session layer has been established the unit switches to *PAD* mode. In this mode operation of the PAD is controlled using the standard X.28 PAD commands listed in the following table:

Command	Description
---------	-------------

CALL	Make an X.25 call
CLR	Clear an X.25 call
ICLR	Invitation to CLR
INT	Send Interrupt packet
LOG	Logoff and disconnect
PAR?	List local X.3 parameters
PROF	Load or save PAD profile
RESET	Send reset packet
RPAR?	List remote X.3 parameters
RSET	Set remote X.3 parameters
SET	Set local X.3 parameters
STAT	Display channel status

9.2.1 CALL Make An X.25 Call

The full structure of a **CALL** command is:

```
CALL [<facilities->]<address>[D<user data>]
```

where:

<facilities-> is an optional list of codes indicating the facilities to be requested in the call (separated by commas, terminated with a dash)

<address> is the destination network address.

<user data> is any optional user data to be included with the call.

The facility codes supported are:

F	Fast select - no restriction
Q	Fast select - restricted response
Gnn	Closed User Group
Gnnnn	Extended Closed User Group
R	Reverse charging
N<NUI>	Network User Identity code (NUI)

Example:

```
CALL R,G12,NMYNUI-56512120DHello
```

places a call to address 56512120 using reverse charging and specifying Closed User Group 12. The string "MYNUI" is your Network User Identity and the string "Hello" appears in the user data field of the call packet.

note:

The particular facilities that are available will vary between X.25 service providers.

If a **CALL** command is issued without the address parameter, it is assumed that you wish to go back on-line to a previously established call (having used the PAD recall facility to temporarily return to the **PAD>** prompt).

Fast select (B-channel only)

When the standard Fast select facility is requested using the "F" facility code, the call packet generated by the **CALL** command is extended to allow the inclusion of up to 124 bytes of user data. For example:

```
CALL F-1234567890DThis DATA sent with call packet
```

would cause an X.25 CALL packet to be sent using the Fast select facility including the message "This DATA sent with call packet" (the Carriage Return used to enter the command is not transmitted). Without the inclusion of the Fast select facility code, only the first 12 characters would be sent.

When a Fast select **CALL** has been made the PAD accepts an extended format response from the called address. This response, consisting of up to 124 bytes of user data, may be appended to the returning call accepted or call clear packet. When one of these packets is received, the user data is extracted and passed from the PAD to the terminal immediately prior to the "CLR DTE . . ." message in the case of a call clear packet or "CON COM" message in case of a call accepted packet.

When a restricted response Fast select call has been made using the **Q** facility code, the call packet indicates that a full connection is not required so that any response to the user data in the **CALL** packet should be returned in a call clear packet.

When the PAD receives an incoming call specifying *Fast select*, the call is indicated to the terminal in the normal way. For example:

```
IC 1234567890 FAC: Q,W:2 COM
```

would indicate that an incoming call had been received requesting *Restricted response fast select* and a window size of 2. The user (or system) then has 15 seconds in which to pass up to 124 bytes of data to the PAD to be included in the clear indication packet that is sent in response to the call.

The PAD does NOT differentiate between standard and restricted response Fast select on incoming calls and, consequently, will always respond with a clear indication.

Network User Identity

The **N** facility code allows you to include your Network User Identity in the call packet. For security reasons the PAD echoes each character as an asterisk (*) during the entry of an NUI. Some X.25 services use the NUI field to pass both a User name and password for validation.

For example, if your User name is *MACDONALD* and your password is *ASDF*, a typical **CALL** command would have the format :

```
CALL NMACDONA;ASDF-56512120
```

where the ";" is used to separate the user name from the password.

Closed User Group (CUG)

Most X.25 networks support Closed User Groups. They are used to restrict subscribers to only making calls or receiving calls from other members of the same CUG. The CUG number effectively provides a form of sub-addressing that is used in conjunction with the NUA to identify the destination address for a call.

When the **G** facility code is specified in a **CALL** packet, it must be followed by the CUG number. This may be a 2 or 4 digit number. If you are a member of a closed user group, the network may restrict you to only making calls to or receiving calls from other members of the same group.

Reverse charging.

Reverse charging, specified using the **R** facility code, allows outgoing calls to be charged to the account of destination address. Whether or not a call is accepted on a reverse charging basis is determined by the service provider and by the type of account held by the called user.

Calling user data

The calling user data field for a normal call may contain up to 12 bytes of user data. If the first character is an exclamation mark (!), the PAD omits the four byte protocol identifier and allows the full 16 bytes as user data. The same is true for a fast select call except that the maximum amount of user data is increased from 124 to 128 bytes.

When entering user data, the tilde character (~) may be used to toggle between ASCII and binary mode. In ASCII mode data is accepted as typed but in binary mode each byte must be entered as the required decimal ASCII code separated by commas. For example to enter the data "Line1" followed by [CR][LF] and "Line2" you would enter:

DLine1~13,10~Line2

Aborting a CALL

An X.25 CALL may be aborted using the X.28 **CLR** command, by pressing [Enter] or by dropping DTR from the terminal while the call is in progress. Dropping DTR will also terminate an established call.

If a call is terminated by the network or by the remote host, the unit returns a diagnostic message before the **NO CARRIER** result code. Messages may be numeric or verbose depending on the setting of the **atv** command.

The following table lists the verbose messages and equivalent numeric codes:

Code	Verbose message
1	Unallocated (unassigned) number.
2	No route to specified transit network
3	No route to destination
4	Channel unacceptable
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented

66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
90	Destination address missing or incomplete
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expired
111	Protocol error, unspecified
127	Interworking, unspecified
128	General level 2 call control failure (probable network failure)

note:

Some verbose messages may be abbreviated by the unit.

9.2.2 CLR Clear An X.25 Call

The **CLR** command is used to clear the current call and release the associated virtual channel for further calls. On completion of call clear the **PAD>** prompt is re-displayed. A call may also be cleared as a result of a number of other situations. If one of these situations occurs, a message is issued to the PAD in the following format :

CLR <Reason> C:<n> - <text>

where:

- <Reason> is a 2/3 character clear down code
- <n> is the numeric equivalent of the clear down code
- <text> is a description of the reason for clear down

The clear down reason codes supported by the unit are listed in the following table:

Reason Code	Numeric Code	Text
DTE	0	by remote device
OOC	1	number busy
INV	3	invalid facility requested
NC	5	temporary network problem
DER	9	number out of order
NA	11	access to this number is barred
NP	13	number not assigned
RPE	17	remote procedure error
ERR	19	local procedure error

ROO	21	cannot be routed as requested
RNA	25	reverse charging not allowed
ID	33	incompatible destination
FNA	41	fast select not allowed
SA	57	ship cannot be contacted

If an unknown reason code is received, the text field is blank.

9.2.3 ICLR Invitation To CLR

The **ICLR** command “invites” the remote X.25 service to CLR the current X.25 session.

9.2.4 INT Send Interrupt Packet

INT causes PAD to transmit an interrupt packet. These packets flow “outside” normal buffering/flow control constraints and are used to interrupt the current activity.

9.2.5 LOG Logoff And Disconnect

LOG is used to terminate an X.25 session. It causes the PAD to clear any active X.25 calls, disconnect and return to AT command mode.

9.2.6 PAR? List Local X.3 Parameters

PAR? lists the local X.3 parameters for the current session.

9.2.7 PROF Load/Save PAD Profile

The **PROF** command is used to store or retrieve a pre-defined set of X.3 PAD parameters (referred to as a PAD profile). The information is stored in system file called **x3prof**. There are four pre-defined profiles numbered 50, 51, 90 and 91. Additionally, you may create four “user PAD profiles” numbered 1 to 4.

Profile 50 is automatically loaded when a PAD is first activated. To load one of the other pre-defined profiles use the **PROF** command followed by the required profile number. For example:

PROF 90

To create a User PAD profile you must use the SET command to configure the various PAD parameters to suit your application and then use the PROF command in the format:

PROF &nn

where **nn** is the number of the User PAD profile to be stored e.g. 03. Alternatively, you may use the web interface to edit the parameter tables directly (**Configure ► X25 PADS ► Parameters**).

The pre-defined profiles (50, 51, 90, 91), cannot be overwritten and are permanently configured as shown in the following table:

Parameter	Profile			
	50	51	90	91
1	1	0	1	0
2	0	0	1	0
3	0	0	126	0
4	5	5	0	20
5	0	3	1	0
6	5	5	1	0
7	0	8	2	2
8	0	0	0	0

9	0	0	0	0
10	0	0	0	0
11	15	15	15	15
12	0	3	1	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	8	8	127	127
17	24	24	24	24
18	18	18	18	18
19	2	2	1	1
20	64	64	0	0
21	0	0	0	0
22	0	0	0	0

As with configuration profiles, stored X.25 PAD profiles are held in non-volatile memory and will not be lost when the unit is switched off.

When used in the format:

```
prof nn
```

the **PROF** command loads the stored profile specified by **nn**.

9.2.8 RESET Send Reset Packet

RESET is used to issue a reset for the current call to the network. It does NOT clear the call but it does return the network level interface to a known state by re-initialising all Level 3 network control variables. All data in transit will be lost.

9.2.9 RPAR? Read Remote X.3 Parameters

RPAR? lists the current X.3 parameter settings for the remote system.

9.2.10 RSET Set Remote X.3 Parameters

RSET is used to set one or more X.3 parameters for the remote system. It is entered in the format:

```
RSET par #:value[,par #:value[,par #:value ...]]
```

9.2.11 SET Set Local X.3 Parameters

SET is used to set one or more of the local X.3 parameters for the duration of the current session. The format for the command is:

```
SET par #:value[,par #:value[,par #:value ...]]
```

9.2.12 STAT Display Channel Status

STAT displays the current status for each logical channel indicating whether it is free or engaged. For example:

```
stat
PAD    STATE
1      ENGAGED
2      FREE
3      FREE
4      FREE
```

10 PPP over Ethernet

PPP over Ethernet (PPPoE) is a means of establishing a PPP connection over the top of an Ethernet connection. The implementation provided on the 2000 series is compliant with RFC 2516, *A Method for Transmitting PPP Over Ethernet*. A typical application would be to allow non-PPPoE enabled devices to access Internet services where the connection to the Internet is provided by an ADSL bridge device.

Using the web pages:

There is no dedicated web page for configuring the unit to use PPPOE; rather there are a number of parameters that appear on other web pages that must be used in conjunction with each other to establish a PPPoE connection over the appropriate Ethernet interface.

In particular, the following configuration pages and parameters are important.

On the appropriate **Configure ► PPP** page, you should configure the following parameters:

Standard: as a minimum requirement the **Username** and **Password** parameters should be initialised. If necessary, you may set the **AODI Enabled** parameter to **Yes** to configure the unit so that it will attempt to renegotiate the PPP link should it go down for any reason.

Advanced: The advanced PPP options on this page should be initialised as required by your ISP. The **Layer 1 Interface** and **Layer 1 Interface #** fields define the physical Ethernet interface over which the PPPoE session will operate. In most cases this is **ETH 0**. The fact that you have selected Ethernet as the physical interface for operation with PPP automatically enables PPPoE mode.

In addition:

Desired Local MRU and **Desired Remote MRU** should be set to **1492**.

Request Local ACFC and **Request Remote ACFC** should be set to **No**.

Request Local PFC and **Request Remote PFC** should be set to **No**.

Using text commands:

There are no specific PPPoE commands available to the user via the text command interface. The appropriate **ppp** commands should be used to set the required options.

11 IPsec and VPN's.

11.1 What is IPsec ?

One inherent problem with the TCP protocol used to carry data over the vast majority of LAN's and the Internet is that it provides virtually no security features. This lack of security, and recent publicity about "hackers" and "viruses", prevent many people from even considering using the Internet for any sensitive business application. IPsec provides a remedy for these weaknesses adding a comprehensive security "layer" to protect data carried over IP links.

IPsec is a framework for a series of IETF standards designed to authenticate users and data, and to secure data by encrypting it during transit. The protocols defined within IPsec include:

- ◆ IKE - Internet Key Exchange protocol
- ◆ ISAKMP - Internet Security Association and Key Management Protocol
- ◆ AH - Authentication Header protocol
- ◆ ESP - Encapsulating Security Payload protocol
- ◆ HMAC - Hash Message Authentication Code
- ◆ MD5 - Message Digest 5
- ◆ SHA-1 - Security Hash Algorithm

and the cryptographic (encryption) techniques include:

- ◆ DES - Data Encryption Standard
- ◆ 3DES - Triple DES
- ◆ AES - Advanced Encryption Standard (also known as Rijndael)

Two key protocols within the framework are AH and ESP. AH is used to **authenticate** users, and ESP applies **cryptographic** protection. The combination of these techniques is designed to ensure the integrity and confidentiality of the data transmission. Put simply, IPsec is about ensuring that:

- (a) only authorised users can access a service and
- (b) that no one else can see what data passes between one point and another.

There are two modes of operation for IPsec, **transport mode** and **tunnel mode**.

In transport mode, only the payload (i.e. the data content), of the message is encrypted. In tunnel mode, the payload and the header and routing information are all encrypted thereby by providing a higher degree of protection.

11.2 Data Encryption methods.

There are several different algorithms available for use in securing data whilst in transit over IP links. Each encryption technique has it's own strengths and weaknesses and this is really, a personal selection made with regard to the sensitivity of the data you are trying to protect. Some general statements may be made about the relative merits but users should satisfy themselves as to suitability for any particular purpose.

DES (64-bit key) – this well-known and established protocol has historically been used extensively in the banking and financial world. It is relatively "processor intensive" i.e. to run efficiently at high data rates a powerful processor is required. It is generally considered very difficult for casual

hackers to attack but may be susceptible to determined attack by well-equipped and knowledgeable parties. Using DES, data rates up to approximately 2Mbits/sec aggregate transmit/receive should be achievable on the 2000 series).

3-DES (192-bit key) – again, this is a well-established and accepted protocol but as it involves encrypting the data three times using DES with a different key each time, it has a very high processor overhead. This also renders it almost impossible for casual hackers to attack and very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties. Using 3-DES, data rates of up to approximately 650Kbits/sec aggregate transmit/receive should be achievable on the 2000 series.

AES (128-bit key) – also known as Rijndael encryption, AES is the new “de-facto” standard adopted by many USA and European organisations for sensitive applications. It has a relatively low processor overhead compared to DES and it is therefore possible to encrypt at higher data rates. As with 3-DES it is almost impossible for casual hackers to attack and is very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties. Using AES, data rates up to approximately 2Mbits/sec aggregate transmit/receive should be achievable on the 2000 series).

To put these into perspective, common encryption programs that are considered “secure” (such as PGP) and on-line credit authorisation services (such as Web-based credit card ordering) generally use 128-bit encryption.

note:

Data rates are the maximum that could be achieved on the Sarian 2000 series platform and may be lower if other applications are running at the same time or small IP packet sizes are used.

What is a VPN?

VPNs (Virtual Private Networks) are networks that use the IPSec protocols to provide one or more secure routes or “tunnels” between endpoints. Users are issued either a shared “secret” key or “public/private” key pair that is associated with their identity. When a message is sent from one user to another, it is automatically “signed” with the user's key. The receiver uses the secret key or the sender's public key to decrypt the message. These keys are used during IKE exchanges along with other information to create session keys that only apply for the lifetime of that IKE exchange.

The Benefits of IPSec

IPSec is typically used to attain confidentiality, integrity, and authentication in the transport of data across inherently insecure channels. When properly configured, it provides a highly secure virtual channel across cheap, globally available networks such as the Internet, or creates a “network within a network” for applications such as passing confidential information between two users across a private network.X.509 Certificates

In the previous section, security between two points was achieved by using a “pre-shared secret” or password. Certificates provide this sort of mechanism but without the need to manually enter or distribute secret keys. This is a complex area but put simply a user's certificate acts a little like a passport providing proof that the user is who they say they are and enclosing details of how to use that certificate to decrypt data encoded with it. Passports however can be forged so there also needs to be proof that the passport has been properly issued and hasn't been changed since it was. On a paper passport this is achieved by covering the photograph with a coating that shows if it has been tampered with, embedding the users name in code in a long string of numbers etc. In the same way, for a Security Certificate to be genuine it has to be protected from alteration as well. Like a passport, you also have to trust that the issuer is authorised and competent to create the certificate.

Certificates use something called a “Public/Private Key Pair”. This a complex area but the principle is that you can create a encryption key made up from two parts, one private (known only to the

user), the other public (known to everyone). Messages encrypted with someone's public key can only be recovered by the person with the Public AND Private key but as encrypting the message to someone in the first place only requires that you know their public key, anyone who knows that can send them an encrypted message, so you can send a secure message to someone knowing only their publicly available key. You can also prove who you are by including in the message your "identity" whereupon they can look up the certified public key for that identity and send a message back that only you can understand. The important principles are that a) your private key cannot be determined from your public key and b) you both need to be able to look up the others certified ID. Once you've established two-way secure link you can use it to establish some rules for further communication.

Before this gets any more complicated we'll assume that Sarian are a competent authority to issue certificates and given that they exist and are valid, see how they are used.

X.509 Certificates

Generally, the issuing and management of certificates will be provided as a managed service by Sarian or it's partners, but some general information is provided here for system administrators.

Certificates are held in non-volatile files on the unit. Any private files are named privxxxx.xxx and cannot be copied, moved, renamed, uploaded or typed. This is to protect the contents. They can be overwritten by another file, or deleted.

Two file formats for certificates are supported:

- ◆ PEM – Privacy Enhanced MIME
- ◆ DER – Distinguished Encoding Rules

Certificate and key files should be in one of these two formats, and should have an extension of ".pem" or ".der" respectively.

note:

The equivalent filename extension for .PEM files in Microsoft Windows is ".CER". By renaming ".PEM" certificate files to ".CER", it is possible to view their makeup under Windows.

The 2000 series maintains two lists of certificate files. The first is a list of "Certificate Authorities" or CA's. Files in this list are used to validate public certificates sent by remote users. Public certificates must be signed by one of the certificates in the CA list before the unit can validate them. Certificates with the filename "ca*.pem" and "ca*.der" are loaded into this list at start-up time. In the absence of any CA certificates, a public certificate cannot be validated.

The second list is a list of public certificates that the unit can use to obtain public keys for decrypting signatures sent during IKE exchanges. Certificates with a filename "cert*.pem" and "cert*.der" are loaded into this list when the unit is powered on or re-booted. Certificates in this list will be used in cases where the remote unit does not send a certificate during IKE exchanges. If the list does not contain a valid certificate communication with the remote unit cannot take place.

Both the host and remote units must have a copy of a file called "casar.pem". This file is required to validate the certificates of the remote units.

In addition, the host unit should have copies of the files "cert02.pem" (which allows it to send this certificate to remote units) and "privrsa.pem". Note that before it can send this certificate, the **Responder ID** parameter in the **Configure ► IPSEC ► IKE** page must be set to "host@sarian.co.uk".

The remote unit must have copies of "cert01.pem" and "privrsa.pem". In addition, any *Eroutes* that are going to use certificates for authentication should be configured as follows:

Our ID should be set to "info@sarian.co.uk". This is the same as the subject *Altname* in certificate cert01.pem which makes it possible for the router to locate the correct certificate to send to the host.

Authentication Method should be set to **RSA Signatures**. This indicates to IKE that RSA signatures (certificates) are to be used for authentication.

When IKE receives a signature from a remote unit, it needs to be able to retrieve the correct public key so that it can decrypt the signature, and confirm that the signature is correct. The certificate must either be on the FLASH file system, or be provided by the remote unit as part of the IKE negotiation. The ID provided by the remote unit is used to find the correct certificate to use. If the correct certificate is found, the code then checks that it has been signed by one of the certificate authority certificates (CA*.pem) that exist on the unit. The code first checks the local certificates, and then the certificate provided by the remote (if any). IKE will send a certificate during negotiations if it is able to find one that has subject *AltName* that matches the ID being used. If not able to locate the certificate, then the remote must have local access to the file so that the public key can be retrieved.

A typical set-up may be that the host unit has a copy of all certificates. This means that the remote units only require the private key, and the certificate authority certificate. This eases administration as any changes to certificates need only be made on the host. Because they do not have a copy of their certificate, remote units rely on the host having a copy of the certificate. An alternative is that the remote units all have a copy of the certificate, as well as the private key and certificate authority certificate, and the host only has it's own certificate. This scenario requires that the remote unit send it's certificate during negotiations. It can validate the certificate because it has the certificate authority certificate.

12 FIREWALL SCRIPTS

A “firewall” is a protection system designed to prevent access to your local area network by unauthorised “external” parties i.e. other users of the internet or other wide area network. It may also limit the degree of access local users have to external network resources. A firewall does not provide a complete security solution; it provides only one element of a fully secure system. Consideration should also be given to the use of user authentication and data encryption. Refer to the IPSec section for details on this.

In simple terms, a firewall is a packet filtering system that allows or prevents the transmission of data (in either direction) based on a set of rules. These rules can allow filtering based on the following criteria the:

- ◆ source and destination IP addresses.
- ◆ source and destination IP port or port ranges.
- ◆ type of protocol in use.
- ◆ direction of the data (in or out).
- ◆ interface type
- ◆ ICMP message type
- ◆ TCP flags (Syn, Ack, Urg, Reset, Push, Fin).
- ◆ TOS field.
- ◆ status of a link and/or data packets on UDP/TCP and ICMP protocols.

In addition to providing comprehensive filtering facilities, Sarian routers also allow you to specify rules relating to the logging of information for audit/debugging purposes. This information can be logged to a pseudo-file on the unit called **fwlog.txt**, the eventlog.txt pseudo-file or to a syslog server. It can also be used to generate SNMP traps.

12.1 Firewall script syntax.

A firewall must be individually configured to match the needs of authorised users and their application requirements. On Sarian routers the actions of the firewall are defined in a script file called **fw.txt**. Each line in this file consists of a label definition, a comment or a filter rule.

A label definition is a string of up to 12 characters followed by a colon. Labels can only include letters, digits and the underscore character and are used in conjunction with the **break** option to cause the processing of the script to jump to a new location.

Any line starting with the hash character (“#”) is deemed to be a comment and ignored.

The syntax for a filter rule is:

```
[action] [in-out] [options] [tos] [proto] [ip-range] [inspect-state]
```

When the firewall is active, the script is processed one line at a time as each packet is received or transmitted. Even when a packet matches a filter-rule, processing still continues and all the other filter rules are checked until the end of the script is reached. The action taken with respect to a particular packet is that specified by the last matching rule. With the “break” option however the script processing can be redirected to a new location or to the end of the script if required. The default action that the firewall assigns to a packet is to block. This means that if the packet does not match any of the rules it will be blocked.

The various fields of a script rule are described below:

[action]

The `[action]` field may be specified as `block`, `pass`, `pass-ifup` or `debug`. These operate as follows:

block:

The `block` action prevents a packet from being allowed through the firewall. When `block` is specified an optional field can be included that will cause an ICMP packet to be returned to the interface from which that packet was received. This technique is sometimes used to confuse hackers by having different responses to different packets or for fooling an attacker into thinking a service is not present on a network.

The syntax for specifying the return of an ICMP packet is:

```
"return-icmp" [icmp-type [icmp-code]]
```

where `[icmp_type]` is a decimal number representing the ICMP type or can be one of the pre-defined text codes listed in the following table:

ICMP type value	ICMP type	Description
1	unreach	
2	echo	
3	echorep	
4	squench	
5	redir	
6	timex	
7	paraprob	
8	timest	
9	timestrap	
10	inforeq	
11	inforep	
12	maskreg	
13	maskrep	
14	routerad	
15	routersol	

The optional `[icmp-code]` field can also be a decimal number representing the ICMP code of the return ICMP packet but if the `[icmp-type]` is `[unreach]` then the code can also be one of the following pre-defined text codes:

ICMP code	Meaning
net-unr	Network unreachable
host-unr	Host unreachable
proto-unr	Protocol unrecognised
port-unr	Port unreachable
needfrag	Needs fragmentation
srcfail	Source route fail

For example:

```
block return-icmp unreach in on ppp 0
```

This rule would cause the unit to return an ICMP Unreachable packet in response to all packets received on **ppp 0**.

Instead of using the **return-icmp** option to return an ICMP packet, **return-rst** can be used to return a TCP reset packet instead. This would only be applicable for a TCP packet. For example:

```
block return-rst in on eth 0 proto tcp from any to 10.1.2.0/24
```

This would return a TCP reset packet when the firewall receives a TCP packet on the Ethernet interface 0 with destination address 10.1.2.*.

pass:

The **pass** action allows packets that match the rule to pass through the firewall.

pass-ifup:

The **pass-ifup** action allows outbound packets that match the rule to pass through the firewall but only if the link is already active.

debug:

The **debug** action causes the unit to tag any packets matching the rule for debug. This means that for every matching rule that is encountered from this point in the script onwards, an entry will be placed in the pseudo-file **fwlog.txt**.

[in-out]

The **[in-out]** field can be **in** or **out** and is used to specify whether the action applies to inbound or outbound packets. When the field is left blank the rule is applied to any packet irrespective of its direction.

[options]

The **[options]** field is used to define a number of options that may be applied to packets matching the rule. These are:

log:

When the **log** option is specified, the unit will place an entry in the **fwlog.txt** file each time it processes a packet that matches the rule. This log will normally detail the rule that was matched along with a summary of the packet contents. If the **log** option is followed by the **body** sub-option, the complete IP packet is entered into the log file so that when the log file is displayed, a more detailed decode of the IP packet is shown.

The **log** field may also be followed by a further sub-option that specifies a different type of log output. This may either be **snmp**, **syslog** or **event**.

If **snmp** is specified an SNMP trap (containing similar information to the normal log entry), is generated when a packet matches the rule.

If **syslog** is specified, a syslog message is sent to the configured syslog manager IP address. This message will contain the same information as that entered into the log file, but in a different format. If the **body** option has been specified, some of the IP packet information is also included. Note that the size of the syslog message is limited to the maximum of 1024 bytes. The syslog message is sent with default priority value of 14, which expands out to facility of USER, and priority INFO.

If **event** is specified the log output will be copied to the **eventlog.txt** pseudo-file as well as the **fwlog.txt** file. The event log entry will contain the line number and hit count for the rule that caused the packet to be logged.

Example:

Say your local network is on subnet 192.168.*.* and you want to block any packets received on **ppp 0** that were “pretending” to be on the local network and log the receipt of any such packets to the **fwlog.txt** file and to a syslog server. The filter rule would be constructed as follows:

```
block in log syslog break end on ppp 0 from 192.168.0.0/16 to any
```

break:

When the **break** option is specified it must be followed by a user-defined label name or the pre-defined **end** keyword. When followed by a label, the rule processor will “jump” to that label to continue processing. When followed by the **end** keyword rule processing will be terminated and the packet will be treated according to the last matching rule.

Example:

```
break ppp_label on ppp 0
# insert rule processing here for packets that are not on ppp 0
break end
ppp_label:
# insert rule processing here for packets that are on ppp 0
```

on:

The **on** option is used to specify the interface to which the rule applies and must be followed by a valid interface name. For example, if you were only interested in applying a particular rule to packets being transmitted or received by **ppp 0**, you would include **on ppp 0** in the rule. Valid interface-names are either **eth n** or **ppp n** where **n** is the instance number.

oneroute:

The **oneroute** option is used to specify that a rule will only match packets associated with the specified Eroute. For example, including the option **oneroute 2** would cause the rule to only match on packets transmitted or received over Eroute 2.

[tos]

The **[tos]** field may be used to specify the Type Of Service (TOS) to match. If included, the **[tos]** field consists of the keyword **tos** followed by a decimal or hexadecimal code identifying the TOS to match. For example, to block any inbound packet on PPP 0 with a TOS of 0 you would use a rule such as:

```
block in on ppp 0 tos 0
```

[proto]

The **[proto]** field is used to specify a protocol to match and consists of the **proto** keyword followed by one of the following protocol identifiers:

Identifier	Meaning
tcp, udp	TCP or UDP packet
udp	TCP packet
tcp	UDP packet
icmp	ICMP packet
decimal number	decimal number matched to protocol type in IP header

The `[proto]` field is also important when “stateful” inspection is enabled for a rule (using the `[inspect-state]` field), as it describes the protocol to inspect (see `[inspect-state]` below).

[ip-range]

The `[ip-range]` field is used to describe the range of IP addresses and ports to match upon and may be specified in one of several ways. The basic syntax is:

```
ip-range = "all" | "from" ip-object "to" ip-object [flags] [icmp]
```

where `ip-object` is an IP address specification. Full details of the syntax with examples are given under the heading “Specifying IP addresses and address ranges” below.

[inspect-state]

The `[inspect-state]` field is used in create rules for “stateful inspection”. This is a powerful option in which the firewall script includes rules that allow the unit to keep track of a TCP/UDP or ICMP session and therefore to only pass packets that match the state of a connection.

Additionally, the `[inspect state]` field can specify an optional OOS (Out Of Service) parameter. This parameter allows the unit to mark any route as being out-of-service for a given period of time in the event that the stateful inspect engine has detected an error.

A full description of how the `[inspect state]` field works is given below under the heading “Stateful inspection”.

Specifying IP addresses and address ranges.

The `ip-range` field of a firewall script rule identifies the IP address or range of addresses to which the rule applies. The syntax for specifying an IP address range is:

```
ip-range = "all" | "from" ip-object "to" ip-object [ flags ] [ icmp ]
```

where:

```
ip-object = addr [port-comp | port-range]
```

```
flags = "flags" { flags } [ !{ flags } ]
```

```
icmp = "icmp-type" icmp-type [ "code" decnum ]
```

```
addr = "any" | ip-addr [ "/"decnum ] [ "mask" ip-addr | "mask" hexnum ]
```

```
port-comp = "port" compare port-num
```

```
port-range = "port" port-num "<>" | "><" port-num
```

```
ip-addr = IP address in format nnn.nnn.nnn.nnn
```

```
decnum = a decimal number
```

```
hexnum = a hexadecimal number
```

```
compare = "=" | "!=" | "<" | "<=" | ">" | ">="
```

```
port-num = service-name | decnum
```

```
service-name = "http" | "telnet" | "ftpd" | "ftpcnt" | "pop3" | "ike" | "xot"  
| "snmp" | "smtp"
```

In the above syntax definition:

- ◆ items in quotes are keywords

- ◆ items in square brackets are optional
- ◆ items in curly braces are optional and can be repeated
- ◆ the vertical bar symbol (“|”) means “or”

An **ip-object** therefore consists of an IP address and an IP port specification, preceded by the keyword **from** or **to** to define whether it is the source or destination address. The most basic form for an **ip-object** is simply an IP address preceded by **from** or **to**. For example, to block all packets destined for address 10.1.2.98 the script rule would be:

```
block out from any to 10.1.2.98
```

An **ip-object** can also be specified using an address mask. This is a way of describing which bits of the IP address are relevant when matching. The script processor supports two formats for specifying masks.

Method 1: The IP address is followed by a forward slash and a decimal number. The decimal number specifies the number of significant bits in the IP address. For example, if you wanted to block all packets in the range 10.1.2.* the rule would be:

```
block from any to 10.1.2.0/24
```

i.e. only the first 24 bits of the address are significant.

Method 2: This same rule could be described another way using the **mask** keyword:

```
block from any to 10.1.2.0 mask 255.255.255.0
```

The IP address can also contain either “addr-ppp n” or “addr-eth n” where “n” is the **eth** or **ppp** instance number. In this case the rule is specifying that the IP address is that allocated to the PPP interface or to the Ethernet interface. This is useful in the situation were IP addresses are obtained automatically and therefore are not known by the author of the filtering rules. For example:

```
block in break end on ppp 0 from addr-eth 0 to any
```

12.2 Filtering on port numbers.

Now lets say there is a Telnet server running on a machine on IP address 10.1.2.63 and you wish to make this accessible. Using the filter from the previous example would block all packets to 10.1.2.*. To make the Telnet server available on 10.1.2.63 we need to add the following line *in front* of the blocking rule:

```
pass break end from any to 10.1.2.63 port=23
```

So, a packet being sent to the Telnet server (port 23) on IP address 10.1.2.63 will match this rule and further checking is prevented by the **break end** option.

The above example illustrates the “=” comparison. Other comparison methods supported are:

Symbol	Meaning
!=	not equal
>	greater than
<	less than
<=	less than or equal to
>=	greater than or equal to

It is also possible to specify a port in range or a port out of range with the “><” or “<>” symbols. For example, to pass all packets to addresses in the range 23 to 28, the rule would be specified as:

```
pass break end from any to 10.1.2.63 port 23><28
```

To simplify references to ports, some commonly used port numbers are associated with the pre-defined strings listed in the table below. For instance, in the example above we could substitute the number 23 with the string `telnet`. This would make the rule:

```
pass break end from any to 10.1.2.63 port=telnet
```

The other port keywords that are defined are:

Keyword	Std. Port	Service
<code>ftpd</code>	20	File Transfer Protocol data port
<code>ftpcnt</code>	21	File Transfer Protocol control port
<code>telnet</code>	23	Telnet server port
<code>smtp</code>	25	SMTP server port
<code>http</code>	80	Web server port
<code>pop3</code>	110	Mail server port
<code>sntp</code>	123	NTP server port
<code>ike</code>	500	Source/destination port for IKE key
<code>xot</code>	1998	Destination port for XOT packets

note:

The above service keywords are pre-defined based on “standard” port numbers. It is possible that these may have been defined differently on your system in which case you should use the port numbers explicitly (not the defined names).

12.3 Filtering on TCP flags.

An `ip-object` can be followed by an optional `[flags]` field. This field allows the script to filter based on any combination of TCP flags. The `[flags]` field is used to specify the flags to check and consists of the `flags` keyword followed by a string specifying the flags themselves. Each letter in this string represents a particular flag type as listed below:

Code	Flag
<code>f</code>	FIN Flag
<code>r</code>	RESET Flag
<code>s</code>	SYN Flag
<code>p</code>	PUSH Flag
<code>u</code>	URG Flag
<code>a</code>	ACK Flag

These flag codes allow the filter to check any combination of flags.

Following on from the previous example, to block packets that have all the flags set you would need to precede the pass rule with the following block rule:

```
block break end from any to 10.1.2.0/24 port=telnet flags frspua
```

Here, the list of flags causes the unit to check that those flags are set. This list may be optionally followed by an exclamation mark (“!”) and a second list of flags that the unit should check for being clear. For example:

```
flags s !a
```

would test for the `s` flag being on and the `a` flag being off with all other flags ignored.

As a further example, lets say we want to allow outward connections from a machine on 10.1.2.33 to a Telnet server. We have to define a filter rule to pass outbound connections and the inbound

response packets. Because this is an outbound Telnet service we can make use of the fact that all incoming packets will have their ACK bits set. Only the first packet establishing the connection will have the ACK bit off. The filter rules to do this would look like this:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet
```

```
pass in break end from any port=telnet to 10.1.2.33 port>1023 flags !a
```

The first rule allows the outward connections, and the second rule above allows the response packets back in which the ACK flag must always be on. This second rule will filter out any packets that do not have the ACK flag on. This will bar any attackers from trying to open connections onto the private network by simply specifying the source port as the telnet port (note that there is a simpler way to achieve the same effect using the inspect state option described below).

12.4 Filtering on ICMP codes.

An `ip-object` can be followed by an optional `[icmp]` field. This allows the script to filter packets based on ICMP codes. ICMP packets are normally used to debug and diagnose a network and can be extremely useful. However they form part of a low-level protocol and are frequently exploited by hackers for attacking networks. For this reason most network administrators will want to restrict the use of ICMP packets.

The syntax for including ICMP filtering is:

```
icmp = "icmp-type" icmp-type ["code" decnum]
```

The `icmp-type` can be one of the pre-defined strings listed in the following table or the equivalent decimal numeric value:

ICMP Type	ICMP Value
Unreach	3
Echo	8
Echorep	0
Squench	4
Redir	5
Timex	11
Paramprob	12
Timest	13
Timestrep	14
Inforeq	15
Inforep	16
Maskreq	17
Maskrep	18
Routerad	9
Routersol	10

The following two rules are therefore equivalent:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type 0
```

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep
```

Both of these rules allow echo replies to come in from interface `ppp 0` if they are addressed to our example local network address (10.1.2.*).

In addition to having a type, ICMP packets also include an ICMP code field. The filter syntax allows for the specification of an optional code field after the ICMP type. When specified the code field must also match. The ICMP code field is specified with a decimal number.

Example:

Suppose we wish to allow only echo replies and ICMP unreachable type ICMP packets from interface PPP 0. Then the rules would look something like this:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep
code 0

pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type unreach
code 0

block in break end on ppp 0 proto icmp
```

The first two rules in this set allow in the ICMP packets that we are willing to permit and the third rule denies all other ICMP packets in from this interface. Now if we ever expect to see echo replies in on **ppp 0** we should allow echo requests out on that interface too. To do that we would have the rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo
```

12.5 Stateful inspection.

The [inspect] field takes the following format:

```
inspect = ["inspect-state" { oos interface-name secs { c=number } { d=number }
{ t=number } } ]
```

The field can be used on its own or with an option **oos** (Out Of Service) parameter.

Stateful inspection is a powerful option that allows the unit to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried. To understand this better lets look at a simple example in which we want to set up a filter to allow all machines on a local network with addresses in the range 10.1.2.*, to access the Internet on port 80. We will need one rule to filter the outgoing packets and another to filter the responses:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80

pass in break end on ppp 0 from any port=80 to 10.1.2.0/24
```

In this example, the first rule allows outgoing http requests on **ppp 0** from any address matching the mask 10.1.2.* providing that the requests are on port 80 (the normal port address for http requests).

The second rule allows http response packets to be received on **ppp 0** providing they are on port 80 and they are addressed to an IP address matching the mask 10.1.2.*.

However, rule 2 creates a potential security "hole". The problem with filtering based on the source port is that you can trust the source port only as much as you trust the source machine. For instance an attacker could do a port scan and provided the source port was set to 80 in each packet, it would get through this filter. Alternatively, on an already compromised system, a "Trojan horse" might be set up listening on port 80.

A more secure firewall can be defined using the "inspect-state" option. The stateful inspection system intelligently creates and manages dynamic filter rules based on the type of connection and the source/destination IP addresses. Applying this to the above example, we can re-design the script to make it both simpler and more effective as described below.

As a consequence of the fact that only the first packet in a TCP handshake will have the SYN flag set, we can use a rule that checks the SYN flag:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80 flags s inspect-
state
```

```
block in break end on ppp 0
```

The first rule matches only the first outgoing packet because it checks the status of the **s** (SYN) flag and will only pass the packet if the SYN flag is set. At first glance however, it appears that the second rule blocks all inbound packets on PPP 0. Whilst this may be inherently more secure, it would also mean that users on the network would not be able to receive responses to their http requests and would therefore be of little use!

The reason that this is not a problem is that the stateful inspection system creates temporary filter rules based on the outbound traffic. The first of these temporary rules allows the first response packet to pass because it also will have the SYN flag set. However, once the connection is established, a second temporary rule is created that passes inbound or outbound packets if the IP address and port number match those of the initial rule but does not check the SYN flag. It does however monitor the FIN flag so that the system can tell when the connection has been terminated. Once an outbound packet with the FIN flag has been detected along with a FIN/ACK response, the temporary rule ceases to exist and further packets on that IP address/port are blocked.

In the above example, if a local user on address 10.1.2.34 issues an http: request to a host on 100.12.2.9, the outward packet would match and be passed. At the same time a temporary filter rule for is automatically created by the firewall that will pass inbound packets from IP address 100.12.2.9 that are addressed to 10.2.1.34 port x (where x is the source port used in the original request from 10.1.2.34).

This use of dynamic filters is more secure because both the source and destination IP addresses/ports are checked. In addition, the firewall will automatically check that the correct flags are being used for each stage of the communication.

The potential for a security breach has now been virtually eliminated because even if a hacker could time his attack perfectly he would still have to forge a response packet using the correct source address and port (which was randomly created by the sender of the http request) and also has to target the specific IP address that opened the connection.

Another advantage of “inspect-state” rules is that they are scaleable i.e. many machines can use the rule simultaneously. In our above example for instance many machines on the local network could all web browse the internet and the inspection engine would be dynamically creating precise inward filters as they are required and closing them when they are finished with.

The **inspect-state** option can be used on TCP, UDP protocols and some ICMP packets. The ICMP types that can be used with the “inspect-state” option are “echo”, “timest”, “inforeq” and “maskreq”.

12.5.1 Using [inspect-state] with flags.

As can be seen above, the **inspect-state** option can be used with flags. To illustrate this we will refer back to the earlier example of filtering using flags. It is possible to simplify the script by using the **inspect-state** option. The original script was:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet

pass in break end from any port=telnet to 10.1.2.33 port>1023 flags a/a
```

Using the inspect state option this can be replaced with a single filter rule:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet flags s/sa
inspect-state
```

No rule is needed for the return packets because a temporary filter will be created that will only allow inbound packets to pass if they match sessions set up by this stateful inspection rule.

A further point to note about the new rule is that the “flags s/sa” specification ensures that it only matches the first packet in a connection. This is because the first packet in a TCP connection has

the SYN flag on and the ACK flag off and so we only match on that combination. The stateful inspection engine will take care of matching the rest of the packets for this connection.

12.5.2 Using [inspect-state] with ICMP.

The [inspect-state] option can be also used with ICMP codes. To allow the use of echo request and to allow echo replies you would have just the one rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo inspect-state
```

The advantage of using `inspect-state`, other than just needing one rule, is that it leads to a more secure firewall. For instance with the `inspect-state` option the echo replies are not allowed in all the time; they will only be allowed in once an echo request has been sent out on that interface. The moment that a valid echo reply comes back (or there is a timeout), echo replies will again be blocked. Furthermore, the full IP address is checked; the IP source and destination must exactly match the IP destination and source of the echo request. If you compare this to the rule to allow echo replies in without using “inspect-state” it would not be possible to check the source address at all and the destination address would match any IP address on our network.

The “inspect-state” option can be used with the following ICMP packet types:

ICMP Type	Matching ICMP Type
Echo	Echo reply
Timest	Timestrep
Inforeq	Inforep
Maskreq	Maskrep

12.5.3 Using [inspect-state] with the Out Of Service option.

The [inspect-state] field can be used with an optional `oos` parameter. This parameter allows the stateful inspect engine to mark as “out of service” any routes that are associated with the specified interface. Such routes will only be marked as out of service if the specified `oos` option parameters are met. The `oos` parameter takes the format:

```
oos interface secs {t=number} {c=number} {d=number}
```

where:

interface specifies the interface with which the firewall rule is associated e.g. `ppp 1`.

secs specifies the length of time in seconds for which the routes that are using the specified interface are marked as out of service.

{t=number} is an optional parameter that specifies the length of time in seconds the unit will wait for a response the packet that matched the rule.

{c=number} is an optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the route is marked as out of service.

{d=number} is an optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the interface is deactivated (only applies to PPP interfaces).

UDP example.

```
pass in
pass out
pass out on ppp 1 proto udp from any to 156.15.0.0/16 port=1234 inspect-state
oos ppp 1 300 t=10 c=2 d=2
```

The first two rules simply configure the unit to allow any type of packets to be transmitted or received (the default action of the firewall is to block all traffic).

The third rule is more complex. What it does is to configure the stateful inspection engine to watch for UDP packets (with any source address) being routed via the **PPP 1** interface to any address that begins with 156.15 on port 1234. If a hit occurs on this rule but the unit does not detect a reply within 10 seconds (as specified by the **t=** parameter), it will increment an internal counter. When this counter reaches the value set by the **c=** parameter, the stateful inspection engine will mark the **PPP 1** interface (and therefore any routes using it), as being out of service for 300 seconds. Similarly, if this counter matches the **d=** parameter the stateful inspection engine will deactivate **PPP 1**. So in the above example, the stateful inspection engine will mark any routes that use **PPP 1** as out of service AND deactivate **ppp 1** if no reply is detected within 10 seconds for two packets in a row.

Routes will come back into service when either the specified timeout expires or if there are no other routes with a higher metric in service.

PPP interfaces will be re-activated when either the routes using them are back in service and there is a packet to route the **AODI mode** parameter is set to On.

TCP example

```
pass out break end on ppp 3 proto tcp flags s inspect-state oos ppp 3 30 t=10
c=2
```

This rule will specifically trace attempts to open socket connections on **PPP 3** and if they fail within 10 seconds twice in a row, will cause the **PPP 3** interface to be flagged as out of service (i.e. it's metric will be set to 16), for 30 seconds. Again, if a matching route with a lower metric has been defined it will then be used whilst **PPP 3** is out of service thus providing a powerful route-backup mechanism.

12.5.4 Assigning DSCP values.

When using QOS, packet priorities will be determined by the DSCP values in their TOS fields. These priorities may have already been assigned but if necessary, the router can be configured to assign them by inserting the appropriate rules in the firewall. This is done by using the **dscp** command.

For example:

```
dscp 46 in on eth 0 from 100.100.100.25 to 1.2.3.4 port=4000
```

would set the DSCP value to 46 for almost any type of packet received on ETH 0 from IP address 100.100.100.25 addressed to 1.2.3.4 on port 4000. This allows you to set the DSCP value for almost any type of packet.

As a further example:

```
dscp 46 in on eth 0 proto smtp from any to any
```

would cause outgoing mail traffic to the same top priority queue (46 is by default a very high priority code in the DSCP mappings).

12.6 The fwlog.txt File.

When the **log** option is specified within a firewall script rule, an entry is created in the **fwlog.txt** pseudo-file each time an IP packet matches the rule. Each log entry will in turn contain the following information:

Timestamp	The time when the log entry is created.
Short Description	Usually "FW LOG" but could be "FW DEBUG" for packets that hit rules with the "debug" action set.
Dir	Either "IN" or "OUT". Indicates the direction the packet is travelling.
Line	The line number of the rule that cause the packet to be logged.

Hits	The number of matches for the rule that caused this packet to be logged.
Iface	The Interface the packet was to be transmitted/received on.
Source IP	The source IP address in the IP packet.
Dest. IP	The destination IP address in the IP packet.
ID	The value of the ID field in the IP packet.
TTL	The value of the TTL field in the IP packet.
PROTO	The value of the protocol field in the IP packet. This will be expanded to text as well for the well-known protocols.
Src Port	The value of the source port field in the TCP/UDP header.
Dst Port	The value of the source port field in the TCP/UDP header.
Rule Text	The rule that caused the packet to be logged is also entered into the log file.

In addition, port numbers will be expanded to text pre-defined port numbers.

12.6.1 Log File Examples

Example: log entry without the **body** option:

```

----- 15-8-2002 16:25:50 -----
FW LOG Dir: IN Line: 11 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 39311
TTL: 128
PROTO: TCP (6)
Src Port: 4232 Dst Port: WEB (80)
pass in log break end on eth 0 proto tcp from 100.100.100.25 to
addr-eth 0
flags S/SA inspect-state
-----

```

Example: log entry with the **body** option:

```

----- 15-8-2002 16:27:56 -----
FW LOG Dir: IN Line: 7 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 40140
TTL: 128
PROTO: ICMP (1)
block return-icmp echorep log body break end proto icmp icmp-type
echo
    From REM TO LOC IFACE: ETH 0
    45 IP Ver: 4
    Hdr Len: 20
    00 TOS: Routine
    Delay: Normal
    Throughput: Normal
    Reliability: Normal
    00 3C Length: 60
    9C CC ID: 40140
    00 00 Frag Offset: 0
    Congestion: Normal
    May Fragment
    Last Fragment
    80 TTL: 128
    01 Proto: ICMP
    0C E1 Checksum: 3297
    64 64 64 19 Src IP: 100.100.100.25

```

```

64 64 64 32      Dst IP:          100.100.100.50
ICMP:
08              Type:          ECHO REQ
00              Code:          0
04 5C           Checksum:      1116
-----

```

Example: Text included in the **eventlog.txt** pseudo-file when the **event** sub-option is specified:

```
16:26:32, 15 Aug 2002, Firewall Log Event: Line: 10, Hits: 3
```

Example: Syslog message where the **body** option is not specified:

```

2002-09-04 16:30:06  User.Info  100.100.100.50  Aug 15 16:31:59
arm.1140 IP Filter -
Filter Rule: block return-icmp unreachable host-unr in log syslog break
end on eth 0 proto tcp from any to 100.100.100.50 port=telnet
Line: 10
Hits: 4

```

Example: Syslog message with the "body" option is specified:

```

2002-08-30 16:19:59  User.Info  100.100.100.50  Aug 10 16:21:56
arm.1140 IP Filter - Filter Rule: block return-icmp unreachable port-unr
in log body syslog break end on eth 0 proto tcp from any to
100.100.100.50 port=telnet
Line: 9
Hits: 3
PKT:
Source IP: 100.100.100.25
Dest IP: 100.100.100.50
ID: 13317
TTL: 128
Protocol: TCP
Source Port: 1441
Dest Port: 23
TCP Flags: S

```

12.7 Debugging a Firewall

During the creation and management of firewall scripts, firewall scripts may need debugging to ensure that packets are being processed correctly. To assist in this, a rule with the **debug** action may be used. If a rule with the debug action is encountered, an entry is made in the **fwlog.txt** pseudo-file each time the packet in question matches a rule from that point on. This gives the administrator the ability to follow a packet through a rule set, and can help determine what, if any, changes are required to the rule set. Rules that specify the debug action would typically be placed near the top of the rule set, so that all matching rules from that point on are entered into the log file.

Entries the **fwlog.txt** file created as the result of a **debug** rule may be identified by the short description "FW_DEBUG" at the top of the log entry.

An example rule set using a **debug** rule:

```

debug in on ppp 2 proto tcp from any to any port=http

pass in break end proto tcp from any to any port=http flags s/sa inspect state

pass out break end proto udp

```

If placed at the top of the rule set, any packet received on interface PPP 2 to destination port 80 will generate a debug entry in the log file for each subsequent rule that it matches. In the example rule set above, a packet that matched the second rule would also match the first rule, and would therefore create two log entries. The same packet would not match the third rule, and so no log entry would be made for this rule.

Because of the extra processor time required to add all of these additional log entries, debug rules should be removed (or commented out) once the rule set is operating as desired.

13 Remote Management

Your 2000 series unit can be accessed and controlled remotely via the ISDN network by using:

- ◆ a V.120 connection to access the text command interface
- ◆ PPP to access the Web Interface
- ◆ PPP to access the text command interface using Telnet
- ◆ the X.25 remote command channel

Remote access via any one of these methods can be used to reconfigure the unit, upload/download files or upgrade the software, examine the event log or protocol analyser traces or to view statistics.

13.1 Remote Management Using V.120

To establish a remote access session using V.120, initiate a V.120 call as normal using the **atd** command. Enter “%%” within 5 seconds of the remote unit answering and you will be prompted to enter your username and password. Correct entry of these will allow access to the text command interface. If the remote unit has been programmed with a Unit ID string in the **Configure ► General** settings the Unit ID will appear as the command line prompt. Three login attempts are permitted before access is denied.

13.2 Remote Management Using Telnet

If you have created a PPP Dial-up Networking entry for the remote unit that you wish to access, any terminal program that supports Telnet may be used to establish a remote connection.

To initiate the connection, launch the DUN. If the remote unit is configured correctly with one of the PPP instances enabled for answering, it will connect and the linked computers icon will appear in the Windows system tray. You may then load your Telnet software.

To configure your Telnet software you must first specify that you require a TCP/IP connection and then enter the appropriate IP address or hostname (e.g. 1.2.3.4 or ss.2000r by default). After ensuring that your software is configured to connect to TCP port number 23 you may then initiate a new connection.

If the connection is successful you will see a connect confirmation message and you will be prompted to enter your username and password. Correct entry of these will allow access to the text command interface. If the remote unit has been programmed with a Unit ID string in the **Configure ► General** settings the Unit ID will appear as the command line prompt.

Three login attempts are permitted before access is denied.

13.3 Remote Management Using FTP

Your unit incorporates an FTP server. FTP allows users to log on to remote hosts for the purpose of inspecting file directories, retrieving or uploading files etc. For PC users, MS-DOS includes FTP support and there are a number of Windows-based specialist FTP client programs such as CuteFTP and Ws_ftp. Many browsers also incorporate FTP support.

To initiate remote access to a unit using FTP, first establish a PPP DUN connection to the unit and then run your FTP software.

13.3.1 FTP under Windows

Once the connection has been established, enter the Web address for the unit. By default this will be:

1.2.3.4 or ss.2000r

If you are using a browser, as opposed to a specific FTP program, you will need to precede the address with "ftp://". For example:

ftp://ss.2000r

This will give you an anonymous FTP login to the remote unit and you should see a listing of the file directory (the format of this will depend on the FTP client software that you are using). With an anonymous login you will be able to view and retrieve files, but NOT upload, rename or delete them.

For full file access, you will need to log in with your correct username and password. To do this, enter the address in the following format:

ftp://username:password@ss.2000r

This will give you full access and will allow you to copy, delete, rename, view and transfer files.

When using a browser CUT, COPY, DELETE and PASTE may be used for manipulating files as if they were in a normal Windows directory. If you are using a specific FTP client program, these operations may be carried out using menu options or buttons.

13.3.2 FTP under DOS

To use FTP under DOS, use Windows DUN to establish the connection and then run the MSDOS prompt program. At the DOS prompt type:

ftp SS.2000R

or

ftp 1.2.3.4

When the connection has been established you will be prompted to enter your username and password. Following a valid login the **ftp>** prompt will be issued and you may proceed to use the various ftp commands as appropriate. To obtain a list of available commands enter "?" at the prompt.

13.4 Remote Management Using X.25

Remote access to your unit may also be carried out over an X.25 connection. The remote unit must first have its **X.25 Remote Command Sub-address** parameter set to an appropriate value (see **Configure ► General**). If the unit then receives an incoming X.25 call where the trailing digits of the NUA match the specified sub-address, the calling user will receive the standard login prompt. On entry of a valid username and password, they will be given access to the command line as if they were connected locally.

14 The Event Log

14.1 What Is The Event Log?

The 2000 series automatically maintain a log of certain types of event in a pseudo file called **eventlog.txt**. The contents of the log can be viewed via the **Status ► Event Log** web page or using by using the **type** command. In either case, the most recent event appears at the top of the log with successively older log entries appearing further down.

The example below shows a small section of a log:

```
16:30:09, 02 Jun 2000, PPP 0 Up
16:30:09, 02 Jun 2000, PPP 0 Start IPCP
16:30:09, 02 Jun 2000, PPP Login OK By Paul Lvl 3
16:30:09, 02 Jun 2000, PPP 0 Start PAP
16:30:09, 02 Jun 2000, PPP 0 Start LCP
16:29:51, 02 Jun 2000, Power Up
```

The **eventlog.txt** pseudo-file acts as a circular buffer so that when the space available for the log is full, new entries are written at the start of the buffer overwriting the oldest entries.

Each entry in the log normally consists of a single line containing the date, time and a brief description of the event. In some cases it may also identify:

- ◆ the type/number of the protocol instance that generated the message (e.g. PPP 0)
- ◆ a reason code
- ◆ additional information such as an X.25 address or ISDN telephone number

The specific events that generate a log entry are pre-defined and cannot be altered. These are listed in the table below along with the name of the firmware module that generates the event message and any additional information that may be included in the log.

Event	Description	Originating module	Comment
01	Power up	Event logger	n/a
02	Event log cleared	Event logger	n/a
03	Reboot	Command	n/a
04	Layer 2 protocol up	LAPB, LAPD, PPP, V120	n/a
05	Layer 2 protocol down	LAPB, LAPD, PPP, V120	n/a
07	Login success	FTP, PPP, Command, Webserver	Username
08	Login fail	FTP, PPP, Command, Webserver	Username
09	Time set / changed	Command	OK or FAIL
13	Web server re-starting	Webserver	n/a
14	Protocol negotiation started	PPP	IPCP, LCP, PAP
15	Async > sync PPP started	PPP	n/a
16	Event delay	Event logger	n/a
17	SMTP request to send email	SMTP	Template filename
18	SMTP send successful	SMTP	n/a
19	SMTP request rejected	SMTP	n/a
20	SMTP request failed	SMTP	n/a
21	Telnet session closed	TCP Utilities	n/a
22	New logcodes.txt file	Flash memory mgr.	n/a
23	Config. Request	SMTP	n/a
24	Anonymous FTP login	FTP	Password

25	FTP session closed	FTP	n/a
26	X.25 CALL request Rx'd	X.25	Called address
27	X.25 connection made	X.25	n/a
28	X.25 CALL cleared	X.25	n/a
29	X.25 CLEAR request Rx'd	X.25	n/a
30	X.25 incoming call Rx'd	X.25	Calling address
31	LAPB call request sent	ISDN call control	Called party number
32	LAPD call request sent	ISDN call control	Called party number
33	LAPB call clear request Rx'd	ISDN call control	n/a
34	LAPD call clear request Rx'd	ISDN call control	n/a
35	LAPB clearing call	ISDN call control	n/a
36	LAPD clearing call	ISDN call control	n/a
37	LAPB incoming call	ISDN call control	Calling party num.
38	LAPD incoming call	ISDN call control	Calling party num.
39	Starting Backup X.25 call	X.25	n/a
40	Watchdog had occurred	Bootloader	n/a
41	Command returned error	Command	Command
42	V120 Disconnect	V120	n/a
43	LAPB Inactivity	LAPB	n/a
44	BIOS Buffers Warning	BIOS	n/a
45	IP Sending ACT_RQ	TCP/IP	source IP, dest IP, dest port
46	Sending DNS Query	TCP/IP	name being queried
47	Data Trigger Match	PAD	Data Trigger String
48	Async Transmit Watchdog	ASYNC	n/a

14.2 The logcodes.txt File

The precise content and format of each entry in the event log, and event priority levels, can be changed by editing the **logcodes.txt** file. This file lists each of the event numbers along with associated priority codes and a string that defines the content and appearance of the log entry. The file is terminated with a line containing the text [END].

14.2.1 Event blocks

Each event block starts with a line containing the text [EVENTS]. This is followed by a line for each event code in the following format:

```
<event code>,<priority code>,<description>
```

where:

<event code> values are pre-defined and should not be changed.

<priority code> values can be set between 0 and 9 to suit your application.

<description> can be edited to suit your application.

The description field may also contain the following format "specifiers":

Specifier	Function
%a	insert protocol instance or B-channel number as appropriate
%c	insert comment field
%e	insert protocol type
%s	insert SAPI field or user access level as appropriate

For example, the [EVENT] block entry:

```
31,3,%e B%a ISDN call req #: %c
```

would generate an entry in the **eventlog.txt** file that would appear similar to:

```
LAPB B1 ISDN call req #: 01234567890
```

where the %e expands to “LAPB”, %a expands to “1” and the %c gives the called party telephone number.

14.2.2 Reason blocks

An event block may be followed by a [Reasons] block containing additional information that will be appended to the event log entry. The reason codes included in these blocks apply to all entries in the preceding [EVENT] block.

Each reason block starts with a line containing the text [REASONS]. This is followed by a separate line for each reason code in the format:

```
<reason code>,<priority code>,<description>
```

The reason codes, and the events to which they apply, are pre-defined and should not be changed. However, as with the event block entries, the associated priority codes and text descriptions may be edited to suit your requirements.

If the priority code is left blank in a reason entry, the reason code will have the same priority as the event to which it applies. Setting the reason priority code to a higher value than its parent event code can be used to cause the event logger to generate an email when the event itself would not normally do so.

14.2.3 Editing the file

A full listing of a typical **logcodes.txt** file is included under the heading Logcodes.txt. To edit the file you will need to copy it from the unit onto your PC. It may then be changed to suit your requirements using a simple text editor such as Windows Notepad. Once the changes are complete, you must then download the new version into the unit.

The format of the logcodes.txt file is strictly defined. Failure to adhere to the formatting rules may result in erroneous or misleading log entries.

15 AT Commands

15.1 D Dial

The **atd** command causes the unit to initiate an ISDN call. The format of the command depends on the mode of operation.

When using the unit to make data calls on one of the B-channels, enter the **atd** command followed by the telephone number. For example, to dial 01234 567890 enter the command:

```
atd01234567890
```

Spaces or hyphens in the number are ignored. If the call is successful the unit will issue the **CONNECT** result code and switch to on-line mode.

Dialling with a specified sub-address

The **atd** command may also be used to route a call to an ISDN sub-address by following the telephone with the letter **s** and the required sub-address. The sub-address may be up to 15 digits long. For example:

```
atd01234567890s003
```

Dialling stored numbers

To dial numbers that have previously been stored within the unit using the **at&z** command, insert the **s=** modifier within the dial string. For example, to dial stored number 3 using the command:

```
atds=3
```

Combining ISDN and X.25 calls

A further option for the **d** command for X.25 applications is to combine the ISDN call and the subsequent X.25 CALL in the same command. To do this, follow the telephone number with the "=" symbol and the X.25 call string. For example:

```
atd01234 567890=123456789
```

Pressing any key while the **d** command is being executed will abort the call attempt.

15.2 H Hang-up

The **ath** command is used to terminate an ISDN call. If the unit is still on-line you must first switch back to command mode by entering the escape sequence i.e. **+++**, wait 1 second and then enter an **at** command or just **at<CR>**.

After entering the **ath** command the call will be disconnected and the **NO CARRIER** result will be issued.

15.3 Z Reset

The **atz** command is used to load one of the stored profiles for the active ASY port. The command is issued in the format **atzn** where n is the number (0 or 1) of the ASY port profile you wish to load.

15.4 &C DCD Control

The **at&c** command is used to configure the way in which the unit controls the DCD signal to the terminal. There are three options:

- &c0** DCD is always On
- &c1** DCD is On only when an ISDN connection has been established
- &c2** DCD is normally On but goes Off for the length of time set by S10 after a disconnect.

15.5 &F Load Factory Settings

The **at&f** command is used to load a pre-defined default set of S-register and **at** command settings (the Factory profile). These are:

```
e1, v1, &c1, &k1, &d2, S0=0, S2=43
```

All other values are set to 0.

15.6 &V View Profiles

The **at&v** command displays a list of the current **at** command and S register values, and the settings for the two stored profiles. For example:

```
at&v
CURRENT PROFILE:
&c1 &d2 &k1 e1 q0 v1 &y0
S0=0 S2=43 S12=50 S31=3 S45=5

STORED PROFILE 0:
&c1 &d2 &k1 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5

STORED PROFILE 1:
&c1 &d2 &k1 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5
OK
```

15.7 &W Write sregs.dat

The **at&w** command is used to save the current command and S registers settings (for the active port), to the file **sregs.dat**. The settings contained in this file can be re-loaded at any time using the **atz** command.

The **at&w** command may be immediately followed by a profile number, either 0 or 1, to store the settings in the specified profile, for example:

```
at&w1
```

would store the current settings as profile 1. If no profile number is specified, profile 0 is assumed.

All S register values and the following command settings are written by **at&w**:

```
e, &c, &d, &k
```

15.8 &Y Set Default Profile

The **at&y** command is used to select the default power-up profile (0 or 1). For example, to ensure that the unit boots up using stored profile 1, enter the command:

```
at&y1
```

15.9 &Z Store phone number

The **at&z** command is used to store “default” telephone numbers within the unit that may subsequently be dialed when DTR dialling is enabled or by using the **s=** modifier in the **atd** dial command. One telephone number may be stored for each **ASY** port. For example to store the phone number 0800 123456 as the default number to be associated with **ASY 2**, use the command:

```
at&z2=0800123456
```

If the number of the **ASY** port is not specified, the number will be stored against the port from which the command was entered i.e. entering the command:

```
at&z=0800123456
```

from **ASY 3** has the same effect as:

```
at&z3=0800123456
```

from any port. Once a number has been stored it may be dialed from the command line using the **atd** command with the **s=** modifier:

```
atds=3
```

This means that any stored number can be dialed from any port. If DTR dialling has been enabled by setting **s33=1** for the port, the number associated with that port will be dialed when the DTR signal for that port changes from **Off** to **On** i.e. DTR dialling can only be used with the number associated with the port to which the terminal is connected.

15.10 \LS Lock Speed

The **atlls** command is used to lock the speed and data format of the port at which it is entered to the current settings so that the non-**at** application commands may be used.

15.11 \PORT Set Active Port

Text commands which affect the settings associated with the serial ports normally operate on the port at which they are entered i.e. entering the **at&k** command from a terminal connected to **ASY 1** will affect only the flow control settings for port 1.

The **at\port** command is used to select a different “active” port from that at which the commands are entered. For example, if your terminal is connected to port 0 and you need to re-configure the settings for port 2, you would first enter the command:

```
at\port=2
```

```
PORT 2
```

```
OK
```

Port 2 is now the active port and any **at** commands or changes to S registers settings which affect the serial ports will now be applied to port 2 only. This includes:

Commands: z, &d, &f, &k, &v, &y, &w,

S registers: s31, s45

The **at\port?** command will display the port to which you are connected and the active port for command/S register settings. For example:

```
at\port?
```

```
PORT 2
```

```
ASY0  
OK
```

Here, ASY2 is the active port and ASY0 is the port at which the command was entered. If the default port and the port to which you are connected are the same, only one entry will be listed.

To reset the default port to the one to which you are connected use the **at\port** command without a parameter.

15.12 **\at** Ignore invalid AT commands

This command is a work-around for use with terminals that generate large amounts of extraneous text. If not ignored, this text can cause many error messages to be generated by the Sarian unit, and may result in a communications failure. To turn on this feature, type the following command:

```
at\at=1
```

To turn off the feature, type the following command:

```
at\at=0
```

When this feature is turned on, the ASY port ignores all commands except real **at** commands. As with other ASY modes this can be saved by **at&w** but is not displayed via **at&v**. To determine whether or not this mode is enabled type:

```
at\at ?
```

The unit will display 0 if the feature is Off, 1 if it is On.

16 “S” Registers

In addition to the **at** commands there are a number of Special (“S”) registers. These registers contain numeric values that may represent time intervals, ASCII characters or operational flags.

To display the contents of a particular “S” register, the **ats** command is used in the form **atsn?** where **n** is the number of the register whose contents are to be shown.

To store a new value into a register, use the **S** command in the form **atsn=x** where **n** is the number of the register to be changed and **x** is the new value. For example, **ats31=4** would store the value 4 in **s31**.

The unit maintains one set of registers for each ASY port. By default, the “S” command operates ONLY on the register set for the active port. To select an alternative default port, use the **at\port=** command first.

Each register can only be set to a limited range of values as shown in the table below:

Reg.	Description	Units	Default	Range
S0	V.120 Answer enable	Rings	0	0-255
S2	Escape character	ASCII	43	0-255
S12	Escape delay	ms	50	0-255
S15	Data forwarding timer	ms	2	0-255
S23	Parity	0 (none), 1 (odd) or 2 (even)	0	0-2
S31	ASY interface speed	refer to full description	n/a	0-11
S33	DTR dialling	0 (off), 1 (on)	0	0,1
S45	DTR loss de-bounce	0.05 seconds	(0.25s)	1-255

16.1 S0 V.120 Answer Enable

Units rings
Default 0
Range 0-255

s0 is used only in V.120 mode to enable or disable automatic answering of incoming ISDN calls. Auto-answering is disabled when **s0** is set to the default value of 0. Setting **s0** to a non-zero value enables auto-answering.

The actual value stored determines the number of “rings” that the unit will wait before answering. For example, the command **ats0=2** enables auto-answering after two incoming rings have been detected.

With each ring the **RING** result code is issued and the value stored in **s1** is incremented. When the value in **s1** equals the value in **s0** the call is answered.

16.2 S2 Escape Character

Units ASCII
Default 43
Range 0-255

The value stored in S2 defines which ASCII character is used as the **Escape character**, which by default is the “+” symbol. Entering this character three times followed by a delay of 1-2 seconds and then an **at** command will cause the unit to switch from on-line mode to command mode.

16.3 S23 Parity

Units N/A
 Default 0
 Range 0-2

The value stored in **s23** determines whether the parity used for the ASY port is set to None (0), Odd (1) or Even (2).

16.4 S15 Data forwarding timer

Units 10ms
 Default 0
 Range 0-255

s15 is used to set the data forwarding timer for the ASY port in multiples of 10ms. The default data forwarding time is 20ms and in normal use this there should be no need to change this. However, setting **s15** to 1 enables a special mode of operation in which data is forwarded as fast as possible for the data rate for which the port is configured (at 115000bps this will typically be 2-3ms).

Note that the default value of 0 is equivalent to setting the register to 2 in order to maintain compatibility with older systems.

16.5 S31 ASY Interface Speed

Units N/A
 Default 0
 Range 0-11

Register **s31** is used to set the speed and data format for the ASY port to which you are currently connected.

The default value for ASY 0 is 0 i.e. the port speed/data format is not set to a specific value, it is determined automatically from the **at** commands that you enter.

The default value for ASY 1, 2 and 3 is 3 i.e. the ports will only accept **at** commands at 115,200bps (8 data bits, no parity and 1 stop bit).

To set the speed of one of the ports to a particular value, the appropriate register should be set to the required value from the following table:

S31	Port speed (bps)
0	Auto-detect
1	Reserved
2	Reserved
3	115,200
4	57,600
5	38,400
6	19,200
7	9,600
8	4,800
9	2,400
10	1,200
11	300

For example, to change the speed of ASY 1 to 38,400bps, connect your terminal to that port with the speed set to 9600bps. Enter the command:

```
ats31=5
```

then change the speed of your terminal to 38,400bps before entering any more AT commands.

The data format used when the **ats31=n** command is entered is selected as the data format for all further commands.

The auto-detect option is only available for ASY0 and ASY1.

16.6 S33 DTR dialling

Default 0
Range 0, 1

s33 is used to enable or disable DTR dialling for the port. When DTR dialling is enabled, the unit will dial the number stored for that port (see **at&z** when the DTR signal from the terminal changes from Off to On.

16.7 S45 DTR Loss De-bounce

Default 5
Range 1-255

The value in **s45** determines the length of time for which the DTR signal from the terminal device must go off before the unit acts upon any options that are set to trigger on loss of DTR. Increasing or decreasing the value in **s45** makes the unit less or more sensitive to “bouncing” of the DTR signal respectively.

17 General System Commands

The application commands described in this section are basic configuration commands that do not relate to specific types of application or network.

17.1 CONFIG Show/Save Configuration

The **config** command is used for the following purposes to to show current or stored configuration settings, to save the current configuration or to specify which configuration is to be used when the unit is powered up or rebooted.

The format of the **config** command is:

```
config <0|1|c> <save|show|powerup>
```

Two separate configurations can be stored, numbered 0 and 1. The first parameter of the **config** command specifies to which configuration the command applies. The letter “c” denotes the current configuration settings, i.e. those currently in use.

The second parameter is one of the following keywords:

show displays the specified configuration (either **0**, **1** or **c** for the current configuration)

save saves the current settings as the specified configuration (either **0** or **1**)

powerup sets the specified configuration (either **0** or **1**) to be used at power-up or reboot.

For example, to display the current configuration use the command:

```
config c show
```

The output will appear similar to the following example:

```
bind PAD 0 ASY 0
pad 0 l2iface LAPB
cmd 0 username sarian
cmd 0 epassword Oz57X0kd
cmd 0 hostname IR2140
OK
```

The config files only contain details of those settings that are different from the unit’s default settings. If you make a setting that is the same as the default setting, it will not appear in a stored configuration.

To save the current settings to configuration file 1, use:

```
config 1 save
```

To use configuration 1 when the unit is powered up or rebooted, use:

```
config 1 powerup
```

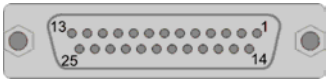
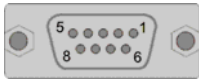
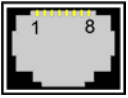
17.2 REBOOT Reboot Unit

The **reboot** command causes the unit to execute a complete hardware reset, loading and running the main image file from cold.

18 ASY port connectors

Depending upon the model, the asynchronous serial ports on 2000 series routers may be presented as a 25-way D sockets, 9-way D sockets or 8-pin RJ45 sockets.

On some models, a combination of the above may be used. The following table lists the pin designations for each type of connector:

		25-way D	9-way D	RJ45
				
Description	RS232 signal	Pin #	Pin #	Pin #
Transmit data	TxD	2	3	6
Receive data	RxD	3	2	3
Ready to Send	RTS	4	7	1
Clear to Send	CTS	5	8	8
Data Set Ready	DSR	6	6	4
Ground	GND	7	5	5
Data Carrier Detect	DCD	8	1	7
Transmitter Clock	TxC	15	n/a	n/a
Receiver Clock	RxC	17	n/a	n/a
Data Terminal Ready	DTR	20	4	2
External Transmitter Clock	ETC	24	n/a	n/a

A range of suitable adapters and cables are available from Sarian Systems.

19 Logcodes.txt

The following is a listing of a typical **logcodes.txt** file. You can edit this file with a text editor to change the events that generate automatic e-mails. Once you have finished editing, save the changes and copy the file onto your unit using FTP.

```
[EVENTS]
01,0,Power-up
40,0,Watchdog
02,1,Clear Event Log
03,0,Reboot
04,3,%e %a up
86,,New IPsec SA created by %c
[EVENTS]
83,,FTP Client Req By %e to %c
[REASONS]
1,,Retry
[EVENTS]
84,,FTP Client Session Closed
[REASONS]
1,,Normal closure
2,,Socket closed
3,,No socket ID available
4,,No connection to remote
5,,No stored confirmation
6,,Internal error
7,,Bad response to command
8,,No response to command
9,,Bad State
[EVENTS]
89,,FTP Client Session Closing
[REASONS]
1,,Inactivity
2,,New Request Received
3,,Transfers Completed
[EVENTS]
87,,New Phase %a IKE Session
[REASONS]
0,,Initiator
1,,Responder
[EVENTS]
88,,IPsec SA Deleted ID %c
[REASONS]
0,,Rolled
1,,Replaced
2,,Remote Deleted
3,,Timed Out
4,,Bytes Ran Out
5,,WEB
6,,Link Deactivated
[EVENTS]
08,3,Login failure by %c: %e
[REASONS]
1,,x25
```

3,,Telnet
4,,v120
5,,IKE
[EVENTS]
09,6,Time set/changed %c
14,2,%e %a Start %c
15,1,PPP %a async-sync
17,1,SMTP req by %e email %c
18,0,SMTP success
21,0,Telnet session closed
22,0,New logcodes.txt file
23,0,Config req by %e
24,0,Anonymous FTP by %c
25,0,FTP session closed
26,0,%e %a X25 Call req #: %c
27,0,%e %a Call req connect
29,0,%e %a Clearing X25 call
30,0,%e %a Inc X25 call #: %c
31,0,%e B%a ISDN call req #: %c
32,0,%e %a ISDN call req #: %c
37,0,%e B%a Inc ISDN call #: %c
38,0,%e %a Inc ISDN call #: %c
33,0,%e B%a Clearing ISDN call
34,0,%e %a Clearing ISDN call
39,0,%e %a Starting Backup X25 Call
41,0,CMD %a Error Result: %c
42,0,V120 %a Disconnect
43,0,LAPB %a Inactivity Timer
44,0,Warning - Req %a bios buffers
45,0,IP Act_Rq to %e %a-%s: %c
46,0,DNS Query on [%c]
47,0,%e %a Data Trigger: %c
48,0,ASY %a Transmit Watchdog
49,9,Tester Unit Email
50,0,%e %a No Transaction Response
51,0,%e %a Overlapped Transactions
52,0,%e %a SAPI 16 Up
53,0,%e %a SAPI 16 Down
55,0,SMTP Retry
56,0,%e %a Excessive Tran Time
57,0,PPP %a Busy. Mapped to PPP %s
58,0,Default Route Out Of Service
59,0,Static Route %a Out Of Service
60,0,Default Route Available
61,0,Static Route %a Available
62,0,DNS Query Failed on [%c]
63,0,Tcpdial Command Failed
64,0,TID Authorising Active
65,0,TID Authorising Off
66,4,%e %a Not Polled
68,0,%e %a X25 Call gone,L2 failed
69,0,%e %a X25 Deactivated
70,0,Eventlog Counters Reset
71,0,Eventlog Max/Day Reached
72,0,DIONE login failed
73,0,S Reg 0 changed %a -> %s
74,0,TCP Req: %c

2000 Series Reference guide

```
[EVENTS]
75,7,%e alarm, machine %s, %c
[REASONS]
01,7, Failed
02,7,Error detected
03,7, Empty
04,7, Critical
05,7, Soap empty, FAIL
06,7, Errors during cycle, FAIL
[EVENTS]
77,0,%e %a Connection Opened %c
78,0,%e %a Connection Closed
85,0,%e %a Orderly Shutdown
81,0,V110 User Rate %c
[EVENTS]
67,0,TPAD %a TID change %c
[REASONS]
01,,Login
02,,Ready
03,,Abort
04,,Conflict Removal
[EVENTS]
05,0,%e %a down
[REASONS]
01,,Inactivity
02,,Remote disconnect
03,,LL disconnect
04,,Upper layer req
05,2,Negotiation failure
06,6,Retransmit failure
07,,DISC transmit
08,5,TEI failure
09,5,TEI lost
10,,Lower deactivated
11,,DISC receive
12,,B Channel clr
13,,Protocol failure
14,,PPP PING Failure
[EVENTS]
07,0,%e Login OK by %c lvl %s
[REASONS]
01,,X25
03,,TELNET
04,,V120
[EVENTS]
10,0,Username %a change to '%c'
11,0>Password %a change
12,0,Hostname change to '%c'
[REASONS]
01,,WEB
02,,CMD
03,,SNMP
[EVENTS]
13,4,WEB restart
[REASONS]
01,,BALLOC fail
[EVENTS]
```

```

16,0,Event delay
[REASONS]
01,,Logger busy
[EVENTS]
19,2,SMTP reject %e
[REASONS]
01,,SMTP busy
02,,NULL template
03,,Recd unexpected data
04,,No Destination Address

[EVENTS]
20,2,SMTP err
[REASONS]
01,,No connection
02,,Socket err
03,,Link err

[EVENTS]
28,0,%e %a X25 call cleared
[REASONS]
01,,Busy
09,,Out of order
17,,Rem proc err
19,,Local proc err
25,,Rev charg not acc
33,,Incom dest
41,,Fast select not sup
57,,Ship absent
03,,Inv facility req
08,,Access barred
11,,Access barred
05,,Net congestion
13,,Not obtainable
21,,RPOA out of order
128,,No response to Call
129,,Restarted.
130,,No buffers.

[EVENTS]
35,0,%e B%a ISDN Call Cleared
36,0,%e %a ISDN Call Cleared
[REASONS]
03,,No route to dest
16,,Normal clearing
17,,User busy
18,,No user
19,,No answer
21,,Call rejected
34,,No cct
38,,Net oor
44,,Req cct not av
50,,Fac not sup
57,,Bearer not auth
58,,Bearer not avail
63,,Service not avail
88,,Incomp dest

```

2000 Series Reference guide

90,,Dest incomplete

[EVENTS]

54,0,SNTP Client

[REASONS]

01,0,Time Set Request

02,1,Retries Exceeded

[EVENTS]

76,0,%e %a Resetting Modem

[REASONS]

01,,Requested by user

02,,No response to commands

03,,CTRL-E heartbeat stopped

04,,Modem enabled or disabled

[EVENTS]

79,0,%e %a Open Failed

[REASONS]

05,,Incompatible line conditions

10,,No lock possible

15,,Protocol error

20,,Message error

25,,Spurious ATU detected

30,,Requested bitrate too high for G.lite

35,,Interleaved profile required for G.lite

40,,Forced silence

45,,Unselectable operation mode

[EVENTS]

80,0,%e %a Initialisation Failed

[REASONS]

01,,Firmware not present

02,,No free buffers

03,,Bad firmware file

04,,Hardware not present

05,,Firmware execution error

[EVENTS]

90,,ISDN Line State Change F%a -> F%s

[EVENTS]

82,,FTP Client Transfer [%c] Completed

[REASONS]

00,,Success

01,,File Not Transferred

02,,Error During Transfer

03,,Couldn't Open File

[EVENTS]

91,,IKE Negotiation Failed

[REASONS]

1,,Retries Exceeded

2,,Inactivity

3,,Bad Packet

4,,No SA Found

5,,No Transform Selected

6,,No Password Available %c

7,,Rx Key Exchange Failed

8,,Rx Nonce Failed
9,,Rx ID Failed
10,,Authorisation Failed
11,,No IKE Available
12,,Rx SA Failed
[EVENTS]
92,,IKE Keys Negotiated
93,,IKE Request Received From IPSec
94,,IKE SA Deleted
95,,GPRS link failed -> power cycle
[END]

20 Email Templates

One of the principal features provided by the event log function is the ability to configure the unit to automatically generate and send an email each time an event of a specified priority, or higher, occurs. The format of the message is determined by the email template specified in the **Configure ► Event Handler ► Email Template** field (normally **event.eml**).

If the standard **event.eml** template supplied with the unit is not suitable, you may create your own template. An email template is simply a text file that defines the appearance and content of the email messages generated by the event logger.

20.1 Template Structure

An email template consists of a header section followed by a body section. One or more blank lines separate the two sections.

The Header Section

The header section **MUST** contain the following three fields:

To:

This field is used to specify at least one recipient's email address. Multiple addresses may be included and must be separated by a space, comma or semicolon character. For example:

To: 123@456.co.uk, 456@123.co.uk; abc.def.co.uk

From:

The "From:" field is normally used to supply the email address of the sending unit but alternatively you may enter a simple string. For example:

From: IR2140

Subject:

The "Subject:" field should contain a string describing the subject of the email message.

Other fields

In addition to the mandatory fields described above, the header section of an email may also contain one or more optional fields. Many such fields are defined in the relevant RFC's but there are some fields that the unit handles a little differently as described below. The unit will insert other fields as necessary if it is required to send attachments with the email

Reply To:

If the unit discovers that this field is not present in the email template, the unit will insert this field into the header. The string used for this field is that configured by the "smtp 0 reply_to" text command (or the "Default Reply Address" field in the Configure > SMTP web page). This allows for different reply addresses, and allows a simple way of using the same (easily configurable) reply address for all emails.

Date:

If this field is present in the header, the unit will insert the current date and time into the header. The date and time are values local to the unit and do not contain any time zone information.

Body Section

The body section may include any text. This text is parsed for any function calls that may be present. Function calls must be enclosed between “<%” and “%>”. These sequences are substituted by text resulting from the function call. The following functions may be used:

Function	Description
TimeSmtplib();	Inserts the unit's date and time.
serial_number();	Inserts the unit's serial number
Smtplib();	Inserts the IP address of the unit as seen by the SMTP server during transmission
email_event()	Inserts a formatted description of the event that caused the email transmission.
Smtplib()	Inserts the unit ID for this device as configured by the “unit identity” field in the Configure > General web page, or the “cmd 0 unitid” text command.
ppplib(“instance”);	Inserts the IP address for a specific PPP instance, where <i>instance</i> is the PPP instance number.

The following are examples of email templates.

1)

```
TO: 123@abc.co.nz
FROM: MyRouter
SUBJECT: Remote Configuration
Time: <% timeSmtplib(); %>
Serial Number: <% serial_number(); %>
Req: CFG_RQ
IP Address: <% smtplib(); %>
PPP 0 IP address: <% ppplib( "0" ); %>
```

2)

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0
Unit: <% smtplib() %>
Event: <% email_event(); %>
This event had sufficient priority to cause the transmission of this
email. Please check the attached logs and review.
```

INDEX

- A**
- access level 52, 109, 173
 - Access Point Name See GPRS: APN
 - active port 22, 176, 177, 179
 - activity timer
 - LAPB 27, 62
 - adapt
 - statistics 127
 - AH protocol 151
 - Always On Dynamic ISDN See AODI
 - ana.txt 28, 29, 134
 - displaying 134
 - answering calls 23, 26, 33, 36, 60, 84, 179
 - AODI
 - NUA 85
 - APACS See TPAD
 - application commands 22
 - ASY ports
 - statistics 127
 - AT commands 20
 - &c 175
 - &f176
 - &v 176
 - &w 35, 125, 176
 - &y 126, 176, 177
 - \AT 178
 - d 175
 - h 175
 - \ls 177
 - \LS 22
 - \port 177
 - s 179
 - z 126, 175
 - auto-answering 179
 - auto-configuration 55
 - auto-start macro 51
- B**
- BACP 89
 - Bandwidth Allocation Control Protocol See BACP
 - B-channel
 - activation 61, 77
 - deactivation 77
 - indicators 7
 - ISDN number 102
 - status 136
 - X.25 94, 143
- C**
- calling numbers 36
 - text commands 36
 - channel bonding See MLPPP
 - CHAP 89
 - character echo 20, 34
 - cmd command 55
 - command mappings 37
 - config
 - command 125, 182
 - power up 125
 - saving changes 125
 - config files 125
 - power-up 51
 - configuration 24
 - pages 25
 - saving changes 25
 - connectors 183
- D**
- data encryption
 - 3DES 151
 - AES 151
 - DES 151
 - data forwarding timer 180
 - data limit
 - reset day of month 91
 - stop level 91
 - warning level 91
 - D-channel
 - always on connection 92
 - bandwidth management 63
 - restart delay 105
 - restarts 105
 - statistics 131, 132
 - window size 63
 - X.25 143
 - DHCP 37
 - lease time 38
 - server status 134, 135
 - dial command 175
 - Dial-up Networking Connection 12, 76, 170
 - dir command 135
 - DNS 54
 - server 38, 41, 86
 - DNS update 39
 - statistics 128
 - DTE/DCE mode
 - LAPB 60
 - LAPD 62
 - DUN See Dial-up Networking Connection
 - Dynamic DNS See DNS
 - Dynamic Eroutes
 - statistics: 129
 - Dynamic Host Configuration Protocol See DHCP
- E**
- email
 - date field 190
 - From field 45, 50, 55, 190
 - Reply to field 190
 - Subject field 45, 50, 55, 190
 - template 44, 50, 191
 - To field 45, 50, 55, 190

trigger priority	44	HDLC	59, 99
Eroute		High Level Data Link Control	See HDLC
text commands	73		
<i>Eroutes</i>	70		
escape		I	
character	21, 34, 179, 180	IGMP	42
delay	34	status	136
escape sequence	21	IKE	
ESP protocol	151	debug	29
eth command	43	text commands	69
Ethernet		IKE protocol	151
statistics	128	inactivity timeout	
Ethernet interface	41	PPP	86
address	41	inactivity timer	
speed	42	LAPB	60
event handler	44, 105	Internet Group Management Protocol	See IGMP
event log	172	IP	
eventlog.txt	44, 135, 172	address	41
		address translation	42
F		gateway	38
file directory	135	heartbeat packets	91
file transfer	See XMODEM	over X.25	92
File Transfer Protocol	See FTP	ping requests	90
filenames	138	route down time	54
files		routes	64
checking	139	statistics	128
copying	138	IP routes	
deleting	138	text commands	66
displaying	139	IPSec	67
listing	139	NAT Traversal	69
moving	139	statistics	129
renaming	139	transport mode	151
filing system	138	tunnel mode	151
Firewall	46	ISDN	
flow control	34, 63	B-channels	7
hardware	17	BRI connector	8
X.25	148	D64S mode	63
front panel	7, 25	MSN	142
FTP	170, 184	status	136
NAT port	54	sub-address	142
relay agents	49		
fw.txt	46	L	
fwstat.txt	47	LAPB	59
		activity timer	27
G		configuration	59
general purpose IP sockets	54	inactivity timer	60
general settings	51	passive timer	61
GPRS		RR timer	60, 62
aerial	9	sync port	60
APN	56	text commands	61
configuration	56	LAPD	62
PIN number	57	keep active	62
signal strength	11	parameters	62
SIM card installation	9	statistics	131
status indicators	52	text commands	64, 75
GSM	See GPRS	LCN	92
		Link Access Procedure Balanced	See LAPB
H		Link Access Protocol D-channel	See LAPD
hang-up command	175	load factory settings	176
		logcodes.txt	173
		logging in	24

Logical Channel Number	See LCN	protocol bindings	94
		pseudo-file	28, 29, 44, 134, 135
		pseudo-port	143
M			
MD5 protocol	151		
MLPPP	76, 86		
parameters	76		
text commands	78		
MSN	26, 60, 84, 85, 142		
Multi-link PPP	See MLPPP		
Multiple Subscriber Numbering			
see MSN	26		
N			
N400 re-try counter	61, 62		
NAT	42, 87		
static mappings	98		
text commands	98		
Network Address Translation	See NAT		
NAT	87		
Network User Identity	See NUI		
NUA			
calling	92		
TPAD	102		
NUI			
mappings	75		
TPAD	103		
nuimap command	75		
O			
Out Of Service routes	159		
P			
PAP	89		
parity	180		
parity settings	34		
password	18, 24, 109, 110		
PPP	85		
Point to Point Protocol	See PPP		
power adapter	8		
power-up profile	See profile		
PPP	76		
advanced parameters	88		
dialout number	85		
inactivity timeout	86		
over X.25	92		
standard parameters	84		
statistics	130		
sub-configurations	83		
text commadns	88, 91		
profile	125		
loading	34, 175		
saving	34, 176		
set default	176, 177		
viewing	176		
Profiles	125		
protocol analyser	28		
configuration	28		
text commands	30		
R			
rate adaptation	26		
text commands	27		
rear panel	8		
reboot command	182		
reject calls	36		
remote command			
address	52		
timeout	52		
remote connection			
establishing	23		
remote management	170		
using FTP	170		
using Telnet	170		
using V.120	170		
using X.25	171		
reset switch	See user switch		
result codes	21, 22, 34		
RIP			
interval	54		
version	42		
route metrics	65		
Routing Information Protocol	See RIP		
RTS/CTS	See flow control		
S			
S registers	20, 21, 176, 179		
S31	22		
saving	176		
save configuration	125		
secondary hostname	52		
secondary IP address	52		
serial number	25, 51		
serial ports			
configuration	33		
connector pinouts	183		
connectors	9		
DCD signal	33, 175		
DTR signal	33, 181		
interface speed	34		
lock speed	177		
naming	53		
set active port	177		
speed	180		
text commands	35		
serial ports			
lock speed	22		
SHA-1 algorithm	151		
Short Message Service	See SMS. See SMS		
Simple Mail Transfer Protocol	See SMTP		
Simple Network Management Protocol	See		
SNMP			
Simple Network Time Protocol	See SNTP		
SMS			
alarms	44, 56, 95		
editing messages	95		

parameters	45, 57	terminal ID	103, 105
template	45	text commands	107
SMTP	95	transaction delay	107
text commands	96	Transaction PAD	See TPAD
SNMP		U	
community string	53	unit ID	25, 51, 170
destination address	54	user name	18, 19, 24, 109, 110, 145
enterprise name	53	PPP	85
enterprise number	53	X.25	145
traps	45	user switch	9
SNTP	97, 100	user task	
text commands	97	filename	55
sregs.dat	125	username	109
statistics	127	users	
clearing	127	access level	109
status		configuration	109
DHCP server	135	password	109
status indicators	25, 52	text commands	109
status pages	134	user name	109
STX/ETX framing	103	V	
sub-address	26, 60, 85	V.110	26
subnet mask	38, 41	fixed rate	27
sync channel		user rate	27
statistics	130	V.1206, 20, 26, 29, 33, 94, 95, 107, 141, 142, 170, 179	
sync ports	99	answering calls	141
system files	138	LAPB parameters	27
system hostname	52	making calls	141
T		mode	26
T1 timer	60, 63	view profiles	176
T200 timer	60, 63	VPN	See Virtual Private Networks
TCP/IP	18	VPN's	152
keep-alive	53	W	
socket inactivity timer	53	web address, default	19
TEI	63	web directory	
Telnet	170	status	136
mode	53	web server	
Terminal Endpoint Identifier	See TEI	status	137
terminal ID		Windows driver	12
TPAD	103	X	
time		X.25	143
setting	100	aborting calls	146
text commands	100, 101	answering NUA	112
time bands	87, 100	auto-macro	112
TPAD		backup interface	114
configuration	102	backup interface parameters	93
data trigger	107	B-channel	143
deactivation timer	104	call user data	103
direct mode	106	calling NUA	112
excessive transaction time	105	calling user data	146
layer 2 interface	104	Closed User Groups	145
LRC	106	configuration	112
merchant number	104	data trigger	114
message numbering	103	D-channel	143
packet size	104		
parity	106		
response timeout	105		
responses	106		
re-transmit	106		
statistics	131		
STX/ETX deletion	106		

2000 Series Reference guide

default packet size	112	statistics	132
fast select	144	status	137
inactivity timeout	113	STX/ETX framing	114
layer 2 interface	112	switch	120
LCN	92, 112	switch mappings	124
load PAD profile	120	text commands	114
macros	110	X.25 over TCP/IP	See XOT
Network User Identity	145	X.28	143
NUA	104, 113	X.28 commands	143
NUI	75, 113	X.29	143
packet size	92	X.3	143
PAD parameters	115	X.31	143
PAD profile	113	X.509 certificates	69, 152
prompt	113	X.75	26
remote command subaddress	171	XMODEM	
restarts	93, 113	file transfer	140
reverse charging	145	XON/XOFF	See flow control
save PAD profile	120	XOT	120, 122