

VIPER

Voice Over IP Enterprise Router

Configuration Manual

Rev 2.1 August 2007



INDEX

Section 1	Introduction	
1.1	Overview of the VIPER	1.1
1.2	About this Manual	1.1
Section 2	Viper Application Guide	2.1
2.1	Introduction to VIPER software variations.	2.1
2.2	VIPER Software.	2.1
2.3	VLINE Software	2.2
2.4	Multi-Drop VLINE Software	2.2
Section 3	VIPER Hardware	3.1
3.1	VIPER Chassis	3.1
3.2	Viper LEDs	3.2
3.3	WAN and Voice Ports	3.3
3.4	Wide Area Ports.	3.4
3.4.1	Clocking.	3.4
3.4.2	ISDN	3.4
3.4.3	2Mbps E1 G703 / 704 Viper	3.4
3.5	Voice Option Cards	3.5
3.5.1	FXS and FXO Cards	3.5
3.5.1.1	Configuring the card for FXS: To a telephone Handset	3.5
3.5.1.2	Configuring the card for FXO: To PABX	3.6
3.5.2	E&M Cards	3.7
3.5.2.1	Configuring the card for E & M	3.7
3.5.3	Configuring the card for AC15.	3.8
3.5.4	Basic Rate ISDN Card	3.9
3.5.5	Primary Rate ISDN Card	3.10
Section 4	Viper Installation Guide	4.1
4.1	Initial Connections	4.1
Section 5	Quick Start - Basic Configuration	5.1
5.1	Basic VIPER Configuration - Routing	5.1
5.1.2	Basic routing over X21 or V35.	5.1
5.1.3	Configuring two Vipers back to back	5.5
5.1.4	Basic routing over ISDN.	5.5
5.1.5	Basic routing via the Ethernet port (Working as a Voice Gateway)	5.9
5.2.1	Basic FXO, FXS, E&M or AC15 configuration	5.12
Section 6	Advanced VIPER Configuration	6.1
6.1.1	Entering Debug Monitor Mode	6.1
6.2	Erasing configuration.	6.1
6.2.1	Saving and restoring configuration	6.1
6.3	Bridging mode	6.2
6.4	Adjusting the FXO, FXS and E&M Voice level	6.3
6.5	AC15 Voice level	6.4

6.6	ISDN back up of an X21 or V35 WAN link	6.4
6.6.1	PAP configuration for ISDN links	65
6.6.2	Numbered WAN links	6.7
6.6.3	Power Reset the Viper	6.11
Section 7	IP Networking	7.1
7.1.1	IP Addresses	7.1
7.1.2	IP Address Mask	7.2
7.1.3	IP Address Subnets	7.3
7.1.4	Different Subnet Sizes	7.3
7.1.5	IP Routing	7.3
7.1.6	IP Routing Metrics	7.4
7.1.7	Selecting IP Addresses	7.4
7.1.7.1	The traditional IP addressing scheme	7.4
7.1.7.2	The unnumbered interface scheme	7.5
7.1.8	Guidelines for choosing IP addresses	7.6
7.1.8.1	Do not use IP addresses, which are not reserved for you	7.6
7.2	Introduction to IPX Networking	7.7
7.2.1	IPX Addresses	7.7
7.2.2	Learning the IPX Network Number	7.7
7.2.3	IPX Routing	7.7
7.2.4	IPX Routing Metrics	7.8
7.3	Protocols	7.8
7.3.1	ARP - Address resolution protocol	7.8
7.3.2	RIP - Routing Information Protocol	7.8
7.3.3	IPX SAP - Service Advertising Protocol	7.9
7.4	Call Charge Limiting	7.9
7.5	ISDN Call Management	7.10
7.5.1	ISDN Number Configuration	7.10
7.5.2	Minimum Call Length	7.11
7.6	IP Express	7.12
Section 8	Viper Menu System	8.1
8.1	General Menu Operation	8.1
8.2	Main Menu	8.3
8.3	GLOBAL Menu	8.4
8.3.1	GLOBAL ISDN Menu	8.5
8.3.2	GLOBAL ISDN CHARGES Menu	8.6
8.3.3	GLOBAL ISDN MSN Menu	8.8
8.3.4	GLOBAL ISDN MSN <i>item</i> Menu	8.8
8.3.5	GLOBAL ISDN ACCESS Menu	8.9
8.3.6	GLOBAL ISDN ACCESS <i>day</i> Menu	8.10
8.3.7	GLOBAL ISDN TIMES Menu	8.11
8.3.8	GLOBAL SNMP Menu	8.11
8.4	NETWORK Menu	8.12
8.4.1	NETWORK <i>name</i> Menu	8.13
8.5	NETWORK <i>name</i> IP Menu	8.14
8.5.1	NETWORK <i>name</i> IP RIP Menu	8.16
8.5.2	NETWORK <i>name</i> IP ROUTES	8.16
8.5.3	NETWORK <i>name</i> IP ROUTES <i>ip</i> Menu	8.17

8.5.4	NETWORK <i>name</i> IP TRANSLATE Menu	8.18
8.5.5	NETWORK <i>name</i> IP TRANSLATE IN Menu	8.18
8.5.6	NETWORK <i>name</i> IP TRANSLATE IN TCP Menu	8.19
8.5.7	NETWORK <i>name</i> IP TRANSLATE IN TCP <i>rule</i> Menu	8.19
8.5.8	NETWORK <i>name</i> IP TRANSLATE IN TCP <i>rule</i> PATTERN Menu	8.20
8.5.9	NETWORK <i>name</i> IP TRANSLATE IN TCP <i>rule</i> NEWSRC Menu	8.21
8.5.10	NETWORK <i>name</i> IP TRANSLATE IN UDP Menu	8.22
8.5.11	NETWORK <i>name</i> IP TRANSLATE IN UDP <i>rule</i> Menu	8.23
8.5.12	NETWORK <i>name</i> IP TRANSLATE IN UDP <i>rule</i> PATTERN Menu	8.23
8.5.13	NETWORK <i>name</i> IP PIPE Menu	8.24
8.5.14	NETWORK <i>name</i> IP PIPE PRIOR Menu	8.25
8.5.15	NETWORK <i>name</i> IP PIPE PRIOR <i>name</i> PATTERN Menu	8.25
8.6	NETWORK <i>name</i> PPP Menu	8.26
8.6.1	NETWORK <i>name</i> PPP PAP Menu	8.27
8.6.2	NETWORK <i>name</i> PPP CHAP Menu	8.28
8.6.3	NETWORK <i>name</i> PPP BAND Menu	8.29
8.7	NETWORK <i>name</i> IPX menu	8.30
8.7.1	NETWORK <i>name</i> IPX NETWORKS Menu	8.31
8.7.2	NETWORK <i>name</i> IPX ROUTES Menu	8.32
8.7.3	NETWORK <i>name</i> IPX ROUTES <i>route</i> Menu	8.33
8.7.4	NETWORK <i>name</i> IPX SAPS Menu	8.34
8.7.5	NETWORK <i>name</i> IPX SAPS <i>sap name</i> Menu	8.34
8.8	NETWORK <i>name</i> ISDN Menu	8.35
8.8.1	NETWORK <i>name</i> ISDN DIALLIST Menu	8.36
8.8.2	NETWORK <i>name</i> ISDN NUMBER Menu	8.37
8.8.3	NETWORK <i>name</i> ISDN CLILIST Menu	8.38
8.9	NETWORK <i>name</i> CHANNELS Menu	8.39
8.10	HARDWARE Menu	8.40
8.10.1	HARDWARE MSPEED Menu	8.41
8.10.2	HARDWARE ETHERNET Menu	8.41
8.10.3	HARDWARE X21 Menu	8.42
8.11	ADMIN Menu	8.43
8.11.1	ADMIN ARP Menu	8.44
8.11.2	ADMIN ARP <i>ip</i> Menu	8.44
8.11.3	ADMIN IPRROUTE Menu	8.45
8.11.4	ADMIN IPRROUTE <i>ip</i> Menu	8.46
8.11.5	ADMIN IP ROUTE FLAGS <i>TYPE</i> Menu	8.47
8.11.6	ADMIN IPRROUTE <i>ip</i> FLAGS Menu	8.48
8.11.7	ADMIN IPXROUTE Menu	8.49
8.11.8	ADMIN IPXROUTE <i>ipx</i> Menu	8.50
8.11.9	ADMIN IPXROUTE <i>ipx</i> ROUTER Menu	8.51
8.11.10	ADMIN IPXROUTE <i>ipx</i> FLAGS Menu	8.51
8.11.11	ADMIN SAP Menu	8.52
8.11.12	ADMIN SAP <i>sap</i> Menu	8.53
8.11.13	ADMIN PHYSICALS Menu	8.54
8.12	STATUS Menu	8.55
8.12.1	FXS Status	8.56
8.12.2	FXO Status	8.57
8.12.3	AC15 Status	8.57
8.12.4	BRI Status	8.58
8.12.5	PRI Status	8.58

8.12.6	ISDN Status	8.58
8.13	STATISTICS Menu	8.59
8.13.1	IP – IP Statistics	8.59
8.13.2	ICMP RECEIVE - ICMP RECEIVE Statistics	8.59
8.13.3	TCP – TCP Statistics	8.60
8.13.5	UDP – UDP Statistics	8.60
8.13.6	SNMP1 – SNMP1 Statistics	8.61
8.13.7	SNMP2 – SNMP2 Statistics	8.61
8.13.8	ETHERNET STATISTICS	8.61
8.14	WAN STATISTICS Menu	8.62
8.14.1	Statistics Menu	8.62
8.15	DEBUG menu	8.62
8.15.1	DEBUG BOUNCE Menu	8.63
Section 9	Voice Over IP Features	9.1
9.1	Voice Over IP	9.1
9.1.1	Status Screen	9.1
9.2	Configuring the Ports	9.2
9.2.1	Configuring the Ports – Analogue Cards	9.2
9.2.2	PORTTYPE Menu – FXS Option card	9.3
9.2.3	PORTTYPE Menu – FXO Option card	9.4
9.2.4	PORTTYPE Menu – E&M and AC15	9.5
9.2.5	PORTOPTS Menu – FXS Option card	9.6
9.2.6	PORTOPTS Menu – FXO Option card	9.7
9.2.7	PORTOPTS Menu – E&M and AC15 Option cards	9.8
9.3	Configuring the Ports – Digital Cards	9.9
9.3.1	VIPER HARDWARE Menu – BRI and PRI Option cards	9.9
9.3.2	PORTOPTS Menu – BRI and PRI Option cards	9.10
9.4	Configuring the Phone Book	9.11
9.5	Configuring IP Prioritisation	9.12
9.6	Frame Relay	9.13
9.6.1	Hardware Configuration	9.13
9.6.2	Link Configuration	9.14
9.6.3	HDLC Transport	9.15
9.7	Multidrop E1 Trunk VLINE	9.16
9.7.4	Configuration examples	9.20
Section 10	Upgrading and Diagnostics	10.1
10.1	Monitor Commands	10.1
10.2	Installing New Software in the Viper Routers	10.4
10.3	Remote uploading of code.	10.5
Section 11	Viper Specification	11.6
Section 12	Glossary	12.1
Appendix A	Menu Structure	
Appendix B	Cable Specifications	

Section 1

Introduction

1.1 Overview of the VIPER

The VIPER provides **IP** and **IPX** routing between a **LAN** and remote networks connected via Basic or Primary Rate ISDN, E1, V.35 or X.21 leased line and Frame Relay. Configuration is via menus, which are available directly on a local management port, or remotely over **TELNET**.

An Advanced Debug option gives access to other options within the VIPER.

The VIPER is designed to serve the needs of the small office and remote Tele-worker, providing LAN connectivity for the remote office via ISDN BRI, a digital circuit (such as Kilostream e.g.) with the option of leased line to 2Mbps.

The VIPER provides Voice over IP facilities, and support supporting (4) different physical line interface options-

- E&M (for connection directly to or between PBX equipment)
- FXS (for the direct attachment of telephones)
- FXO (for the connection to telephone ports on a PBX)
- Basic Rate ISDN (2 Basic Rate channels supporting up to 4 simultaneous calls)
- Primary Rate ISDN (E1 G703) for PBX's with a 2Mbps or PRI Interface.

1.2 About this Manual

This manual describes how to install and configure the VIPER. Although it includes basic information on how to configure networks, it should be noted that setting up IP and IPX networks is a complex business involving the configuration of other network components. You should consult other reference material for additional information on network design and configuration.

The following two sections provide the information needed to install the router and configure it as part of a very simple network. If you are already familiar with router configuration, this should provide you with enough information to get started.

Section 2 Provides an overview of the Vipers applications

Section 3 Provides descriptions of the hardware features of the VIPER and all of its variants.

Section 4 Provides an installation guide.

Section 5 Provides examples of some simple configuration to connect two VIPERs together and then add voice functionality on top of that configuration.

Section 6 Describes details of 'Advanced Configuration' features available on the VIPER.

Section 7 Provides an overview of IP Networking

Section 8 Provides details of the Vipers Menu Options.

Section 9 Provides details of the Vipers Voice Over IP Options.

Section 10 Provides an overview of diagnostics and upgrade options.

The **last three sections** provide additional technical information about the router including some information on the Multidrop E1 Trunk variant of VLINE unit, together with a glossary of terms used in this manual.

Section 2

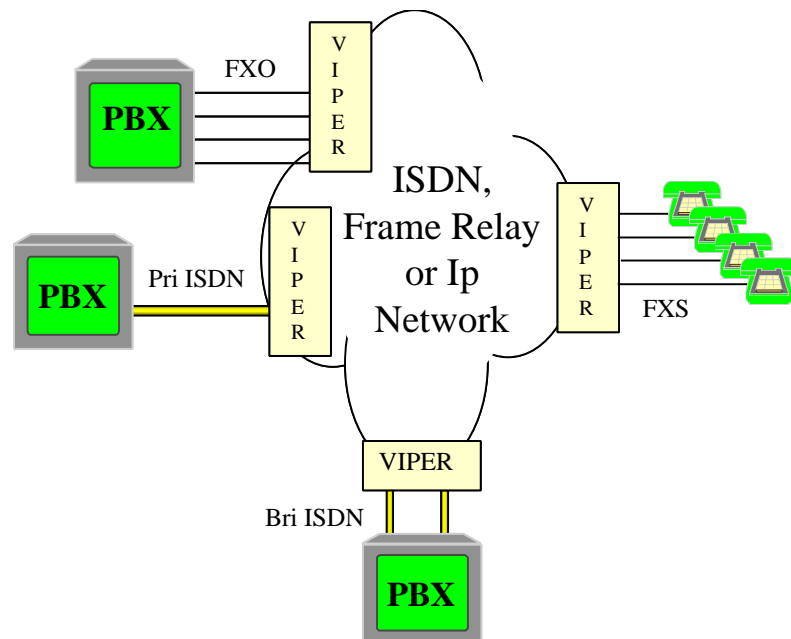
VIPER Application Guide

2.1 Introduction to VIPER software variations.

The VIPER routers while looking identical have the ability to be used in multiple different ways. There are three key sets of VIPER software, which provide enhanced functionality. This section provides a brief overview of the various flavours of VIPER.

2.2 VIPER Software.

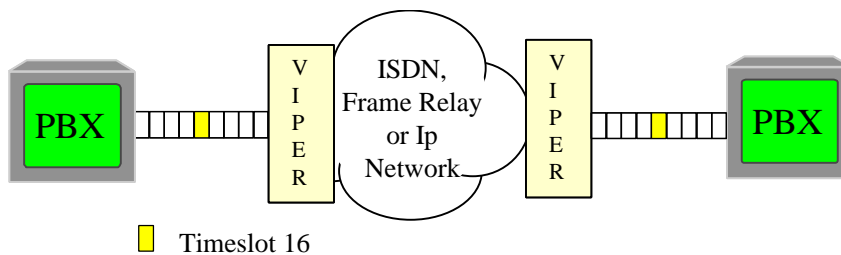
When using standard VIPER software the VIPER works as a Voice over IP Router, converting dialled digits to IP Addresses, and then using the IP network to route those calls over the IP network. In this mode the viper can provide conversion from FXS to E1 or BRI ISDN or to E&M and or FXO. The diagram below provides an overview of a network operating with 'VIPER' software.



2.3 VLINE Software

VLINE software is a point to point variation of the VIPER, allowing transportation of voice and data traffic over an IP Network. This is particularly useful when handling some of the PBX signalling systems, which require transparent data handling within Timeslot 16. Using VLINE the VIPER transports timeslot 16 transparently. VLINE may be thought of as TDM Over IP for up to 10 64Kbps PCM timeslots. When using VLINE software the VIPERs tend to have a 1 to 1 relationship with the remote VIPERs as shown in the diagram below.

Note - E&M/AC15 and FXO / FXS do not function over VLINE; it is for digital cards only.



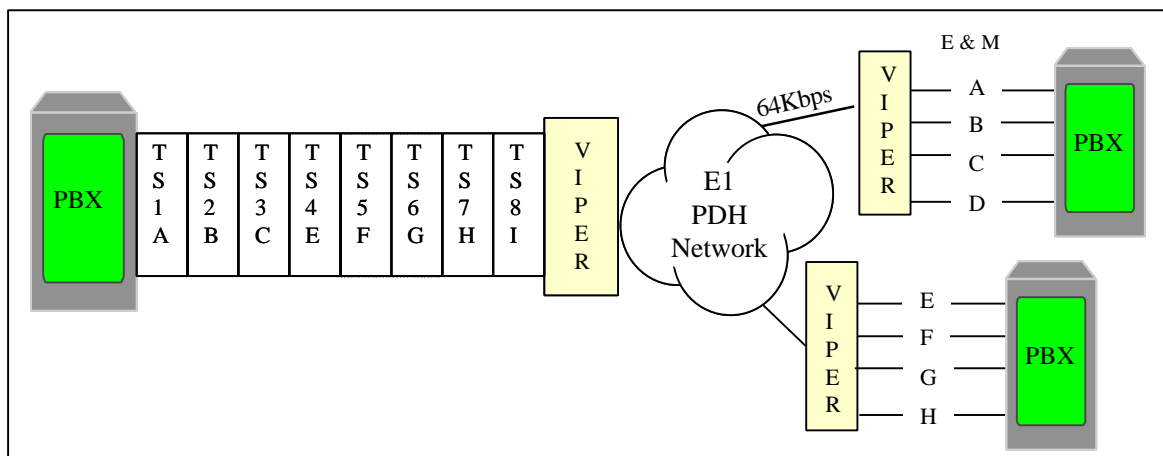
2.4 Multi-Drop VLINE Software

The VLINE software may also be used to operate over a PDH network and to provide in effect and distributed multidrop voice system, where each remote site occupies 1 x 64Kbps timeslot into which the Viper inserts multiple voice calls or various traffic mixtures.

As can be seen below at central site we are placing Voice Stream 'A' into timeslots 1, Voice Stream 'B' into timeslot 2 etc and these are routed through the network inside 1 to N 64Kbps timeslots within the PDH network to the remote site where a Viper unpacks the timeslot and supports local analogue ports, and the 1 to four traffic streams.

Note: This software requires different hardware to operate than the previous applications. The key difference is the main processor and additional hardware components.

Note: FXO / FXS do not operate over Multi-Drop VLINE E & M works in an enhanced 'Always On' state over Multidrop Vline software.



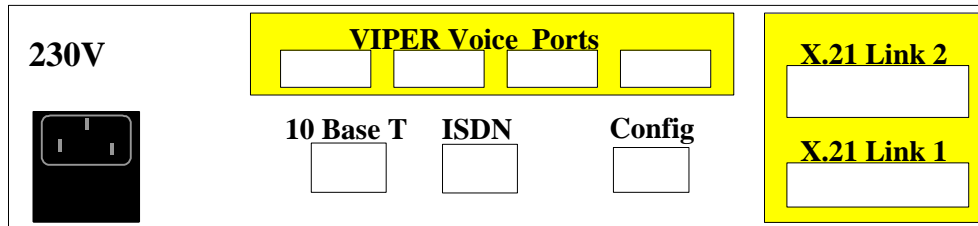
Section 3

VIPER Hardware

3.1 VIPER Chassis

The following diagram shows the rear of a standard 230-250 vac VIPER Chassis indicating the relative positions of the various connections.

Diagram of VIPER rear panel – 230 – 250 Vac Version

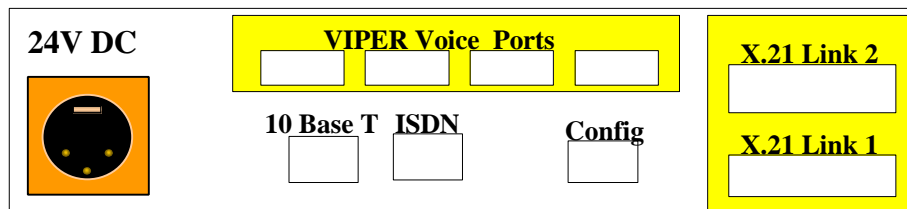


Depending on which of the VIPER variants you are using, different sockets will be available in the area labelled VIPER Voice Ports.

There is a 24-volt DC version of the VIPER.

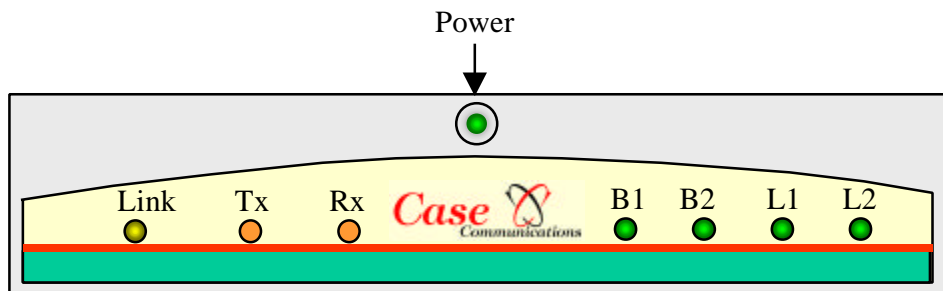
Externally this looks similar but has a circular socket for the 24-volt input as shown below.

Diagram of VIPER rear panel – 24 volt DC Version



3.2 Viper LEDs

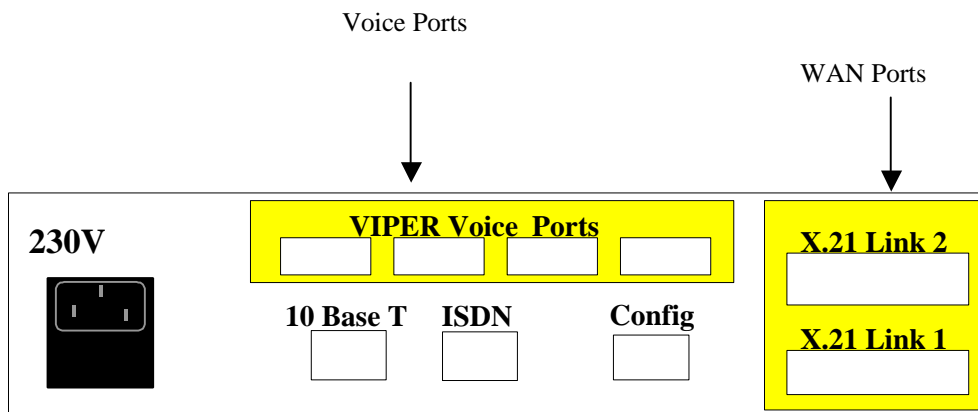
The following sections describe the functions of the LEDs visible on the front of each of the units. The diagram below shows the arrangement of LEDs on the front on the VIPER units.



- The Power LED indicates that the unit is receiving power.
- The TX and RX indicate activity on the Ethernet Interface.
- The Link light will illuminate when the unit is correctly connected to a 10BaseT network/hub.
- The L1 and L2 LEDs indicate activity on the WAN ports, i.e. WAN Link 1 and WAN Link 2.
- The B1 and B2 LEDs indicate activity on the BRI ISDN port and correspond to channel B1 and B2.

3.3 WAN and Voice Ports

The VIPER accepts a variety of Voice options, which plug into the unit displayed below as VIPER Analogue ports. The following section explains the various option cards that fit into the viper. Wide Area Ports are fitted to the VIPER in the slot on the right hand side; these can be either dual X.21 or dual V.35 ports. It is also possible to connect the VIPER to third party routers or to Ethernet switches via its LAN port and to use the VIPER as a Voice Gateway. None of these options are hot swappable. The VIPER needs to be powered down if an option card has to be removed or installed.



Depending on which of the 4 VIPER variants you are using, different sockets will be available in the area labelled VIPER Analogue Ports.

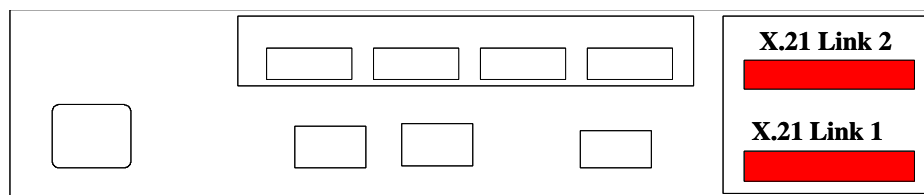
The options are

- 4 Port FXS or FXO
- 4 Port E&M or AC15
- Single Primary Rate ISDN / E1 to 2Mbps
- Dual Basic Rate ISDN Ports

3.4 Wide Area Ports.

The VIPER can support two Wide Area Ports via a dual port PIM (Port Interface Modules) fitted to the right of the VIPER as shown in the diagram below. Note Port 2 is the top port and port 1 the lower port.

There are two different types available, X21 and V35. Both are identical except they have the ports labelled with X21 or V35. These options have no strapping and are automatically recognised by the VIPER.



3.4.1 Clocking.

The VIPER WAN ports are designed to accept clocks from an external source. However WAN Link 2 is also capable of providing a clock for testing VIPERs in back to back mode and for supporting devices that are using the 'HDLC Pass through' feature.

Note that internal clocking is not needed for normal operation because the clock is provided from the leased line, but it is very useful for back-to-back testing of two VIPERs. When you set an X.21 port to generate a clock, it appears on pins 7 and 14 of the 15-pin connector. The clock applies only to transmitted data - received data is still clocked by the standard clock, which must be provided on pins 6 and 13 as usual. Some hardware ports cannot generate a clock. For these the speed is shown as a zero in brackets, like this: (0).

3.4.2 ISDN

The ISDN port on the rear of the VIPER allows the Router to operate over an ISDN network. With the standard VIPER the ISDN port is a Basic rate port, while the E1 Multi-Drop VIPER supports a 2mbps Primary Rate ISDN or E1 port

3.4.3 2Mbps E1 G703 / 704 Viper Trunk

There is a version of the Viper, which supports an E1 G.703 2Mbps Trunk, which is presented out of the Basic rate ISDN port. While the E1 Viper appears similar to the standard viper the hardware is actually a different build and uses a different processor.

3.5 Voice Option Cards

The following sections describe the various options. The pin outs of the VIPER analogue ports are provided. The connector pin outs are numbered with 1 on the left when looking at the end of the connector with the actual wire going away from you and with the lock tab at the top.

3.5.1 FXS and FXO Cards

The FXS and FXO cards are used to provide support for telephones or for PBX analogue ports, which provide long line extensions. FXO and FXS use the same card but the card is jumpered differently to allow for each mode of operation.

Note The FXO/FXS cards look similar to the AC15 / E&M cards, the way to recognise the difference is that the FXS / FXO cards have 4 transformers, while the E&M and AC15 have 8 Transformers.

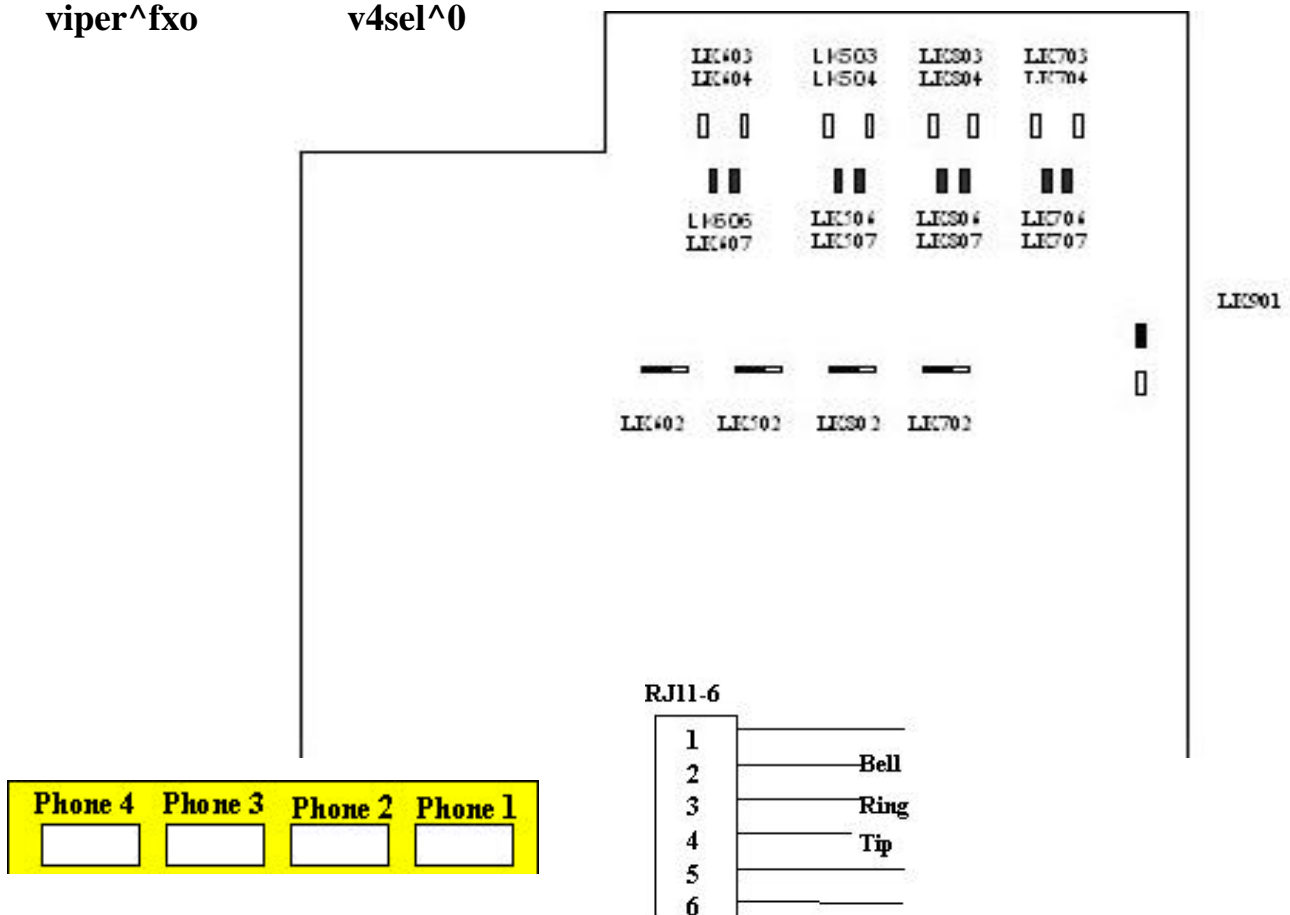
3.5.1.1 Configuring the card for FXS: To a telephone Handset

To set the card up to operate as a Foreign Exchange Subscriber (FXS) set the straps as in the diagram below FXS setting and the following command added.

In addition from the 'Debug' Menu enter the two commands: (**NB** ^ indicates a space is to be entered)

viper^fxo

v4sel^0



This option provides 4 x RJ11-6 phone sockets, into which standard Phones/Fax Machines may be connected using the short conversion cables supplied. The sockets are Master Sockets and support both Tone and Pulse Dialling. The diagram above shows how these are wired.

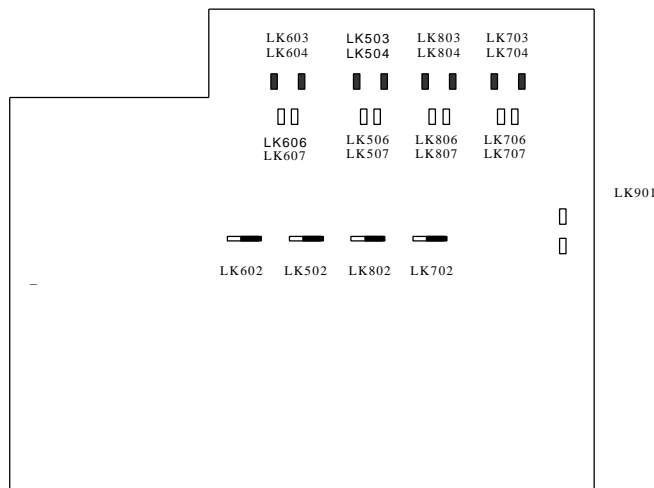
3.5.1.2 Configuring the card for FXO: To PABX

To set the card up to operate as a Foreign Exchange Office (FXO) the card needs to be strapped as shown below and the following command added.

From the 'Debug' Menu enter the following two commands. **NB** ^ indicates a space.

viper^fxs

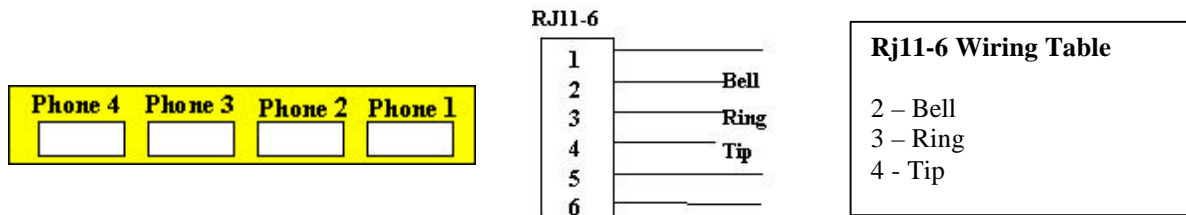
v4sel^15



Remove Straps – LK606, LK607, LK506, LK507, LK806, LK807, LK706, LK707 and LK901

Add Straps – LK603, LK604, LK503, LK504, LK803, LK804, LK703 and LK704.

Fit Straps to right – LK502, LK602, LK702 and LK802.**FXO Wiring**



This option provides 4 x RJ11-6 phone sockets, which connect to a PBX long line extension port. The sockets are Master Sockets and support both Tone and Pulse Dialling. The diagram above shows how these are wired.

3.5.2 E&M Cards

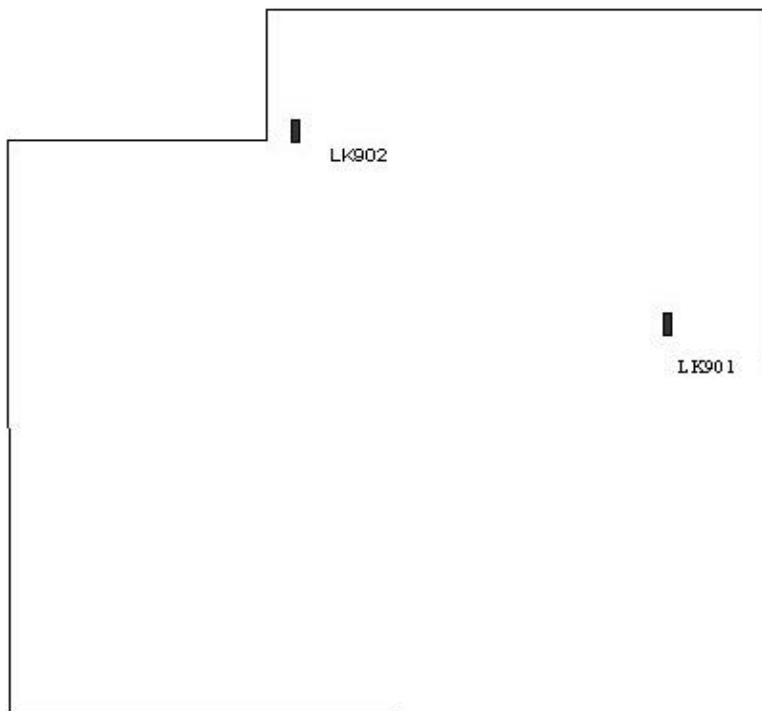
The same card is used for E&M and AC15 but strapped differently and a command is entered in the Command mode to select the required method of operation.

3.5.2.1 Configuring the card for E & M

To set the card for E & M add the straps to LK901 and LK902 (LK 901 provides -48 VDC while 902 provides signal ground) and then set the following two commands from the debug menu
 NB ^ indicates a space.

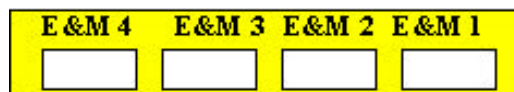
viper^e&m

v4sel^0

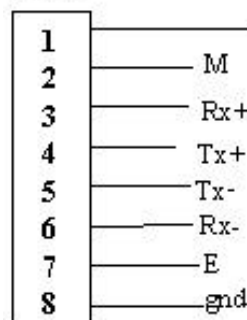


Fit
 LK901 & LK902

E&M Wiring



RJ45-8



E & M RJ 45-8 Wiring Table

2= M	←
3= Rx+	←
4=Tx+	→
5=Tx-	→
6=Rx-	←
7=E	
8= Ground	

This option provides 4 x RJ45-8 sockets for connection to the E&M ports of the PABX. Un-terminated cables are provided for this purpose. The software provides an option for 2 Wire E&M. In this case pins 4 and 5 are used for the voice path.

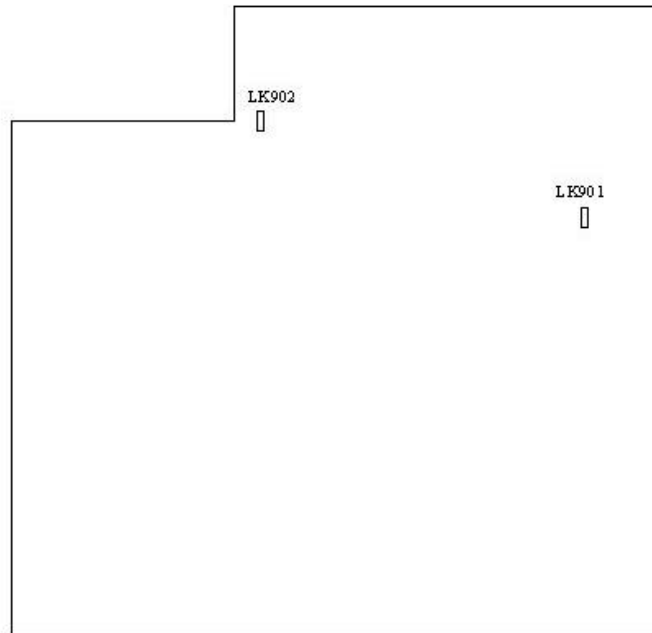
3.5.3 Configuring the card for AC15.

This option provides 4 x RJ45-8 sockets for connection to the AC15 ports of the PABX. Un-terminated cables are provided for this purpose

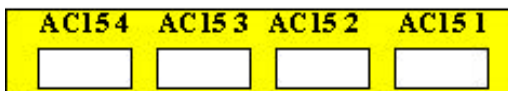
To set the card for AC15 remove the straps from LK901 and LK902 and then set the following command from the debug menu

viper^ac15

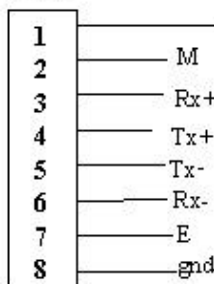
v4sel^15



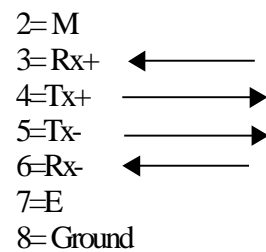
AC15 Wiring



RJ45-8



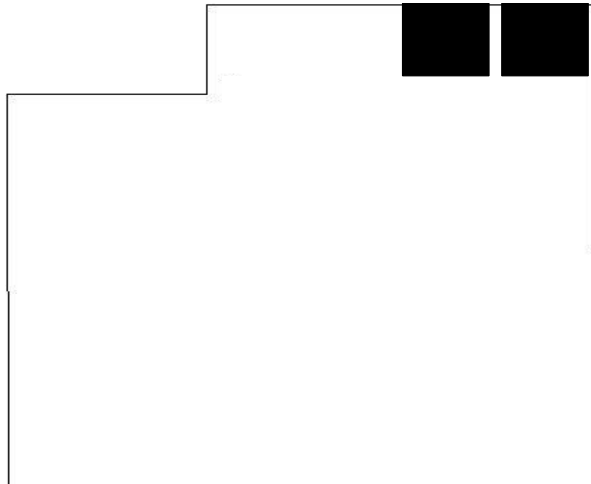
RJ 458 Wiring Table



This option provides 4 x RJ45-8 sockets for connection to the AC15 ports of the PABX. Un-terminated cables are provided for this purpose.

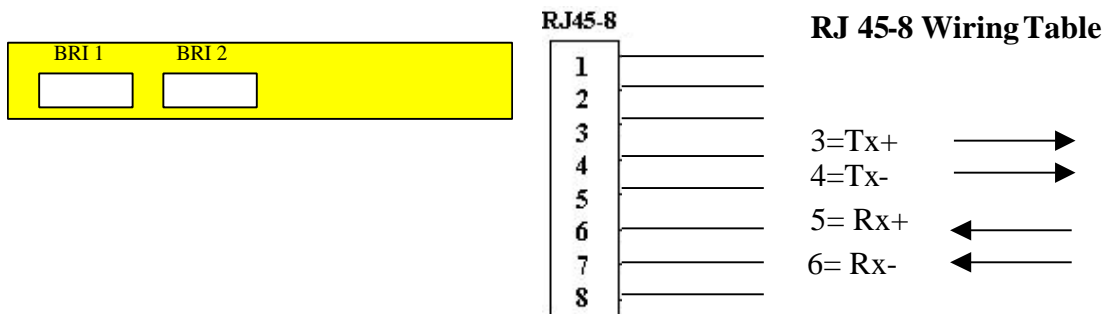
3.5.4 Basic Rate ISDN Card

The Basic Rate ISDN card provides 2 BRI ports that provide a total of 4 x B channels. Each B channel operates at 64 kbps and is meant to carry user data. There is no strapping options used on this card and it is automatically recognised by the VIPER.



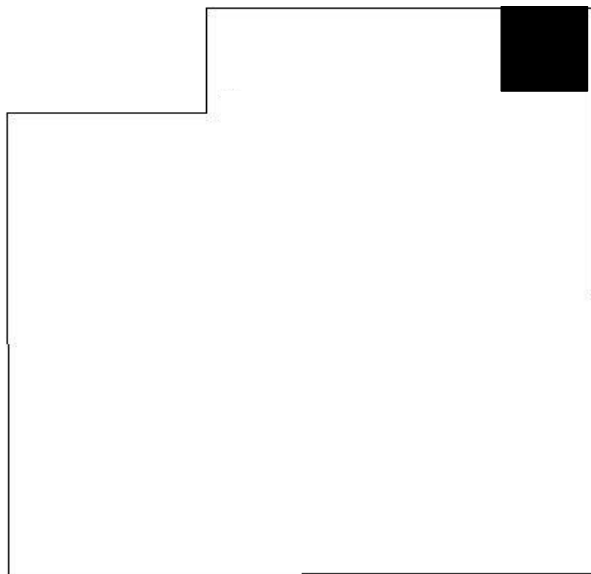
This option provides 2 x RJ45-8 sockets for connection to BRI ports of the PABX. Un-terminated cables are provided for this purpose.

BRI Card Wiring



3.5.5 Primary Rate ISDN Card

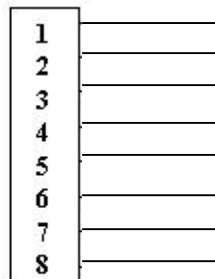
The Primary Rate ISDN card provides 1 x PRI port that provides a total of 10 x B channels. Each B channel operates at 64 kbps and carries voice into the Viper prior to compressing that voice for transmission over the network. There is no strapping options used on this card and it is automatically recognised by the VIPER. The Pri card can be used with both VLINE software transporting 10 timeslots from site A to Site B in effect providing TDM Over IP, or in full Viper mode, where the Viper looks at the dialled digits entering timeslot 16 and converting those digits to an IP Address and port on the network.



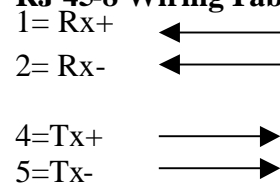
PRI Wiring



RJ45-8



RJ 45-8 Wiring Table



This option provides a single RJ45-8 sockets for connection to PRI ports of the PABX. Un-terminated cables are provided for this purpose.

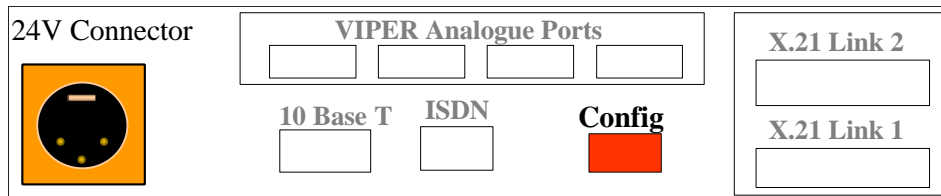
Section 4

Viper Installation Guide

4.1 Initial Connections

The router is supplied with a mains adapter to provide power. Connect this to the socket marked 230V ~50Hz as indicated on the appropriate rear view diagram below.

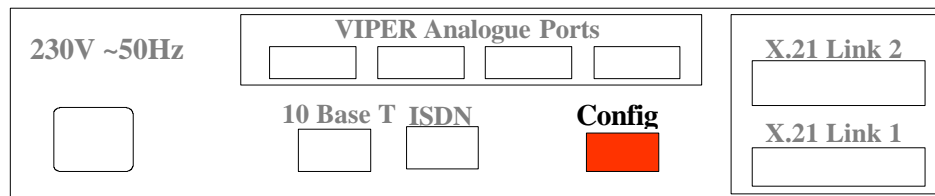
A 24 Volt DC variant is also available. The rear connectors on the DC variants are identified by a three pin circular socket as shown below:



A configuration cable is also supplied with the router. One end of the configuration cable has an RJ11 or RJ45 connector. Connect this to the port marked “Config” as indicated on the rear view diagrams below. The other end of the configuration cable has a standard V.24/RS232 9-pin connector. This is suitable for connection to a terminal or PC serial port.

Please ensure that you are using the cable supplied with the product. Connect the configuration to the RJ45 connector as shown here.

Diagram of VIPER rear panel



PC Configuration

- VT 100 Emulation
- 19200 Bps
- 8 Bits No Parity
- No Hardware Flow Control

Set your PC or terminal to 19200 bits per second, 8 bits, no parity. The configuration port only supports a 3-wire interface, so if you should disable any hardware flow control options on the Terminal or Terminal Emulation software that you are using.

Switch on the power to the router. The router will go through a power up sequence, which can take up to a minute. During this period some of the LEDs on the front panel will flash alternately to indicate that all is proceeding correctly.

After this period, you should get a menu appearing on the PC or terminal. If not, hit RETURN a few times. You should now configure the router using the information provided in the subsequent sections of the manual.

After basic configuration has been entered you may connect up the WAN, Ethernet and Voice option links.

Section 5

Quick Start - Basic Configuration

When some configuration items are changed, it is necessary to reboot the router. This can be done by power recycling the Viper, or by using the REBOOT command.

Note 1. When entering any of the configuration pages, all changes are automatically saved when you leave the option page, therefore do not experiment with changes.

Note 2 – VIPER Menu options are selected by entering the option number, to go up a level you may enter a (.) (Full stop or type in the command 'Quit'.)

Note 3 - The VIPER has been designed to allow scripting of configurations, therefore by joining various scripts together its possible to automatically re-configure the VIPER from a local terminal.

Note 4 – Its possible to upload or download VIPER configuration data to a PC, thereby saving the configuration for re-submitting at a later date.

5.1 Basic VIPER Configuration - Routing

This section will show how to set up a basic routing configuration over the X21 and, ISDN links as well as over Ethernet using the Viper as a 'Voice Gateway'. Later sections will show how to configure the voice option cards and other miscellaneous configuration details that may be of use, including ISDN backup of the X21/V35 Links

This configuration is assuming that you are starting with a VIPER unit with no configuration, ether from originally unpacking the router or from erasing the configuration.

This configuration has to be implemented so that the VIPERs know how they communicate with the outside world.

5.1.2 Basic routing over X21 or V35.

To set up basic routing on a VIPER you will need the following information:

- i. Name of the local VIPER – this can be anything, for example the location.
- ii. IP address of the Ethernet port of the VIPER including the Mask.
- iii. IP address of the remote, e.g. the remote VIPERs IP address including the Mask
- iv. The name of the remote. – e.g. its location.

For the following example we will use the local name London, IP address of the Ethernet port **10.1.1.1** and mask 255.255.255.0, remote IP of 20.1.1.1 and mask 255.255.255.0, remote name Birmingham.

This configuration gives you unnumbered WAN ports, i.e. they have no IP address assigned to them. It is possible to number them, and details of that will be covered in a later section.

The first step is to give the VIPER its name.

Serial Step 1. From the Main Menu select option 0 GLOBAL and then option 0 NAME. Enter the name London followed by RETURN.

Serial Step 2. Quit out of that menu by pressing . (full stop) once to get back to the Main Menu which now shows London Main Menu at the top of the screen.

Serial Step 3. The next step is to configure the Ethernet port with the IP address and Mask.

Serial Step 4. From the Main Menu select option 1 NETWORK to get to the following screen:

London NETWORKS		
Command	Description	Current Value
0	DEFAULT_ETH	Ethernet Interface
1	DEFAULT_WAN	Configuration In Only
&	ADD	Add new item
%	DELETE	Delete item
.	QUIT	Previous menu

Serial Step 5. Select option 0 DEFAULT_ETH to display the following screen:

London NETWORKS		
Command	Description	Current Value
0	NAME	Name
1	IP	IP configuration
2	PPP	PPP configuration
3	IPX	IPX configuration
4	ISDN	ISDN configuration
5	CHANNELS	Select channels to use
.	QUIT	Previous menu

Serial Step 6. Select option 1 'IP' to get the screen shown below:

London		
Command	Description	Current Value
0	ENABLE	IP routing
1	LOCAL	Local IP address
2	REMOTE	Remote IP address (if not Ethernet)
3	MASK	IP address mask
4	RIP	RIP
5	RIPMETRIC	RIP Metric weighting for link
6	ROUTES	Associated static routes
7	TRANSLATE	Address translation rules
8	PIPE	IP Express
9	FILTBROAD	Filter Directed Broadcast
.	QUIT	Previous menu

Serial Step 7. Select option 1 LOCAL and type in the IP address 10.1.1.1 followed by RETURN

Serial Step 8. Select option 3 MASK and type in the MASK 255 . 255 . 255 . 0 followed by RETURN. Please note that this can also be entered in its **CIDR** format of /24

Serial Step 9. Quit out of that menu.

The last step in this configuration part of the configuration is optional, but we recommend you undertake this step to ensure that it's clear which entries have been configured.

Serial Step 10. From the London NETWORKS menu select option 0 NAME

Serial Step 11. Type in eth followed by RETURN. This is only a suggested name.

Serial Step 12. Quit out of the London NETWORKS menu to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 DEFAULT_WAN	Configuration In Only	0.0.0.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

The last step on this configuration is to configure a single WAN port.

Serial Step 13. Select option 0 DEFAULT_WAN

Serial Step 14. Select option 1 IP to get the same menu as shown above for the Ethernet port.

Serial Step 15. Select option 2 REMOTE and type in the Remote IP address 20.1.1.1 followed by RETURN.

Serial Step 16. Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN (or again use the **CIDR** format) the menu will now look like:

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	0.0.0.0 /0
2 REMOTE	Remote IP address (if not Ethernet)	20.1.1.1
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	0 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

Note: For a simple network the VIPERs do not need a Local IP address set on the WAN ports for a simple point-to-point link. For more complex networks then it may be necessary to add IP Addresses to the WAN ports.

Serial Step 17. Quit out of the menu

Serial Step 18. Select option 5 Channels to get a menu that will allow us to set up the type of port used for this entry. In this case we want to set up it up as X21 and for ease of use we will use X21 link 2.

Serial Step 19. Select option '3' X21L2

Serial Step 20. From the submenu that is displayed select option 1 YES.

Serial Step 21. Quit out of that menu and verify that the X21L2 has got a current value of YES

Serial Step 22. Quit out of that menu.

The final step in this part of the configuration is n optional but for clarity it is recommended that it the name is changed.

Serial Step 23. Select option 0 NAME and type in the chosen name followed by RETURN, as this link is going to be connected to Birmingham we will use that as the name.

Serial Step 24. Quit out of that menu and the following should appear:
This screen above shows that we have 2 networks set up.

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Leased Circuit: Link 2	20.1.1.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

1. Network 0 is a Leased Link over X21 to a router called Birmingham and has the IP range 20.1.1.0 assigned to it.
2. Network 1 is the local Ethernet and has the range 10.1.1.0 assigned to it.

Everything connected to the VIPER's Ethernet port either directly or through a switch will need to be told that Birmingham on IP range 20.1.1.0 can be access via the VIPER which has been configured with an IP of 10.1.1.1

Some equipment will be able to learn the route, but in some instances a static route on the equipment will have to be configured. See your equipments manual for information on how to do that.

The final step of this basic routing configuration is to reboot the VIPER to ensure that the changes have been activated.

Serial Step 25. From the London NETWORKS screen quit that menu and go to the Main Menu.

Serial Step 26. Select option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.

Serial Step 27. After about 10 seconds the Main Menu will then reappear.

Alternatively you can power reset the VIPER, although a soft reboot takes a lot less time as the VIPER doesn't need to go through its power on sequence again.

The remote VIPER will need to be configured in exactly the same way except the names and IP addresses are swapped around.

Then when the VIPERs are connected over an X21 link or simulator they will talk to each other and it's possible to send and receive pings over the link.

As most people don't have a X21 link or simulator handy it is possible to configure one of the VIPERs to provide a clock on the X21 Link 2 to the other VIPER and use a standard X21 crossover cable to connect the VIPERs together. Details of the pin out of the X21 crossover cable can be found in Appendix B

5.1.3 Configuring two Vipers back to back via their serial ports.

To configure one of the VIPERs to provide a clock perform the following:

Back to Back Step 1 From the Main Menu select option 2 HARDWARE and then option 6 X21L2

Back to Back Step 2 The select option 0 SPEED and type in 64000 followed by RETURN.

Back to Back Step 3 Quit out of that menu and the HARDWARE menu back to the Main Menu.

Then reboot the VIPER as described above in Serial Steps 25 and 26 above.

The two Vipers should then communicate via Link 2 and the X.21 cross over cable.

5.1.4 Basic routing over ISDN.

To set up basic routing on a VIPER you will need the following information:

- v. Name of the local VIPER – this can be anything, for example the location.
- vi. IP address of the Ethernet port of the VIPER including the Mask.
- vii. IP address of the remote, e.g. the remote VIPER's IP address including the Mask
- viii. The name of the remote. – E.g. its location.
- ix. ISDN numbers for both locations.

For the following example we will use the local name London, IP address of the Ethernet port 10.1.1.1 and mask 255.255.255.0, remote IP of 20.1.1.1 and mask 255.255.255.0, remote name Birmingham with ISDN addresses 1111 for London and 2222 for Birmingham.

The first step is to give the VIPER its name.

ISDN Step 1. From the Main Menu select option 0 GLOBAL and then option 0 NAME. Enter the name London followed by RETURN.

ISDN Step 2. Quit out of that menu by pressing a full stop (.) once to get back to the Main Menu which now shows London Main Menu at the top of the screen.

ISDN Step 3. The next step is to configure the Ethernet port with the IP address and Mask.

ISDN Step 4. From the Main Menu select option 1 'NETWORK' to get to the following screen:

London NETWORKS		
Command	Description	Current Value
0	DEFAULT_ETH	Ethernet Interface
1	DEFAULT_WAN	Configuration In Only
&	ADD	Add new item
%	DELETE	Delete item
.	QUIT	Previous menu

ISDN Step 5. Next select option 0 DEFAULT_ETH to get the following screen:

London NETWORKS		
Command	Description	Current Value
0	NAME	Name
1	IP	IP configuration
2	PPP	PPP configuration
3	IPX	IPX configuration
4	ISDN	ISDN configuration
5	CHANNELS	Select channels to use
.	QUIT	Previous menu

ISDN Step 6. Next select option 1 'IP' to get the following screen:

ISDN Step 7. Then select option 1 IP to get the following screen.

London		
Command	Description	Current Value
0	ENABLE	IP routing
1	LOCAL	Local IP address
2	REMOTE	Remote IP address (if not Ethernet)
3	MASK	IP address mask
4	RIP	RIP
5	RIPMETRIC	RIP Metric weighting for link
6	ROUTES	Associated static routes
7	TRANSLATE	Address translation rules
8	PIPE	IP Express
9	FILTBOARD	Filter Directed Broadcast
.	QUIT	Previous menu

ISDN Step 8. Select option 1 LOCAL and type in the IP address 10.1.1.1 followed by RETURN

ISDN Step 9. Select option 1 LOCAL and type in the IP address 10.1.1.1 followed by RETURN.

ISDN Step 10. Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN. Please note that this can also be entered in its **CIDR** format of /24

ISDN Step 11. Quit out of the menu.

The final step on this part of the configuration is optional, it's recommended to do this so that it's clear which entries have been configured.

ISDN Step 12. From the London NETWORKS menu select option 0 NAME

ISDN Step 13. Type in 'eth' followed by RETURN. **NB** This is only a suggested name.

ISDN Step 14. Quit out of the London NETWORKS menu to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 DEFAULT_WAN	Configuration In Only	0.0.0.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

The last step on this configuration is to configure a single WAN port for ISDN.

ISDN Step 15. Select option 0 DEFAULT_WAN

ISDN Step 16. Select option 1 IP to get the same menu as shown above for the Ethernet port.

ISDN Step 17. Select option 2 REMOTE and type in the Remote IP address 20.1.1.1 followed by RETURN.

ISDN Step 18. Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN (or again use the **CIDR** format) the menu will now look like:

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	0.0.0.0 /0
2 REMOTE	Remote IP address (if not Ethernet)	20.1.1.1
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	0 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

Note for simple networks its not necessary to apply IP Addresses to the WAN links, however for some more complex network giving the WAN ports an IP address maybe necessary.

ISDN Step 19. Quit out of that menu.

ISDN Step 20. Select option 4 ISDN to this menu:

London		
Command	Description	Current Value
0 DIALLIST	List of numbers to dial	0 numbers
1 CLILIST	List of acceptable calling numbers	Not checked
2 CLIACTION	Dialback on CLI Match	NO
3 ACCESS	Use access control	NO
4 MINCALL	Control Minimum Call Lengths	NO
5 CLEAR	Cleardown time	25
6 DAY CLEAR	Daytime cleardown time	25
7 EVE CLEAR	Evening cleardown time	50
8 WKEND CLEAR	Weekend cleardown time	100
. QUIT	Previous menu	

ISDN Step 21. Select option 0 DIALLIST

ISDN Step 22. From the submenu that is displayed select option &

ISDN Step 23. Select option 0 NO

ISDN Step 24. Select option 0 NUMBER and type the ISDN number of the remote site, in this case it is 2222

ISDN Step 25. Quit out of that menu and verify that NO has got a current value of 2222

ISDN Step 26. Quit out of that menu and the subsequent menu.

The final step in this part of the configuration is again optional but for clarity it is recommended that it the name is changed.

ISDN Step 27. Select option 0 NAME and type in the chosen name followed by RETURN, as this link is going to be connected to Birmingham we will use that as the name.

ISDN Step 28. Quit out of that menu and the following should appear:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	ISDN No: 2222	20.1.1.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

This screen shows that we have 2 networks set up.

Network 0 is an ISDN link that dials to a router called Birmingham and has the IP range 20.1.1.0 assigned to it. Network 1 is the local Ethernet and has the range 10.1.1.0 assigned to it.

Everything connected to the VIPER's Ethernet port either directly or through a switch will need to be told that Birmingham on IP range 20.1.1.0 can be access via the VIPER which has been configured with an IP Address of 10.1.1.1

While some equipment will be able to learn the route, other instances a static route will have to be configured on the equipment. See your equipment manual for information for instructions on how to configure a static route.

The final step of this basic routing configuration is to reboot the VIPER to ensure that the changes have been activated.

ISDN Step 29. From the London NETWORKS screen quit that menu and go to the Main Menu.

ISDN Step 30. Select option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.

ISDN Step 31. After about 10 seconds the Main Menu will then reappear.

Alternatively you could just do step 1 and the unplug the VIPER, but a soft reboot takes a lot less time as the VIPER doesn't need to go through it's power on sequence again.

5.1.5 Basic routing via the Ethernet port (Working as a Voice Gateway)

This section can also be used to configure a back-to-back LAN link between Vipers on the same LAN. The configuration is the same except that there is no need for a static route to be configured.

Some networks require the use of an external equipment to provide a WAN link for example over ADSL, G.SHDSL etc. In that case the VIPER will need to pass any relevant data over the Ethernet port to an external device and through to a different core network, e.g. Internet. In this case the VIPER will be acting as a 'Voice Gateway' and will only be passing Voice traffic over the link.

For the following example we will use the local name London, IP address of the Ethernet port 10.1.1.1 and mask 255.255.255.0, remote IP of 20.1.1.1 and mask 255.255.255.0, remote name Birmingham. We also need information about the Gateway devices through which the VIPERs will be communicating, i.e. the Gateway's IP address. In this example we will use the address 10.1.1.100 as London's IP address and 20.1.1.100 as Birmingham's IP address.

The first step is to give the VIPER its name.

Eth Gate Step 1. From the Main Menu select option 0 GLOBAL and then option 0 NAME. Enter the name London followed by RETURN.

Eth Gate Step 2. Quit out of that menu by pressing '.' (full stop) once to get back to the Main Menu which now shows London Main Menu at the top of the screen.

The next step is to configure the Ethernet port with the IP address and Mask.

Eth Gate Step 3. From the Main Menu select option 1 NETWORK to get to the following screen:

London NETWORKS		
Command	Description	Current Value
0	DEFAULT_ETH	Ethernet Interface
1	DEFAULT_WAN	Configuration In Only
&	ADD	Add new item
%	DELETE	Delete item
.	QUIT	Previous menu

Eth Gate Step 4. Next select option '0' 'DEFAULT_ETH' to get the following screen:

London NETWORKS		
Command	Description	Current Value
0	NAME	Name
1	IP	IP configuration
2	PPP	PPP configuration
3	IPX	IPX configuration
4	ISDN	ISDN configuration
5	CHANNELS	Select channels to use
.	QUIT	Previous menu

Eth Gate Step 5. Then select option 1 IP to get the following screen:

London		
Command	Description	Current Value
0	ENABLE	IP routing
1	LOCAL	Local IP address
2	REMOTE	Remote IP address (if not Ethernet)
3	MASK	IP address mask
4	RIP	RIP
5	RIPMETRIC	RIP Metric weighting for link
6	ROUTES	Associated static routes
7	TRANSLATE	Address translation rules
8	PIPE	IP Express
9	FILTBROAD	Filter Directed Broadcast
.	QUIT	Previous menu

Eth Gate Step 6. Select option 1 (LOCAL) and type in the IP address 10.1.1.1 followed by RETURN

Eth Gate Step 7. Select option 3 (MASK) and type in the MASK 255.255.255.0 followed by RETURN. Please note that this can also be entered in its **CIDR** format of /24

The next stage of configuration is to tell the VIPER how to get out of the Ethernet network, i.e. the IP address of the Gateway. This is done by adding a static route. If configuring a pair of Vipers for back-to-back operation via their Ethernet ports then this part is not required, jump to Step 10.

Eth Gate Step 8. Select option 6 ROUTES and then type & to add a new item.

Eth Gate Step 9. Select option ‘0’ IP:0.0.0.0 to get to a sub-menu that allows you to set the static route options:

London NETWORK STATIC ROUTE		
Command	Description	Current Value
0 ADDRESS	Target IP network (0=default route)	0.0.0.0 /0
1 ROUTER	IP address of next router	0.0.0.0 /0
2 MASK	IP mask (0=default route)	255.255.255.255 /32
3 METRIC	Cost of route	8
. QUIT	Previous menu	

Eth Gate Step 10. Select option 1 ROUTER and type in 10.1.1.100 i.e. the IP address of the Gateway. The other three entries can be left as default so that *all* traffic from the VIPER is routed to the Gateway.

The final step in this part of the configuration process is optional, it’s recommended to do this so that it’s clear which entries have been configured.

Eth Gate Step 11. From the London NETWORKS menu select option 0 NAME

Eth Gate Step 12. Type in eth followed by RETURN. This is only a suggested name.

Eth Gate Step 13. Quit out of the London NETWORKS menu to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 DEFAULT_WAN	Configuration In Only	0.0.0.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

The last step on this configuration is to tidy up the WAN entry. As we’re not using a WAN connection on this configuration example we could delete it without any problems.

Eth Gate Step 14. Select option % ‘DELETE’

Eth Gate Step 15. Select option 0 ‘DEFAULT_WAN’. The screen will then refresh with the WAN entry now deleted.

The final step of this basic routing configuration is to reboot the VIPER to ensure that the changes have been activated.

Eth Gate Step 16. From the London NETWORKS screen quit that menu and go to the Main Menu.

Eth Gate Step 17. Select option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.

Eth Gate Step 18. After about 10 seconds the Main Menu will then reappear.

Alternatively you can ‘Power Reset’ the VIPER, but a soft reboot is quicker as the VIPER doesn’t need to go through it’s power on sequence again.

5.2 Basic VIPER Configuration - Voice

This section details how to add the Voice Over IP configuration to the VIPERs. This should be configured after adding the Routing configuration as detailed above.

There are up to three possible type of functionality available to the voice cards depending on the type of card. They are:

RXONLY – The port can only receive calls and cannot dial out. Available on all analogue cards. i.e. FXO, FXS, E&M and AC15.

DIRECT – When the line goes off-hook then the VIPER will automatically dial a single number as configured in the configuration. Available on all analogue cards, i.e. FXO, FXS, E&M and AC15

DIALOUT – When the line goes off-hook then the VIPER supplies a dial tone and the user can dial any available number in the configuration.

There are also three available Vocoders available of the VIPER. It’s recommended that both ends of a VIPER voice link be set to the same Vocoder. The Vocoders available are:

- **G729A** G.729A @ 8kpbs (NB 9.2Kbps with overheads on WAN)
- **G711** G.711 (A-law) @ 64kbps (NB 80Kbps with overheads on WAN)
- **G726_32** G.726 @ 32kpbs

These are available on most analogue cards, i.e. FXO, E&M and AC15. The FXS card doesn’t have this option as it interfaces directly to a PABX system.

5.2.1 Basic FXO, FXS, E&M or AC15 configuration

This section will detail how to configure all 4 ports for a VIPER fitted with an analogue card. All 4card types are basically configured in the same way. There are some options that are card specific and they will be covered in the advance section.

The functionality that we will be using is DIRECT

This configuration is basically for line extension of PABX to a remote site with normal telephones. So when the telephones at the remote site go off-hook they will receive a dial tone from the PABX at the local site and can be treated just like a normal telephone extension.

To configure this we need to know the IP addresses of the local VIPER and remote VIPER (10.1.1.1 and 20.1.1.1 respectively) and phone numbers that we will be using within the VIPER network, in this case 11-14 for the local VIPER and 21-24 for the remote.

- Analogue step 1.** From the Main Menu select option 2 HARDWARE
- Analogue step 2.** From the resulting menu select option 3 VIPER (if Frame Relay is not active on the VIPER then the option number will be different)
- Analogue step 3.** Select option 0 VPORT1 to get the following menu:

London VIPER PORT 1 CONFIGURATION		
Command	Description	Current Value
0 PORTTYPE	Port Functionality	RXONLY
1 PORTNO	Port Destination	
2 PORTOPTS	Port Options	
3 VOCODER	Port Encoding Scheme	G729A
. QUIT	Previous menu	

- Analogue step 4.** Select option 0 PORTTYPE to select the functionality in this case we want DIRECT
- Analogue step 5.** Then quit out of that menu.
- Analogue step 6.** Select option 1 PORTNO and type in 21 this is the number that we will be assigning to the remote port that we want to connect to.
- Analogue step 7.** The other two options can be ignored a basic configuration.
- Analogue step 8.** Quit out of that menu and then select option 1 VPORT2 and repeat the above but with a PORTNO of 22
- Analogue step 9.** Then repeat this to configure the last two ports.
- Analogue step 10.** Quit out of the VIPER menu and go back to the HARDWARE menu.

The next stage of the configuration requires setting up a list of available phone numbers within the VIPER network. This is called Yellow Pages, shortened to YPAGES in the configuration menus. The YPAGES need to be identical throughout the whole of the network

- Analogue step 11.** Select option 4 YPAGES.
- Analogue step 12.** We then need to add a number of new items to cover the phone numbers we are using in the network. In this case we have 4 local and 4 remote ports, so we need 8 new items. Select & 8 times
- Analogue step 13.** Select option 0 Y0 to get a sub-menu that lets us configure the phone number, IP address of the VIPER that is associated to that phone number and port number.
- Analogue step 14.** Select option 0 DNUMBER and type in 21
- Analogue step 15.** Select option 1 DESTIP and type in the IP address of the remote VIPER, in this case we use 20.1.1.1

Analogue step 16. Select option 2 and type in the port number that we want to connect to on the remote VIPER. In this case we want port 1. Setting this to 0 for an FXS option would make all unused telephones ring on the remote VIPER and for the other voice option cards would mean that the call would go to the first available unused port on the remote VIPER

The menu will then look like this:

London VIPER YELLOW PAGES		
Command	Description	Current Value
0 DNUMBER	Number to Dial	21
1 DESTIP	IP Address of Destination	20.1.1.1
2 DESTCHAN	Port to Call on Destination Unit	1
. QUIT	Previous menu	

Analogue step 17. Quit out of that menu and proceed with configuring entries for the remaining 3 ports of the remote VIPER.

Analogue step 18. After that we need to configure the 4 local ports as well but using IP 10.1.1.1 and phone numbers 11-14. After which the menu should look like:

London YELLOW PAGES			
Index	Phone No.	IP Address	Port Number
0 Y0	21	20.1.1.1	1
1 Y1	22	20.1.1.1	2
2 Y2	23	20.1.1.1	3
3 Y3	24	20.1.1.1	4
4 Y4	11	10.1.1.1	1
5 Y5	12	10.1.1.1	2
6 Y6	13	10.1.1.1	3
7 Y7	14	10.1.1.1	4
& ADD	Add new item		
% DELETE	Delete item		
. QUIT	Previous menu		

These exact entries need to be replicated in the remote VIPER to ensure that no calls are lost or misdirected to the wrong port.

Analogue step 19. Quit out of that menu and then quit out of that menu to return to the Main Menu.

Analogue step 20. The VIPER will then need to be rebooted to ensure that the configuration has been activated.

5.2.2 Basic BRI and PRI configuration

This section will detail how to configure the digital BRI or PRI card option. The main difference in configuration between these card and the analogue cards is that this has one channel that can be

configured and this channel is for up to 4 B Channels for the BRI card and up to 10 B Channels for the PRI.

Both digital cards are capable of recognising a dialled number from within their standard packet structure and route that number according to the Yellow Pages configuration.

To configure this we need to know the phone number and IP address for both ends of the link. In this example we are using IP 10.1.1.1 and phone number 11-14 for London and IP 20.1.1.1 and phone number 21-24 for Birmingham.

The default state in which the VIPERs come up with for the BRI and PRI option cards means that the only configuration needed is the Yellow Pages. There are hardware options available and these will be described in later sections.

Bri-Pri Step 1. From the Main Menu select option select option 4 YPAGES.

Bri-Pri Step 2. We then need to add a number of new items to cover the phone numbers we are using in the network. In this case we have 4 local and 4 remote ports, so we need 8 new items. Select & 8 times

Bri-Pri Step 3. Select option 0 Y0 to get a sub-menu that lets us configure the phone number, IP address of the VIPER that is associated to that phone number and port number.

Bri-Pri Step 4. Select option 0 DNUMBER and type in 21

Bri-Pri Step 5. Select option 1 DESTIP and type in the IP address of the remote VIPER, in this case we use 20.1.1.1

Bri-Pri Step 6. For option 2 DESTCHAN the default “hunt group” options will be suitable for this configuration example.

Bri-Pri Step 7. The menu will then look like this:

London VIPER YELLOW PAGES		
Command	Description	Current Value
0 DNUMBER	Number to Dial	21
1 DESTIP	IP Address of Destination	20.1.1.1
2 DESTCHAN	Port to Call on Destination Unit	0
. QUIT	Previous menu	

Bri-Pri Step 8. Quit out of that menu and proceed with configuring entries for the remaining 3 ports of the remote VIPER.

Bri-Pri Step 9. After that we need to configure the 4 local ports as well but using IP 10.1.1.1 and phone numbers 11-14. After which the menu should look like:

London YELLOW PAGES			
Index	Phone No.	IP Address	Port Number
0 Y0	21	20.1.1.1	0
1 Y1	22	20.1.1.1	0
2 Y2	23	20.1.1.1	0
3 Y3	24	20.1.1.1	0
4 Y4	11	10.1.1.1	0
5 Y5	12	10.1.1.1	0
6 Y6	13	10.1.1.1	0
7 Y7	14	10.1.1.1	0
& ADD	Add new item		
% DELETE	Delete item		
. QUIT	Previous menu		

These exact entries need to be replicated in the remote VIPER to ensure that no calls are lost or misdirected to the wrong port.

Bri-Pri Step 10. Quit out of that menu and then quit out of that menu to return to the Main Menu.

Bri-Pri Step 11. The VIPER will then need to be rebooted to ensure that the configuration has been activated.

Section 6

Advanced VIPER Configuration

6.1.1 Entering Debug Monitor Mode

This section will cover some of the more advanced configuration options within the Viper. These options are entered from what is called the Debug Monitor.

To Debug Monitor follow the steps below:

1. From the Main Menu select option 7 DEBUG
2. Select option 0 MONITOR
3. Then a > prompt will appear.

To exit from the Debug Monitor mode:

1. From the > prompt press. (Full stop) followed by RETURN

Note: At no time should the + character be entered into the Debug Monitor, this is for use by qualified personnel only.

6.2 Erasing configuration.

To erase the configuration of an existing VIPER router you have to:

1. Set up a terminal or terminal emulator as described in Section 4.1 and connect it to the VIPER.
2. Power up the VIPER and wait until it has finished its power up sequence.
3. The terminal emulator will then show the following screen:

London Main Menu		
Command	Description	Current Value
0 GLOBAL	System Configuration	
1 NETWORK	Configure networks, routes etc	2 entries
2 HARDWARE	Configure Hardware	
3 ADMIN	Administration of running system	
4 STATUS	Current Status	
5 STATISTICS	Recent Statistics	
6 WANSTATS	Recent WAN Statistics	
7 DEBUG	Debugging facilities	
. QUIT	Previous menu	

4. Select option 0, then option 9 and press Y.

6.2.1 Saving and restoring configuration

There are a couple of commands available that can show the configuration of the VIPER to the terminal and from there you can save it to a text file and can set the configuration from a text file.

Note: These commands do not save any additional configuration that is set from the Debug Monitor, e.g. bridge mode and voice gain levels.

These configuration files are not designed to be read and understood by anything other than the VIPER and are not designed to be modified in any way.

To save the configuration:

1. Enter Debug Monitor mode as described above.
2. Type in config show
3. On the terminal emulator select the option that captures the screen to a text file and start it. This varies from emulator to emulator, see the help file in your specific terminal emulator for more information.
4. Press RETURN and a small number of lines will appear.
5. Stop the capture option on the terminal emulator; the text file should then be saved.
6. Locate that saved file and open it up into a simple text file editor like Notepad or Wordpad.
7. Ensure that the starting line of the text file is *1 and the end line is ** if not then amend the text file. This is to ensure that any extraneous characters that show in the text file do not cause problems when loading back into a VIPER.
8. You will also have to document any Debug Monitor changes that you have made.

To load the configuration:

1. Enter Debug Monitor mode as described above.
2. Type in config set followed by RETURN.
3. On the terminal emulator select the option that sends files as an ASCII string.
4. Locate the desired configuration file from the terminal emulator.
5. When the terminal emulator has sent the configuration file press RETURN.
6. The VIPER should respond with the > prompt, if not then there is a problem with the configuration file and it has invalid characters wither at the start or at the end.
7. Then you will have to enter any additional Debug Monitor commands, e.g. bridge, that are not saved in the configuration file.
8. Quite out of Debug Monitor mode by pressing . (full stop) and RETURN.
9. Reboot the VIPER by selecting option 2 REBOOT
10. When the VIPER has rebooted it would then be running the configuration.

6.3 Bridging mode

When passing Ethernet traffic over a specified WAN link (i.e. X21 or ISDN) the VIPER functions as a Router. As such it routes the traffic between two networks with different IP address ranges, e.g. in the basic configuration examples we used 10.1.1.1 and 20.1.1.1

It is also possible for the VIPER to act as a Bridge between two separate networks.

To configure this option:

1. From the Main Menu select option 7 DEBUG and then option 0 MONITOR to enter the Debug Monitor.
2. Type in bridge 1 followed by RETURN
3. Quit out of the CLI by pressing '.' (full stop) followed by RETURN
4. Select option 2 REBOOT and type y to confirm the reboot.
5. When the VIPER reboots the Main Menu will show the following:

London Main Menu		
Command	Description	Current Value
0 GLOBAL	System Configuration	
1 NETWORK	Configure networks, routes etc	2 entries
2 HARDWARE	Configure Hardware	
3 BRIDGE	Configure Bridge Functions	BRIDGE Enabled
4 ADMIN	Administration of running system	
5 STATUS	Current Status	
6 STATISTICS	Recent Statistics	
7 WANSTATS	Recent WAN Statistics	
8 DEBUG	Debugging facilities	
. QUIT	Previous menu	
NOTICE BRIDGING - Routing Functions Disabled!		

As can be seen this configuration adds a new option to the Main Menu 3 BRIDGE, which allows configuration of various Bridge functions like spanning tree and filtering.

Details of the options available in Bridge mode will be described in later sections.

Note: Setting to bridge '0' disables Bridge mode and restores the VIPER to routing mode.

6.4 Adjusting the FXO, FXS and E&M Voice levels

It is possible to configure the gain settings on the analogue voice cards and to set them independently on each of the 4 channels. There are many reason to do this, for example if the voice is too quiet or too loud or if there is interference on the voice line such as echo or feedback.

There are two commands available that set the voice gains and they are:

gengain – sets the voice gain for the voice traffic going to the remote end

vvolume – sets the voice gain for voice traffic coming out of the VIPER to the phone/PABX

The format of both commands are exactly the same and it is:

gengain <Port> <Value>

vvolume <Port <Value>

6.4.1 Command Port Value

Command – is either **gengain** or **vvolume**

Port - is the port number that you want to set, starting from 0 for port 1 up to 3 for port 4.

Value – is the gain setting wanted on that port. A value of 100 = 0dB, a value of 90 = -10dB and a value of 110 = 10dB. 0dB is the default setting and should be OK for the majority of situations.

For an example to set the first port on a FXS card so that the audio gain to the local telephone is set to -9dB and the audio gain to the remote end is set to 3dB configure the following:

1. Enter Debug Monitor mode
2. Type in 'vvolume' 0 91 followed by RETURN.
3. The VIPER will respond with Channel 0 Volume Adjustment is -9dB
4. Type in 'gengain' 0 103 followed by RETURN.
5. The VIPER will respond with Channel 0 General input gain is 3dB
6. Quit out of Debug Monitor mode and reboot the VIPER to activate the changes.

Note: If a voice link is too quiet then it is suggested that the gain is set so that both ends “share” the gain. So if a 6dB increase is needed use **gengain** to set 3dB on one end and **vvolume** to set the remaining 3dB at the other end.

6.5 AC15 Voice level

The AC15 voice option card works in a different way to other analogue voice cards, in as much as it uses a 2280Hz tone on the voice lines, and requires different commands to set the gain.

The commands are ‘**acgain**’ and ‘**acvolume**’ and are activated for all four channels and not on a channel-by-channel basis like the ‘**vvolume**’ and ‘**gengain**’ commands.

So the command to set voice gain coming out of the VIPER to -9dB and the voice gain going to the remote end to 3dB the following:

1. Enter Debug Monitor mode
2. Type in acvolume 91 followed by RETURN.
3. The VIPER will respond with Channel 0 Volume Adjustment is -9dB
4. Type in acgain 103 followed by RETURN.
5. The VIPER will respond with Channel 0 General input gain is 3dB
6. Quit out of Debug Monitor mode and reboot the VIPER to activate the changes.

6.6 ISDN back up of an X21 or V35 WAN link

It is possible for the VIPER to provide an ISDN back up service to the X21/V35 WAN link. This set up in addition to the basic X21/V35 configuration as describe above.

Assuming that you have followed the configuration example you will have a VIPER configured with the name London and IP address of 10.1.1.1 talking to a remote VIPER called Birmingham with an IP address of 20.1.1.1

The additional information that is needed to set up ISDN back up is the ISDN numbers for the local and remote VIPERs. In this example the local London end has 1111 and the remote has 2222.

ISDN BU Step 1. From the Main Menu select option 1 NETWORK to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Leased Circuit: Link 2	20.1.1.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

ISDN BU Step 2. Select option 0 Birmingham

ISDN BU Step 3. Select option 4 ISDN to get this menu:

London		
Command	Description	Current Value
0 DIALLIST	List of numbers to dial	0 numbers
1 CLILIST	List of acceptable calling numbers	Not checked
2 CLIACTION	Dialback on CLI Match	NO
3 ACCESS	Use access control	NO
4 MINCALL	Control Minimum Call Lengths	NO
5 CLEAR	Cleardown time	25
6 DAY CLEAR	Daytime cleardown time	25
7 EVE CLEAR	Evening cleardown time	50
8 WKEND CLEAR	Weekend cleardown time	100
. QUIT	Previous menu	

- ISDN BU Step 4.** Select option '0' DIALLIST
- ISDN BU Step 5.** From the submenu that is displayed select option &
- ISDN BU Step 6.** Select option '0' N0
- ISDN BU Step 7.** Select option '0' NUMBER and type the ISDN number of the remote site, in this case it is 2222
- ISDN BU Step 8.** Quit out of that menu and verify that N0 has got a current value of 2222
- ISDN BU Step 9.** Quit out of that menu and all subsequent menus until you return to the Main Menu.
- ISDN BU Step 10.** Then reboot the VIPER to activate the change.

This will set up the VIPER so that if the primary route via the X21/V25 WAN links fails then it can dial the ISDN line to connect to the remote VIPER only when there is traffic that needs to be sent to the remote end. If there is no traffic then the VIPER will not dial on the ISDN line.

6.6.1 PAP configuration for ISDN links

The VIPER can also provide security for the ISDN WAN link, so that only authorised connections are made. These aren't set in the above sample configuration as in most instances they aren't required.

More information on the various options available for **PAP** and **CHAP** are covered later in this manual.

In this example we'll be setting up PAP configuration. To do this we need to know the name of the local VIPER, the name of the remote VIPER, the name of the link between them and any passwords that you want to set up (these are optional)

In our example the local VIPER is called London and the remote VIPER Birmingham. We have set the name of the link from London to Birmingham as Birmingham and from Birmingham to London as London. This is the primary reason why we were specific in naming the links between the two VIPERs with the name of the remote VIPER, it makes configuring PAP/CHAP easier. The passwords that we will be using are pass at London and word at Birmingham.

This example is assuming that you have configured the WAN link as described previously on the London VIPER, either for standard ISDN or for ISDN backup.

PAP Conf. Eg 1. From the Main Menu select option 1 NETWORK

PAP Conf. Eg 2. The select option 0 Birmingham

PAP Conf. Eg 3. Then select option 2 PPP to be presented with the following menu:

London		
Command	Description	Current Value
0 PAP	Password Authentication Protocol	disabled
1 CHAP	Challenge Handshake Authentication	-
2 MPDMAX	ISDN channels req'd to start link	0
3 BANDWIDTH	Bandwidth on demand	disabled
. QUIT	Previous menu	

PAP Conf. Eg 4. Select option 0 PAP

London		
Command	Description	Current Value
0 PEERID	Peer user id (default=NETWORK NAME)	
1 PEERPASS	Peer password to check against	
2 LOCALID	Local user id (default=GLOBAL NAME)	
3 LOCALPASS	Local password to send to peer	
. QUIT	Previous menu	

PAP Conf. Eg 5. Select option 1 PEERPASS and type in pass followed by RETURN

PAP Conf. Eg 6. Select option 3 LOCALPASS and type in word followed by RETURN

PAP Conf. Eg 7. The screen will now look like:

London		
Command	Description	Current Value
0 PEERID	Peer user id (default=NETWORK NAME)	
1 PEERPASS	Peer password to check against	pass
2 LOCALID	Local user id (default=GLOBAL NAME)	
3 LOCALPASS	Local password to send to peer	word
. QUIT	Previous menu	

Note: PEERID will automatically be set to the WAN link name, i.e. Birmingham and LOCALID to the VIPER name, i.e. London. There is no need to change these entries unless extra security is required but they do have to match to the remote end.

PAP Conf. Eg 8. Quit out of that menu and you should see the following:

London		
Command	Description	Current Value
0 PAP	Password Authentication Protocol	in+out
1 CHAP	Challenge Handshake Authentication	-
2 MPDMAX	ISDN channels req'd to start link	0
3 BANDWIDTH	Bandwidth on demand	disabled
. QUIT	Previous menu	

This shows us that there is some PAP configuration set to make the WAN link more secure.

PAP Conf. Eg 9. Quit out of that menu until you return to the Main Menu and then reboot the VIPER to action the changes.

PAP Conf. Eg 10. Repeat these changes for the remote VIPER, but swapping around the pass and word entries.

CHAP is set up in a similar way, except instead of single passwords for the local and remote there are two secrets for when the VIPER is calling or answering.

6.6.2 Numbered WAN links

The VIPER is capable of handling WAN ports that have been given IP addresses of their own, i.e. Numbered WAN links. The default configuration described previously used Unnumbered WAN links. One reason to use Numbered WAN links is if you only want to pass voice traffic over the link and no Ethernet traffic. Numbered WAN links can also be useful for VIPERs set to Bridge mode.

To set up Numbered WAN links it will be necessary to provide IP addresses from a different range to those in use on the two separate Ethernet networks that will be linked. In the previous examples we have used 10.1.1.1 for the London VIPER and 20.1.1.1 for Birmingham. So we will use the IP addresses 5.1.1.1 and 5.1.1.2 for the WAN links of London and Birmingham respectively.

This example is assuming that you are running from a blank VIPER.

1. From the Main Menu select option 0 GLOBAL and then option 0 NAME. Enter the name London followed by RETURN.
2. Quit out of that menu by pressing . (full stop) once to get back to the Main Menu which now shows London Main Menu at the top of the screen.

The next step is to configure the Ethernet port with the IP address and Mask.

3. From the Main Menu select option 1 NETWORK and the following screen should be displayed.

London NETWORKS		
Command	Description	Current Value
0	DEFAULT_ETH	Ethernet Interface
1	DEFAULT_WAN	Configuration In Only
&	ADD	Add new item
%	DELETE	Delete item
.	QUIT	Previous menu

4. Next select option 0 DEFAULT_ETH to get the following screen:

London NETWORKS		
Command	Description	Current Value
0	NAME	Name
1	IP	IP configuration
2	PPP	PPP configuration
3	IPX	IPX configuration
4	ISDN	ISDN configuration
5	CHANNELS	Select channels to use
.	QUIT	Previous menu

5. Then select option 1 IP to get the following screen:

London		
Command	Description	Current Value
0	ENABLE	IP routing
1	LOCAL	Local IP address
2	REMOTE	Remote IP address (if not Ethernet)
3	MASK	IP address mask
4	RIP	RIP
5	RIPMETRIC	RIP Metric weighting for link
6	ROUTES	Associated static routes
7	TRANSLATE	Address translation rules
8	PIPE	IP Express
9	FILTBOARD	Filter Directed Broadcast
.	QUIT	Previous menu

6. Select option 1 LOCAL and type in the IP address 10.1.1.1 followed by RETURN
7. Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN. Please note that this can also be entered in its **CIDR** format of /24
8. Quit out of that menu.

The last step on this configuration step is optional, it's recommended to do this so that it's clear which entries have been configured.

9. From the London NETWORKS menu select option 0 NAME
10. Type in eth followed by RETURN. This is only a suggested name.
11. Quit out of the London NETWORKS menu to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 DEFAULT_WAN	Configuration In Only	0.0.0.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

Note: If you don't want to use the Ethernet port then just don't configure it. It isn't possible to delete an Ethernet port on a VIPER, as the next time it powers up or is rebooted it will just recreate the DEFAULT_ETH link.

The last step on this configuration is to configure a single WAN port.

12. Select option 0 DEFAULT_WAN
13. Select option 1 IP to get the same menu as shown above for the Ethernet port.
14. Select option 1 LOCAL and type in the Local IP address 5.1.1.2 followed by RETURN.
15. Select option 2 REMOTE and type in the Remote IP address **5.1.1.2** followed by RETURN.
16. Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN (or again use the **CIDR** format) the menu will now look like:

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	5.1.1.1 /0
2 REMOTE	Remote IP address (if not Ethernet)	5.1.1.2
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	0 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

Next we need to set up a static route so that the VIPER will know that IP range 20.1.1.0 can be accessed through VIPER 5.1.1.2

17. Select option 6 ROUTES and press & to create a blank static route.
18. Select option 0 IP 0.0.0.0
19. Select option 0 ADDRESS and type in the remote Ethernet IP address 20.1.1.1 followed by RETURN.
20. Select option 1 ROUTER and type in the IP address of the remote WAN link 5.1.1.2 followed by RETURN. The screen should look like:

London NETWORK STATIC ROUTE		
Command	Description	Current Value
0 ADDRESS	Target IP network (0=default route)	10.1.1.1 /0
1 ROUTER	IP address of next router	5.1.1.2 /0
2 MASK	IP mask (0=default route)	255.255.255.255 /32
3 METRIC	Cost of route	8
. QUIT	Previous menu	

21. Quit out of that menu and the subsequent menu.

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	5.1.1.1 /0
2 REMOTE	Remote IP address (if not Ethernet)	5.1.1.2
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	1 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

22. Quit out of that menu
23. Select option 5 Channels to get a menu that will allow us to set up the type of port used for this entry. In this case we want to set up it up as X21 and for ease of use we will use X21 link 2.
24. Select option 3 X21L2
25. From the submenu that is displayed select option 1 YES.
26. Quit out of that menu and verify that the X21L2 has got a current value of 'YES'
27. Quit out of that menu.

The last step of the configuration is again optional but for clarity it is recommended that the name is changed.

28. Select option 0 NAME and type in the chosen name followed by RETURN, as this link is going to be connected to Birmingham we will use that as the name.
29. Quit out of that menu and the following should appear:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	ISDN No: 2222	5.1.1.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

This screen shows that we have 2 networks set up.

1. Network 0 is an ISDN link to a router called Birmingham and has the IP range 5.1.1.0 assigned to it and will dial ISDN number 2222.
2. Network 1 is the local Ethernet and has the range 10.1.1.0 assigned to it.

The final step of this basic routing configuration is to reboot the VIPER to ensure that the changes have been activated.

30. From the London NETWORKS screen quit that menu and go to the Main Menu.
31. Select option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.
32. After about 10 seconds the Main Menu will then reappear.

6.6.3 Power Reset the Viper

Alternatively you could just undertake step 1 and 'power reset' the VIPER. However a soft reboot takes a lot less time as the VIPER doesn't need to go through its power on sequence again.

The remote VIPER will need to be configured in exactly the same way except the names and IP addresses are swapped around.

Section 7

IP Networking

7.1 Introduction to IP Networking

An IP network uses various standard protocols, but the most fundamental of these is IP itself. This states that all data is packaged into datagrams. An IP datagram contains a header and data. The header in turn is divided into various fields, of which the most important is the destination address. This specifies the desired destination of the datagram. IP does not provide a guarantee that a datagram will be delivered to the destination address. If there is a problem, such as overloading of a section of the network, a datagram may be lost. It is the responsibility of protocols, which use IP to add error recovery, if it is needed. Error recovery is typically dealt with in one of three ways:

By using TCP

Which is a protocol, which is specifically designed to provide error recovery.

By a property of the application.

An application may provide error recovery as a side effect of the way it works. For example, if an application sends a datagram to request information, the lack of a reply indicates that the request must be re-sent.

By not requiring error recovery.

Some applications may not need error recovery. An example of this is a network clock, which periodically sends the current time to clients. If a message is lost, the client can simply assume its own clock is sufficiently accurate until the next update is received.

7.1.1. IP Addresses

Each **IP datagram** is routed based on its IP header. This contains (amongst other items) the IP address of the destination for the datagram. A router looks up the destination address in its routing table and deals with the datagram based on what it finds in the table. While a router could simply have all possible addresses in its routing table, such a table would be impossibly large. To reduce the size of routing tables, IP addresses are grouped into networks. This means that a router need only list, at most, every network in its table instead of every individual address. There are about a thousand times more addresses than networks, so this makes the storage and indexing of routing tables much easier. In practice, a router may have explicit routes listed for a tiny fraction of all possible networks, with a default route used for any others.

The IP address is 32 bits and is considered to have two parts, called *the network number* and the *host number*. IP addresses are written as four decimal numbers separated by dots, with each number representing eight bits of the address, and therefore ranging from 0 to 255. This notation is called “dotted quad”.

Traditionally, IP addresses are classified based on their value as follows:

Class A

This covers addresses in the range 1.0.0.0 to 126.255.255.255 allowing only 126 Class A networks, each of which has up to 16,777,214 addresses.

Loopback

This is a special group of addresses covering the range 127.0.0.0 to 127.255.255.255, which cannot be allocated to specific hosts. These addresses are reserved for testing such that the IP software should ensure that anything sent to one of these addresses should be looped back and received as if it were coming from an external source. Datagrams with these addresses should never leave the originating host.

Class B

This covers addresses in the range 128.0.0.0 to 191.255.255.255 allowing 16,382 class B networks, each of which has up to 65,534 addresses.

Class C

This covers addresses in the range 192.0.0.0 to 223.255.255.254 allowing 2,097,150 class C networks, each of which has up to 254 addresses.

Class D

These are special addresses used for multicasting (transmission to several destinations simultaneously). They cover the range 224.0.0.0 to 239.255.255.255.

Class E

These are the range 240.0.0.0 to 247.255.255.255, which is reserved for experimentation and future standardisation.

Broadcast

This is the address 255.255.255.255, which represents a broadcast to the local network.

It is easier to see why these particular ranges are used if the addresses are written in binary. Here is a table showing the bit patterns with a bit shown as 'n' if it is part of the network number and 'a' if it is part of the host number.

Class A	0nnn nnnn aaaa aaaa aaaa aaaa aaaa aaaa
Loopback	0111 1111 aaaa aaaa aaaa aaaa aaaa aaaa
Class B	10nn nnnn nnnn nnnn aaaa aaaa aaaa aaaa
Class C	1100 nnnn nnnn nnnn nnnn nnnn aaaa aaaa
Class D	1110 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
Class E	1111 0??? ??? ???? ??? ???? ??? ????
Broadcast	1111 1111 1111 1111 1111 1111 1111 1111

You can see from this that the loopback network appears to be a Class A network. However, the loopback network is always treated specially. In general, ordinary network numbers cannot have either all zero bits or all one bits in the 'n' bits.

7.1.2 IP Address Mask

The structure of IP addresses is usually described by referring to the address mask. This concisely describes the division of an IP address into network number and host number, as described in the above section. The binary representation of the address mask has a one bit corresponding to each bit in the network number portion of the IP address, and a zero bit for the host number. Here are the masks for the normal IP address classes:

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

When describing a network number, it is common to write the network number as "address/masksize". For example, "192.1.2.0/24". This means the mask is 24 bits or 255.255.255.0. While it is theoretically possible to have a mask with non-contiguous 1 bit, there is no benefit it doing so, and a lot of equipment does not support it.

7.1.3 IP Address Subnets

The address masks used often differ from those listed above because **subnetting**. This is the division of a network into several smaller networks. Subnetting is used to conserve the number of IP network numbers required and to simplify routing. It can simplify routing because a number of subnets can be treated by external networks as if they were a single network.

Subnetting simply uses a more specific address mask than normal for the address class. For example, the class C network 192.0.1.0 could be divided into 14 subnets each with 14 hosts by using the mask 255.255.255.240, which is 1111 1111 1111 1111 1111 1111 1111 0000 in binary. This is typically written as 192.0.1.0/28. The portion of the host number, which is covered by the mask, is called the subnet number. This means that the IP address has three parts: the network number, the subnet number, and the host number. Values in each of these parts which have a binary representation of all ones or all zeros can not be assigned to networks or hosts and usually have a predefined special meaning. This is why the class C example does not have 16 subnets or 16 hosts per subnet.

Normally each subnet corresponds to a physical network. For example, if an office building has an independent network on each floor, and the building as a whole has one connection to external networks, the building could be assigned one network number and subnetting could be used to assign a subnet per floor. This allows external routers to have only one routing table entry for the building, while internal routing between subnets ensures that traffic does not leave a physical network unnecessarily.

7.1.4 Different Subnet Sizes

Division of a network into subnets of different sizes can be very useful because many networks are composed of physical networks of quite different sizes. For example, a head office might have an Ethernet with twenty hosts and require connection to branch offices, which have networks of five machines each. Using the same size subnet mask, the best that can be achieved is to use a mask of 255.255.255.224 (in binary this ends ...1110 0000, so it can be written ".../27"). This gives six subnets as follows:

- binary ...001a aaaa, decimal ...32 to ...63
- binary ...010a aaaa, decimal ...64 to ...95
- binary ...011a aaaa, decimal ...96 to ...127
- binary ...100a aaaa, decimal ...128 to ...159
- binary ...101a aaaa, decimal ...160 to ...191
- binary ...110a aaaa, decimal ...192 to ...223

However, if the branch offices use the mask 255.255.255.248 (...1111 1000, or /29) there are now up to twenty subnets available. These are: (...0100 0aaa) ...64 to (...1101 1aaa) ...216, each of which can have up to six hosts. Note that some subnets cannot be used because the head office would see them as invalid. These are the eight which are of the form ...000x xaaa (...0/8/16/24) and ...111x xaaa (...224/232/240/248). These include the values, which are invalid under either of the two masks. In general, where there are several masks in use, an address is not valid as a host address unless it is valid with all masks.

The term "Variable Length Subnet Masks (VLSM)" is often used to describe this type use of subnet masks.

7.1.5 IP Routing

The routing of IP datagrams is based on the destination address. When a router receives a datagram, it extracts the network and host portions of the destination IP address (when subnetting is used, the network portion includes both the network number and the subnet number) and reaches one of these conclusions:

- The router is on the specified network, and the host address specifies the router itself
- The router is on the specified network, but the host is not the router itself
- The router is not on the specified network, but it knows another router which is closer to the destination
- The network is unknown

The router uses its routing table to find out which of these applies. In theory, the router has a table of all known IP networks. If the router matches an address against any suitable entries in the routing table, it selects the best one, and forwards the datagram as specified in that entry. If the router does not find an entry, it considers the datagram to be undeliverable and may send an error message to the address specified in the datagram as being its source.

In practice, a routing table is smaller than this theoretical model. Firstly, not all routes may be entered. Typically only the best is entered, but a small number of alternatives may be used to provide a way to recover from failures. **RIP** is used, only the best route need be entered because **RIP** can automatically replace a failed route with the next best working route. Secondly, a routing table may use a *default route*, which is used when no specific route can be found. This allows a router, which connects to the Internet to list only local networks in its routing table and to send all traffic, addressed to non-local routes over its Internet connection. This has the side effect that such a router cannot tell if a destination address specifies a non-existent network.

7.1.6 IP Routing Metrics

The above section describes how a router uses a routing table to find possible routes to a destination. When there are several potential routes, some method for choosing between them must be used. One such method is to assign to each route an estimate of how good it is and to use this as the basis for deciding the best route. Such estimates are called *route metrics*. A simple metric is the minimum number of routers on a path to a destination. This is the *hop count*, which is computed automatically by the **RIP**. The hop count is used by preferring the route with the smallest hop count.

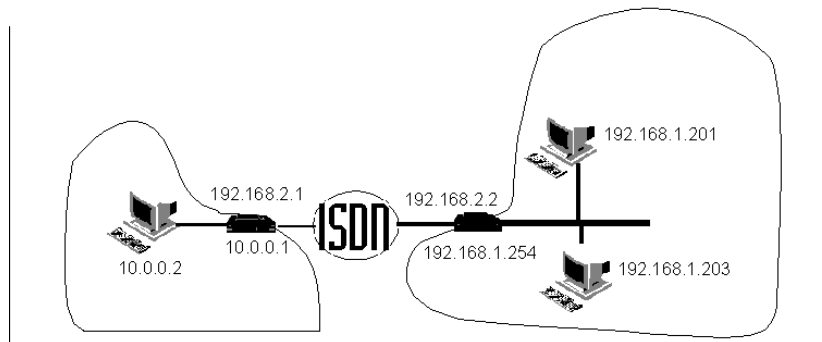
7.1.7 Selecting IP Addresses

There are two important addressing schemes. They differ only in their treatment of point-to-point links (i.e. dialup and leased lines). The traditional scheme is described first, followed by a description of the newer “unnumbered interface” scheme.

7.1.7.1 The traditional IP addressing scheme

Each physical network (e.g. Ethernet) is allocated a network number. For example, an Ethernet which connects twenty machines might be allocated the network number 192.168.1.0, which is a class C network. This network number may actually be a subnet. This is a common arrangement to conserve addresses. Twenty machines could be accommodated within a subnet, which uses five bits for the host portion of the address. For example, using an address mask of 255.255.255.224, the range 192.168.1.32 to 192.168.1.64 covers one subnet of the above class C network.

As well as the obvious networks, which connect ordinary host machines, there may be other networks, which serve to connect routers. A point-to-point link between two routers is itself a network and must be allocated a network number. Such a network can only have two hosts (the routers themselves) so it only needs the smallest size subnet. This corresponds to the mask 255.255.255.252, which allows only four addresses. (Note: the mask 255.255.255.254 cannot be used because the maximum value of the host portion of an address is reserved to represent the broadcast address). Here is a diagram of a small network showing the assignment of addresses.

Diagram of traditional addressing example

In this example, there are two LANs connected over the ISDN by routers. A line is drawn around each LAN and you can see that the routers each have two addresses. One address on the LAN and another for the ISDN link.

7.1.7.2. The unnumbered interface scheme

In order to reduce the number of separate IP addresses, which need to be allocated, the unnumbered addressing scheme was devised. It allows a router to use the same address for several links. The rules are that:

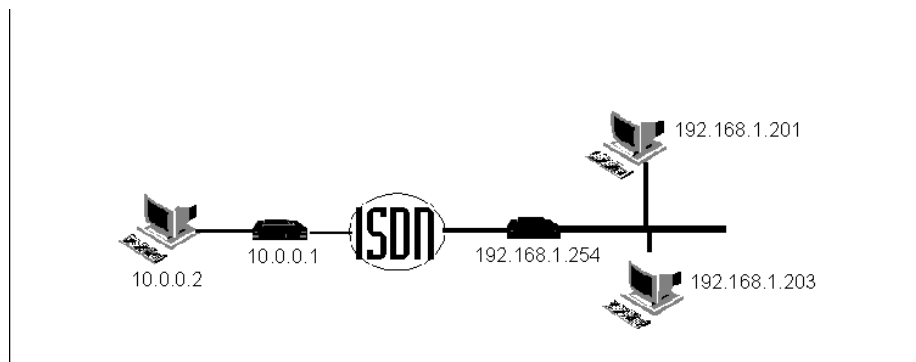
- Each broadcast (such as Ethernet) network needs a network number.
- Each router needs at least one IP address.
- Point-to-point links can reuse an address assigned to the router.

Normally this means that only one IP address is allocated to a router, and this is the address of the Ethernet port. Note that unnumbered addressing exposes the shared address and mask to devices, which would not see these values. This means that they must support this type of operation. For example, suppose that a router is assigned the address 10.0.0.1 because its Ethernet uses the network 10.0.0.0/24. Any device connected to it must be prepared to send all frames addressed to 10.0.0.<anything> to this router. With the traditional addressing scheme, only the addresses 10.0.0.1 (the router) and 10.0.0.255 (the broadcast address) need be supported.

This scheme is discussed in RFC 1716 2.2.7, where it is specified that the IP address which is reused for point-to-point links be called the *router-id*.

Here is an example of a network using unnumbered interfaces. Compare this with the diagram in the previous section. You can see that it requires less configuration as well as using fewer addresses.

Diagram of unnumbered interface example



7.1.8 Guidelines for choosing IP addresses

There are a few rules, which should be followed when configuring an IP network. Each rule given here is accompanied by an explanation of why the rule should be followed. In some cases a network administrator may want to ignore a rule and, since IP protocol implementations are not subject to a centralised approval process, many implementations take care to avoid relying on other equipment obeying all the rules to allow more flexibility and to avoid problems if a device on the network breaks a rule accidentally due to an erroneous implementation.

Draw a diagram of the proposed network

This is very important. When you are connecting networks with routers, it can be very easy to confuse one network with another, to overlook a need for a static route, or even to assign an address belonging to the wrong network. A simple diagram, showing which addresses belong on each part of the network, can avoid many of these problems.

7.1.8.1 Do not use IP addresses, which are not reserved for you

IP network numbers are allocated to organisations as necessary. All connections to the **Internet** must use officially allocated addresses to avoid conflict with other users of the Internet. If a host were to try to use an address not allocated to it, either data destined for it would go to the host, which had been allocated the address, or the data would be lost. Several groups of IP addresses have been reserved for hosts, which do not connect to the Internet. These are:

- One Class A network: 10.0.0.0 (10.0.0.0/8)
- Sixteen Class B networks: 172.16.0.0 to 172.31.0.0 (172.16.0.0/20)
- 256 Class C networks: 192.168.0.0 to 192.168.255.0 (192.168.0.0/16)

In general, hosts should be assigned addresses from one of these ranges if they have not been assigned official Internet addresses. If hosts are configured to use other addresses, and the network is later connected to the Internet, they will normally need to be reconfigured to use valid addresses even if they do not need to be able to use the Internet themselves. This is so that a router, which connects to the Internet, can tell whether or not an address refers to a local host or to a host on the Internet.

Avoid assigning an invalid address to a host

As described in the section **IP addresses**, both the subnet portion and the host portion of an IP address have two prohibited values. These are the values whose binary representation is all zeros and all ones. Even without converting values to binary, it is easy to tell which values these are. They are the minimum and maximum values. For example, with subnet mask 255.255.255.240 (... 1111 0000) the network number 192.168.3.0 is divided into subnets 192.168.3.0, 192.168.3.16, 192.168.3.32, 192.168.3.48, ... 192.168.3.240. Of these, 192.168.3.0 and 192.168.3.240 are the prohibited pair. Similarly, on an individual subnet, for example 192.168.3.32, the first and last host numbers are prohibited (here 192.168.3.32 and 192.168.3.47). Some implementations of IP may permit the use of

the all zeros value in a host or subnet number, but it is inadvisable to exploit this because this is not widely supported. The all ones value is the broadcast address, so it can never be assigned to a host.

Where possible, use address masks of the same size

Some equipment does not support the division of a network into different size subnets (as described in the **Section 6.1.4** - Different subnet sizes). Such a division is correct, but avoiding it may avoid problems. Unfortunately, it is often not practical to avoid using different size address masks when different size networks are interconnected.

7.2 Introduction to IPX Networking

The IPX family of protocols uses **datagrams** to transport data in a manner similar to **IP**. Where **TCP** provides an error recovery mechanism for use with IP, IPX has an equivalent called **SPX**. IPX addresses are somewhat different, as explained in the next section.

7.2.1 IPX Addresses

An IPX address has two parts. These are the *network number* and the *node number*. The network number is 32 bits and the node number is 48 bits. The node number is determined by the physical network address. For example, every piece of Ethernet hardware has a unique Ethernet address built in. Since the size of an Ethernet address is 48 bits, when IPX is used over an Ethernet, the Ethernet address is used as the node number. When IPX is used over other types of network, which have smaller addresses, the node number is padded with zeros. The network number must be manually assigned to each network, but as a special case, the value zero is reserved to indicate the local network.

7.2.2 Learning the IPX Network Number

Although the network number must be manually assigned to an IPX network, it is usually not necessary to configure this address into every host on the network. This is because some machines may be able to learn the network number by listening for other machines on the network. This relies on the fact that only one network number can be assigned to each physical network, so any message received must specify the local network number.

IPX networks are usually based around servers and clients, and applications written for IPX networks usually have the property that clients cannot communicate with each other without the assistance of a server. This means that clients cannot communicate on a network until they discover a server, which means that they can learn the network number from the first server that they discover.

To guarantee that the lack of a network number never prevents a machine from communicating, it is necessary that the network number be known by all servers and all routers. In practice, routers can usually learn the network number also, because clients usually communicate via a router only after they have already attached to a server. This guarantees that the router can learn the network number from the client. The main exception to this is a network, which has no servers. Some networks consist only of clients, which communicate with servers via a router. In this case, only the router needs to know the network number because clients can learn it from the router.

7.2.3 IPX Routing

When a router receives an IPX datagram, it extracts the destination network number and looks up this network in its routing table. If the network is one directly connected to the router, the destination node address must be examined to see if the datagram is destined for the router itself. If the destination is not the router itself, the datagram passed on via the directly connected network. When the network is not directly connected, the routing table will specify another router which is closer to the destination

and which is on a directly connected network. The datagram can be sent to this other router, which will forward it as necessary.

7.2.4 IPX Routing Metrics

When there are several potential routes to a destination, the best is selected by comparing *metrics*. IPX uses two different metrics: hop count and ticks. The *hop count* is a count of the number of routers on a path to a destination, while *ticks* is an estimate of the time taken to follow a path. Both are calculated automatically **RIP**. The route with the lowest ticks value is considered the best route, and where there are several with the same ticks value, the one with the lowest hop count is preferred.

7.3 Protocols

This section describes the various protocols used by the router. While its is not normally necessary to understand these protocols, it can be useful to know what the router is doing when trying to find a network problem.

7.3.1 ARP - Address resolution protocol

This is used when an **IP address** must be resolved (i.e. translated) to an Ethernet address. It allows this process to be done completely automatically. For this reason, it is nearly always used on Ethernet networks.

ARP works by broadcasting an *ARP Request*, which asks for the owner of a specified IP, address to reply giving their Ethernet address. If the machine, which owns that IP address, is available, it replies with an *ARP Reply*. The Ethernet address sent in the reply is saved so that it can be used in future without sending a new request and waiting for a new reply. However, to allow for machines being moved between networks, the address is discarded when it becomes too old. This age is generally about ten minutes. The routers ARP cache can be examined from the ADMIN ARP menu. ARP is defined in "RFC-826".

7.3.2 RIP - Routing Information Protocol

RIP is used to exchange routing information with other routers. It is actually the name for two different protocols, which use the same basic methods. One is used with **IP** and the other with **IPX**. A router can use RIP to learn about and dynamically update routes to other networks. When it is powered on, it can send out a RIP request asking for any routes to networks, which other routers may know about. This information, which is entered into the routing table, can be continually updated as new routes become available or old ones are timed out.

The standards, which specify the RIP protocol, suggest that RIP 'advertisements' are sent about every 30 seconds by every router on the network. This is so that no router will have out of date information in its routing table for more than 30 seconds. This works fine for local networks where a broadcast every 30 seconds is not significant, but on links such as **ISDN** lines in particular, it can keep a link up when no other useful traffic is present.

There are two ways around this particular problem. The first is to turn off RIP completely on dial up links and use *static routes*. This means that you never have to worry about RIPs but you have to enter the static routes by hand. The other solution is to use *triggered RIP*. This works by assuming that, unless the router is told otherwise, the routes to networks at the end of its dial-up links will always be valid. If the routes do change, then the routers will bring up the link and update their routing tables. This works well if your networks are stable but will not have the intended effect (of reducing costs) if networks are frequently added or removed.

The IP version of RIP is defined in "RFC-1058".

7.3.3 IPX SAP - Service Advertising Protocol

This provides a mechanism whereby services can be located on an **IPX** network. A machine can broadcast a *Request* or a *Get Nearest Server Request* to find a server. To make this work, any routers on the local network must keep a table of non-local servers so that they can reply to such requests. This is done by listening for and sending SAP broadcasts. Every router broadcasts its SAP table every 60 seconds. By listening for broadcasts from other routers, a router can keep its SAP table updated with a complete list of all services.

Servers act the same way except each always has its own services listed in its own SAP table. An entry in a SAP table is deleted if no broadcast has been received for three minutes, which describes the service. This ensures that services are no longer considered to be available if a server becomes unreachable.

7.4 Call Charge Limiting

All routers in the VIPER Range include a call charge-limiting feature, which operates on all ISDN links. This mechanism limits the use of such links to prevent unexpected large bills to result from bad network configurations, or faulty network components.

The following example shows the default settings of the Charge Limiting feature present on all VIPER Routers.

Command	Description	Current Value
0 CALLRATE	ISDN call cost (per minute)	5
1 CALLMINIMUM	Minimum ISDN call cost	5
2 SPENDRATE	Total spending per 30 days	10000
3 CREDITLIMIT	Maximum accumulated credit	1000
4 STARTUPCREDIT	Initial credit at each system startup	1000
5 CREDIT	Current credit	(981)
. QUIT	Previous menu	

This mechanism which defaults to the above enabled state, controls the spending on ISDN calls over a rolling period of time.

To describe the use of this feature I will use the analogy of a bucket, containing a quantity of gold coins. It requires a number of coins to make an ISDN call and a number of coins every minute to keep the call going, just like you are feeding money into a pay phone. This is the first two values shown above, in this case 5. This means that 5 coins are taken out of the bucket to start a call and 5 more coins are taken out every minute. If there are not 5 coins in the bucket when the router tries to bring up an ISDN connection to a new destination the call will not be made, and if during a call there are not 5 coins to pay for the next minute the call will be closed.

The bucket can only contain a limited number of coins, which is controlled by the CREDITLIMIT value. Any additional coins that are added to the bucket once it is full are lost. The STARTUPCREDIT field tells the system how many coins to put in the bucket to start with. In this case it is the same as the size of the bucket indicating that the bucket will be full when the router is turned on or Reset.

The credit field tells you how many coins there are currently in the bucket. This is a display field and cannot be changed by the user.

Above the bucket is a leprechaun making coins out of straw, and dropping them into the bucket. If the bucket is already full they just fall on the floor and are wasted. The SPENDRATE field indicates how

fast he is working. In the above example he is making 10000 coins every 30 days. He is a magical leprechaun and works 24 hours a day at a very steady rate, producing 1 coin every 4.32 minutes in the above example.

By changing the values in the configurable fields you can control this process very closely. If you wish to disable the mechanism, you set the CALLRATE and CALLMINIMUM to zero so that the bucket remains full all the time and no calls are prevented. You could instead make the bucket so small that it can never contain enough coins to make a single call. This will prevent all outgoing calls.

In normal use it is expected that calls be made using the reservoir of coins in the bucket, and the constant slow filling tops the bucket up over time. This cover both the case of a large number of short calls being made, or a few long calls being made over any period of time.

In the above example enough coins are being made each day to make 67 minutes worth of calls the bucket contains enough for 200 minutes worth of calls. This means that it is adjusted for a user who makes on average 67 minutes worth of calls in a day but on some days may make up to 200 minutes worth of calls.

It should be understood that this mechanism is designed mainly to prevent surprise ISDN bills caused by network components holding links up when not expected to. It could also be used to restrict access where the services provided by the router are publicly available and open to misuse.

When the usage limit is exceeded the bucket will be empty and calls will be barred. The system will automatically recover if the source of the problem is removed. After about half an hour a short call may be made again, if you are using the default settings, since 6 coins will have been added enough to pay for 1 minute of call. If the problem persists this will immediately be spent and the call will be barred again. This behaviour should cause the used to become suspicious and correct the problem.

This mechanism does not prevent the unit from answering so it remains possible for a network administrator to dial into the unit and by examining the log find the source of the problem.

7.5 ISDN Call Management

All routers in the VIPER Range include an ISDN interface. On the MultiDrop E1 Vipers product this takes the form either a Primary Rate (ISDN30) Rj 45 120 Ohm interface presented in the same position as the ISDN 2 port on the standard Viper. This section describes the facilities in the routers that allow you to control use of this interface when it's a Bri ISDN Interface.

7.5.1 ISDN Number Configuration

The DIALLIST menu has several pieces of information for each number. Here is an example:

	Number to dial	Charge rate	Priority	Failed
0 N0 (1 call)	456789	LOCAL	10	-
1 N1	01442236336	NATIONAL	20	1h24m
& ADD	Add new item			
% DELETE	Delete item			
. QUIT	Previous menu			

The number of calls currently active to each number is shown. Also the charge rate, a priority and an indication of when there was last a failure to get through. By selecting a number, these things, including the number, but not the number of calls, can be edited. The dial list is sorted by priority,

with 0 the highest, and then by charge rate, cheapest first. Real-time fields such as the number of calls and the times since failures will not be refreshed on the screen unless, enter is pressed.

Command	Description	Current Value
0 NUMBER	Number to dial	01442236336
1 PRIORITY	Priority of number	20
2 CHARGERATE	Charge rate for this number	NATIONAL
3 INTERFACE	Interfaces to use (ordered choice)	BASICPRIMARY
4 LASTFAILURE	Elapsed time since failed to connect	1h24m
. QUIT	Previous menu	

The LASTFAILURE option shows how long since an attempt to call this number was unsuccessful. It is cleared when a successful call starts or ends. It is used to choose which number will be used for an outgoing call. Starting at the top of the priority list, all numbers with recent failures (currently defined as less than 8 minutes) are skipped. If all numbers have recent failures, then the one that failed longest ago is used. This field can be cleared manually, for example if the problem has been cleared up, by selecting it and pressing return or entering 0. It can also be set to a non-zero value, for example 1 (1 second), to temporarily inhibit the use of that number. The number may still however be used if the other numbers fail.

There are 4 options for the charge rate; these are used to control the minimum call length, when this feature is enabled, as described later.

Command	Description	Current Value
0 LOCAL	Local rate	
1 REGIONAL	Regional rate	
2 NATIONAL	National rate	<<<<<<
3 INTERNATIONAL	International rate	
. QUIT	Previous menu	

7.5.2 Minimum Call Length

When an ISDN call is successfully connected you are immediately charged a fixed amount. Since you have already paid this, it is most cost effective if you then hold the call up for the whole amount of time that you have paid for. After this initial period you can then revert back to the normal idle time-out periods. The call will not be dropped at the end of the minimum call length if data crossed the link in the last 10 seconds of the period.

This can be controlled, using a table of minimum call duration's together with the Charge Rate field now associated with all ISDN numbers. The following GLOBAL ISDN screen shows how these minimum values are set in seconds.

Command	Description	Current Value
0 CHARGES	Charge limiter	
1 MSN	Multiple Subscriber Numbering	
2 ACCESS	Access Control	
3 CHECKCLI	Check CLI Before Answering	NO
4 DAYTIMES	Daytime Minimum Call Duration's	L:60 R:45 N:30 I:20
5 EVETIMES	Evening Minimum Call Duration's	L:180 R:120 N:60 I:25
6 WEEKENDTIMES	Weekend Minimum Call Duration's	L:180 R:120 N:60 I:30
. QUIT	Previous menu	

The DAYTIMES, EVETIMES and WEEKENDTIMES options take you to another screen allowing the individual times to be adjusted.

Command	Description	Current Value
0 LOCAL	Minimum Local Call Duration	60
1 REGIONAL	Minimum Regional Call Duration	45
2 NATIONAL	Minimum National Call Duration	30
3 INTERNATIONAL	Minimum International Call Duration	20
. QUIT	Previous menu	

The local value must be higher than each of the other values since this value is used by the answering end of the connection.

Command	Description	Current Value
0 DIALLIST	List of numbers to dial	2 numbers
1 CLILIST	List of acceptable calling numbers	Not checked
2 CLIACTION	Dialback on CLI Match	NO
3 ACCESS	Use access control	NO
4 MINCALL	Control Minimum Call Lengths	NO
5 CLEAR	Cleardown time	60
6 DAY CLEAR	Daytime cleardown time	60
7 EVE CLEAR	Evening cleardown time	60
8 WKEND CLEAR	Weekend cleardown time	100
. QUIT	Previous menu	

The use of minimum call lengths can then be enabled on an individual destination basis, using the MINCALL option on the NETWORK ISDN menu.

7.6 IP Express

This section describes the (QoS) IP Prioritisation mechanism present on the VIPER. This mechanism is vital in enabling the Voice over IP mechanism to operate correctly.

The mechanism is enabled in two stages. First a global switch is used to enable the mechanism on the router as a whole. This reduces the buffering on output WAN links, to enable more precise control of the traffic on the link. This will reduce the overall speed of the router slightly when running at high link speeds, but is insignificant at lower link speeds. The following example shows this switch in the Menu Structure.

Command	Description	Current Value
0 NAME	Router NAME	Top
1 IP	IP enabled	YES
2 IPX	IPX enabled	YES
3 PRIOR	IP Express PIPE enabled	YES
4 SNTP	SNTP IP Address	0.0.0.0 /0
5 SYSLOG	SYSLOG IP Address	0.0.0.0 /0
6 SYSPASS	System password	
7 ISDN	ISDN configuration	
8 ERASE	Erase all configuration	
. QUIT	Previous menu	

Then on each Network that is configured in the router it is possible to control the amount of bandwidth allocated to a list of IP Address/Port combinations. Two new screens allow this to be configured. The first screen accessed from the IP Menu allows the total amount of bandwidth that you wish to reserve for priority traffic to be specified. Setting this value to zero disables the priority mechanism on this port. This screen also allows you to specify the size of the fragments that non-priority traffic will be broken up into, when priority traffic is being transported. This value should be adjusted to achieve sufficient priority performance while reducing the impact on non-priority traffic.

Command	Description	Current Value
0 RESBAN	Reserved bandwidth (bytes/sec)	2000
1 FRAGSIZE	Fragment size	128
2 PRIOR	IP Prioritisation	1 entry
. QUIT	Previous menu	
COMMAND: NETWORK Bottom IP PIPE		

The PRIOR option on this menu takes you to the list of IP Address/Port combinations. These are presented using the standard list mechanism, allowing entries to be added or removed. Selecting an entry takes you to a further screen allowing modification of the Address and Port.

Code	IP Address	Port number
0 P0	10.0.0.1	2001
1 P1	0.0.0.0	2000
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

The address and port can be set to any value required by your application. An IP address of zero acts as a wildcard matching any UDP frame sent to any IP Address on the specified port. A port of Zero also acts wild matching all UDP frames sent to the specified IP Address. You should not leave both IP Address and Port set to zero for the same entry. For WAN links this table of entries it then used to test all outbound frames. Frames that match the criteria are then sent in preference to non-priority traffic up until the reserved bandwidth limit is reached.

Setting up this table on the Ethernet port enables a slightly different mechanism. By setting the reserved bandwidth to any non-zero value you activate a second queue for inbound frames received

from Ethernet. Frames are then tested, as soon as they are received by the hardware, against the list of values specified on the Ethernet Network, and those that match are placed on the priority queue. This priority queue is then always serviced in preference to the normal queue, passing the frames on up into the main routing procedures. The fragment size is not used on the Ethernet port.

Command	Description	Current Value
0 ADDRESS	IP Address (0 Matches any Address)	0.0.0.0 /0
1 PORT	Port number	2000
. QUIT	Previous menu	

The priority mechanisms only operate while priority traffic is flowing. This means that while no priority traffic is present the normal data gets full use of the link and is not fragmented. As soon as priority traffic is seen the fragmenting mechanism is activated. This will automatically deactivate again a few seconds after the last priority frame is processed.

The bandwidth reservation mechanism is also dynamic in that it will fill the reserved bandwidth with priority frames provided there are frames to send. If there are no more priority frames ready for transmission, fragments of normal frames will be sent instead. Once all the priority bandwidth is used up the priority and non-priority queues will then be serviced equally, with frames being taken from either queue, on a first come first served basis.

Section 8

Viper Menu System

The majority of the configuration is done via menus. This section describes them in detail. You can reach the menus by connecting to the router through a management port or via Telnet. Access via Telnet can be password protected.

8.1 General Menu Operation

There are no specific commands to save any configuration changes - all changes are saved automatically. However some changes to the configuration require the router to be rebooted before they take effect. You should therefore reboot the router after making any changes to the configuration. Since most configuration changes take place immediately it is recommended not to reconfigure the router while user traffic is being handled.

There is one command, which erases the entire currently stored configuration - including any settings pre-set before shipment. It is advised that this command be used rarely and with a great deal of caution. It is much safer to change individual settings or to delete unwanted items from the appropriate menus.

All menus have the same structure. Here is an explanation of the general structure of a menu, based on the following example:

London IP ROUTING TABLE						
Destination	Msk Router	Flags	Age	Me	Type	Name

-	PREVIOUS PAGE					
0	IP:147.1.16.254	/32 0.0.0.0		2s	0	Self eth0
1	IP:255.255.255.255	/32 0.0.0.0	N	2s	0	Self (-)
2	IP:10.255.255.255	/32 255.0.0.0	N	2s	1	Bcst London
3	IP:147.1.16.255	/32 255.255.255.0	N	2s	1	Bcst eth0
4	IP:147.1.255.255	/32 255.255.0.0	N	2s	1	Bcst eth0
5	IP:192.168.10.255	/32 255.255.255.0	N	2s	8	Bcst Birmingham
6	IP:147.1.16.0	/24 0.0.0.0	T	2s	1	Fwd eth0
7	IP:192.168.10.0	/24 147.1.16.100	T	2s	8	Fwd London
8	IP:0.0.0.0	/ 8 0.0.0.0		2s	0	Drop (-)
9	IP:127.0.0.0	/ 8 0.0.0.0		2s	0	Self (-)
+	NEXT PAGE					
&	ADD	Add new item	%	DELETE	Delete item	. QUIT

Previous menu						

NOTE: manual changes to this table are transient use the NETWORKS menu for permanent changes

The heading contains the router name, here London (as set with the GLOBAL NAME command), and the title of the menu. The main section has one option per line. Each option has:

- A shortcut key.
- An option name.
- A description. On some menus (such as the ADMIN IPRROUTE menu shown here) this is a summary of an item, which can be expanded by choosing it from the menu.
- Where applicable, a current value. If the item describes a list, this is simply the number of items in the list. If the item cannot be changed, the value is shown in brackets.

To select an item from a menu, you can either hit the single shortcut key, or type in the whole command name followed by a space or RETURN If you use the shortcut key or the command

followed by RETURN to enter a sub-menu, you remain at the sub-menu and can give several commands from that sub-menu until you select QUIT. This is more convenient for manual operation. If you type in the command name followed by <SPACE> to enter a sub-menu, the sub-menu will quit automatically after one command. This is necessary to allow a list of commands to be stored in a file.

If you have started typing the name, and want to use a shortcut key, you must erase the partial command name before the shortcut key will be recognised. The full command name is most useful for creating a file of commands to be sent to a router automatically. When you use a shortcut key, the full command name is automatically added to the command being entered. This ensures that the commands you have used to get to any menu are always shown at the bottom of the screen. The area between the menu and the command you are entering is used to show any relevant notes or warnings.

You can hit <ENTER> to redraw the menu. This is particularly useful when the menu shows a list, which can be updated automatically. The <ESCAPE> key can be used to cancel the current operation. This can be useful if the wrong option is chosen from the menu and you do not wish to change the selected option.

There are some standard options, which always have the same meaning if they appear on a menu. These are:

QUIT - Previous Menu

This appears on every menu, and allows you to quit to the previous menu without selecting any option.

PREVIOUS PAGE

This appears when there are items before those listed. Selecting this option redraws the menu starting up to ten items back from this menu. This is not a command itself because it simply scrolls through the same menu. You can choose any option on a menu by entering its full name regardless of whether or not it is on the section visible.

NEXT PAGE

This appears when there are items after those listed. Selecting this option redraws the menu starting up to ten items further down the current menu. This is not a command itself because it simply scrolls through the same menu. You can choose any option on a menu by entering its full name regardless of whether or not it is on the section visible.

ADD - Add new item

This appears when the menu is a list of items, which you can add to. When you select ADD, a new item is added to the menu. The corresponding shortcut key is <&>(ampersand). If the menu is redrawn immediately, the new item is at the top. This makes it convenient to select the new item to define the details within the item.

DELETE - Delete item

This appears when the menu is a list from which you can delete items. When you select DELETE, you are presented with a new menu called DELETE ITEM. Select the item to be deleted from this menu. If you decide not to delete any item, you can use the QUIT option to exit from the DELETE ITEM menu without selecting any item.

8.2 Main Menu

London Main Menu		
Command	Description	Current Value
0 GLOBAL	System Configuration	
1 NETWORK	Configure networks, routes etc	2 entries
2 HARDWARE	Configure Hardware	
3 ADMIN	Administration of running system	
4 STATUS	Current Status	
5 STATISTICS	Recent Statistics	
6 WANSTATS	Recent WAN Statistics	
7 DEBUG	Debugging facilities	
. QUIT	Previous menu	

The main menu has these options:

GLOBAL - System Configuration

This leads to the GLOBAL menu, configuring the items, which apply to the router as a whole.

NETWORK

This leads to the NETWORK menu, which configures the networks known to the router. It also allows the networks to be associated with specific ports.

HARDWARE - Configure Hardware

This leads to the HARDWARE menu, which configures the various hardware-specific aspects of the ports. Use the NETWORK name CHANNELS menu to tell the router what networks are connected to each port.

ADMIN - Administration of running system

This leads to the ADMIN menu which allows the user to view and modify the various internal tables, and which also provides commands used for network administration.

STATUS - Current Status

This presents a summary on one screen of the current status of the router, showing which links are operating and descriptions of any detected faults.

STATISTICS - Recent Statistics

This leads to the STATISTICS menu, which allows the user to view statistics gathered from various parts of the router.

WANSTATS - Recent WAN Statistics

This leads to the WAN STATISTICS menu, which allows the user to view statistics gathered from the various WAN links connected to the Router.

DEBUG - Debugging facilities

This leads to the DEBUG menu, which provides facilities for debugging the router and its environment.

QUIT - Previous Menu

Selecting this option quits from the main menu. If you are connected via a *Telnet session*, it closes the session. If you are directly connected to a management port on the router, it presents the MAIN menu again.

8.3 GLOBAL Menu

London		
Command	Description	Current Value
0 NAME	Router NAME	London
1 IP	IP enabled	YES
2 IPX	IPX configuration	IPX enabled
3 PRIOR	IP Express PIPE enabled	NO
4 SNTP	SNTP IP Address	0.0.0.0 /0
5 SYSLOG	SYSLOG IP Address	0.0.0.0
6 SYSPASS	System password	
7 ISDN	ISDN Configuration	
8 SNMP	SNMP configuration	None + None
9 ERASE	Erase all configuration	
. QUIT	Previous menu	

 COMMAND: GLOBAL

The items on this menu affect the router as a whole. They are:

NAME - Router name

This configures the router name, which is used in the heading of most menus. This is used to avoid confusion when configuring several routers as it reminds you which one you are connected to. It is also used as the default *Local User ID* within PAP/CHAP negotiation for PPP links.

IP - IP enabled

This allows you to disable all **IP** functions. This is not recommended since most of the remote bridge management functions will cease to operate.

IPX - IPX configuration

This leads to a menu that allows you to disable all **IPX** functions.

PRIOR - IP Express PIPE enabled

This allows you to enable IP Prioritisation on the router as a whole. This option also enables the use of proprietary UDP/IP header compression on WAN links between pairs of similar Routers.

SNTP - SNTP IP Address

This informs the router of the address of an SNTP Time server from which to set the routers own clock.

Note: The time and date are stored in volatile RAM and so are lost if the VIPER is rebooted or powered off. This option allows the VIPER to continuously update the time and date from a separate source.

SYSLOG - SYSLOG IP Address

This informs the router where to send the log messages directed to **SYSLOG**.

SYSPASS - System password

This is the password, which must be given when connecting via Telnet.

ISDN Configuration

This leads to the GLOBAL ISDN menu.

SNMP Configuration

This leads to the GLOBAL SNMP menu.

ERASE - Erase all configuration

Erases all configuration in the router, restoring it to the factory default state. Routing table entries are not cleared by this function, so you should normally reset the unit after performing this operation if you are connected to a network.

QUIT - Previous menu

Returns to the MAIN Menu.

8.3.1 GLOBAL ISDN Menu

London		
Command	Description	Current Value
0 CHARGES	Charge limiter	
1 MSN	Multiple Subscriber Numbering	
2 ACCESS	Access Control	
3 CHECKCLI	Check CLI Before Answering	NO
4 CHAPANS	Attempt to negotiate CHAP on answer	YES
5 DAYTIMES	Daytime Minimum Call Duration's	L:60 R:45 N:30 I:20
6 EVETIMES	Evening Minimum Call Duration's	L:180 R:120 N:60 I:25
7 WEEKENDTIMES	Weekend Minimum Call Duration's	L:180 R:120 N:60 I:30
. QUIT	Previous menu	

COMMAND: GLOBAL ISDN

The items on this menu lead to further menus to configure features, which affect all ISDN calls. They are:

CHARGES - Charge limiter

This leads to the GLOBAL ISDN CHARGES menu, which configures the call charge limiting facility.

MSN - Multiple Subscriber Numbering

This leads to the GLOBAL ISDN MSN menu, which configures the relationship between analogue lines on the router and the numbers associated with incoming calls.

ACCESS - Access Control

This leads to the GLOBAL ISDN ACCESS menu, which allows the access control time periods to be controlled.

CHECKCLI - Check CLI Before Answering

This switch enables the additional security of checking the CLI of the incoming call before it is answered. This switch must be set if you are using the Dial back mechanism, and may be set for additional security.

Ensure that you have set up appropriate CLI lists against each destination before setting this switch or you may no longer be able to dial in to the unit!

CHAPANS - Attempt to negotiate CHAP on answer

Normally the router will always attempt to negotiate PPP authentication starting with CHAP and then falling back to PAP. This can cause a problem when connecting to some other brands of router. This switch allows you to turn off CHAP negotiation completely on answer, to get over this problem.

DAYTIMES - Daytime Minimum Call Duration's

This leads to the GLOBAL ISDN DAYTIMES menu, which allows the daytime minimum call duration's to be set.

EVETIMES - Evening Minimum Call Duration's

This leads to the GLOBAL ISDN EVETIMES menu, which allows the evening minimum call duration's to be set.

WEEKENDTIMES - Weekend Minimum Call Duration's

This leads to the GLOBAL ISDN WEEKENDTIMES menu, which allows the weekend minimum call duration's to be set.

QUIT - Previous menu

Returns to the GLOBAL menu.

8.3.2 GLOBAL ISDN CHARGES Menu

	Command	Description	Current Value
0	CALLRATE	ISDN call cost (per minute)	5
1	CALLMINIMUM	Minimum ISDN call cost	5
2	SPENDRATE	Total spending per 30 days	10000
3	CREDITLIMIT	Maximum accumulated credit	1000
4	STARTUPCREDIT	Initial credit at each system startup	1000
5	CREDIT	Current credit	(1000)
.	QUIT	Previous menu	

COMMAND: GLOBAL ISDN CHARGES

This feature is intended to provide a means by which the total cost of ISDN calls can be limited. Typically, a telephone company charges for calls depending on their duration. There is usually also a minimum charge per call. Charging may be at different rates depending on the number dialled, the time of day, the discount plans subscribed to, special offers, and many other factors. Only the minimum charge and duration of calls are taken into account in limiting the total cost. None of the other factors are taken into account because the charge limiter is intended only to impose a maximum cost, not to record the actual cost incurred.

The charge limiting facility estimates the call costs in *credits*. These are similar to money, but not directly equivalent to any particular currency. Credits are spent when a call is connected and at a steady rate as long as the call is connected. If all credits are exhausted while a call is connected the call is cleared. When the router needs to place an outgoing call, if there are insufficient credits to cover the minimum charge, no outgoing call will be attempted. In either of these cases, a message is logged via

SYSLOG.

The default settings allow an average of up to thirty-three calls per day and just over an hour of calls. The maximum permitted in any one day is two hundred calls and three hours twenty minutes of connect time. If this is not sufficient, it is easily increased, however if the router is connected for long periods every day it may be more economical to use a leased line.

Notes

Since the charge limiter does not take into account that different numbers are charged at different rates, calls to premium rate numbers, services such as INMARSAT, and some international numbers, may cost significantly more than the estimate used by the call charge limiter.

Calls made from analogue lines attached to the router are not included in the charge limiting facility. This is because the charge limiter is intended only to guard against accidental mis-configuration.

Incoming calls are not included in the charge limiting facility.

Incoming calls are usually free.

Reverse charge (collect) calls connected to the router will not be controlled by the charge limiter.

Some phone companies charge for calls, which are not connected. The charge limiter does not cover these calls.

The individual items on the menu are:

CALLRATE - ISDN call cost

This value determines how fast credits are spent while connected. Credits are deducted from the current credit as they are used. For example, with the default value, 5, the current credit is decreased by one credit every twelve seconds.

CALLMINIMUM - Minimum ISDN call cost

This is the minimum amount deducted from the current credit per call. For example, with the default values, calls under one minute cost five credits while calls over one minute are charged by time used.

SPENDRATE - Total spending per 30 days

This determines the rate at which credits are accumulated. It is expressed as an average over 30 days because it is common for ISDN charges to be billed monthly, and this allows a direct comparison between the charge limit and the actual bills. Credits are added to the current credit at a continuous, steady rate. For example, with the default value of 10000 credits per 30 days, one credit is added every 4.32 minutes.

CREDITLIMIT - Maximum accumulated credit

When the current credit reaches this value, it will stop accumulating credit. This is to avoid building up a very large credit if the router does not make calls at the maximum rate. For example, if a router makes, on average, a hundred short calls per day, with the default configuration it would build up five hundred credits per day. Eventually the current credit would be so large that the charge limiting facility would permit enormous costs to be incurred.

STARTUPCREDIT - Initial credit at each system start-up

The router does not keep a permanent record of the current credit. Each time it is switched on it simply starts with a fixed amount of credit. This command sets this amount.

CREDIT - Current credit

This item shows the current credit. It is automatically updated as credit is used and accumulated. It cannot be changed directly.

QUIT - Previous menu

Returns to the GLOBAL ISDN menu.

8.3.3 GLOBAL ISDN MSN Menu

Test code	Called number	Phone line
0 I0	1	1
1 I1	2	2
2 I2	3	1
3 I3	3	2
& ADD	Add new item	% DELETE
menu		Delete item
		. QUIT Previous menu

This menu allows you to configure Multiple Subscriber Numbering (MSN). This is a service offered with ISDN allows several numbers to connect to the same line. When a call is placed to that line, the number dialled is included with the incoming call indication and allowing the call to be handled differently depending on the called number. Typically, up to ten numbers are available, and the phone company may charge either for the MSN service as a whole or according to how many numbers are provided.

The router uses MSN as a method of routing analogue calls only. Data calls are always handled internally. For analogue calls, you can specify which lines will ring for any incoming call. If no MSN is configured, all lines will ring. Obviously a call can be answered on any ringing line.

MSN is configured by creating entries in a table for each incoming number and specifying which line is activated by that entry. To make several lines ring, you create an entry for each line. In the example menu above, numbers 1 and 2 correspond to lines 1 and 2, while the number 3 rings both lines 1 and 2. Any other incoming analogue calls will be rejected. Note that the called number must be specified, as it will appear in the incoming call from the exchange. For lines connected to BT in the UK, this is only the last digit of the phone number, however on other lines it may be the full phone number. You can see the format of incoming numbers when incoming calls are logged via **SYSLOG**.

When you select an item from this menu, you are shown the GLOBAL ISDN MSN *item* menu, which allows you to configure this item.

8.3.4 GLOBAL ISDN MSN *item* Menu

London ISDN MSN		
Command	Description	Current Value
0 NUMBER	Number called (as sent from exchange)	1
1 PHONE	Phone to ring (0=none)	1
. QUIT	Previous menu	
COMMAND: GLOBAL ISDN MSN I0		

This menu shows one entry from the MSN table. The configurable items are:

NUMBER - number called

When the number presented with the incoming call matches this, the phone line specified in this entry is offered the call. To match a call, which presents no number, leave this blank. Note that when you subscribe to the MSN service all calls should specify the desired number, so this is typically only useful where a router can be moved between several ISDN lines. If you enter only a question mark (?), this entry will match all calls regardless of the number dialed.

PHONE - Phone to ring

This specifies which line should be offered the call. The value zero can be specified to indicate that no line should ring. This is useful to disable an entry temporarily. The lines are numbered as printed on the rear panel of the router.

QUIT - Previous menu

Returns to the GLOBAL ISDN menu.

8.3.5 GLOBAL ISDN ACCESS Menu

Command	Description	Current Value
0 MONDAY	Monday access control	0:00-12:00, 12:00-24:00
1 TUESDAY	Tuesday access control	0:00-12:00, 12:00-24:00
2 WEDNESDAY	Wednesday access control	0:00-12:00, 12:00-24:00
3 THURSDAY	Thursday access control	0:00-12:00, 12:00-24:00
4 FRIDAY	Friday access control	0:00-12:00, 12:00-24:00
5 SATURDAY	Saturday access control	0:00-0:00, 0:00-0:00
6 SUNDAY	Sunday access control	0:00-0:00, 0:00-0:00
. QUIT	Previous menu	

COMMAND: GLOBAL ISDN ACCESS		

This menu gives an overall view of the daily settings of the access control function. The times shown are when access is allowed, the default settings allowing access 24 hours on weekdays. The individual items on the menu are:

MONDAY - Monday access control

This leads to the GLOBAL ISDN ACCESS MONDAY menu, which allows the individual times to be adjusted.

TUESDAY - Tuesday access control

This leads to the GLOBAL ISDN ACCESS TUESDAY menu, which allows the individual times to be adjusted.

WEDNESDAY - Wednesday access control

This leads to the GLOBAL ISDN ACCESS WEDNESDAY menu, which allows the individual times to be adjusted.

THURSDAY - Thursday access control

This leads to the GLOBAL ISDN ACCESS THURSDAY menu, which allows the individual times to be adjusted.

FRIDAY - Friday access control

This leads to the GLOBAL ISDN ACCESS FRIDAY menu, which allows the individual times to be adjusted.

SATURDAY - Saturday access control

This leads to the GLOBAL ISDN ACCESS SATURDAY menu, which allows the individual times to be adjusted.

SUNDAY - Sunday access control

This leads to the GLOBAL ISDN ACCESS SUNDAY menu, which allows the individual times to be adjusted.

QUIT - Previous menu

Returns to the GLOBAL ISDN menu.

8.3.6 GLOBAL ISDN ACCESS *day* Menu

Command	Description	Current Value
0 ON1	Enable calls from	8:00
1 OFF1	Disable calls from	19:00
2 ON2	Enable calls from	0:00
3 OFF2	Disable calls from	0:00
. QUIT	Previous menu	
COMMAND: GLOBAL ISDN ACCESS day		

This menu allows the start and stop times of the two periods each day to be controlled. The individual items on the menu are:

ON1 - Enable calls from

Set the start time of the first access window of the day.

OFF1 - Disable calls from

Set the end time of the first access window of the day.

ON2 - Enable calls from

Set the start time of the second access window of the day.

OFF2 - Disable calls from

Set the end time of the second access window of the day.

QUIT - Previous menu

Returns to the GLOBAL ISDN ACCESS menu.

8.3.7 GLOBAL ISDN TIMES Menu

Command	Description	Current Value
0 LOCAL	Minimum Local Call Duration	60
1 REGIONAL	Minimum Regional Call Duration	45
2 NATIONAL	Minimum National Call Duration	30
3 INTERNATIONAL	Minimum International Call Duration	20
. QUIT	Previous menu	

COMMAND: GLOBAL ISDN TIMES		

This menu allows the minimum call duration's to be set for each charge band within one time period. The individual items on the menu are:

LOCAL - Minimum Local Call Duration

Set the minimum call duration for local calls.

REGIONAL - Minimum Regional Call Duration

Set the minimum call duration for regional calls.

NATIONAL - Minimum National Call Duration

Set the minimum call duration for national calls.

INTERNATIONAL - Minimum International Call Duration

Set the minimum call duration for international calls.

QUIT - Previous menu

Returns to the GLOBAL ISDN menu.

8.3.8 GLOBAL SNMP Menu

Command	Description	Current Value
0 COMMUNITY	Name	
1 MANIP	Manager IP Address	0.0.0.0 /0
2 ACESSTYPE	SNMP Access Type	None
3 TCOMMUNITY	Trap Community Name	
4 TRAPIP	Trap IP Address	0.0.0.0 /0
5 TRAPTYPE	Trap Types to Send	None
6 CONTACT	Contact Name to Report	
7 LOCATION	Location to Report	
. QUIT	Previous menu	

COMMAND: GLOBAL SNMP		

This screen allows the SNMP management system present in the routers to be controlled. By default all access is denied.

The SNMP agent present in the routers conforms to MIB II as defined in RFC 1213, except that the TCP, EGP and Transmission Groups are not supported and the cold start trap is not generated.

Currently only read access is allowed.

The individual items on the menu are:

COMMUNITY - Community Name

This value allows the community name that the agent expects to see in all request messages to be specified. This value will be used to validate all received messages. Any messages, which do not contain this Community Name, will be discarded and an Authentication Failure Trap generated, if enabled.

MANIP - Manager IP Address

This option allows you to select a specific IP Address from which all SNMP Requests will be expected. If this value is left at its default value of 0.0.0.0 the agent will respond to management requests from anyone on the network using the correct Community Name.

ACCESSTYPE - SNMP Access Type

This option controls what sort of access will be allowed to the variables within the router. Currently only the Disabled and Read Only options are available.

TCOMMUNITY - Trap Community Name

This value allows the community name that will be put into any Trap messages to be selected.

TRAPIP - Trap IP Address

This value selects the destination IP address to which all Trap Messages will be sent. While left at its default value of 0.0.0.0 no Trap Messages will be sent.

TRAPTYPE - Trap Types to Send

This value allows the type of Trap Messages generated to be controlled.

CONTACT - Contact Name to Report

This entry allows the value reported by an access to the 'sysContact' MIB Object to be set.

LOCATION - Location to Report

This entry allows the value reported by an access to the 'sysLocation' MIB Object to be set.

QUIT - Previous menu

Returns to the GLOBAL menu.

8.4 NETWORK Menu

London NETWORKS			
Command	Description	Current Value	
0 UNCONFIGURED	!! Invalid !!	0.0.0.0	
1 Birmingham	Leased Circuit: Link 1	20.1.1.0	
2 eth	Ethernet Interface	10.1.1.0	
& ADD	Add new item	% DELETE	Delete item
. QUIT	Previous menu		
NOTE: please select the UNCONFIGURED network and configure it			
COMMAND: NETWORK			

This menu allows you to configure the networks that this router knows about. The items are:

A network name

This selects a network and presents its details on the NETWORK *name* menu.

ADD - Add new item

This menu creates a new network. Its name is *UNCONFIGURED*. There is a new unconfigured network on the example menu above. You should select the new network and set its name and other details to the values you require.

DELETE - Delete item

This allows you to delete a network. References to the deleted network are automatically removed from other tables (such as the IP routing table).

QUIT - Previous menu

Returns to the Main Menu.

8.4.1 NETWORK *name* Menu

London NETWORKS		
Command	Description	Current Value
0 NAME	Name	Birmingham
1 IP	IP configuration	
2 PPP	PPP configuration	
3 IPX	IPX configuration	
4 ISDN	ISDN configuration	
5 CHANNELS	Select channels to use	
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham

This menu shows the details relating to a single network. It has these options:

NAME - Name

This allows you to set the name for this network. This name appears on various menus. It is also used as the default *Peer user ID* when authenticating incoming calls. This default can be superseded with the NETWORK *name* PPP PAP PEERID command. You should not have two networks with the same name, because the name is shown on several menus to identify the network, and also it would not be possible to select the second by name from this menu (however the shortcut key will work as normal).

IP - IP configuration

This leads to the NETWORK *name* IP menu, which allows you to configure the **IP** parameters for this network.

PPP - PPP configuration

This leads to the NETWORK *name* PPP menu, which allows you to configure the **PPP** parameters of this network.

IPX - IPX configuration

This leads to the NETWORK *name* IPX menu, which allows you to configure the **IPX** parameters of this network.

ISDN - ISDN configuration

This leads to the NETWORK *name* ISDN menu, which allows you configure items relating to the use of ISDN connections with this network.

CHANNELS - Select channels to use

This leads to the NETWORK *name* CHANNELS menu, which allows you to define fixed links used to connect to this network. You do not need to explicitly enable ISDN access because it is used automatically when a phone number is entered under the NETWORK *name* ISDN DIALLIST menu.

QUIT - Previous menu

Return to the NETWORK menu.

8.5 NETWORK *name* IP Menu

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	0.0.0.0 /0
2 REMOTE	Remote IP address (if not Ethernet)	20.1.1.1
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	1 route
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	
COMMAND: NETWORK Birmingham IP		

This menu shows you the current **IP** parameters for a network and allows you to change them. They are:

ENABLE - IP routing

This allows you to disable IP routing to this network. If you want to configure a network for **IPX** only, you must disable this option. If you want to disable a network for both IP and IPX, you can delete it from the NETWORK menu.

LOCAL - Local IP address

This is the IP address of your router for this network. The earlier sections on IP Addresses and Selecting IP Addresses will help you to fill in this value. If you are configuring this network in accordance with the unnumbered interface model of addressing, this value must be 0.0.0.0 to indicate that the router should reuse the IP address assigned to the **Ethernet** interface.

REMOTE - Remote IP address (if not Ethernet)

This is only relevant when this network is between a router and one other device (normally another router) over a **WAN** link. It is the IP address of the other device. When the network uses broadcast hardware (i.e. **Ethernet**), this value is ignored.

MASK - IP address mask

This is the IP address mask for this network. You can enter normal address masks as /n where n is the number of bits in the mask, i.e. the **CIDR** format. For example, a mask 255.255.255.0 can be entered as /24. Values on menus are shown in both formats.

RIP - RIP

This leads to the NETWORK *name* IP RIP menu that allows you to configure how **RIP** is used with this network. Any RIP options enabled are shown in abbreviated form in the *Current Value* column of the menu. The abbreviations are the single letter codes in brackets on the NETWORK *name* IP RIP menu.

RIPMETRIC - RIP Metric weighting for link

This value indicates the weighting to be given to this link when it is advertised by RIP. All routes crossing this link will have their metric increased appropriately. This feature can be used to ensure a preferred route is normally used and the route with the additional weighting is only used when the primary route has failed.

Be careful not to set this value too high since the maximum before a destination becomes unreachable is only 16.

This value is also used by IPX RIP, where the Hop count is increased in the same way as for IP RIP and the ticks are increased by an additional 4 for every 1 increase in the hop count.

ROUTES - Associated static routes

This leads to the NETWORK *name* IP ROUTES menu that lists **static routes, which** are associated with this network.

TRANSLATE - Address translation rules

This leads to the NETWORK *name* IP TRANSLATE menu that configures the address translation rules which are used on data coming from or sent to this network.

PIPE - IP Express

This leads to the NETWORK *name* IP PIPE menu that configures the IP prioritisation mechanism for frames being sent to this destination. Or from this destination if Ethernet.

FILTBROAD - Filter Directed Broadcast

This option allows you to only send directed broadcasts across this link while it is connected. This means that directed broadcasts do not cause a dial up link to be established, and do not keep an existing dial up link alive.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

8.5.1 NETWORK *name* IP RIP Menu

London IP RIP FLAGS		
Command	Description	Current Value
0 DISCARD	(D) Discard RIP from this network	NO
1 RIPTX	(T) Send RIP updates to this network	NO
2 RIPAGE	(A) Age RIP entries, No RIP Spoofing	YES
3 RIP-2	(2) Enable Transmission of RIP-2	NO
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP RIP

This menu allows you to configure **RIP** for this network. This applies to IP RIP only - IPX RIP is not configurable. The options are:

DISCARD - Discard RIP from this network

This allows you to prevent RIP updates being received from this network. Typically, RIP updates can be accepted from any network, but in some cases, either for security reasons or to guard against misconfiguration, it is desirable to refuse to accept automatic routing updates.

RIPTX - Send RIP updates to this network

This allows you to send periodic RIP updates to this network. By default, this is disabled because a dialup link would be kept constantly connected by the periodic traffic. You can safely enable RIP transmissions to any permanent links, such as Ethernet and leased lines.

RIPAGE - Age RIP entries - No IP RIP Spoofing

Normally RIP entries learnt across Dial Up links are aged out and lost a few minutes after the link drops. Setting this option to NO allows you to prevent this happening so that the router continues to advertise routes to dial up destinations. It also enables a mechanism where RIP broadcasts over dialup links are not sent where no new information is being transmitted.

RIP-2 - Enable Transmission of RIP-2

This option enables the transmission of **RIP-2** frames on this interface. The router can always understand RIP-2 frames when they are received. This option enables the transmission of RIP-2 format Frames (i.e. including a subnet mask). These frames are sent on the standard RIP broadcast Address, in what the RIP-2 standard describes as RIP 1 compatibility mode.

QUIT - Previous menu

Returns to the NETWORK *name* IP menu.

8.5.2 NETWORK *name* IP ROUTES

London NETWORK ROUTES			
Destination	Router	Mask	Metric
0 IP:192.168.3.0	IP:0.0.0.0	IP:255.255.255.0	8
& ADD	Add new item	% DELETE	Delete item
. QUIT	Previous menu		

COMMAND: NETWORK Birmingham IP ROUTES

This lists the **static routes**, which are associated with a network. On the menu, each choice is a summary of one route, which can be expanded by choosing it. The fields are, from left to right, the local address, the next hop router address, address mask and the metric. Section 6.1 (Introduction to IP Networking) explains what these mean. The options are:

A route

This selects a single route and presents its details on the NETWORK *name* IP ROUTES *ip* menu.

ADD - Add new item

This menu creates a new static route. Its name is **IP:0.0.0.0**. You should select the new route and set its details to the values you require.

DELETE - Delete item

This allows you to static route. References to the deleted route are automatically removed from the IP routing table.

QUIT - Previous menu

Returns to the NETWORK *name* IP menu.

8.5.3 NETWORK *name* IP ROUTES *ip* Menu

London NETWORK STATIC ROUTE		
Command	Description	Current Value
0 ADDRESS	Target IP address (0=default route)	192.168.3.0
1 ROUTER	IP address of next router	0.0.0.0
2 MASK	IP mask (0=default route)	255.255.255.0 /24
3 METRIC	Cost of route	8
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP ROUTES IP:192.168.3.0

This menu shows one route, which belongs to a configured network by expanding it into these items:

ADDRESS - Target IP address

This, in combination with the mask, specifies which IP addresses are covered by this route.

ROUTER - IP Address of next router

This specifies where the route goes. For point-to-point links, it is ignored because the link leads to only one directly connected device. However it is needed for **Ethernet** networks, to determine which device on the network is the target of this route.

MASK - IP mask

This, in combination with the IP address, specifies which IP addresses are covered by this route.

METRIC - Cost of route

When there is a choice between several routes, the router uses this value to select the best route.

QUIT - Previous menu

Returns to the NETWORK *name* IP ROUTES menu.

8.5.4 NETWORK *name* IP TRANSLATE Menu

London		
Command	Description	Current Value
0 IN	Rules for incoming sessions	1tcp+1udp
1 OUT	Rules for outgoing sessions	1tcp+2udp
2 USETCP	Use TCP Rules for all sessions	NO
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP TRANSLATE		

IN - Rules for incoming sessions

Leads to the NETWORK *name* IP TRANSLATE IN menu, which deals with the translations, which apply to data received from this network.

OUT - Rules for outgoing sessions

Leads to the NETWORK *name* IP TRANSLATE OUT menu, which deals with the translations that apply to data sent to this network. Since this menu has exactly the same options as the one dealing with incoming data, it is not described separately. See the NETWORK *name* IP TRANSLATE IN menu for details of these options.

USETCP - Use TCP Rules for all sessions

This option allows you to specify that all UDP and ICMP sessions use the rules defined for TCP. Provided your UDP sessions use IP address and port numbers in a similar way to you TCP sessions, this option provides more powerful features, and removes the need to enter two sets of rules.

Enabling this option disables use of all UDP Rules you may have set up.

QUIT - Previous menu

Returns to the NETWORK *name* IP menu.

8.5.5 NETWORK *name* IP TRANSLATE IN Menu

London		
Command	Description	Current Value
0 TCP	Rules for incoming TCP sessions	1 rule
1 UDP	Rules for incoming UDP sessions	1 rule
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP TRANSLATE IN		

This menu deals with the rules for handling incoming sessions. The rules are divided into submenus by protocol.

TCP - Rules for incoming TCP sessions

Leads to the NETWORK *name* IP TRANSLATE IN TCP menu that deals with the translations that apply to new TCP sessions coming from this network.

UDP - Rules for incoming UDP sessions

Leads to the NETWORK *name* IP TRANSLATE IN UDP menu that deals with the translations that apply to new UDP sessions coming from this network.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE menu.

8.5.6 NETWORK *name* IP TRANSLATE IN TCP Menu

London NETWORK TRANSLATION TCP IN			
Item	Pattern => S:S->D:D		
0 I:0	0.0.0.0/0:0..65535 -> 0.0.0.0/0:25..25 => C:C->P:C		
& ADD	Add new item	% DELETE	Delete item
. QUIT	Previous menu		
COMMAND: NETWORK Birmingham IP TRANSLATE IN TCP			

This menu allows you to configure the rules, which deal with new incoming TCP sessions. When a new TCP session is detected, it is tested against each rule in turn until one is found which is applicable. If no suitable rule is found, the session is blocked. Rules are tested in the order in which they appear on this list, but the list is in no particular order, so patterns in rules should not match overlapping ranges if it is important to distinguish between them.

The options are:**A translation rule**

This selects a rule and presents its details on the NETWORK *name* IP TRANSLATE IN TCP *rule* menu.

ADD - Add new item

This menu creates a new rule. You should select the new rule and set its details to the values you require.

DELETE - Delete item

This allows you to delete a rule. If the rule applies to a session, which is still in progress, the session will not be affected.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN menu.

8.5.7 NETWORK *name* IP TRANSLATE IN TCP *rule* Menu

London TCP		
Command	Description	Current Value
0 PATTERN	Pattern to test against	
1 NEWSRC	Translated source details	dynamic:32768-65535
2 NEWDST	Translated destination details	COPY:COPY
. QUIT	Previous menu	
COMMAND: NETWORK Birmingham IP TRANSLATE IN TCP I:0		

This menu expands a rule for handling one type of TCP session. The type is selected by the PATTERN part, and the translation to be performed is described by the rest of the rule. When a new TCP session is detected which matches the pattern, the translation described in the rest of the rule is installed in the session table.

PATTERN - Pattern to test against

This leads to the NETWORK *name* IP TRANSLATE IN TCP *rule* PATTERN menu that shows the components of the pattern to which this rule applies.

NEWSRC - Translated source details

This leads to the NETWORK *name* IP TRANSLATE IN TCP *rule* NEWSRC menu, which defines the values of the address, and port, which are the translation of the source address, and source port of the session matching this rule.

NEWDST - Translated destination details

This leads to the NETWORK *name* IP TRANSLATE IN TCP *rule* NEWDST menu that defines the values of the address and port that are the translation of the destination address and destination port of the session matching this rule. Since this menu has exactly the same options as the one dealing with the source address and port, it is not described separately. See the NETWORK *name* IP TRANSLATE IN TCP *rule* NEWSRC menu for details of these options.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN TCP menu.

8.5.8 NETWORK *name* IP TRANSLATE IN TCP *rule* PATTERN Menu

London TCP			
Command	Description	Current Value	
0 SRCMINADDR	Source address minimum value	0.0.0.0	/0
1 SRCMAXADDR	Source address maximum value	255.255.255.255	/32
2 SRCMINPORT	Source port minimum value	0	
3 SRCMAXPORT	Source port maximum value	65535	
4 DSTMINADDR	Destination address minimum value	0.0.0.0	/0
5 DSTMAXADDR	Destination address maximum value	255.255.255.255	/32
6 DSTMINPORT	Destination port minimum value	25	
7 DSTMAXPORT	Destination port maximum value	25	
. QUIT	Previous menu		
COMMAND: NETWORK Birmingham IP TRANSLATE IN TCP I:0 PATTERN			

This menu describes a pattern, which is used to select which rule applies to a new session.

SRCMINADDR - Source address minimum value

Specifies the minimum source address that this pattern can match.

SRCMAXADDR - Source address maximum value

Specifies the maximum source address that this pattern can match. If the maximum specified here is less than the minimum, this is taken to mean that the pattern matches exactly one value, and that value is the minimum. When you add a new rule, it starts off with all addresses set to zero, so to make the pattern match one address it is only necessary to fill in that address as the minimum.

SRCMINPORT - Source port minimum value

Specifies the minimum source port that this pattern can match.

SRCMAXPORT - Source port maximum value

Specifies the maximum source port that this pattern can match. If the maximum is less than the minimum, the pattern can never match any session.

DSTMINADDR - Destination address minimum value

Specifies the minimum source address that this pattern can match.

DSTMAXADDR - Destination address maximum value

Specifies the maximum source address that this pattern can match. Just as with the maximum value for the source address, if this is less than the minimum the pattern matches only the address specified by the minimum.

DSTMINPORT - Destination port minimum value

Specifies the minimum destination port that this pattern can match.

DSTMAXPORT - Destination port maximum value

Specifies the maximum destination port that this pattern can match. If the maximum is less than the minimum, the pattern can never match any session.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN TCP *rule* menu.

8.5.9 NETWORK *name* IP TRANSLATE IN TCP *rule* NEWSRC Menu

London SESSION VALUES		
Command	Description	Current Value
0 NEWADDR	Where to get address	SOURCE
1 ADDRPOOLMIN	Start of address pool	0.0.0.0 /0
2 ADDRPOOLMAX	End of address pool	0.0.0.0 /0
3 NEWPORT	Where to get port number	SOURCE
4 PORTPOOLMIN	Start of port pool	0
5 PORTPOOLMAX	End of port pool	0
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP TRANSLATE IN TCP I:0 NEWSRC		

NEWADDR - Where to get address

This selects the translated address. It can specify either that the address is to be taken from the session, which matched the pattern in this rule, or that it is to be allocated from a pool of available addresses. If a session needs to allocate an address, but the pool is empty (either because all addresses in the pool are already in use, or because the pool is defined to be empty by making the maximum less than the minimum), then the session is discarded.

ADDRPOOLMIN - Start of address pool

When the address is to be allocated from a pool, this specifies the minimum address in the pool. This value is ignored if the address is not allocated from a pool.

ADDRPOOLMAX - End of address pool

When the address is to be allocated from a pool, this specifies the maximum address in the pool. This value is ignored if the address is not allocated from a pool. If the maximum pool address is less than the minimum pool address, no address can be allocated from the pool. If both the maximum and minimum addresses are zero, the IP address negotiated on this connection by PPP will be used.

NEWPORT - Where to get port number

This selects the translated port number. It can specify either that the port number is to be taken from the session, which matched the pattern in this rule, or that it is to be allocated from a pool of available port numbers. When a pool is used, the port number is always copied from the original session unless that port number is already in use. This applies even if the value is outside the range of values in the pool.

PORTPOOLMIN - Start of port pool

When the port number is to be allocated from a pool, this specifies the minimum port number in the pool. This value is ignored if the port number is not allocated from a pool.

PORTPOOLMAX - End of port pool

When the port number is to be allocated from a pool, this specifies the maximum port number in the pool. This value is ignored if the port number is not allocated from a pool.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN TCP *rule* menu.

8.5.10 NETWORK *name* IP TRANSLATE IN UDP Menu

London NETWORK TRANSLATION UDP IN		
Item	Pattern	-> Translation
0 I:0	0.0.0.0/0:0..65535	-> COPY:COPY
& ADD	Add new item	% DELETE Delete item
. QUIT	Previous menu	
COMMAND: NETWORK Birmingham IP TRANSLATE IN UDP		

This menu allows you to configure the rules, which deal with new incoming UDP sessions. When a new UDP session is detected, the source and destination are each tested against the list of rules until one is found which matches. The translation described in the rule is installed in the session table. This is done independently for the source and destination, so a new session may create two entries in the session table: one for the source and one for the destination. Rules are tested in the order in which they are listed on this menu, which is sorted to make the most general rule come last. The options are:

A translation rule

This selects a rule and presents its details on the NETWORK *name* IP TRANSLATE IN UDP *rule* menu.

ADD - Add new item

This menu creates a new rule. You should select the new rule and set its details to the values you require.

DELETE - Delete item

This allows you to delete a rule. If the rule applies to a session, which is still in progress, the session will not be affected.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN menu.

8.5.11 NETWORK *name* IP TRANSLATE IN UDP *rule* Menu

London UDP		
Command	Description	Current Value
0 PATTERN	Pattern to test against	
1 NEW	Translated address and port	COPY:COPY
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP TRANSLATE IN UDP I:0		

This menu expands a rule for handling one group of UDP connections. The type is selected by the PATTERN part, and the translation to be performed is described by the rest of the rule.

PATTERN - Pattern to test against

This leads to the NETWORK *name* IP TRANSLATE IN UDP *rule* PATTERN menu which shows the components of the pattern to which this rule applies.

NEW - Translated address and port

This leads to the NETWORK *name* IP TRANSLATE IN UDP *rule* NEW menu, which defines the values of the address and port, which are the translation of the address and port that matched the pattern in this rule. Since this menu has exactly the same options as the one dealing with the new TCP source address and port, it is not described separately. See NETWORK *name* IP TRANSLATE IN TCP *rule* NEWSRC menu for details of these options.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN UDP *rule* menu.

8.5.12 NETWORK *name* IP TRANSLATE IN UDP *rule* PATTERN Menu

London UDP		
Command	Description	Current Value
0 MINADDR	Minimum address value	0.0.0.0 /0
1 MAXADDR	Maximum address value	255.255.255.255 /32
2 MINPORT	Minimum port value	0
3 MAXPORT	Maximum port value	65535
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP TRANSLATE IN UDP I:0 PATTERN		

MINADDR - Minimum address value

Specifies the minimum source address that this pattern can match.

MAXADDR - Maximum address value

Specifies the maximum source address that this pattern can match. If the maximum specified here is less than the minimum, this is taken to mean that the pattern matches exactly one value, and that value is the minimum. When you add a new rule, it starts off with all addresses set to zero, so to make the pattern match one address it is only necessary to fill in that address as the minimum.

MINPORT - Minimum port value

Specifies the minimum source port that this pattern can match.

MAXPORT - Maximum port value

Specifies the maximum source port that this pattern can match. If the maximum is less than the minimum, the pattern can never match any session.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE IN UDP *rule* menu.

8.5.13 NETWORK *name* IP PIPE Menu

Command	Description	Current Value
0 RESBAN	Reserved bandwidth (bytes/sec)	0
1 FRAGSIZE	Fragment size	256
2 PRIOR	IP Prioritisation	0 entries
. QUIT	Previous menu	
COMMAND: NETWORK Birmingham IP PIPE		

This menu allows you to control the use of the IP prioritisation function on the link to this destination. Setting the RESBAN field to zero disables the function on this link. None of the fields on this menu are used if IP Prioritisation is disabled globally. The individual items on the menu are:

RESBAN - Reserved bandwidth

This field controls how much bandwidth to reserve for priority traffic on this link. Setting this value to zero disables the priority mechanism on this link. On the Ethernet network setting this value to any non-zero value enables the priority queue for data arriving from Ethernet.

FRAGSIZE - Fragment size

This value allows you to control the size into which non-priority frames are broken as they are transferred while priority traffic is flowing. This provides a control on the maximum delay incurred by a priority frames. That is a priority frame can be delayed by up to the time taken for a fragment to be transmitted. Reducing the fragment size reduces the maximum delay but does reduce the efficiency of transfer of non-priority traffic.

PRIOR - IP Prioritisation

This leads to NETWORK *name* IP PIPE PRIOR menu where the list of IP Addresses and Ports can be established.

QUIT - Previous menu

Returns to the NETWORK *name* IP menu.

8.5.14 NETWORK *name* IP PIPE PRIOR Menu

London PRI		
Code	IP Address	Port number
0 P0	192.16.1.1	4000
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP PIPE PRIOR		

This menu allows you to configure the List of IP Address and Port pairs that will be treated as priority traffic when they are detected in the Destination of a UDP frame. The options are:

A destination address

This leads you to the NETWORK *name* IP PIPE PRIOR *rule* menu, where the individual address and port can be set.

ADD - Add new item

This menu creates a new IP Address/Port destination. You should select the new destination and set its details to the values you require.

DELETE - Delete item

This allows you to delete a destination.

QUIT - Previous menu

Returns to the NETWORK *name* IP PIPE menu.

8.5.15 NETWORK *name* IP PIPE PRIOR *name* PATTERN Menu

London IP PRIORITISATION		
Command	Description	Current Value
1 PORT	Port number	4000
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP PIPE PRIOR P name		

This menu allows a single IP Address/Port combination to be set. Setting an IP Address of zero, acts as a wildcard so matching all UDP frames directed at the specified port. Setting the Port Number to zero, also acts as a wildcard matching all UDP frames directed at the specified Address. A value must be entered against one of the fields. The options are:

ADDRESS - IP Address

This entry specified the Destination IP Address to look for.

PORT - Port number

This entry specifies the Destination UDP Port to look for.

QUIT - Previous menu

Returns to the NETWORK *name* IP PIPE PRIOR menu.

8.6 NETWORK *name* PPP Menu

London		
Command	Description	Current Value
0 PAP	Password Authentication Protocol	in+out
1 CHAP	Challenge Handshake Authentication	in+out
2 MPDMAX	ISDN channels req'd to start link	0
3 BANDWIDTH	Bandwidth on demand	disabled
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham PPP		

The items on this menu allow the configuration of the Point-to-Point Protocol (PPP) for this network. Since two different authentication protocols are provided, the router selects automatically between them.

The rules for selection are:

- If only one authentication method is configured, that one is used.
- If both methods are configured, the router will initially propose CHAP, but will use PAP if the peer negotiates that instead.
- If neither method is configured, the router will use PAP with a blank password.
- The rules apply independently to calling and answering, so it is possible to use CHAP for one and PAP for the other.

The items are:

PAP - Password Authentication Protocol

This leads to the NETWORK *name* PPP PAP menu, which allows you to configure PAP authentication.

CHAP - Challenge Handshake Authentication

This leads to the NETWORK *name* PPP CHAP menu, which allows you to configure CHAP authentication.

MPDMAX - ISDN channels req'd to start link

This value is the number of dialup calls that this router will attempt to *initiate* to this destination. If a Leased line is configured to this destination, then this number represents the number of backup calls placed when the leased line fails. If no Leased Line is configured to this destination then this value is the number of calls that will be used when a link to this destination is required.

Notes:

- This value does not limit the number of incoming calls, which can be accepted.
- Only one call per network is dialled at a time. Only after a call is connected (or fails) can another be attempted.
- The values of zero or one in this field are equivalent. This means that a Leased Line will be backed up by a single ISDN call if it fails, providing an ISDN number has been configured.

BANDWIDTH - Bandwidth on Demand

This leads to the NETWORK *name* PPP BANDWIDTH menu, which allows you to configure the bandwidth on demand facilities.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

8.6.1 NETWORK *name* PPP PAP Menu

London		
Command	Description	Current Value
0 PEERID	Peer user id (default=NETWORK NAME)	
1 PEERPASS	Peer password to check against	
2 LOCALID	Local user id (default=GLOBAL NAME)	
3 LOCALPASS	Local password to send to peer	
. QUIT	Previous menu	
COMMAND: NETWORK Birmingham PPP PAP		

The items on this menu allow the configuration of the Password Authentication Protocol (PAP).

PEERID - Peer user id

Peer Identification used during PAP authentication. This is the name that the router uses to recognise an incoming caller. If this is left blank, then the network name (*Birmingham* in this example) is used as default.

PEERPASS - Peer password to check against

Peer password used during PPP authentication. This is the password that the router checks when an incoming call claims to be from this network.

LOCALID - Local user id

Local identification used during PPP authentication. This is the name that the router uses when it dials out to this network. If this is left blank, then the router name, as set by the GLOBAL NAME command, is used (*London* in this example)

LOCALPASS - Local password to send to peer

Local password used during PPP authentication. This is the password that the router sends when dialling out to this network.

QUIT - Previous menu

Returns to the NETWORK *name* PPP menu.

8.6.2 NETWORK *name* PPP CHAP Menu

London		
Command	Description	Current Value
0 PEERID	Peer user id (default=NETWORK NAME)	
1 PEERCALLX	Secret for checking when calling	
2 PEERANSX	Secret for checking when answering	
3 LOCALID	Local user id when calling	
4 LOCALCALLX	Secret for responding when calling	
5 LOCALANSX	Secret for responding when answering	
6 REPINT	Challenge repeat interval (seconds)	60
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham PPP CHAP		

The items on this menu allow the configuration of the Challenge Handshake Authentication Protocol (CHAP). Note that, unlike PAP, we cannot select the name to send during authentication on answer. This is because CHAP requires the name to be sent before identifying the other party. Therefore the name sent when answering is always the router's global name (*Birmingham* in this example).

PEERID - Peer user id

Peer Identification used during CHAP authentication. This is the name that the router uses to recognise an incoming caller. If this is left blank, then the network name (*Birmingham* in this example) is used as default.

PEERCALLX - Secret for checking when calling

When this peer answers a call from us and we send challenges to it, this is the secret used to check the responses. If the peer is another VIPER router, this value should be their LOCALANSX value.

PEERANSX - Secret for checking when answering

When this peer calls us and we send challenges to it, this is the secret used to check the responses. This is the normal form of authentication for incoming calls. If the peer is another VIPER router, this value should be their LOCALCALLX value.

LOCALID - Local user id when calling

When we call this peer we use this name to identify us to our peer. There is no default setting for this entry.

LOCALCALLX - Secret for responding when calling

When we call this peer and we receive challenges from it, this is the secret used to create the responses. This is the normal form of authentication for outgoing calls. If the peer is another VIPER router, this value should be their PEERANSX value.

LOCALANSX - Secret for responding when answering

When we answer a call from this peer and we receive challenges from it, this is the secret used to create the responses. If the peer is another VIPER router, this value should be their PEERCALLX value.

REPINT - Challenge repeat interval (seconds)

This is the interval after which the router will demand re-authentication. The time is measured from when the initial authentication finished. The transmission of data is not interrupted while

awaiting re-authentication, but if the correct response is not received or if no response is received after several challenges, the connection will be cleared. If the interval is specified as zero, no re-authentication will be used.

QUIT - Previous menu

Returns to the NETWORK *name* PPP menu.

8.6.3 NETWORK *name* PPP BAND Menu

Command	Description	Current Value
0 MAXCHANS	Maximum Channels to Open (0=Disabled)	0
1 OPENTHRESH	Threshold to open first extra link	6000
2 OPENDURATION	Duration to open extra link	1
3 CLOSETHRESH	Threshold to close extra link	1500
4 DIRECTION	Direction to test thresholds against	OUT
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham PPP BAND

This menu allows close control over the activation of additional ISDN channels as the router experiences additional load. Setting the first value to zero disables this feature so causing the other values on the menu to be ignored. The individual items on the menu are:

MAXCHANS - Maximum Channels to Open

This value determines the maximum number of channels to open in response to increased load. The later values on this menu determine when these additional channels will be brought on line. Setting this value to zero disables Bandwidth On Demand but does not disable Dial Backup of Leased Lines.

OPENTHRESH - Threshold to open first extra link

This value indicates the load level at which to consider opening additional links. It is measured in characters per second. The default value representing about 75% load on a 64K bps link.

OPENDURATION - Duration to open extra link

This determines how long the load must remain above the rate set in the previous field before an additional channel is raised.

CLOSETHRESH - Threshold to close extra link

This value indicates the load level at which to stop sending data along the additional links. The additional links will then remain active and idle until the link idle timer expires. The length of this timer is set on the NETWORK *name* ISDN menu.

DIRECTION - Direction to test thresholds against

This value leads to an additional menu that allows the direction in which traffic is measured to be controlled. Normally this value should be set to out at each end of a link, so that both ends are not measuring the same thing, and both attempting to bring up an additional call at the same time. The Inbound measurement is mainly for use when connecting to non-VIPER routers, which do not initiate additional calls.

QUIT - Previous menu

Returns to the NETWORK *name* PPP menu.

8.7 NETWORK *name* IPX menu

London		
Command	Description	Current Value
0 ENABLE	IPX Routing	YES
1 IPXUPDATES	Always update IPX Routing Tables	YES
2 IPXLEARN	Initial IPX Learning Period	100
3 NETWORKS	IPX Networks	
4 ROUTES	Associated static routes	0 routes
5 SAPS	Associated static saps	0 saps
6 LEARNROUTES	Learn static routes now	
7 LEARNAPS	Learn static saps now	
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IPX

This menu shows you the current **IPX** parameters for a network and allows you to change them. They are:

ENABLE - IPX routing

This allows you to disable IPX routing to this network. If you want to configure a network for **IP** only, you must disable this option. If you want to disable a network for both IP and IPX, you can delete it from the NETWORK menu.

IPXUPDATES - Always update IPX Routing Tables

By default the router will dial up a remote router to inform it of changes to the IPX routing table. If there are no changes the link is allowed to drop and spoofing software continues to advertise the remote routes and services. In some large networks, services are coming and going all the time, which would cause the link to be brought up too often.

This option allows you to instruct the router only to exchange IPX routing information with remote routers when the link is brought up for another reason. The link is allowed to come up within the first minute of Power On or Reset to allow initial routing information to be collected.

IPXLEARN - Initial IPX Learning Period

When using IPX routing over dial up links a learning call or calls are necessary when the router is first powered up or reset. This mechanism allows routing table information to be transferred from one end to another. This configuration value allows the duration of this learning period to be adjusted. The value is in seconds and starts 10 seconds after the unit comes out of reset.

NETWORKS - IPX Networks

This leads to the NETWORKS *name* IPX NETWORKS menu, which allows you to configure specific IPX network numbers for the various supported frame types.

ROUTES - Associated static routes

This leads to the NETWORKS *name* IPX ROUTES menu, which allows you to enter static IPX Routing Entries.

SAPS - Associated static saps

This leads to the NETWORKS *name* IPX SAPS menu, which allows you to configure specific IPX SAP Entries.

LEARNROUTES - Learn static routes now

This option causes all those entries already in the IPX routing table that pass across this link to be made permanent. You may then use the ROUTES option to manipulate the list you have just created.

LEARNSAPS - Learn static saps now

This option causes all those entries already in the SAP table that pass across this link to be made permanent. You may then use the SAPS option to manipulate the list you have just created.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

8.7.1 NETWORK *name* IPX NETWORKS Menu

London		
Command	Description	Current Value
0 EIIENABLE	Ethernet II enable	YES
1 EIINETWORK	Ethernet II network number	00000000
2 SNAPENABLE	SNAP enable	YES
3 SNAPNETWORK	SNAP network number	00000000
4 E8022ENABLE	802.2 enable	YES
5 E8022NETWORK	802.2 network number	00000000
6 E8023ENABLE	802.3 enable	YES
7 E8023NETWORK	802.3 network number	00000000
8 PPPENABLE	PPP enable	YES
9 PPPNETWORK	PPP network number	00000000
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IPX NETWORKS

This menu shows you the current **IPX** parameters for the different Ethernet frame types for a network and allows you to change them. For networks, which describe the local Ethernet, the PPP option is not relevant and will be ignored. For dialup line and leased lines, only the PPP setting is relevant. It is not normally useful to configure PPP as well as an Ethernet frame type on the same network. The options are:

EIIENABLE - Ethernet II enable

This allows you to disable the **Ethernet II** frame type for IPX routing to this network.

EIINETWORK - Ethernet II network number

This allows you to set the IPX network number for use with the **Ethernet II** frame type on this network. The value 0 indicates that the network number should be learned automatically.

SNAPENABLE - SNAP enable

This allows you to disable the **SNAP** frame type for IPX routing to this network.

SNAPNETWORK - SNAP network number

This allows you to set the IPX network number for use with the **SNAP** frame type on this network. The value 0 indicates that the network number should be learned automatically.

E8022ENABLE - 802.2 enable

This allows you to disable the **Ethernet 802.2** frame type for IPX routing to this network.

E8022NETWORK - 802.2 network number

This allows you to set the IPX network number for use with the **Ethernet 802.2** frame type on this network. The value 0 indicates that the network number should be learned automatically.

E8023ENABLE - 802.3 enable

This allows you to disable the **Ethernet 802.3** frame type for IPX routing to this network.

E8023NETWORK - 802.3 network number

This allows you to set the IPX network number for use with the **Ethernet 802.3** frame type on this network. The value 0 indicates that the network number should be learned automatically.

PPPENABLE - PPP enable

This allows you to disable **PPP** for IPX routing to this network. PPP is not used on direct Ethernet connections, only on dialup lines or leased lines.

PPPNETWORK - PPP network number

This allows you to set the IPX network number for use with **PPP** on this network. The value 0 indicates that the network number must be learned automatically as part of the PPP handshake.

QUIT - Previous menu

Returns to the NETWORK *name* IPX menu.

8.7.2 NETWORK *name* IPX ROUTES Menu

London NETWORK ROUTES					
Network	Router	Node	Hops	Ticks	Frame Type
0 IPX:42000000	44000000	12:34:56:78:91:23	2	5	PPP
& ADD	Add new item				
% DELETE	Delete item				
. QUIT	Previous menu				

COMMAND: NETWORK Birmingham IPX ROUTES					

This menu allows you to configure the list of IPX Routes that will be associated with this Destination.

It is necessary to configure the network types associated with this interface before creating new routing entries from this menu. The options are:

An IPX Route

This leads you to the NETWORK *name* IPX ROUTES *route* menu, where the individual fields within this entry can be set.

ADD - Add new item

This menu creates a new IPX Route through this interface. You should select the new route and set its details to the values you require.

DELETE - Delete item

This allows you to delete a route.

QUIT - Previous menu

Returns to the NETWORK *name* IPX menu.

8.7.3 NETWORK *name* IPX ROUTES *route* Menu

London NETWORK STATIC ROUTE		
Command	Description	Current Value
0 REMOTE	Remote network	00000000
1 LOCAL	Network number for next hop	(00000000)
2 NODE	Node number of next hop router	00-00-00-00-00-00
3 HOPS	Hop count	2
4 TICKS	Route length	5
5 FRAMETYPE	Ethernet frame type for next hop	PPP
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IPX ROUTES IPX:network		

This menu allows a single IPX Route through this interface to be configured. The options are:

REMOTE - Remote network

This entry specifies the Remote Network number that is entry defines the route to.

LOCAL - Network number for next hop

This entry specifies the first network that the frame will cross in order to reach its final destination.

This entry is read only. The value displayed is based on the Frame Type that you specify. This is looked up in the network table for this interface, to identify the next directly connected network.

NODE - Node number of next hop router

This entry specifies the Node number (usually the MAC address) of the next router the frame must pass through to reach the destination Network.

HOPS - Hop count

This entry specifies the Hop Count to be advertised to other routers via IPX RIP when information about this route is distributed.

TICKS - Route length

This entry specifies the Number of Ticks to be advertised to other routers via IPX RIP when information about this route is distributed.

FRAMETYPE - Ethernet frame type for next hop

This entry specifies the Frame Type to be used to pass this frame to the next hop router. This entry defaults to PPP, which is correct for all WAN links.

This value is used to index the Networks table for this interface, to identify the next hop network number. The Networks table should be set up for this interface before using this menu.

QUIT - Previous menu

Returns to the NETWORK *name* IPX ROUTES menu.

8.7.4 NETWORK *name* IPX SAPS Menu

London NETWORK SAPS		
Service Name	Sock Network	Service Type
0 DummyFileServer	0346 42000000	File Server (SLIST source)
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IPX SAPS		

This menu allows you to configure the list of IPX SAP Entries that will be associated with this Destination.

It is necessary to configure the network types associated with this interface and the routes through this interface before creating SAP entries from this menu. The options are:

An IPX SAP

This leads you to the NETWORK *name* IPX SAPS *sap* menu, where the individual fields within this entry can be set.

ADD - Add new item

This menu creates a new IPX SAP that can be accessed through this interface. You should select the new SAP entry and set its details to the values you require.

DELETE - Delete item

This allows you to delete a SAP entry.

QUIT - Previous menu

Returns to the NETWORK *name* IPX menu.

8.7.5 NETWORK *name* IPX SAPS *sap name* Menu

London NETWORK STATIC SAP			
Command	Description		Current Value
0 SNAME	Server Name		DummyFileServer
1 SADDR	IPX address of server	00000000:	00-00-00-00-00-00
2 SOCK	server socket number		02b5
3 TYPE	service type		0004
. QUIT	Previous menu		

COMMAND: NETWORK Birmingham IPX SAPS <i>sap name</i>			

This menu allows a single SAP Entry available through this interface to be configured. The options are:

SNAME - Server Name

This entry specifies the SAP Service Name that is entry defines.

SADDR - IPX address of server

This entry provides access to a further sub-menu that allows the destination network and node number on which this service resides, to be specified. A static route to this network must be set up before static SAP entries to this network will function.

SOCK - server socket number

This entry specifies the socket number that is associated with this service.

TYPE - service type

This entry provides access to a future sub-menu that allows the service type associated with this SAP to be selected.

QUIT - Previous menu

Returns to the NETWORK *name* IPX SAPS menu.

8.8 NETWORK *name* ISDN Menu

London		
Command	Description	Current Value
0 DIALLIST	List of numbers to dial	1 number
1 CLILIST	List of acceptable calling numbers	Not checked
2 CLIACTION	Dialback on CLI Match	NO
3 ACCESS	Use access control	NO
4 MINCALL	Control Minimum Call Lengths	NO
5 CLEAR	Cleardown time	25
6 DAY CLEAR	Daytime cleardown time	25
7 EVE CLEAR	Evening cleardown time	50
8 WKEND CLEAR	Weekend cleardown time	100
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham ISDN

This menu allows you to configure how **ISDN** is to be used to connect to a network. The options are:

DIALLIST - List of numbers to dial

This leads to the NETWORK *name* ISDN DIALLIST menu, which allows you to enter the phone numbers used to call this network. If no phone numbers are entered, the router will never attempt to dial out to this network, but it may accept incoming calls from this network.

CLILIST - List of acceptable calling numbers

This leads to the NETWORK *name* ISDN CLILIST menu, which allows you to specify that calls from this network must be from particular ISDN lines. If the CLILIST is empty, all calls will be accepted. Note that this restriction on calls is completely independent of PPP authentication (configured on the NETWORK *name* PPP PAP menu). Incoming calls must authenticate themselves even if the CLILIST is used.

CLIACTION - Dialback on CLI Match

The field allows you to enable the dialback mechanism on calls to this destination. When an incoming call arrives on one of the numbers in the CLILIST for this destination, instead of answering the call it is rejected, and a couple of seconds later the destination is called back using the standard numbers in the DIALLIST.

This option only operates if the Global Check CLI before answering option has been enabled on the GLOBAL ISDN menu.

ACCESS - Use Access Control

This field allows you to enable timed access control when calling this network. It enables use of the controlled access periods (configured on the GLOBAL ISDN ACCESS menu).

MINCALL - Control Minimum Call Lengths

The field allows you to enable the control of minimum call lengths. Enabling this option causes the minimum length of any call to this destination to be controlled using the table of minimum call lengths set in the GLOBAL ISDN TIMES menu, together with the current time and the call rate assigned to the number in the DIALLIST.

Once outside the initial minimum period the other cleardown times on this menu are then used. Only traffic in the last 10 seconds of the minimum call period will prevent the call being dropped at the end of the period. If the time is not set in the router this mechanism will not operate and the CLEAR or DAY CLEAR values will be used.

CLEAR - Cleardown time

When an ISDN call is connected and no traffic has used the connection for a long enough time, the call is cleared. This value sets how long this period is. It is measured in seconds. You may wish to increase this value to make better use of the call charge banding provided by your telecommunications supplier. Setting this field to zero enables the three following menu items, which allow the value of this setting to vary with the time of day and week.

DAY CLEAR - Daytime cleardown time

When the CLEAR field is set to zero this value indicates the link idle time during the daytime period, and when the clock in the router is not set. A "monitor command" can set when this period is.

EVE CLEAR - Evening cleardown time

When the CLEAR field is set to zero this value indicates the link idle time during the evening period. This period is all weekday times outside the daytime period.

WKEND CLEAR - Weekend cleardown time

When the CLEAR field is set to zero this value indicates the link idle time during the weekend period. This period is all of Saturday and Sunday.

QUIT - Previous menu

Returns to the NETWORK *name* IP menu.

8.8.1 NETWORK *name* ISDN DIALLIST Menu

London DIAL LIST				
	Number to dial	Charge rate	Priority	Failed
0 N0	<blank>	NATIONAL	5	-
1 N1 (1 call)	08450798667	NATIONAL	5	-
2 N2	08453535667	NATIONAL	5	-
& ADD	Add new item	% DELETE	Delete item	
. QUIT	Previous menu			
NOTE: please select the blank entry and enter its value				
COMMAND: NETWORK Birmingham ISDN DIALLIST				

This is the list of ISDN numbers to dial to reach this network. The numbers are used in the displayed order unless calls to a specific number have failed in which case the next number in the list is tried. Once all numbers have failed the number that failed longest ago is tried again.

An item

This leads to the NETWORK *name* ISDN DIALLIST N0 menu, which allows you to enter the details of an individual ISDN number.

ADD - Add new item

This menu creates a new entry for a phone number. It is initially blank. You should select the new entry and enter the information required.

DELETE - Delete item

This allows you to delete an ISDN number.

QUIT - Previous menu

Returns to the NETWORK *name* ISDN menu.

8.8.2 NETWORK *name* ISDN NUMBER Menu

London ISDN NUMBER		
Command	Description	Current Value
0 NUMBER	Number to dial	08450798667
1 PRIORITY	Priority of number	5
2 CHARGERATE	Charge rate for this number	NATIONAL
3 LASTFAILURE	Elapsed time since failed to connect	-
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham ISDN DIALLIST N0		

This menu allows you to set up an ISDN number and associate some additional information with it.

NUMBER - Number to dial

This allows the ISDN number itself to be edited. There is no fixed limit to the length of a phone number. A blank number is displayed as <blank>. Everything else is shown as entered. The number used includes any blanks, punctuation, spaces, or other characters exactly as you enter it.

PRIORITY - Priority of number

This allows the priority of this number in relation to the other numbers in the list for this destination to be set. The list will be shown sorted with zero as the highest priority. Numbers of equal priority will be sorted by charge rate, cheapest first.

CHARGERATE - Charge rate for this number

This allows the charge band for this number to be selected. This is used by the minimum call length mechanism.

LASTFAILURE - Elapsed time since failed to connect

This option shows how long since an attempt to call this number was unsuccessful. It is cleared when a successful call starts or ends. It is used to choose which number will be used for an outgoing call. Starting at the top of the priority list, all numbers with recent failures (currently defined as less than 8 minutes) are skipped. If all numbers have recent failures, then the one that failed longest ago is used. This field can be cleared manually, if the problem has been cleared, by selecting it and pressing return or entering 0. It can also be set to a non-zero value, to temporarily inhibit the use of that number. The number may still however be used if the other numbers fail.

QUIT - Previous menu

Returns to the NETWORK *name* ISDN menu.

8.8.3 NETWORK *name* ISDN CLILIST Menu

London CLI LIST	
	Calling Number

0 I0	<blank>
1 I1	0123456789
& ADD	Add new item
% DELETE	Delete item
. QUIT	Previous menu

NOTE: 'x' is a wildcard that matches any digit	
NOTE: please select the blank entry and enter its value	
COMMAND: NETWORK Birmingham ISDN CLILIST	

This is the list of phone numbers from which calls will be accepted from this network. This is in addition to the authentication required by the NETWORK *name* PPP PAP menu. This list is checked *in conjunction with* authentication so:

- It is possible to have two networks calling from the same phone number if they have different names or passwords.
- It is possible to have two networks using the same name and password if they are calling from different phone numbers.
- Incoming calls are answered, and the name and password is accepted before any checking is done. This means that the caller will always be charged for the call.
- Calls, which are rejected, cause a message to be logged via **SYSLOG**.

The commands on this menu are:

An item

This selects an item for you to overwrite its phone number. There is no fixed limit to the length of a phone number. A blank number is displayed as <blank>. Everything else is shown as entered. The number checked includes any blanks, punctuation, spaces, or other characters exactly as you enter it. Note that, depending on the telephone network that the router is connected to, the calling number may not be in the same format as you would use to make an outgoing call. Using a letter x in the number will provide a wildcard entry, so 12x4 will permit calls from ISDN numbers 1214, 1224 and so on.

ADD - Add new item

This menu creates a new entry for a phone number. It is initially blank. You should select the new entry and enter the number required.

DELETE - Delete item

This allows you to delete a phone number.

QUIT - Previous menu

Returns to the NETWORK *name* ISDN menu.

8.9 NETWORK *name* CHANNELS Menu

This menu allows you to configure fixed channels used to connect to a network. Note that outgoing dialup connections are automatically enabled when a phone number is entered on the dial list (as configured on the NETWORK *name* ISDN DIALLIST menu).

London		
Command	Description	Current Value
0 ETHERNET	Ethernet	NO
1 ETHERNET2	Secondary Ethernet	NO
2 X21L1	Leased Line channel 1	NO
3 X21L2	Leased Line channel 2	NO
4 FRL1	Frame Relay Address 1	0
5 FRCIR1	Frame Relay CIR 1	0
6 FRL2	Frame Relay Address 2	0
7 FRCIR2	Frame Relay CIR 2	0
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham CHANNELS

This allows you to configure fixed channels used to connect to a network. Note that outgoing dialup connections are automatically enabled when a phone number is entered on the dial list (as configured on the NETWORK *name* ISDN DIALLIST menu).

ETHERNET - Ethernet

This declares that the specified network is on the local Ethernet.

ETHERNET2 – Secondary Ethernet

This declares that the specified network is on the local Ethernet.

X21L1 – Leased line channel 1

This declares that the specified network is connected via port 1 on the optional X.21 or V.35 card.

X21L2 – Leased line channel 2

This declares that the specified network is connected via port 2 on the optional X.21 or V.35 card.

FRL1 - Frame Relay Address 1

This is the address of Frame Relay WAN link 1.

FRCIR1 - Frame Relay CIR 1

This sets the Committed Information Rate for WAN link 1 over the optional X.21 or V.35 card in bit/s.

FRL2 - Frame Relay Address 2

This is the address of Frame Relay WAN link 1.

FRCIR2 - Frame Relay CIR 2

This sets the Committed Information Rate for WAN link 2 over the optional X.21 or V.35 card in bit/s.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

8.10 HARDWARE Menu

This menu allows you to configure hardware-specific parameters. It does not allow you to associate networks with particular hardware devices. That is done on the NETWORKS menu.

London		
Command	Description	Current Value
0 MSPEED	Management port speed	19200
1 ETHERNET	Configure Ethernet	
2 FRELAY	Configure Frame Relay	
3 VIPER	Configure VIPER Options	
4 YPAGES	Configure VIPER Phone Book	
5 X21L1	Leased Line channel 1	
6 X21L2	Leased Line channel 2	
. QUIT	Previous menu	
COMMAND: HARDWARE		

This allows you to configure hardware-specific parameters. Use the NETWORK *name* CHANNELS menu to tell the router what networks are connected to each port.

The options here are:

MSPEED - Management port speed

This leads to the Management Port Baud Rate menu that allows you to set the management post speed to one of the following speeds (9600, 19200, 38400, 57600 or 115200) 19200 is the default speed.

ETHERNET - Configure Ethernet

This leads to the HARDWARE ETHERNET menu, which allows you to configure the Ethernet port.

FRELAY - Configure Frame Relay

This leads to the HARDWARE FRELAY menu, which allows you to configure the Frame Relay settings

VIPER - Configure VIPER Options

This leads to the HARDWARE VIPER menu, which allows you to configure the VIPER ports.

YPAGES - Configure VIPER Phone Book

This leads to the HARDWARE YPAGES menu, which allows you to control the mapping between Dialed phone numbers and destination IP Addresses.

X21Ln - X.21 leased line channel *n*

Each such item leads to a HARDWARE WAN link menu for that serial line.

Note: This will appear as V35 if the V35 option is fitted to the VIPER.

QUIT - Previous menu

Returns to the MAIN Menu.

8.10.1 HARDWARE MSPEED Menu

London Management Port Baud Rate		
Command	Description	Current Value
0 9600	bps	
1 19200	bps	19200
2 38400	bps	
3 57600	bps	
4 115200	bps	
. QUIT	Previous menu	

COMMAND: HARDWARE MSPEED		

This allows you to set the baud rate of the Config port at the rear of the VIPER. This change is activated when you return to the Main Menu. If connecting via a telnet session then there will be no visible effect. If connected via the rear Config port then communications will be garbled until the terminal emulator is changed to match.

The available options are:

SPEED –

The required speed in bps.

QUIT - Previous menu

Returns to the MAIN Menu.

8.10.2 HARDWARE ETHERNET Menu

London Configure Ethernet		
Command	Description	Current Value
0 ADDRESS	Ethernet address	00-40-93-00-00-15
. QUIT	Previous menu	

COMMAND: HARDWARE ETHERNET		

This menu allows you to view the Ethernet-specific parameters. The options here are:

ADDRESS - Ethernet address

This shows the MAC address, which belongs to this router. It may be useful to know this value for network diagnostics, but the value can not be modified.

QUIT - Previous Menu

Returns to the HARDWARE menu.

7.10.3 FRELAY – Configure Frame Relay Menu

See Section 8.6 for more information on the optional Frame Relay configuration.

7.10.4 VIPER – Configure VIPER Options

See Section 8.1 for more information on VOIP voice configuration.

7.10.5 YPAGES – Configure VIPER Phone Book

See Section 8.1 for more information on VOIP voice configuration.

8.10.3 HARDWARE X21 Menu

London Configure WAN link		
Command	Description	Current Value
0 SPEED	Link speed (bps, 0=external clock)	0
1 EXTSPEED	External clock speed	0
. QUIT	Previous menu	

COMMAND: HARDWARE ... X21...		

This menu appears to allow you to configure any X.21 link. The options here are:

SPEED - Link speed

This allows you to make the port generate a clock. Note that this is not needed for normal operation because the clock is provided from the leased line, but it is very useful for back-to-back testing of two routers. When you set an X.21 port to generate a clock, it appears on pins 7 and 14 of the 15-pin connector. The clock applies only to transmitted data - received data is still clocked by the standard clock, which must be provided on pins 6 and 13 as usual. Some hardware ports cannot generate a clock. For these the speed is shown as a zero in brackets, like this: (0).

EXTSPEED - External clock speed

This value provides information to the router about the speed of the external clock. It is not used if clock is being generated locally.

Its value is used to improve the operation of Multilink over links of speeds greater than 64Kbps, and to provide improved diagnostic information. If this value is left as zero the router will assume a 64Kbps clock.

QUIT - Previous Menu

Returns to the HARDWARE menu.

8.11 ADMIN Menu

London		
Command	Description	Current Value
0 TELNET	Telnet Connection	
1 PING	Ping	
2 ARP	Examine ARP cache	0 entries
3 IPRROUTE	Examine IP routing table	1 entry
4 IPXROUTE	Examine IPX routing table	0 entries
5 SAP	Examine IPX SAP table	0 entries
6 PHYSICALS	Examine Physical table	
. QUIT	Previous menu	

COMMAND: ADMIN		

The items on this menu are used to examine the running system and to perform some administrative tasks. They are:

TELNET - TELNET Connection

This allows you to enter an **IP address** and attempts to open a **TELNET** session to that address either to another VIPER or another TELNET compatible device.

PING - Ping

This command provides the **ping** facility, which tests connectivity and response time. When you enter the **IP address** the ping is sent and the router waits up to two seconds for a response. If a response is received, the response time is given. Pressing RETURN will repeated the pin with the same IP address.

ARP - Examine ARP cache

This leads to the ADMIN ARP menu, which allows you to examine and modify the **ARP** cache.

IPROUTE - Examine IP Routing table

This leads to the ADMIN IPROUTE menu, which allows you to examine and modify the IP routing table. The operation of this table is described in Section 4.1 (Introduction to IP Networking).

IPXROUTE - Examine IPX Routing table

This leads to the ADMIN IPXROUTE menu, which allows you to examine and modify the IPX routing table. The operation of this table is described in the section 4.2.1 (IPX Routing).

SAP - Examine IPX SAP table

This leads to the ADMIN SAP menu, which allows you to examine and modify the IPX SAP table. The operation of this table is described in Section 4.3.3 (IPX SAP - Service Advertising Protocol).

PHYSICALS - Examine PHYSICALS table

This leads to the ADMIN PHYSICALS menu, which allows you to view the physical state of the external connections.

QUIT - Previous Menu

Returns to the MAIN menu.

8.11.1 ADMIN ARP Menu

This menu lists the contents of the ARP cache, with each item being a summary of one entry in the cache. The format of the summary is:

IP:147.1.16.205 00:aa:00:29:d7:fa 2m8s

These are, from left to right, the IP address, the Ethernet address, and the age of the entry. Section 4.3.1 (ARP - Address resolution protocol) explains what these mean. If the Ethernet address is not valid (either because it was never discovered, or because it has expired), it is shown as `?:?:?:?:?:?:?:?`. If you select an entry, you are presented with the ADMIN ARP *ip* menu.

The QUIT option on this menu returns to the ADMIN menu.

8.11.2 ADMIN ARP *ip* Menu

London ARP ITEM		
0 IP	IP address	193.123.116.12
1 MAC	MAC address	a7-a7-a7-a7-a7-a7
2 VALID	address translation is valid	NO
3 RETRIES	retries remaining	1
4 AGE	time since last updated	(4s)
. QUIT Previous menu		
COMMAND: ADMIN ARP IP:193.123.116.12		

This menu shows one ARP cache entry expanded to show its details. The parts of a cache entry are:

IP - IP address

This is the IP address of this entry.

MAC - MAC address

This is the **MAC** (Ethernet) address associated with this entry. If the address is not valid because it has expired, the last known value is shown.

VALID - address translation is valid

This indicates whether or not the MAC address associated with this entry is valid. If the address is invalid because it has expired, you can alter this indication to make it valid again. However, if the MAC address has not been determined, manually declaring it valid will cause the router to use the invalid address. For this reason, you should not normally alter an entry in the ARP cache.

RETRIES - retries remaining

When the router first decides that it needs to use an Ethernet address, it creates an ARP cache entry for the desired IP address. This menu item shows how many more *ARP requests* that the router will send before deciding that the IP address cannot be resolved.

AGE - time since last updated

This shows the time since this entry was last modified (either by manual modification or by receiving an ARP request or reply).

QUIT - Previous Menu

Returns to the ADMIN ARP menu.

8.11.3 ADMIN IPRROUTE Menu

London IP ROUTING TABLE						
Destination	Msk Router	Flags	Age	Me	Type	Name
0 IP:192.168.1.254	/32 0.0.0.0		1s	0	Self	ETH
1 IP:255.255.255.255	/32 0.0.0.0	N	1s	0	Self	(-)
2 IP:192.168.1.255	/32 255.255.255.0	N	1s	1	Bcst	ETH
3 IP:192.168.2.255	/32 255.255.255.0	N	1s	1	Bcst	Birmingham
4 IP:192.168.1.0	/24 0.0.0.0	T	1s	1	Fwd	ETH
5 IP:192.168.2.0	/24 0.0.0.0	T	1s	1	Fwd	Birmingham
6 IP:0.0.0.0	/ 8 0.0.0.0		1s	0	Drop	(-)
7 IP:127.0.0.0	/ 8 0.0.0.0		1s	0	Self	(-)
8 IP:224.0.0.0	/ 3 0.0.0.0		1s	0	Drop	(-)
& ADD	Add new item					
% DELETE	Delete item					
. QUIT	Previous menu					

NOTE: manual changes to this table are transient, use the NETWORKS menu for permanent changes.

This menu lists the contents of the IP routing table, with each item being a summary of one entry in the table. If you select an entry, you are presented with the ADMIN IPRROUTE *ip* menu, which is an expanded view of the route, and includes fields, which cannot be displayed on the summary. The columns shown on the summary are as follows. The name in brackets is the name as it appears on the expanded list. See the explanations on the expanded list for details of what each item means.

Destination (IP)

The IP address that the route must match.

Msk (MASK)

The address mask used by this route

Router (ROUTER)

The address of the next hop router OR mask value for broadcasts.

Flags (FLAGS)

Various IP routing flags

Age (AGE)

The age of this route

Me (METRIC)

Route metric

Type (TYPE)

Action to be performed which this entry matches an address

Name (INTERFACE)

Name of associated interface

QUIT - Previous Menu

Returns to the ADMIN menu.

8.11.4 ADMIN IPRROUTE ip Menu

London IP ROUTE		
Command	Description	Current Value
0 IP	IP address	192.168.1.0
1 MASK	address mask	255.255.255.0 /24
2 TYPE	type of route	FORWARD
3 METRIC	cost of route	1
4 FLAGS	routing flags	T
5 ROUTER	next hop/broadcast mask	0.0.0.0
6 AGE	time since last update	(18m26s)
7 EXPIRES	time until route expires (RIP only)	(-)
8 INTERFACE	name of next hop network	(ETH)
. QUIT	Previous menu	

COMMAND: ADMIN IPRROUTE IP:192.168.1.0

This menu displays one IP routing table entry expanded to show its details. An IP routing entry consists of:

IP - IP address

This is the IP address of this entry. When an address is being looked up, this value is used in conjunction with the IP address mask, which is the next item.

MASK - address mask

When an IP address is being looked up, each entry in the IP routing table is tested in turn. If, for a particular entry, the part of the target address selected by this mask matches the IP address specified in the previous field, the entry is used to route the target IP address.

TYPE - type of route

This leads to the ADMIN IP ROUTE FLAGS *TYPE* Menu.

METRIC - cost of route

When there is a choice between several routes, the router uses this value to select the best route. See Section 4.1.6 (IP Routing Metrics) for an explanation of how this works.

FLAGS - routing flags

This leads to the ADMIN IPRROUTE *ip* FLAGS menu, which allows you to examine flags, associated with the route. Any flags, which are enabled, are shown in abbreviated form in the *Current Value* column of the menu. The abbreviations are the single letter codes in brackets on the ADMIN IPRROUTE *ip* FLAGS menu.

ROUTER - IP address of router to use

This gives some extra information about specifies where the route goes. When the route type is FORWARD, this may be the address of the next hop router. For a route type of BROADCAST this value is instead the mask, which specifies where the broadcast goes. See Section 4.1 (Introduction to IP Networking) for an explanation of how routing works.

AGE - time since last use

This is only relevant when **RIP** is in use. It shows the time since this route was last updated by RIP. If the route is a permanent route (not affected by RIP), the time will always show as zero.

EXPIRES - time until route expires**INTERFACE - name of associated interface**

This value is determined by the *ROUTER* portion of the routing entry. It is available as part of the routing entry mainly to avoid having to look up the value each time the entry is used. It is also useful when examining the table because it shows which network on the NETWORK menu is responsible for the route.

QUIT - Previous Menu

Returns to the ADMIN IPRROUTE menu.

8.11.5 ADMIN IP ROUTE FLAGS TYPE Menu

London IP ROUTE FLAGS		
Command	Description	Current Value
0 SELF	this is one of our addresses	<<<<<<<
1 FORWARD	forward to next hop	
2 ICMPHOST	produce ICMP host unreachable error	
3 ICMPNET	produce ICMP net unreachable error	
4 BROADCAST	broadcast as per mask	
5 DISCARD	discard	
. QUIT	Previous menu	

COMMAND: ADMIN IPRROUTE IP:192.168.42.200 TYPE		

This menu shows the type of route this entry is.

SELF – this is one of our addresses

This address is one set in configuration of the VIPER like the Ethernet port or one like the Loopback address 127.0.0.0 that is assigned to the VIPER in software.

FORWARD – forward to next hop

This address is forwarded on its specified INTERFACE. Examples of entries like this include the IP address range and netmask that is assigned to a port, e.g. if a port is set to 10.1.1.1 with a netmask of 255.255.255.0 then a FORWARD IPRROUTE will appear that has and IP 10.1.1.0 and netmask 255.255.255.0

ICMPHOST – produce ICMP host unreachable error

This address had produced an error. This VIPER hasn't received a reply to its ARP request to the specified address, i.e. the destination host doesn't exist.

ICMPNET – produce ICMP net unreachable error

This address had produced an error. This VIPER hasn't received a reply to its ARP request to the specified address; in this case the destination network doesn't exist.

BROADCAST – broadcast as per mask

This is a broadcast address.

If a port is set to 10.1.1.1 with a netmask of 255.255.255.0 then a BROADCAST IPRROUTE will appear that has and IP 10.1.1.255 and netmask 255.255.255.255 then any frame being sent to address 10.1.1.2 would know where to go.

DISCARD – discard

This address is dropped, i.e. ignored and not transmitted by the VIPER.

QUIT - Previous Menu

Returns to the ADMIN IPRROUTE *ip* menu.

8.11.6 ADMIN IPRROUTE *ip* FLAGS Menu

London IP ROUTE FLAGS		
Command	Description	Current Value
0 RIPTX	(T) advertise route via RIP	NO
1 RIVIPER	(R) route was learnt via RIP	NO
2 NOICMP	(N) generate no ICMP errors	YES
3 DELETED	(D) route has been deleted	NO
. QUIT	Previous menu	

COMMAND: ADMIN IPRROUTE IP:10.255.255.255 FLAGS		

This menu displays the flags associated with one IP routing table entry. The letter in brackets at the beginning of each flag's description is the abbreviation, which appears on the ADMIN IPRROUTE *ip* menu when the flag is enabled. The flags are:

RIPTX - advertise route via RIP

This flag controls whether or not the route is advertised in periodic RIP broadcasts.

RIVIPER - route was learnt via RIP

This flag records the origin of this route. Routes learnt from **RIP** broadcasts expire automatically and can be updated by subsequent broadcasts.

NOICMP - generate no ICMP errors

This flag controls whether or not ICMP error frames can be generated in response to a frame which matches this route. The routes, which have this flag set, are routes describing broadcasts and routes describing certain special addresses.

DELETED - route has been deleted

This flag is set when a route is deleted while you are examining it. The route is not used and it retained only until you exit from the menu displaying it.

QUIT - Previous Menu

Returns to the ADMIN IPRROUTE *ip* menu.

8.11.7 ADMIN IPXROUTE Menu

London IPX ROUTING TABLE							
Network	Router	Node	Hps	Tks	Age	L/R Name	
0 IPX:00000002	00000000	00:00:00:00:00:00	1	1	1h16m	L eth0	
1 IPX:00000001	00000000	00:00:00:00:00:00	1	1	1h16m	L eth0	
2 IPX:99900000	00000000	00:00:00:00:00:00	1	1	1h16m	L Birmingham	
3 IPX:00000123	00000001	00:00:01:01:59:81	2	6	2s	R eth0	
& ADD	Add new item	% DELETE	Delete item	. QUIT	Previous menu		

NOTE: manual changes to this table are transient use the NETWORKS menu for permanent changes
 This menu lists the contents of the IPX routing table, with each item being a summary of one entry in the table. If you select an entry, you are presented with the ADMIN IPXROUTE *ipx* menu. The columns shown on the summary are as follows. The name in brackets is the name as it appears on the expanded list. See the explanations on the expanded list for details of what each item means.

Network (NET)

The IPX network address that the route describes

Router (ROUTER)

The IPX network address of the next hop router

Node (ROUTER)

The IPX node address of the next hop router

Hps (HOPS)

The number of hops to this network

Tks (TICKS)

The number of tick to this network

Age (AGE)

The time since this route was last updated

L/R (FLAGS)

Local or remote indicator

Name (INTERFACE)

Name of interface to use

QUIT - Previous Menu

Returns to the ADMIN menu.

8.11.8 ADMIN IPXROUTE *ipx* Menu

London IPX ROUTE		
Command	Description	Current Value
0 NET	remote network	00000001
1 ROUTER	IPX address of router 00000000:	00-00-00-00-00-00
2 FLAGS	routing flags	D
3 HOPS	hop count	1
4 TICKS	route length	1
5 AGE	time since last updated	(1h31m)
6 INTERFACE	name of associated interface	(eth0)
7 FRAMETYPE	Ethernet frame type	(Enet 802.3)
. QUIT	Previous menu	

COMMAND: ADMIN IPXROUTE IPX:00000001

This menu shows one IPX routing table entry expanded to show its details. An IPX routing entry consists of:

NET - remote network

This indicates the network number of those IPX addresses, which the route covers.

ROUTER - IPX address of router to use

This specifies where the route goes. It must be the address of a router on a directly connected network. Since IPX addresses have two components, this item leads to the ADMIN IPXROUTE *ipx* ROUTER menu.

FLAGS - routing flags

This leads to the ADMIN IPXROUTE *ipx* FLAGS menu, which allows you to examine flags, associated with the route. Any flags, which are enabled, are shown in abbreviated form in the *Current Value* column of the menu. The abbreviations are the single letter codes in brackets on the ADMIN IPXROUTE *ipx* FLAGS menu.

HOPS - hop count

This shows the distance to the remote network. This is used by the router to decide between routes as explained in Section 4.2.4 (IPX Routing Metrics).

TICKS - route length

This is another measure of the distance to the remote network. This is used by the router to decide between routes as explained in Section 4.2.4 (IPX Routing Metrics).

AGE - time since last updated

This is only relevant when RIP is in use. It shows the time since this route was last updated by RIP. If the route is a permanent route (not affected by RIP), the time will always show as zero.

INTERFACE - name of associated interface

This value is determined by the *ROUTER* portion of the routing entry. It is available as part of the routing entry mainly to avoid having to look up the value each time the entry is used. It is also useful when examining the table because it shows which network on the NETWORK menu is responsible for the route.

FRAMETYPE - Ethernet frame type

This shows which kind of Ethernet frame is used on the network when routing data to this network.

QUIT - Previous Menu

Returns to the ADMIN IPXROUTE menu.

8.11.9 ADMIN IPXROUTE *ipx* ROUTER Menu

London IPX ADDRESS		
Command	Description	Current Value
0 NETWORK	network number	00000000
1 NODE	node number	01-02-03-04-05-06
. QUIT	Previous menu	
COMMAND: ADMIN IPXROUTE IPX:00000000 ROUTER		

This menu shows an IPX address expanded into its component parts. An IPX address consists of:

NETWORK - network number

As described in IPX addresses, this indicates the network to which the device with this address is directly connected.

NODE - node number

As described in IPX addresses, this indicates the individual device on the network specified by the network number.

QUIT - Previous Menu

Returns to the ADMIN IPXROUTE *ipx* menu.

8.11.10 ADMIN IPXROUTE *ipx* FLAGS Menu

London IPX ROUTE FLAGS		
0 DIRECT	(D) directly connected	YES
1 STATIC	(S) static route	NO
2 DELETED	(X) route has been deleted	(NO)
. QUIT	Previous menu	
COMMAND: ADMIN IPXROUTE IPX:00000001 FLAGS		

This menu displays the flags associated with one IPX routing table entry. The letter in brackets at the beginning of each flag's description is the abbreviation, which appears on the ADMIN IPXROUTE *ipx* menu when the flag is enabled. The flags are:

DIRECT - (D) directly connected

This flag indicates whether or not the route leads to another router or to a directly connected network.

STATIC - (S) static route

This flag indicates whether or not this route is static, and stored as part of the units configuration.

DELETED - (X) route has been deleted

This flag is set when a route is deleted while you are examining it. The route is not used and it retained only until you exit from the menu displaying it.

QUIT - Previous Menu

Returns to the ADMIN IPXROUTE *ipx* menu.

8.11.11 ADMIN SAP Menu

London SAP TABLE				
Service Name	Sock	Hop	Age	Service Type
0 SERVER_1	0451	1	57s	File Server (SLIST source)
1 CASE COMMS	8104	2	20s	NetWare 386 or RSPX Remote Console
2 CASECOMMS	0451	2	20s	File Server (SLIST source)
& ADD	Add new item			
% DELETE	Delete item			
. QUIT	Previous menu			
NOTE: manual changes to this table are transient				
COMMAND: ADMIN SAP				

This menu lists the contents of the SAP table, with each item being a summary of one entry in the table. If you select an entry, you are presented with the ADMIN SAP *sap* menu. The columns shown on the summary are as follows. The name in brackets is the name as it appears on the expanded list. See the explanations on the expanded list for details of what each item means.

Service Name (SNAME)

The name of the service

Sock (SOCK)

The server socket number in hex

Hop (HOPS)

The number of hops to the server

Age (AGE)

The time since this entry was last updated

Service Type (TYPE)

A description of the type of service

8.11.12 ADMIN SAP *sap* Menu

London SAP LIST			
Command	Description		Current Value
0 SNAME	Server Name		ARIES SERVER
1 SADDR	IPX address of server	0000001	:00-de-20-00-26-b7
2 SOCK	server socket number		1105
3 TYPE	service type		0004
4 HOPS	hop count		2
5 FLAGS	flags		
6 AGE	time since last updated		(36s)
7 INTERFACE	name of associated interface		(eth0)
8 FRAMETYPE	Ethernet frame type		(Enet 802.3)
. QUIT	Previous menu		

COMMAND: ADMIN SAP ARIES SERVER			

This menu shows one SAP table entry expanded to show its details. A SAP table entry consists of:

SNAME - server name

The name of the service described by this entry.

SADDR - IPX address of server

This gives the IPX address of the server, which is providing the service, described by this entry. Since IPX addresses have two parts, this item leads to the ADMIN SAP *sap* SADDR menu that expands the address into its components. This menu is not described because it is exactly the same as the ADMIN IPXROUTE *ipx* ROUTER menu.

SOCK - server socket number

The socket number of the service. This is an arbitrary number, which must be specified in messages intended for this service. On this menu the number is shown in decimal, while on the summary it is shown in hex. This allows you to see both formats easily.

TYPE - service type

The service type. On the summary this is shown as the name of the service, while the value on this menu is shown numerically (in decimal). If you select this item, you are shown a menu of possible service types, giving names as well as numeric values. The selected service type is indicated by a marker in the rightmost column, like this:

S:0004 File Server (SLIST source) <<<<<<

HOPS - hop count

This is a measure of the distance to the server. Hop counts are described in Section 4.2.4 (IPX Routing Metrics).

FLAGS - flags

This entry leads to a sub-menu where you can set the individual flags associated with this entry.

AGE - time since last updated

This shows the time since a description of this service was last received in a SAP. SAPs are described in more detail in Section 4.3.3 (IPX SAP - Service Advertising Protocol).

INTERFACE - name of associated interface

This shows which network on the NETWORK menu is responsible for the route to the server, which is providing this service.

FRAMETYPE - Ethernet frame type

This shows which kind of ethernet frame is used on the network when routing data to this server.

QUIT - Previous Menu

Returns to the ADMIN menu.

8.11.13 ADMIN PHYSICALS Menu

This menu displays the physical connections of the router, each entry represents one connection i.e. X21 or ISDN B channel. An example display is:

#	Link	Name	St	L2	LCP Mode	Idlet	Speed
0	LAN	DEFAULT_ETH	Co	Unk	-	-	-
1	M.1 -		Fr	PPP	Starting	HDLC	-
2	M.2	ISDN1->11	Co	PPP	AuthOK	HDLC 29s	-
3	M.3	ISDN2->12	Co	PPP	AuthOK**	HDLC 29s	-
4	M.4 -		Fr	Unk	-	-	115200

RETURN to Re-display Any Character to Exit >

These are, from left to right, reference number, slot reference number, name of destination network, status, level 2 functionality, LCP State, transmission mode, idle time, and, speed.

Reference Number

A number only used for display purposes indicating the number of links on the router. 0 always indicates Ethernet.

Link

Of the forms. 1 where 1 indicates the link number in slot s. The Viper, has 2 slots - WAN Module 1 and WAN Module 2, the slot number may be 1 or 2.

Name

The name of the configured network on which this link is defined. If the link uses ISDN then an indication of the called or calling party is displayed.

Status

This is an indication of the current usage of the link. It may be one of:

- Fr - Free
- Id - Identifying call
- St - Connecting
- Co - Connected

L2

PPP for WAN links. Unk(unknown) for Ethernet or unconnected links.

LCP

The Link Control Protocol of the PPP link. When this indicates AuthOK then the link is operational. Two symbols after AuthOK indicate compression has been negotiated on the link, one symbol for each direction. An Asterisk indicates software Stac compression a up arrow indicates hardware Stac compression.

Mode

Transmission mode - HDLC or ASYNC.

Idlet

A no-traffic timer used for ISDN. When reaching 0 the call is disconnected.

Speed

The current speed of the link if configured in the router.

8.12 STATUS Menu

```

London STATUS
-----
CODEVERSION          V4.20  24 Sep 2004
OPTIONS              F-Relay
UPTIME               3h51m
RAMUSED              11%
IOCARD               card: Dual X.21
CPU USAGE            0.0%
DATE                 Tuesday 12th June 2007
TIME                 13:30:11
VIPER-PVM4-137      FXO/FXS-4 (48104) Software Version 130
VIPER-PVM4-FXS 1    (0) On Hook
VIPER-PVM4-FXS 2    (1) Off Hook
+  NEXT PAGE

. QUIT              Previous menu
-----
Pressing the + key also displays:

```

```

London STATUS
-----
PREVIOUS PAGE
VIPER-PVM4-FXS 3    (6) Off Hook
VIPER-PVM4-FXS 4    (7) Off Hook Rx: 2850 bps Tx: 900 bps
Q.921-?             State: 4
ISAC-ISDN-BRI      State: 3+PS1
Q.921-?             State: 1
. QUIT              Previous menu
-----

```

This screen presents information about the router, including the option cards fitted. In this example the VIPER has a X21 card and a FXO/FXS voice option card fitted that has been set to FXS. Different voice option cards will have different items for the available ports. For example an FXO card will show something like:

```

VIPER-PVM4-137      FXO/FXS-4 (48104) Software Version 130
VIPER-PVM4-FXO 1    (0) No Ring
VIPER-PVM4-FXO 2    (0) No Ring
VIPER-PVM4-FXO 3    (0) No Ring
VIPER-PVM4-FXO 4    (0) No Ring

```

The items in this menu are:

CODEVERSION

The version of the software loaded into the Router. The first letter indicates which type of router this code version is for. Any trailing letters indicate test or special build versions.

OPTIONS

This shows any options set on software of the VIPER, in the example above it shows that Frame Relay is an option. This doesn't mean that the option is active.

UPTIME

The time since the router was last switched on or rebooted.

RAMUSED

The proportion of the total RAM available currently being used.

IOCARD/ANALOGUE-n

This part of the screen shows details of the various WAN options fitted to the router.

CPU USAGE

The proportion of the total CPU power available currently is being used.

DATE

The current date is shown if it is set, otherwise this line is not shown.

TIME

The current time is shown if it is set, otherwise this line is not shown. Both the date and time can be set in DEBUG MONITOR mode or by using the SNTP option to obtain the date and time from a time server.

Note: The time and date are stored in volatile RAM and so is lost on reboot or poweroff.

The remaining lines give the status of the voice option card fitted along with the ISDN interfaces fitted to the unit. The example above is with an FXO/FXS card and has been set to FXS.

8.12.1 FXS Status

VIPER-PVM4-137	FXO/FXS-4 (48104) Software Version 130
VIPER-PVM4-FXS 1	(0) On Hook
VIPER-PVM4-FXS 2	(1) Off Hook
VIPER-PVM4-FXS 3	(6) Off Hook
VIPER-PVM4-FXS 4	(7) Off Hook Rx: 2850 bps Tx: 900 bps
Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1

VIPER-PVM4-137 FXO/FXS-4 (48104) Software Version 130

This line shows the type of card fitted and, where applicable, the software version used on the voice option card.

VIPER-PVM4-FXS 1 (0) On Hook

This line shows the status of port 1 of the FXS card. In this case it is on hook and there is no call in progress or being made. The(0) means that there is no activity on the port.

VIPER-PVM4-FXS 2 (1) Off Hook

This line shows the status of port 2 of the FXS card. In this case it is off hook and the (1) status in this case means that there is a dial tone on the port, i.e. there has been no phone number digit dialled.

A (3) means that there have been phone number digits dialled and so far they are all valid within the VIPER's YPAGES.

A (5) means that an invalid phone number, or part of phone number, has been dialled.

VIPER-PVM4-FXS 3 (6) Off Hook

This line shows the status of port 3 of the FXS card. In this case it is off hook and the (6) status in this case means that there is a ring tone on the port, i.e. the call made was valid within the VIPER's YPAGES and the remote end is ringing.

VIPER-PVM4-FXS 4 (7) Off Hook Rx: 2850 bps Tx: 900 bps

This line shows the status of port 4 of the FXS card. In this case it is off hook and there is a call in progress. RX is the amount of "data" received from the connected telephone and TX is the amount of "data" going out to the telephone.

The (7) means that a call is in progress.

The remaining lines show the status of the ISDN port.

8.12.2 FXO Status

VIPER-PVM4-137	FXO/FXS-4 (48104) Software Version 130
VIPER-PVM4-FXO 1	(0) No Ring
VIPER-PVM4-FXO 2	(0) No Ring
VIPER-PVM4-FXO 3	(0) No Ring
VIPER-PVM4-FXO 4	(0) No Ring
Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1

With a FXO voice option card the status screen will show the above.

Most of the status will mimic the FXS card, except that if there are no calls in progress then the VIPER shows the status as No Ring.

When a call is in progress then there will be the RX and TX values shown as in the FXS card.

8.12.3 AC15 Status

VIPER-PVM4-138	E&M/AC15-4 (48104) Software Version 130
VIPER-PVM4-AC15 1	(0) Idle Level 0
VIPER-PVM4-AC15 2	(0) Idle Level 0
VIPER-PVM4-AC15 3	(0) Idle Level 0
VIPER-PVM4-AC15 4	(0) Idle Level 0
Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1

With an AC15 voice option card the status screen will show the above.

In the above screen there are no calls in progress, during call set up the Idle Level will change and when a call is in progress then there will be the RX and TX values shown just like the FXS.

8.12.4 BRI Status

VIPER-PVMI-0	VISDN (48104) Software Version 130
Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1
Q.921-?	State: 4
ISAC-VISDN-BRI1	LT-S State: G2
Q.921-?	State: 4
Q.921-?	State: 4
ISAC-VISDN-BRI2	LT-S State: G2
Q.921-?	State: 4

With a PRI voice option card fitted the status screen will show the above. The ISAC-ISDN-BRI and Q921 lines above and below it show the status of the ISDN port. The remaining lines show the status of the two BRI ports on the BRI voice option card.

8.12.5 PRI Status

VIPER-PVMI-0	VISDN (48105) Software Version 130
Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1
Q.921-?	State: 4
FALC-PRI-VISDN	State: 3-signal-frame-multiframe
Q.921-?	State: 4

With a PRI voice option card fitted the status screen will show the above. The ISAC-ISDN-BRI and the Q.921 entries directly above and below it are the status of the ISDN port on the VIPER. The remaining Q.921 lines and the FALC-PRI-VISDN entries show the status of the PRI voice option. In the above example the PRI is inactive and not connected. The available states

8.12.6 ISDN Status

Q.921-?	State: 4
ISAC-ISDN-BRI	State: 3+PS1
Q.921-?	State: 1

Q.921-? State: 4

This line shows the state of the ISDN port. In this case there is no activity on the ISDN port.

ISAC- ISDN-BRI State: 3+PS1

This line shows the status of the ISDN port. PS1 means that this ISDN has compatible with the ETSI Euro-ISDN standard.

Q.921-? State: 1

This line shows the state of the ISDN port. In this example there is no activity on the ISDN port, as indicated by the question mark.

8.13 STATISTICS Menu

London STATISTICS		
Command	Description	Current Value
0 IP	IP Statistics	
1 ICMP RECEIVE	ICMP RECEIVE Statistics	
2 ICMP SEND	ICMP SEND Statistics	
3 TCP	TCP Statistics	
4 UDP	UDP Statistics	
5 SNMP1	SNMP1 Statistics	
6 SNMP2	SNMP2 Statistics	
7 ETHERNET	ETHERNET Statistics	
. QUIT	Previous menu	

COMMAND: STATISTICS		

This menu leads to various lists of statistics. These statistics are volatile, i.e. they are reset on reboot or power up.

8.13.1 IP – IP Statistics

IP STATISTICS	
Total packets received	11
Total packets dropped	0
Total packets dropped due to wrong version	0
Destination unreachable packets received	0
Packets not for this router	0
Forwarded packets	24
Packets dropped due to protocol	0
Packets delivered	11
Packets sent	24
Packets dropped due to no route	0
Fragments received	0

This menu shows the **IP** activity on the VIPER.

8.13.2 ICMP RECEIVE - ICMP RECEIVE Statistics

ICMP RECEIVE STATISTICS	
Messages received	22
Messages received with ICMP-specific errors	0
Destination unreachable messages received	0
ICMP time Exceeded messages received	0
Parameter problem messages received	0
Source Quench messages received	0
Redirect messages received	0
Echo (request) messages received	18
Echo reply messages received	4
Timestamp (request) messages received	0
Timestamp reply messages received	0

This menu shows the **ICMP** Receive activity.

These are the messages received by the VIPER from other devices in the network. These are error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

8.13.3 ICMP SEND - ICMP SEND Statistics

ICMP SEND STATISTICS	
Messages sent	27
Destination unreachable messages sent	0
Echo (request) messages sent	9
Echo reply messages sent	18
Timestamp reply messages sent	0

This menu shows the **ICMP** Send activity.

These are the messages sent by the VIPER to other devices in the network. These are error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

8.13.4 TCP – TCP Statistics

TCP STATISTICS	
Active Opens	0
Received with bad TCP checksum	0
Bytes received	72
Bytes sent	8972
Passive Opens	2
Segments Received	92
Segments Sent	66
Segments Retransmitted	0
Resets received	0
Packets for invalid socket	0

This menu shows the **TCP** activity for the **TCP** Internet Protocol.

8.13.5 UDP – UDP Statistics

UDP STATISTICS	
Datagrams delivered to UDP users	520
Datagrams for which there is no application	0
Error Datagrams not including above	0
Datagrams sent	1038

This menu shows a list of the **UDP** activity for the **UDP** Internet Protocol.

8.13.6 SNMP1 – SNMP1 Statistics

SNMP1 STATISTICS	
PDU's delivered to SNMP entity from transport service	0
PDU's passed from SNMP protocol to transport service	0
Unsupported SNMP version PDU's Delivered	0
PDU's delivered with unknown community name	0
PDU's delivered not allowed by community named	0
ASN.1 parsing errors	0
Get-Request and Get-Next MIB objects retrieved	0
Set-Request MIB objects altered	0
Get-Request MIB objects accepted and processed	0
Get-Next MIB objects accepted and processed	0
Set-Request MIB objects accepted and processed	0
Get-Response MIB objects accepted and processed	0

These statistics show the **SNMP** activity.

8.13.7 SNMP2 – SNMP2 Statistics

SNMP2 STATISTICS	
Valid SNMP PDU's with ErrorStatus tooBig	0
Valid SNMP PDU's with ErrorStatus noSuchName	0
Valid SNMP PDU's with ErrorStatus badValue	0
Valid SNMP PDU's with ErrorStatus genErr	0
Get-Response PDU's generated	0
SNMP Trap PDU's generated	0

These statistics show the **SNMP** Trap activity.

8.13.8 ETHERNET STATISTICS

Frames Correctly Received	0
Frames discarded internal busy	0
Frames discarded bad format	0
Unicast Frames Received	0
Multicast Frames Received	0
Bytes Received	0
Frames Correctly Transmitted	0
Transmission aborted, external errors	521
Transmission failed internal busy	0
Bytes transmissions Attempted	44786
Unicast transmissions Attempted	0
Multicast transmissions Attempted	521

These statistics show the Ethernet activity.

8.14 WAN STATISTICS Menu

London WAN STATISTICS		
Command	Description	Current Value
0 X.21 Link 1	X.21 Link 1 Statistics	
1 X.21 Link 2	X.21 Link 2 Statistics	
2 ISDN2 B1	ISDN2 B1 Statistics	
3 ISDN2 B2	ISDN2 B2 Statistics	
. QUIT	Previous menu	

COMMAND: WANSTATS		

This menu leads to various screens of statistics for the various WAN links. The list of screens will be different for each router depending on the options and cards fitted.

In the above example all four entries show a similar screen.

8.14.1 Statistics Menu

X.21 Link 1 STATISTICS	
Correctly Received Frames	0
Received Frames Lost	0
Corrupt Received Frames	0
Total Received Frames	0
Correctly Received Bytes	0
Correctly Transmitted Frames	0
Transmit Frames Lost	0
Failed Frame Transmissions	0
Total Transmitted Frames	0
Total Transmitted Bytes	0

This menu shows the number of frames that have been handled by the relevant WAN port. All of the X21, V35 and Frame Relay WAN port shows identical statistics screens.

8.15 DEBUG menu

London		
Command	Description	Current Value
0 MONITOR	Debugging monitor	
1 BOUNCE	Reboot on error	BOUNCE
2 REBOOT	Reboot Now	
. QUIT	Previous menu	

COMMAND: DEBUG		

This menu provides options for use when debugging the router itself. They are:

MONITOR - Debugging monitor

Provides access to a command-line oriented monitor. Use the 'q' command to return to the menus. It is necessary to enter the monitor to upgrade the router software.

There are some valid entries that can be used that have already been mentioned so far in this manual. There are other and there are more details on them in a later section.

BOUNCE - Reboot on error

This leads to the DEBUG BOUNCE menu, which allows you to select the router behaviour when it discovers an internal problem.

REBOOT - Reboot router

Reboots the router. It is necessary to reboot the router after some types of configuration change. Note that all Telnet sessions will be closed when the router is rebooted, so if you give this command from a Telnet session, you will have to reconnect if you want to use the menus again.

QUIT - Previous Menu

Returns to the MAIN menu.

8.15.1 DEBUG BOUNCE Menu

London DEBUG ACTION		
Command	Description	Current Value
0	DEBUG	Enter debugger on any error
1	BOUNCE	Reboot on error
.	QUIT	Previous menu

COMMAND: DEBUG BOUNCE		

The router continually checks itself for errors. If it discovers an internal error, it can either reboot itself, which will almost always allow the network to continue operating normally, or it can halt in a debugger, which stops it working but allows the fault to be checked. Normally a router is configured to reboot on error. This menu allows you to select the desired behaviour.

DEBUG - Enter debugger on any error

This option makes the router halt in the debugger when it detects any kind of internal error. It is not normally practical to use this option when direct access to the router is not easy, because it is necessary to switch off the router to restart it after using the debugger in this way.

BOUNCE - Reboot on error

This option makes the router reboot when it detects any kind of internal error.

QUIT - Previous Menu

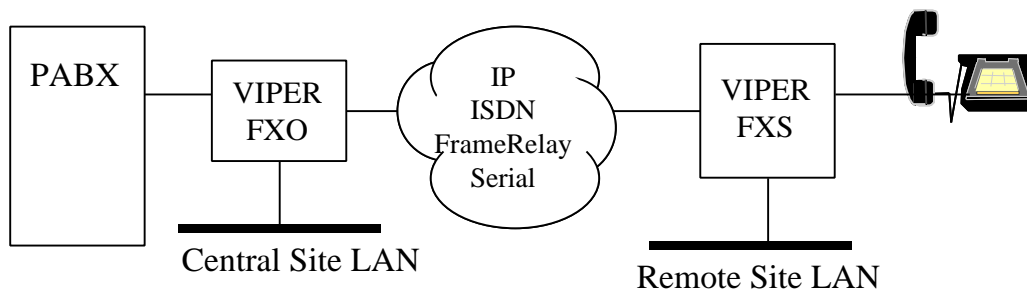
Returns to the DEBUG menu.

Section 9 Voice Over IP Features

9.1 Voice Over IP

The VIPER unit is available in six variants, depending on the interface presented to the external telephonic equipment. Three variants (FXO, E&M and AC15) are for connection to the analogue telephone exchange, a fourth (FXS) is for the direct connection of telephones and fax machines and the last two (BRI and PRI) are for connecting to the digital telephone exchange.

In its simplest form a pair of units are connected to each other via a leased line, Frame Relay Network, ISDN dial up connection or via Ethernet and a third party router with the VIPER acting as a Voice Gateway. One common example of a simple network is with a FXS unit at a remote site with an FXO or E&M unit at the central site. The diagram below shows this configuration, and shows how the data networks at the two sites are also connected by the same pair of units.



There are two additional configuration screens relating to analogue connections.

The first allows the behaviour of the new ports to be controlled. This is slightly different for each of the different variants of the board.

The second is a directory for mapping phone numbers onto individual ports on specific units. This list is the same for all variants. In addition to this additional lines of information are available on the Status screen for you to monitor the status of the additional features.

9.1.1 Status Screen

The example status screen below shows that the unit is running the VIPER code indicated by the V in the code version number. The type of viper board and the status of the individual ports is shown in the 3 VIPER status lines lower down.

The Software Version number indicates the code version being run on the Voice Compression Co-processor. This is held in a separate Flash chip from the main code and can be remotely upgraded.

The individual port status lines indicate whether ports are On or Off hook. On the FXO, E&M and AC15 boards they also indicate whether Ring has been detected. When a voice call is connected these lines indicate the data throughput of the specific link. The two digital boards (BRI and PRI) show the status of the ports.

CODEVERSION	V4.20 24 Sep 2004
OPTIONS	F-Relay
UPTIME	8m8s
RAMUSED	6%
IOCARD	card: Dual X.21
CPU USAGE	1.0%
VIPER-PVM4-137	FXO/FXS-4 (48104) Software Version 130
VIPER-PVM4-FXS 1	(0) On Hook
VIPER-PVM4-FXS 2	(0) On Hook
+ NEXT PAGE	
. QUIT	Previous menu

COMMAND: STATUS	

9.2 Configuring the Ports

The following VIPER menu accessible from the HARDWARE menu allows the functionality of the individual ports to be controlled. Each port can be configured for a different option and selecting one of the options in this menu will present you with a sub-menu to set the available options. The example below is for the analogue voice cards.

London VIPER PORT CONFIGURATION		
Command	Description	Current Value
0 VPORT1	Port 1 VIPER Options	
1 VPORT2	Port 2 VIPER Options	
2 VPORT3	Port 3 VIPER Options	
3 VPORT4	Port 4 VIPER Options	
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER		

9.2.1 Configuring the Ports – Analogue Cards

London VIPER PORT 1 CONFIGURATION		
Command	Description	Current Value
0 PORTTYPE	Port Functionality	RXONLY
1 PORTNO	Port Destination	
2 PORTOPTS	Port Options	
3 VOCODER	Port Encoding Scheme	G729A
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER VPORT1		

This menu allows you to set the options for the specified port.

PORTTYPE

The selects a sub-menu that allows you to set the functionality of the port. Each available port of the Option card can be set to a different functionality.

PORTNO

This is the entry for the number internally in the VIPER network that this port dials. This is only required for certain PORTTYPEs, i.e. DIRECT.

PORTOPTS

The selects a sub-menu that allows you to set the options of the selected port.

VOCODER

The selects a sub-menu that allows you to set encoding option for the port. It is possible for different ports on the same Option card to be set to different encoding options. The available options are G729A, G711 and G726 @ 32kbps.

9.2.2 PORTTYPE Menu – FXS Option card

PORTTYPE field for the FXS option card can be set to one of the following

London VIPER PORT TYPE		
Command	Description	Current Value
0 RXONLY	Receive Calls Only	<<<<<<
1 DIRECT	Permanently Mapped to Supplied Number	
2 DIALOUT	Dial Out	
. QUIT	Previous menu	

COMMAND:	HARDWARE VIPER VPORT1 PORTTYPE	

RXONLY - Receive Calls Only

This option specifies that calls can only be made out of this unit to the Phone/Fax plugged into this port. This means that if a call is placed to this port the phone will ring and the user can answer it normally. If the phone is picked up, the user will not get dial tone. Instead a constant number unobtainable type tone will be heard.

DIRECT - Permanently Mapped to Supplied Number

This option allows the port to receive calls as specified above. When the receiver is lifted to make an outgoing call, the user does not have to dial. Instead the number specified in the associated PORTNO field is automatically called.

The number is looked up in the Yellow Pages so an entry for the associated phone number must be present in the YPAGES list. Provided a valid destination IP Address and Port can be located, an attempt is made to connect to the indicated port. If the attempt is successful and the remote port is on an FXS, the remote phone will start ringing, and you will hear the ring tone. If instead the remote unit is an FXO or E&M unit the remote port will go off hook and you will hear dial-tone from the remote exchange.

This option is used when you wish to use VIPER to extend one or two lines from your exchange to a remote location. Using this configuration when one of the remote phone is picked up, apart from a slight delay the operation will be as if the user was in the office.

DIALOUT - Dial Out - Esc to Outside Line

This option is the most flexible allowing the user to control, the type of connection and where he is to connect to by dialling different numbers.

When the receiver is raised, the user will hear dial-tone. If he then dials the escape sequence as specified in the associated PORTNO field, he will be connected to a free ISDN channel, as if he was using the OUTSIDE option described above. Once a B Channel has been allocated he will then hear dial-tone again, indicating that he can dial his external number.

If instead of dialling the escape sequence, any number that is recognised from the YPAGES list is dialled the user will be connected to that port. If the attempt is successful and the remote port is on an FXS, the remote phone will start ringing, and he will hear the ring tone. If instead the remote unit is an FXO or E&M unit the remote port will go off hook and he will hear dial-tone from the remote exchange.

If you have a number of VIPERs connected to the same network you can use this option to connect to any other port on what in this case becomes a distributed telephone exchange.

9.2.3 PORTTYPE Menu – FXO Option card

The following options are available for the PORTTYPE field.

London VIPER PORT TYPE		
Command	Description	Current Value
0 RXONLY	Dial into Exchange Only	
1 DIRECT	Connect Call to Supplied Number	<<<<<<
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER VPORT1 PORTTYPE		

RXONLY - Dial into Exchange Only

This option specifies that calls can only be made out of this unit into the PABX. This means that if this PABX rings the extension, which is connected to this port, the VIPER will not answer. When this option is set the associated PORTNO field is ignored.

DIRECT - Connect Call to Supplied Number

This option indicates that when an incoming call is received on this port (somebody rings the extension onto which this port is connected). The VIPER will attempt to connect to the number specified in the associated PORTNO field.

The number is looked up in the Yellow Pages so an entry for the associated phone number must be present in the YPAGES list. Provided a valid destination IP Address and Port can be located, an attempt is made to connect to the indicated port. If the attempt is successful the phone connected to the remote port will ring. When the remote phone is picked up the local port will go Off Hook and the call will be connected.

Note that the local phone does not go Off Hook until the remote phone is answered, this ensures that hunt groups, voice mail and other redirection facilities present on the PABX still continue to function as normal.

9.2.4 PORTTYPE Menu – E&M and AC15

The following options are available for the PORTTYPE field.

NOTE: On the initial versions of the E&M and AC15 units Port 1 is labelled on the back of the unit as Phone 3 and Port 2 is labelled Phone 4.

London VIPER PORT TYPE		
Command	Description	Current Value
0 RXONLY	Dial into Exchange Only	
1 DIRECT	Connect Call to Supplied Number	<<<<<<
2 ANSWER	Answer Call and wait for dial	
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER PORT1TYPE		

RXONLY - Dial into Exchange Only

This option specifies that calls can only be made out of this unit into the connected E&M/AC15 PABX. This means that if the PABX attempts to open a connection to this port, the VIPER unit will not answer. When this option is set the associated PORTNO field is ignored.

DIRECT - Connect Call to Supplied Number

This option indicates that when an incoming call is received on this port. The VIPER will attempt to connect to the number specified in the associated PORTNO field.

The number is looked up in the Yellow Pages so an entry for the associated phone number must be present in the YPAGES list. Provided a valid destination IP Address and Port can be located, an attempt is made to connect to the indicated port. If the attempt is successful the phone connected to the remote port will ring, and a ring tone will be sent out from the port. When the remote phone is picked up the M wire will be connected to Earth to indicate that the call has been answered.

ANSWER - Answer Call and wait for dial

This option indicates that when an incoming call is received on this port. The VIPER will output dial tone and expect to see further dial digits presented to indicate which port to connect to.

Any number that is recognised from the YPAGES list is dialled and the user will be connected to that port. If the attempt is successful and the remote port is on an FXS, the remote phone will start ringing, and he will hear the ring tone. If instead the remote unit is an FXO or E&M unit the remote port will go off hook and he will hear dial-tone from the remote exchange.

As soon as the remote port is connected. Either an FXS phone is answered or an FXO port goes off hook the M wire will be Earthed to indicate that the call is complete.

If you have a number of VIPERs connected to the same network you can use this option to connect to any other port on what in this case becomes a distributed telephone exchange.

9.2.5 PORTOPTS Menu – FXS Option card

London HARDWARE VIPER OPTS		
Command	Description	Current Value
0 EARTHLOOP	(L) Earth Loop at end of call	NO
1 PFE	(F) Disable post filter	NO
2 HPFE	(H) Disable high pass filter	NO
3 SCE	(S) Disable silence suppression	NO
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER VPORT1 PORTOPTS		

EARTHLOOP – (L) Earth loop at end of call

This field enables the extension format “earthloop”, also known as earth calling or earth disconnect.

Used on medium to large customer telephone systems (PABX's). This type of line is supposed to stop call collision, which can be described as an incoming call that has been answered by an outgoing call (both outgoing and incoming seized the line at the same time). Earth calling lines were designed to guard against this. The customer telephone system puts an earth on the RING wire when making outgoing calls and this causes the exchange to seize. The exchange then looks for a loop that the telephone system extends once the earth condition has been taken off. The customer system must be connected to a good earth.

When this option's current value is set to NO the port will be set to “loop calling”. The line is seized by a loop condition, put on by the telephone. This is normally used on residential and small key systems, you pick up the phone and the line is seized.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and “loop calling”.

PFE – (F) Disable post filter

This field enables or disables the post filter. The post filter is applied in the decoding section of the port, i.e. this applies to the voice coming out of the VIPER to the telephone.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

HPFE – (H) Disable high pass filter

This field enables or disables the high pass filter. The high pass filter is applied in the encoding section of the port, i.e. this applies to the voice coming out of the telephone to the VIPER. When enabled this filter filters out the low end frequencies lower than the average human ear can hear.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

SCE – (S) Disable silence compression

This field enables or disables silence compression.

Silence compression means that the VIPER compresses the voice call so that it uses less bandwidth when the call is silent, even in brief periods of time.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with silence compression enabled.

9.2.6 PORTOPTS Menu – FXO Option card

London HARDWARE VIPER OPTS		
Command	Description	Current Value
0 PULSE	(P) Pulse dial out on this port	NO
1 PROGTONE	(T) Call Progress Tone Ends Call	NO
2 EARTHLOOP	(L) EarthLoop Detect Ends Call	NO
3 DIGITA	(A) Digit A Detect Ends Call	NO
4 DIGITB	(B) Digit B Detect Ends Call	NO
5 DIGITC	(C) Digit C Detect Ends Call	NO
6 DIGITD	(D) Digit D Detect Ends Call	NO
7 PFE	(F) Disable post filter	NO
8 HPFE	(H) Disable high pass filter	NO
9 SCE	(S) Disable silence suppression	NO
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER VPORT1 PORTOPTS

PULSE – (P) Pulse dial out on this port

This field enables or disables Pulse dialling facility on this port.

Pulse dialling is used with older PABX systems and is when the PABX detects the rapid connect/disconnect and interprets this as a number.

Newer PABX systems can use tone dialling which is where specific frequencies are interpreted as numbers.

This option leads to a sub-menu that allows you to set the current value to YES or NO and is provided for backward compatibility. The default option is NO so that only tone dialling is allowed on the port.

PROGTONE – (T) Call Progress Tone Ends Call

This field enables or disables the facility for the VIPER to drop a call if it detects any tone that is assigned to the Call Progress signals. Call Progress tones provide information regarding the status or progress of a call to customers, operators, and connected equipment. In circuit-associated signalling, these audible tones are transmitted over the voice path within the frequency limits of the voice band. The two most common Call Progress tones are the dial tone and busy tone. If enabled then if the VIPER detects one of these tones it will immediately drop the call.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO so that dial and busy tones can be passed over the call without dropping the call.

EARTHLOOP – (L) EarthLoop Detect Ends Call

This field enables the facility for the VIPER to stop calls if it detects earthloop on the line.

This option can be used if the connected PABX system is incompatible with earth calling or earth disconnect dialling.

DIGITA – (A) Digit A Detect Ends Call

This field enables the facility for the VIPER to drop calls if it detects DTMF Digit A.

DIGITB – (B) Digit B Detect Ends Call

This field enables the facility for the VIPER to drop calls if it detects DTMF Digit B.

DIGITC – (C) Digit C Detect Ends Call

This field enables the facility for the VIPER to drop calls if it detects DTMF Digit C.

DIGITD – (D) Digit D Detect Ends Call

This field enables the facility for the VIPER to drop calls if it detects DTMF Digit D.

The above extra Digits are rarely used except for network control and some carriers even prohibit their use, in which case the above options would need to be set to YES.

PFE – (F) Disable post filter

This field enables or disables the post filter. The post filter is applied in the decoding section of the port, i.e. this applies to the voice coming out of the VIPER to the telephone.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

HPFE – (H) Disable high pass filter

This field enables or disables the high pass filter. The high pass filter is applied in the encoding section of the port, i.e. this applies to the voice coming out of the telephone to the VIPER. When enabled this filter filters out the low end frequencies lower than the average human ear can hear.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

SCE – (S) Disable silence compression

This field enables or disables silence compression.

Silence compression means that the VIPER compresses the voice call so that it uses less bandwidth when the call is silent, even in brief periods of time.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with silence compression enabled.

9.2.7 PORTOPTS Menu – E&M and AC15 Option cards

London HARDWARE VIPER OPTS		
Command	Description	Current Value
0 PULSE	(P) Pulse dial out on this port	NO
1 2WIRE	(2) Use 2 Wire Interface not 4	NO
2 DELAYDIAL	(Y) Delayed Dialing Procedures	NO
3 PFE	(F) Disable post filter	NO
4 HPFE	(H) Disable high pass filter	NO
5 SCE	(S) Disable silence suppression	NO
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER VPORT1 PORTOPTS

PULSE – (P) Pulse dial out on this port

This field enables or disables Pulse dialling facility on this port.

Pulse dialling is used with older PABX systems and is when the PABX detects the rapid connect/disconnect and interprets this as a number.

Newer PABX systems can use tone dialling which is where specific frequencies are interpreted as numbers.

This option leads to a sub-menu that allows you to set the current value to YES or NO and is provided for backward compatibility. The default option is NO so that only tone dialling is allowed on the port.

2WIRE - (2) Use 2 Wire Interface not 4

This option sets the port to use 2 Wire E&M instead of the standard 4 Wire. In 4- Wire mode there are separate pair of wires for transmit and receive, with 2 Wire the same pair are used for transmit and receive.

DELAYDIAL -(Y) Delayed Dialing Procedures

This option sets the port to delay dialling signalling. This is a process that was created by the industry as an alternative to the standard dialling signalling. If there are problems with calls being dropped or failing to be connected then using this option in the VIPER and the PABX connected to it may help.

PFE – (F) Disable post filter

This field enables or disables the post filter. The post filter is applied in the decoding section of the port, i.e. this applies to the voice coming out of the VIPER to the telephone.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

HPFE – (H) Disable high pass filter

This field enables or disables the high pass filter. The high pass filter is applied in the encoding section of the port, i.e. this applies to the voice coming out of the telephone to the VIPER. When enabled this filter filters out the low-end frequencies lower than the average human ear can hear.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

SCE – (S) Disable silence compression

This field enables or disables silence compression.

Silence compression means that the VIPER compresses the voice call so that it uses less bandwidth when the call is silent, even in brief periods of time.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with silence compression enabled.

9.3 Configuring the Ports – Digital Cards

The two digital cards (BRI and PRI) are configured in a different way to the analogue cards. The Yellow Page entries are configured in exactly the same way.

9.3.1 VIPER HARDWARE Menu – BRI and PRI Option cards

On VIPERs with digital voice option cards fitted the VIPER menu that is accessible from the HARDWARE menu allows the functionality of the whole interface.

London VIPER PORT CONFIGURATION		
Command	Description	Current Value
0 PORTNO	Port Destination	
1 PORTOPTS	Port Options	
2 VOCODER	Port Encoding Scheme	G729A
3 DIGITSREQ	Digits required to make ISDN call	0
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER		

The available options are:

PORTNO - Port Destination

This is the entry for the number internally in the VIPER network that this port dials.

PORTOPTS – Port Options

The selects a sub-menu that allows you to set the options of the BRI option card.

This is for the whole card and not for a single port.

VOCODER – port encoding screen

The selects a sub-menu that allows you to set encoding option for the port.

This selection is for the whole card. The available options are G729A, G711 and G726 @ 32kbps.

DIGITSREQ - Digits required to make ISDN call

This selects how many digits need to be entered before the VIPER initiates an ISDN call.

9.3.2 PORTOPTS Menu – BRI and PRI Option cards

London HARDWARE VIPER OPTS		
Command	Description	Current Value
0 ISDNCLK	(G) Generate ISDN Clock	NO
1 L2MASTER	(N) ISDN Layer 2 Master (NT mode)	NO
2 ULAW	(U) Use u-law for ISDN, not A-law	NO
3 PFE	(F) Disable post filter	NO
4 HPFE	(H) Disable high pass filter	NO
5 SCE	(S) Disable silence suppression	NO
. QUIT	Previous menu	

COMMAND: HARDWARE VIPER PORTOPTS

ISDNCLK – Generate ISDN Clock

This option allows the digital voice option card to generate a clock internally and send it out on the digital port(s). This can be used as a clock master for those installations with PABX systems that requires an external clock source for a port. It can also be used for test purposes.

L2MASTER – ISDN Layer 2 Master (NT Mode)

This option is used to set the voice option port as a master Network Terminal port. This option is often used combined with the ISDNCLK option so that the voice option part can be connected directly to another similar port, e.g. BRI to another BRI.

If this options is set to NO then the voice option port is used in TE mode, i.e. Terminal Emulation.

ULAW - Use u-law for ISDN, not A-law

This option allows the voice option card to use **u-law** on the port. **U-law** is the algorithm that is the standard used in North American and Japan. If this is set to NO then **a-law** is used and that is the European standard.

PFE – (F) Disable post filter

This field enables or disables the post filter. The post filter is applied in the decoding section of the port, i.e. this applies to the voice coming out of the VIPER to the telephone.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

HPFE – (H) Disable high pass filter

This field enables or disables the high pass filter. The high pass filter is applied in the encoding section of the port, i.e. this applies to the voice coming out of the telephone to the VIPER. When enabled this filter filters out the low end frequencies lower than the average human ear can hear.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with the filter enabled.

SCE – (S) Disable silence compression

This field enables or disables silence compression.

Silence compression means that the VIPER compresses the voice call so that it uses less bandwidth when the call is silent, even in brief periods of time.

This option leads to a sub-menu that allows you to set the current value to YES or NO. The default option is NO and with silence compression enabled.

9.4 Configuring the Phone Book

The following YPAGES menu accessed from the HARDWARE menu allows a list of mappings between phone numbers, and IP Address and port numbers to be made.

London YELLOW PAGES					
Index	Phone No.	IP Address	Port Number		
0 Y0	20	172.16.1.102	0		
1 Y1	32	203.1.1.1	2		
2 Y2	31	203.1.1.1	1		
3 Y3	12	172.16.1.101	2		
4 Y4	11	172.16.1.101	1		
5 Y5	22	172.16.1.102	2		
6 Y6	21	172.16.1.102	1		
& ADD	Add new item	% DELETE	Delete item	. QUIT	Previous menu

COMMAND: HARDWARE YPAGES					

The following screen allows the individual fields of each entry to be configured.

London VIPER YELLOW PAGES		
Command	Description	Current Value
0 DNUMBER	Number to Dial	31
1 DESTIP	IP Address of Destination	203.1.1.1
2 DESTCHAN	Port to Call on Destination Unit	1
. QUIT	Previous menu	

COMMAND: HARDWARE YPAGES Y2		

The number to dial, as its name suggests is the phone number that will be recognised. The associated DESTIP and DESTCHAN values will then be used to contact another VIPER unit. The DESTIP field is the IP address of the destination VIPER. The DESTCHAN field relates to the VIPER port number on the destination unit. A port number of 0 'zero' may be used in which case the connection will be made to any free port on the destination VIPER. If the destination unit is an FXS all free ports will ring.

9.5 Configuring IP Prioritisation

In order for Voice and Data to share the same data pathway, it is necessary to ensure that the Voice IP frames get priority over data frames, so that the perceived voice quality is maintained.

This is achieved by using the IP Prioritisation mechanism already present in VIPER routers. You should read Section 7.6 (VIPER IP Express) for more details on how this mechanism works and is configured. A brief description of the values you should use when working with VIPER is included here.

The following menu display shows the recommended settings for operating 2 voice channels over a 64k WAN link (Leased Line or ISDN). These settings should be set into the NETWORK <name> IP PIPE menu, at each end of the link.

London		
Command	Description	Current Value
0 RESBAN	Reserved bandwidth (bytes/sec)	2400
1 FRAGSIZE	Fragment size	256
2 PRIOR	IP Prioritisation	3 entries
. QUIT	Previous menu	

The next display shows the list of entries accessed through the PRIOR option on the above screen. By letting the IP Address be zero, and hence a wildcard, this configuration will work for any VIPER. VIPER uses the three port numbers shown for its operation.

London PRI		
Code	IP Address	Port number
0 P0	0.0.0.0	57000
1 P1	0.0.0.0	57001
2 P2	0.0.0.0	57002
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

COMMAND: NETWORK Birmingham IP PIPE PRIOR		

If you are planning to route the voice traffic across Ethernet the same values should be used on the Ethernet port, i.e. the Router through which the VIPER is connected to the remote end will need the same three ports numbers given priority, i.e. port numbers 57000-57002

9.6 Frame Relay

Frame Relay can be enabled as an option on the VIPER. Once enabled a number of additional menu entries and some new screens are presented to allow this feature to be controlled.

9.6.1 Hardware Configuration

Firstly the Leased Line ports themselves need to be configured for Frame Relay Operation. This is done by entering the specific HARDWARE Menu for the Leased line and setting the IFTYPE to the required value. The following shows the values that can be selected on a channel that is not capable of generating clock, and hence can only act as a DTE.

VIPER WAN LINK TYPE		
Command	Description	Current Value
0 LEASED	Standard Leased Line	<<<<<<
1 FRAMEREL	Frame Relay Connection - No Management	
2 FRQ933	Frame Relay with Q933 Management	
3 FRDQ933	Frame Relay with Dummy Q933 Management	
. QUIT	Previous menu	

On links that can generate clock additional options are available.

VIPER WAN LINK TYPE		
Command	Description	Current Value
0 LEASED	Standard Leased Line	
1 FRAMEREL	Frame Relay Connection - No Management	
2 FRQ933	Frame Relay with Q933 Management	
3 FRDQ933	Frame Relay with Dummy Q933 Management	
4 HDLC	Standard HDLC Frames	
5 FRSERVICE	Simple Frame Relay Service	<<<<<<
. QUIT	Previous menu	

LEASED

This default option selects Leased Line operation, without Frame Relay. On units without the Frame Relay option installed this is the only option.

FRAMEREL

This option selects Frame Relay operation without any management protocol. In effect a Frame Relay Header is appended to all frames, and the frame is then sent. Frame Relay flow control mechanisms do operate.

FRQ933

This option selects the operation of the Local Management Interface (LMI) as specified in Q.933 Annex A, using DLCI zero.

FRQD933

This option selects the operation of the Local Management Interface (LMI) as specified in Q.933 Annex A, using DLCI zero, with the exception that if bad responses are being received from the Network frames are still transmitted.

HDLC

This option, available only on ports that can generate clock, provides a mechanism for transporting HDLC frames from 'legacy synchronous data' devices over a Frame Relay connection.

FRSERVICE

The option allows the possibility of onward routing Frame Relay frames, and is mainly for test and specialist applications only.

9.6.2 Link Configuration

Having set the hardware to one of the standard Frames Relay options (FRAMEREL, FRQ933 or FRQD933), you can now select that a selected Destination can be reached over this link. This is done in the NETWORK CHANNELS menu for the destination in question.

London		
Command	Description	Current Value
0 ETHERNET	Ethernet	NO
1 ETHERNET2	Secondary Ethernet	NO
2 X21L1	Leased Line channel 1	NO
3 X21L2	Leased Line channel 2	NO
4 FRL1	Frame Relay Address 1	7
5 FRCIR1	Frame Relay CIR 1	32000
6 FRL2	Frame Relay Address 2	0
7 FRCIR2	Frame Relay CIR 2	0
. QUIT	Previous menu	

 COMMAND: NETWORK Birmingham CHANNELS

To select to access this Destination over Frame Relay you set the Frame Relay Address of the link you wish to use to a non-zero value. This value will be the DLCI that identifies this link and you need to set this to the value provided by your Frame Relay service provider.

At the same time you need to set the Committed Information Rate that this channel has been allocated. Again this information depends on the service you have obtained from your service

provider. In the example above it has been set to 32000 bits per second. It is this value that is used as the basis for the throttling performed on this link.

This is all that is necessary for configuring a basic Frame Relay connection.

9.6.3 HDLC Transport

Having established a basic Frame Relay connection between two routers you can then transport 'legacy synchronous' HDLC frames across the same link using a different DLCI.

The second port of each router (the port that can generate clock) has been set to HDLC at each end. The first port has been set to FRQ933, and the LAN link from one to the other has been configured using a first DLCI at each end.

Now the additional FRELAY menu accessed from the HARDWARE menu is used to connect port 2 on each unit to a second DLCI on port 1.

HDLC_PASS FRELAY					
Index	Address	Port1	Port2	CIR	
0	I0	21	Link1	Link2	32000
&	ADD	Add new item			
%	DELETE	Delete item			
.	QUIT	Previous menu			
COMMAND: HARDWARE FRELAY					

The individual entries in this list are modified using the following menu.

HDLC_PASS FRAME RELAY INTERCONNECT			
Command	Description	Current Value	
0	FRADDRESS	Address of Frame Relay Channel	21
1	PORT1	First Port to Connect	Link1
2	PORT2	Second Port to Connect	Link2
3	BITRATE	Committed Information Rate of Channel	32000
.	QUIT	Previous menu	
COMMAND: HARDWARE FRELAY I0			

FRADDRESS

This field specifies the DLCI that will be used for this interconnection.

PORTn

These two fields indicate the two ports that are logically connected together through the Router. When this value is selected a further menu is presented listing the all the possible hardware links that you could have fitted. Please avoid selecting links that have not been configured for Frame Relay or that doesn't exist.

BITRATE

This is the Committed Information Rate that will be used for throttling purposes over the Frame Relay interface to the network.

This same menu is used when ports are set to FRSERVICE. In this case you can set up logical connections between the ports set to FRSERVICE.

The use of the HDLC pass-through or the Frame Relay Service (FRSERVICE) is not compatible with the IP Prioritisation features present on the Routers, and so should not be used when trying to transport Voice, unless the size and quantity of the HDLC frames can be controlled externally.

9.7 Multidrop E1 Trunk VLINE

9.7.1 Multipdrop E1 Trunk Description

The Viper can also be supplied to run an E1 G703 / 704 Trunk, using VLINE software. This VLINE E1 Trunk version comprises of a new Motherboard and new software. It is not possible to modify existing VLINE or Viper units into this version. The E1 trunk replaces the ISDN port on the chassis; this means that this version is incapable of ISDN backup.

This version is compatible with the digital Voice Option cards (BRI and PRI) and with analogue E&M Voice Option cards but with the voice channel permanently on so that the E&M voice ports can be used as wires only, for applications such as Radio over IP or broadcasting.

The modified version of software is not compatible with the non-E1 Trunk builds of VLINE or Viper. The software is very similar to the ordinary versions, so this section will only deal with the differences and also give some configuration examples.

The Main Menu is the same as ordinary Viper or VLINE units.

The STATUS screen shows the E1 Trunk version of software:

```

London STATUS
-----
CODEVERSION      VL4.30-selex  19 Jun 17:27
UPTIME           5m35s
RAMUSED          23%
IOCARD           card: None
CPU USAGE        0.0%
FALC-PRI         State: 3-signal-frame-multiframe

. QUIT          Previous menu
-----
The HARDWARE screen shows a new option:

```

```

London

Command          Description          Current Value
-----
0 MSPEED         Management port speed      19200
1 ETHERNET       Configure Ethernet
2 VLINE          Configure VLINE Options
3 X21L1          Leased Line channel 1
4 X21L2          Leased Line channel 2
5 PRI            ISDN primary rate          PRI (Slave)

. QUIT          Previous menu
-----

```

The PRI option allows you to set what type of E1/PRI option you want to use.

London Configure PRI		
Command	Description	Current Value
0 TYPE	Set type of interface	PRI
1 ISDNCLK	Generate ISDN Clock	NO
. QUIT	Previous menu	

Selecting the 'TYPE' option allows selection of the E1/PRI type:

London Configure PRI type		
Command	Description	Current Value
0 PRI	Primary Rate Interface	PRI
1 KAI	Kilostream Aggregate Interface	
2 KAINOCRC	Kilostream Aggregate No CRC-4	
3 RAW	Unframed 2Mbit Interface	
. QUIT	Previous menu	

The four available options are:

- PRI** – This sets the E1 port so that it is a standard PRI/E1 interface and uses the timeslots in a manner that is compatible with other PRI/E1 interfaces. This option can then be treated just like the ISDN port on a standard unit and can be configured in exactly the same way including as backup to an X.21 port.
- KAI** – Kilostream Aggregate Interface. This option can be used for point-to-multipoint installations where there is a single central point and a number of satellite points in a PDH or similar network. This option can also be used when it is necessary to convert the E1 port to a standard X21 port (using a suitable Converter.) This option has CRC4 enabled.
- KAINOCRC** – This is the same as **KAI** but it has the CRC4 option disabled.
- RAW** – This option sends the data down the E1 trunk in an unframed structure using all 32 timeslots.

Please note that after selecting the required configuration you will need to reboot the unit to action the change, otherwise it won't be possible to continue the E1 configuration.

The ISDNCLK option allows you to set the E1 port to Master or Slave. The default setting and the one most used is Slave. With Master you still have to set the required clock speed under the HARDWARE / X21L2 menu.

9.7.2 KAI and KAINOCRC additional menu screens

In the NETWORKS menu select the option for the E1 network connection, or create it and configure the basics like name of the link and IP addresses.

London NETWORKS		
Command	Description	Current Value
0 NAME	Name	Birmingham
1 IP	IP configuration	
2 PPP	PPP configuration	
3 IPX	IPX configuration	
4 ISDN	ISDN configuration	
5 CHANNELS	Select channels to use	
. QUIT	Previous menu	

The CHANNELS option will show a different screen:

London		
Command	Description	Current Value
0 ETHERNET	Ethernet	NO
1 ETHERNET2	Secondary Ethernet	NO
2 X21L1	Leased Line channel 1	NO
3 X21L2	Leased Line channel 2	NO
4 START	KAI start channel	1
5 END	KAI end channel	2
. QUIT	Previous menu	

The two additional options are START and END and these are the selected start and end timeslots for the KAI channel. As stated previously it is possible to have multiple separate KAI entries using different timeslots that are routed by the PDH network to the required destination.

The START entry needs to be anything other than 0 to be enabled and the END entry needs to be equal or greater than the START entry. Neither entry can be 0 or 16.

Please note that the unit needs to be rebooted to action any changes to this option. If we create multiple KAI entries then the HARDWARE menu will look like:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Leased Circuit: KAI-1 1..2	20.1.1.0
1 Liverpool	Leased Circuit: KAI-1 5..6	40.1.1.0
2 Manchester	Leased Circuit: KAI-1 3..4	30.1.1.0
3 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

This shows the local Ethernet IP address range along with the IP address range and the KAI timeslots used for the three remote units.

9.7.3 RAW additional menu screens

In the NETWORKS menu select the option for the E1 network connection, or create it and configure the basics like name of the link and IP addresses.

The CHANNELS screen will show a different option:

London NETWORKS		
Command	Description	Current Value
0 NAME	Name	Birmingham
1 IP	IP configuration	
2 PPP	PPP configuration	
3 IPX	IPX configuration	
4 ISDN	ISDN configuration	
5 CHANNELS	Select channels to use	
. QUIT	Previous menu	

The additional option enables or disables unstructured E1 data on this network. After setting this option as required it is recommended that the unit is rebooted to action the configuration change.

London		
Command	Description	Current Value
0 ETHERNET	Ethernet	NO
1 ETHERNET2	Secondary Ethernet	NO
2 X21L1	Leased Line channel 1	NO
3 X21L2	Leased Line channel 2	NO
4 RAW	Unstructured E1	YES
. QUIT	Previous menu	

After configuration the NETWORKS screen will look like:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Leased Circuit: Unframed E1	20.1.1.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

9.7.4 Configuration examples

The PRI option for the E1 VLINE unit is configured in exactly the same way as a standard ISDN connection. See Sections 5.1.4 and 6.6 for more information.

The RAW option is configured in the same way as a standard X.21 WAN port except that the CHANNEL is set to RAW. See Section 5.1.2 for more information.

The KAI and KAINOCRC options are configured differently to the other options and so this manual will go into greater detail with the configuration. Both of these options are configured in exactly the same way, all that is different between them is whether CRC4 is enabled or disabled.

9.7.5 KAI/KAINOCRC Configuration example

To set up basic routing on a VLINE you will need the following information:

- i. Name of the local VLINE – this can be anything, for example the location.
- ii. IP address of the Ethernet port of the VLINE including the Mask.
- iii. IP address of the remote units, e.g. the remote VLINE's IP addresses including the Masks
- iv. The name of the remotes. – E.g. its location.
- v. The timeslots that are used for each separate remote site. The PDH network will then route these separate timeslots to their required destination.

For the following example we will use the local name London, IP address of the Ethernet port 10.1.1.1 and mask 255.255.255.0

The first remote will have an IP of 20.1.1.1 and mask 255.255.255.0 and is called Birmingham. The second remote will have an IP of 30.1.1.1 and mask of 255.255.255.0 and is called Manchester. Both Birmingham and Manchester will put data into timeslots 1 and 2 locally and at London timeslots 1 and 2 are used for data destined for Birmingham and timeslots 3 and 4 for Manchester. The connected PDH network is capable to cross-connecting the timeslots as needed for the installation.

The first step is to give the unit a name.

KAI E1 Step 1. From the Main Menu select option 0 GLOBAL and then option 0 NAME. Enter the name London followed by RETURN.

KAI E1 Step 2. Quit out of that menu by pressing a full stop (.) once to get back to the Main Menu which now shows London Main Menu at the top of the screen.

KAI E1 Step 3. The next step is to set the unit up in the required KAI mode, from the Main Menu select option 2 HARDWARE

KAI E1 Step 4. Select option 5 PRI and then option 0 TYPE to get the following screen:

London Configure PRI type		
Command	Description	Current Value
0 PRI	Primary Rate Interface	
1 KAI	Kilostream Aggregate Interface	KAI
2 KAINOCRC	Kilostream Aggregate No CRC-4	
3 RAW	Unframed 2Mbit Interface	
. QUIT	Previous menu	

KAI E1 Step 5. Select the required KIA option, either KAI or KAINOCRC as required by the network provider.

- KAI E1 Step 6.** Quit out of that menu and quit all the way to the Main Menu.
- KAI E1 Step 7.** Then reboot the unit to activate the KAI option by selecting option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.
- KAI E1 Step 8.** After about 10 seconds the Main Menu will then reappear.
- KAI E1 Step 9.** The next step is to configure the Ethernet port with the IP address and Mask.
- KAI E1 Step 10.** From the Main Menu select option 1 'NETWORK' to get to the following screen:

London NETWORKS		
Command	Description	Current Value
0	DEFAULT_ETH	Ethernet Interface
1	DEFAULT_WAN	Configuration In Only
&	ADD	Add new item
%	DELETE	Delete item
.	QUIT	Previous menu

- KAI E1 Step 11.** Next select option 0 DEFAULT_ETH to get the following screen:

London NETWORKS		
Command	Description	Current Value
0	NAME	Name
1	IP	IP configuration
2	PPP	PPP configuration
3	IPX	IPX configuration
4	ISDN	ISDN configuration
5	CHANNELS	Select channels to use
.	QUIT	Previous menu

- KAI E1 Step 12.** Then select option 1 IP to get the following screen:

London		
Command	Description	Current Value
0	ENABLE	IP routing
1	LOCAL	Local IP address
2	REMOTE	Remote IP address (if not Ethernet)
3	MASK	IP address mask
4	RIP	RIP
5	RIPMETRIC	RIP Metric weighting for link
6	ROUTES	Associated static routes
7	TRANSLATE	Address translation rules
8	PIPE	P Express
9	FILTBOARD	Filter Directed Broadcast
.	QUIT	Previous menu

- KAI E1 Step 13.** Select option 1 LOCAL and type in the IP address 10.1.1.1 followed by RETURN

- KAI E1 Step 14.** Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN. Please note that this can also be entered in its **CIDR** format of /24
- KAI E1 Step 15.** Quit out of the menu.

The next step on this part of the configuration is optional, it's recommended to do this so that it's clear which entries have been configured.

- KAI E1 Step 16.** From the London NETWORKS menu select option 0 NAME
- KAI E1 Step 17.** Type in 'eth' followed by RETURN. **NB** This is only a suggested name.
- KAI E1 Step 18.** Quit out of the London NETWORKS menu to get the following screen:

London NETWORKS		
Command	Description	Current Value
0 DEFAULT_WAN	Configuration In Only	0.0.0.0
1 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

The next step on this configuration is to configure the first KAI WAN port.

- KAI E1 Step 19.** Select option 0 DEFAULT_WAN
- KAI E1 Step 20.** Select option 1 IP to get the same menu as shown above for the Ethernet port.
- KAI E1 Step 21.** Select option 2 REMOTE and type in the Remote IP address 20.1.1.1 followed by RETURN.
- KAI E1 Step 22.** Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN (or again use the CIDR format) the menu will now look like:

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	0.0.0.0 /0
2 REMOTE	Remote IP address (if not Ethernet)	20.1.1.1
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	0 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

- KAI E1 Step 23.** Quit out of that menu.
- KAI E1 Step 24.** Select option 5 CHANNELS to get the following screen:

London			
Command	Description	Current Value	
0	ETHERNET	Ethernet	NO
1	ETHERNET2	Secondary Ethernet	NO
2	X21L1	Leased Line channel 1	NO
3	X21L2	Leased Line channel 2	NO
4	START	KAI start channel	0
5	END	KAI end channel	0
.	QUIT	Previous menu	

KAI E1 Step 25. Select option 4 START and type in the required starting timeslot for this KAI connection, in this example it is 1 followed by RETURN.

KAI E1 Step 26. Select option 5 END and type in the required end timeslot, in this case it is 2 followed by RETURN.

KAI E1 Step 27. Quit out of that menu.

KAI E1 Step 28. Select option 0 NAME and type in the required name for this KAI link, in this example it is Birmingham followed by RETURN.

KAI E1 Step 29. Quit out of that menu to get the following screen:

London NETWORKS			
Command	Description	Current Value	
0	Birmingham	Dial In Only	20.1.1.0
1	eth	Ethernet Interface	10.1.1.0
&	ADD	Add new item	
%	DELETE	Delete item	
.	QUIT	Previous menu	

Note that the Birmingham entry is described as being “Dial In Only” this is due to the fact that a reboot is required to activate the changes and until the unit has been rebooted it will show that message.

KAI E1 Step 30. Select option & ADD to add a blank new entry in the Network screen:

London NETWORKS			
Command	Description	Current Value	
0	UNCONFIGURED	!! Invalid !!	0.0.0.0
1	Birmingham	Dial In Only	20.1.1.0
2	eth	Ethernet Interface	10.1.1.0
&	ADD	Add new item	
%	DELETE	Delete item	
.	QUIT	Previous menu	
NOTE: please select the UNCONFIGURED network and configure it			

KAI E1 Step 31. Select option 0 UNCONFIGURED

- KAI E1 Step 32.** Select option 1 IP to get the same menu as shown above for the Ethernet port.
- KAI E1 Step 33.** Select option 2 REMOTE and type in the Remote IP address 30.1.1.1 followed by RETURN.
- KAI E1 Step 34.** Select option 3 MASK and type in the MASK 255.255.255.0 followed by RETURN (or again use the CIDR format) the menu will now look like:

London		
Command	Description	Current Value
0 ENABLE	IP routing	YES
1 LOCAL	Local IP address	0.0.0.0 /0
2 REMOTE	Remote IP address (if not Ethernet)	30.1.1.1
3 MASK	IP address mask	255.255.255.0 /24
4 RIP	RIP	A
5 RIPMETRIC	RIP Metric weighting for link	1
6 ROUTES	Associated static routes	0 routes
7 TRANSLATE	Address translation rules	0in+0out
8 PIPE	IP Express	disabled
9 FILTBROAD	Filter Directed Broadcast	NO
. QUIT	Previous menu	

- KAI E1 Step 35.** Quit out of that menu.
- KAI E1 Step 36.** Select option 5 CHANNELS to get the following screen:

London		
Command	Description	Current Value
0 ETHERNET	Ethernet	NO
1 ETHERNET2	Secondary Ethernet	NO
2 X21L1	Leased Line channel 1	NO
3 X21L2	Leased Line channel 2	NO
4 START	KAI start channel	0
5 END	KAI end channel	0
. QUIT	Previous menu	

- KAI E1 Step 37.** Select option 4 START and type in the required starting timeslot for this KAI connection, in this example it is 3 followed by RETURN.
- KAI E1 Step 38.** Select option 5 END and type in the required end timeslot, in this case it is 4 followed by RETURN.
- KAI E1 Step 39.** Quit out of that menu.
- KAI E1 Step 40.** Select option 0 NAME and type in the required name for this KAI link, in this example it is Manchester followed by RETURN.
- KAI E1 Step 41.** Quit out of that menu to get the following screen:

The unit now requires a reboot to activate the changes in configuration.

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Dial In Only	20.1.1.0
1 Manchester	Dial In Only	30.1.1.0
2 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

KAI E1 Step 42. Quit out of that menu to return to the Main Menu.

KAI E1 Step 43. Select option 7 DEBUG and then option 2 REBOOT and type y to confirm the reboot.

KAI E1 Step 44. After about 10 seconds the Main Menu will then reappear.

KAI E1 Step 45. Select option 1 NETWORKS and get the following screen:

London NETWORKS		
Command	Description	Current Value
0 Birmingham	Leased Circuit: KAI-1 1..1	20.1.1.0
1 Manchester	Leased Circuit: KAI-1 3..4	30.1.1.0
2 eth	Ethernet Interface	10.1.1.0
& ADD	Add new item	
% DELETE	Delete item	
. QUIT	Previous menu	

As can be seen now the unit recognises the two KAI networks.

Both remote sites are configured in a similar same way except they only need the single KAI link to the London unit and use the START entry of 1 and END entry of 2.

If a link is required from one remote site to the other then that is easily accomplished by setting up a static route on the KAI Network entry and that is discussed elsewhere in this manual.

The network that links up all of these sites will be able to cross-connect timeslots 3 and 4 coming out of the London unit onto timeslots 1 and 2 going into the Manchester unit.

Section 10 Upgrading and Diagnostics

10.1 Monitor Commands

These are a list of commands that can be used in the DEBUG MONITOR mode.

The majority of these commands are used for test purposed and it is not recommended that users use any of these commands. The use of these commands potentially could cause problems with the VIPER and/or the network attached to it to such an extent as to stop the VIPER from working.

? [command]

Display help [about **command**]

| anything...

Do nothing (comment)

abc link bchan

Connect analogue link **link** to B channel **bchan**

aring link 0/1

Switch ringing off/on on analogue link **link**

artype link type {onticks offticks}+

Set ring cadence on analogue link.

Link type is 0 for incoming calls and 1 for outgoing calls The ring will come on for **onticks** ticks and then go off for **offticks** ticks, so 'artype 0 0 100 100' will switch ringing on link 0 for incoming calls to a 100 ticks-long ring followed by a 100 ticks-long pause.

bxr [startaddr [endaddr [net]]]

Send bogus IPX RIP

This sends a RIP containing addresses from **startaddr** (default 0x40000000) to **endaddr** (default startaddr+0x10) to network **net** (default 0)

bxs [startaddr [endaddr [net]]]

Send bogus IPX SAP

This sends a SAP containing addresses from **startaddr** (default 0x40000000) to **endaddr** (default startaddr+0x10) to network **net** (default 0)

c

Clear debug trace.

cdo object-id

Delete config object **object-id**

ce

Erase all configuration.

cen

Erase all configuration except permanent settings.

cid

Get new configuration object-ID

CIDR

Classless Inter-Domain Routing.

cnitem object-id last-ptr

Get next config item in object **object-id** where **last-ptr** is 0 or the last value returned.

cnoobject object-id

Get the config object after object **object-id**.

config [show|set]

Show or set configuration.

config show displays the currently stored configuration. If the output from this file is captured or logged, it can be re-transmitted after a **config set** command to restore the configuration (barring permanent settings).

csave object-id string

Save **string** in configuration object **object-id**.

d

Display debug trace

date [dd/mm/yyyy]

Display [or set] the date.

hstart phys

Start HDLC link on physical **phys**

ilearn

Open all ISDN links

ipxping net.n.o.d.e.i.d [size]

Send IPX ping [of size] to MAC-address **net.n.o.d.e.i.d**

ispoofs

Display all IPX spoofs

isdntest norm/bloop/l1loop

Set ISDN loop mode to norm, bloop or l1loop

mempool

Display memory pool information

multilink [0]

Start up any multilink connection [or stop them]

mr address {[b/w/l] numitems}+

Read memory from **address** for **numitems** bytes words or longs

mw address {[b/w/l] value}*

Write **byte**, **word** or **long value(s)** to memory starting at **address**.

p conno

Display TCP connection **conno**

peak <start-time> <end-time>

Set the peak charging period.

ping ip-addr

Send a ping to **ip-addr**

profile begin/end/list/show

Start/stop/list/reset/show profiling information

remup [auto]

Start a remote upload. After successfully using this command, send a .DAT file to this router using TFTP. Then use the 'upload' command. Use the **auto** option to automatically load the file into Flash once it is received

sizes

Display some sizes of objects from the source code

slogicals

Display all logicals

smsg

Display all message timers

sntp

Send an SNTP request

sphysicals

Display all physicals

syslog priority text

Send a SYSLOG message of priority **priority** and contents **text**.

t {tracetype tracelevel}*

Set trace level where **tracetype** is one of:
analogue, arp, async, auth, ethernet, hdlc, init
io, ip, ipx, ipxrip, ipxsap, ipxspooof, ipxtbit, isdn
main, mmi, mp, nat, physical, ppp, qmc, rip
route, snmp, startup, tcp, telnet, tsa, udp, all

If *all* is used, all traces will be set to **tracelevel**.

tracetype should be set to: 1 or more to trace all errors, 4 or more to trace DBG_INFO messages, and 128 or more to dump all buffers

telnet ip-addr

Telnet to **ip-addr**

traceout 0/1

1: Send trace output to this stream

0: Stop sending trace output to this stream

tasks

Display all tasks

time [hh[:mm[:ss]]]

Display [or set] the time.

tserver

Display telnet server connections

udptest [stop] size freq ip.add.re.ss port

Start [or stop] a UDP test with frames sized **size** at frequency **freq** frames/second to IP address **ip.add.re.ss**, UDP port **port**.

upload [wait]

Upload code (once file has been received) after 'remup' command

Use the **wait** option to wait for the TFTP transfer before uploading code into Flash.

+ Enter debugger. This command should only be used under exceptions circumstances.

10.2 Installing New Software in the Viper Routers

Firstly you will need a terminal communications package that is capable of 115200bps operation.

With this terminal package connect up to the unit and check that the menu screens are appearing as expected.

Now go into the Hardware Menu and set the Management port speed to 115200, if it is not already set to this speed. Now quit back up the menu system to the main menu. As you do this, the management port speed will change, and the menus will be garbled. At this point set your terminal package to 115200bps. You should now see the menu screens correctly again.

Now go into the DEBUG MONITOR mode options. Once at the monitor '>' prompt type '+' to get into the debugger.

The screen should show:

Debugger (pl7)

Trap: 0020, pc=0081005c, sr=2000 [NT S I0 NX NN NZ NV NC]

Data: 00800400 00810060 672af571 00000001 00bffd6 00bffd6 00bffa0 008291e4

Addr: 00807884 0085aff3 004015ac 0089118c 00bff948 00bffbc 00bff8d0 00bff8c8

0081005c unlk %a6

debug command

debug>Enter dollar:

Press the \$ key to continue.

Using your communications package send the code image (S-Record file) to the unit. It should be sent as a basic ASCII file. Do **NOT** use any sort of protocol Z-Modem etc, just send the file as raw ASCII.

At this speed the code will take about 1 minute to load. You will not get any feedback during this process. Once complete you should go back into the terminal emulation mode of your package. You can now hit RETURN and you should get back the 'debug>' prompt.

Now hit 'z' and the new version will be checked and then loaded into Flash. The following messages will appear while this is happening.

Please wait...Erasing 5 Sectors...Programming...Done

If an error message occurs instead do not proceed with the programming but repeat the download process.

Provided the above messages appeared you should now power the unit off and on.

Depending of the software that has been sent to the VIPER the menus will now be presented at 115200bps or will have gone back to the default 19200bps speed.

You can now go into the menus and reset the management port speed back to its original value.

If the software that has been sent to the VIPER was operational software, i.e. the main code to change it from the standard V4.20 then the MAC address of the VIPER could be erased.

This can be set by going back into DEBUG MONITOR mode after the VIPER has rebooted and type in the following:

eth xx-xx-xx

Followed by RETURN, then quit out of DEBUG MONITOR mode. The numbers to replace the xx-xx-xx example above are the last six digits on the label on the underside of the VIPER. For example if the VIPER has **300 3 01 30 01 030930** on the label then we enter the command eth 03-03-30 to set the MAC address.

Take care when entering the MAC number, if it has been entered incorrectly then it may not be possible to re-enter it. Reloading the software again should allow access to setting the MAC address again.

10.3 Remote uploading of code.

The following procedure describes how to perform a remote software upload on a router with software version 2.195 or greater.

1. Enter the monitor and issue the command 'remup' or 'r'. This prepares the router to receive the new software image and reserves space for it. The router should respond with:

Allocated space, starting at xxxxxxxx. Now send file via TFTP

2. Send the '.dat' file for the router you are using via tftp in binary mode. On Unix this is done using the following sequence if you are already in the directory containing the image file.

```
$ tftp ip.ad.dr.ess          {Using IP Address of Router}
tftp>bin
tftp>put file.dat           {Where file.dat is the code image}
Sent n bytes in n.n seconds
```

3. Back in the monitor, enter the command 'upload' or 'up'. If the transmitted code is OK, you will see:

CRC check OK
Programming... Please wait for reset...

4. Wait for the reset. If you are connected with a Telnet session, you will need to reconnect to the router.

5. To do the above without waiting for the TFTP transfer to finish, use either the command 'remup auto' or, after using the 'remup' command, use 'upload wait' as follows:

>upload wait
Waiting for TFTP...

Once the file has been received, the router will automatically load it into Flash. In the meantime, the router will function normally. If a file is not received after a few minutes the router will release the reserved space and continue normal operation.

Section 11

Viper Specifications

This section describes the various routing protocols and other standard software components present in latest version of VIPER routers.

Ethernet

Handling of the following Frame types over CSMA/CD.

- Ethernet II
- SNAP
- IEEE 802.2
- IEEE 802.3

IP Routing Protocols

- Address Resolution Protocol (ARP - RFC:826)
- Internet Protocol (IP - RFCs:760, 791, 815)
- Internet Control Message Protocol (ICMP - RFCs:777, 792)
- Routing Information Protocol (RIP - RFC:1058)
- RIP II (RFC:1723) - Run in RIP 1 compatibility mode.
- Static Initialisation of Routing Entries
- Spoofing of RIP to reduce traffic over Dial Up Links.

IPX Routing

- Internetwork Packet Exchange (IPX) including Propagated NetBIOS IPX type 20 frames.
- Routing Information Protocol (RIP)
- Service Advertising Protocol (SAP)
- Spoofing of RIP and SAP to reduce traffic over Dial Up links.
- Static initialisation of RIP and SAP routing tables.
- Auto learning of local Network Numbers and Types.

WAN Services

Point-to-Point Protocol (PPP - RFCs:1661,1662) is run over all WAN Links. Both Protocol Field and Address and Control Field Compression are supported. The following extensions to PPP are also supported.

- PPP Multilink Protocol (MP - RFC:1990) with Bandwidth on Demand
- PPP Authentication (PAP - RFC:1334)
- PPP Challenge Handshake Authentication Protocol (CHAP - RFC:1994)
- PPP Control Protocol (IPCP - RFC:1332) - includes support for Van Jacobson Header Compression, and both numbered and un-numbered links.
- PPP Internetworking Packet Exchange Protocol (IPXCP - RFC:1552) - includes support for Telebit Header compression.
- PPP Compression Control Protocol (CCP - RFC:1962)
- PPP Stac LZS Compression Protocol (PPP-STAC - RFC:1974)
- PPP in Frame Relay (RFC:1973)
- Compression IP/UDP/RTP Headers for Low-Speed Serial Links (CRTP -Internet Draft draft-ietf-avt-crtp)
- IP Express - reserved bandwidth and IP Prioritisation Mechanism.

ISDN

- Calling Line Identification (CLI)
- Multiple Subscriber Numbering (MSN)
- Dialback Mechanism based on CLI
- Call Charge Limiter
- Access Control - Out of Hours call barring facility.

Management

- User Datagram Protocol (UDP - RFC:768)
- Transmission control Protocol (TCP - RFCs: 675, 761, 793)
- Using Telnet Protocol (TELNET - RFCs:854, 855)
- Using Simple Network Management Protocol (SNMP - RFCs: 1155, 1157, 1212)
- Conforms to MIB-II (RFC:1213) except the TCP, EGP and Transmission Groups are not supported.
- SYSLOG system logging performed on UDP port 514

Other

- Remote Software Upgrade using Trivial File Transfer Protocol (TFTP - RFC:1350).
- Distribution of Network time using Simple Network Time Protocol (SNTP - RFC:2030)
- Network Address Translation (NAT) - based on ideas in RFCs 1631 and 1919.

Section 12

Glossary

This section explains terms used elsewhere in the manual.

10Base2

Connection to **Ethernet** using coaxial cable and BNC connectors.

10Base5

Connection to **Ethernet** using AUI cable and 15 pin D type connectors.

10BaseT

Connection to **Ethernet** using **twisted pair** cable and RJ45 connectors.

a-law

An a-law algorithm is a standard algorithm, used in European Digital communications systems to optimize, i.e., modify, the dynamic range of an analogue signal for digitizing. The A-law algorithm provides a slightly larger dynamic range than the **u-law** at the cost of worse proportional distortion for small signals. By convention, a-law is used for an international connection if at least one country uses it.

ARP Address Resolution Protocol

ARP is used to resolve **IP** addresses into physical network addresses. IP hosts use this protocol when they know the IP address of a host but not it's physical (Ethernet) address. ARP is defined in "RFC-826".

Basic Rate ISDN

A type of ISDN line which carries the equivalent of two telephone calls. This is often referred to as $2B+D$ because a basic rate ISDN line is divided into three streams of data: two B channels, which are exclusively reserved for data, and one D channel, which carries the messages which make and clear calls.

CIDR

Classless Inter-Domain Routing. This replaced the previous generation of IP address syntax, classful networks. It allowed increased flexibility when dividing ranges of IP addresses into separate networks and made more efficient use of increasingly scarce IPv4 addresses.

CIR

Committed Information Rate. This is a specified guaranteed data rate that the carrier is to provide. When the data rate exceeds the CIR, the network starts dropping packets, so CIR should be a balance between the minimum and maximum bandwidth requirements.

CHAP

The Challenge-Handshake Authentication Protocol (CHAP) authenticates a user to an Internet access provider. RFC 1994:

PPP Challenge Handshake Authentication Protocol (CHAP) defines the protocol.

CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link, and may happen again at any time afterward. The verification is based on a shared secret (such as the client user's password).

CHAP is more secure than PAP as an authentication protocol.

Datagram

A quantity of data, which is sent, received, and routed as a unit.

Dynamic routes

These are routes that are learned via a routing protocol such as **RIP**. They are maintained automatically. Commands, which make changes to dynamic routes, are usually effective only temporarily because the same route will be learned again from the other routers in the network.

Ethernet

A type of **LAN** invented by the Xerox Corporation at the Palo Alto Research Centre. Originally Ethernet was specified to transfer data over thick coaxial cable at a speed of 10 Mbps. This is connected to individual machines via an AUI cable (known as **10base5**). One variant uses a thin coaxial cable, and is sometimes called *Cheapernet* or *Thinnet*. It is also known as **10base2**. Another variant uses **twisted pair** cable. This type of Ethernet is called **10baseT**. Newer variants have been produced which run at higher speeds than the original. The VIPER routers support the four frame types:

- Ethernet 802.2
- Ethernet 802.3
- Ethernet II
- Ethernet SNAP

These are different formats used to encapsulate the data.

Frame Relay

Frame relay is a technique of data transmission of sending data quickly and efficiently using a relay of frames to one or many destinations from one or many end-points.

ICMP Internet Control Message Protocol

This is an adjunct to **IP**, and provides the ability to exchange error and control messages between local and remote hosts or routers. The **ping** facility uses one kind of ICMP message. It is used to test communication between two devices on a network. The originator of the 'ping' sends an *ICMP Echo* and the target host replies with *ICMP Echo Reply*. ICMP is defined in "RFC-792".

Internet

(Usually "The Internet"). A particular global **internetwork** composed of a very large number of independently administered networks.

internetwork

(Also called an Internet). A network composed of smaller networks that may be independently administered. Compare with Internet.

Internet Protocol (IP)

This is a standard protocol widely used for **internetworking**. IP messages carry data from an originating computer to a destination computer, possibly passing through routers. The term "IP" is often used to refer to the collection of protocols usually used with IP itself. Some of these are: **ICMP ARP RIP SNMP TCP TELNET UDP**. IP is defined in "RFC-791".

IP Address

An address used by **IP**. These are explained in the section IP addresses.

IPX Internetwork Packet eXchange

A standard protocol devised by Novell. The term "IPX" is often used to refer to the family of protocols usually found on Novell networks. These include: **RIP SAP** and **SPX**.

IPX Address

An address used by **IPX**. These are explained in the section IPX addresses.

ISDN Integrated Services Digital Network

This is the name of the network which carries both voice and data calls. It is used by telephone companies to provide customers with a standard type of connection, instead of the traditional different types that required different equipment to handle voice and data calls. It takes advantage of the fact that modern telephone networks digitise voice calls by extending the digital capabilities to the customer. The basic unit of ISDN is a 64000 bits-per-second connection. This is the equivalent of a traditional phone line.

LAN Local Area Network

A network operating over short distances, usually at high speed. One very popular LAN is **Ethernet**.

LCP - Link Control Protocol

This is one of the several protocols negotiated over a **PPP** link. It is always the first to be negotiated and is an indication of the state of the link. When the state reaches Opened then it is ready for use by other protocols e.g. IP, IPX.

MAC Medium Access Control

This is what deals with a physical network, such as **Ethernet**.

PING

This is a facility used for testing. It involves sending a test message (using **ICMP**) and using the response, if any, to diagnose any possible problems. The **PING** command is available on the ADMIN menu.

PAP

Password Authentication Protocol is a simple authentication protocol used to authenticate a user to a remote access server or ISP.

PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure; it is used as a last resort when the remote access server does not support a stronger authentication protocol like CHAP

PPP - Point-to-Point protocol

This is a method of transmitting multi-protocol datagrams over point-to-point links.

RIP Routing Information Protocol

This is the name for two related, but different, protocols. One is used with **IP** and the other with **IPX**. Both are used to exchange routing information with other routers. They are described in the section RIP. The IP version of RIP is defined in "RFC-1058".

RJ11

A standard type of connector. It can accommodate up to six wires, and the RJ11 plug can connect with an RJ45 socket by connecting to the centremost six wires of the RJ45 socket. It is the standard connector for telephone lines in several countries.

RJ45

A standard type of connector. It can accommodate up to ten wires, and the smaller **RJ11** plug can connect with an RJ45 socket by connecting to the centremost six wires of the RJ45 socket. It is the standard connector for **Basic Rate ISDN** and **twisted pair Ethernet**.

SAP Service Advertising Protocol

This is a method of discovering services on an **IPX** network. It is explained in the section **IPX SAP**.

SNMP Simple Network Management Protocol

This is used to configure equipment, to examine status and statistics, and to report problems. SNMP is defined in "RFC-1157".

SNTP

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over data networks. NTP uses UDP port 123 as its transport layer.

SPX - Sequenced Packet eXchange

This is a protocol that provides a reliable connection over an **IPX** network.

Static routes

These are routes that have been permanently entered into a routing table. Static routes are only affected by the relevant commands - they do not change automatically. Compare with **dynamic routes**.

Subnet

This is a subdivision of an IP network. Subnets are explained in the section **IP address subnets**.

SYSLOG

A method of collecting together message logs from many systems. Each system sends short text messages to a syslog recorder. The recording system may record these in any desired manner including writing them to a file, sending them on to other systems, and printing them out. The VIPER routers can send messages about important events to a syslog recorder. This is configured by the **GLOBAL SYSLOG** command.

Syslog messages are transported by **UDP** datagrams sent to port 514.

TCP Transmission Control Protocol

TCP provides transport level connections between hosts. It is designed to provide a reliable connection and handles error detection, lost packets and packets that arrive out of sequence. It is also called "TCP/IP" because it uses **IP**. The entire collection of IP protocols is also frequently referred to as "TCP/IP". **TELNET** uses TCP for its connections. TCP is defined in "RFC-793".

TELNET

Telnet is the **TCP/IP** standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a remote host at another site as if the user's terminal was directly connected to the remote machine.

The VIPER routers use Telnet to allow access to the exactly the same menus as when you connect directly using a terminal. The section **Access via TELNET** describes this in more detail. TELNET is defined in "RFC-854".

Twisted pair

A type of cable containing two wires twisted about each other. It is used because it is cheap and simple, it has good immunity to external noise, and it radiates signals to a relatively small extent.

UDP User Datagram Protocol

UDP is a transport protocol designed to provide a connectionless mode service. It does not provide the error handling and automatic retransmission of **TCP**. UDP is used by the VIPER routers to support **RIP** and **SYSLOG**. UDP is defined in "RFC-768".

u-law

The u-law (commonly written as μ -law) algorithm is an algorithm, primarily used in the digital telecommunication systems of North America and Japan.

The A-law algorithm provides a slightly larger dynamic range than the μ -law at the cost of worse proportional distortion for small signals. By convention, A-law is used for an international connection if at least one country uses it.

V.24 / RS232

This is a standard method of connecting a low speed serial channel. While V.24 and RS232 are actually separate standards, the terms are often used interchangeably to refer to the type of serial port, which they describe.

V.35

A standard type of serial port.

WAN Wide Area Network

A network which covers a large area, usually at relatively low speed.

X.21

A standard type of serial port USING A 15 Way D type connector.

Appendix A Vipers Menu Structure

The following table shows all the screens and how they relate to each other.

0 GLOBAL - System Configuration

- 0 NAME - Router NAME
- 1 IP - IP enabled
- 2 IPX - IPX enabled
- 3 PRIOR - IP Express PIPE enabled
- 4 SNTP - SNTP IP Address
- 5 SYSLOG - SYSLOG IP Address
- 6 SYSPASS - System password
- 7 ISDN - ISDN Configuration
 - 0 CHARGES - Charge limiter
 - 1 MSN - Multiple Subscriber Numbering
 - 2 ACCESS - Access Control
 - 3 CHECKCLI - Check CLI Before Answering
 - 4 DAYTIMES - Daytime Minimum Call Duration's
 - 5 EVETIMES - Evening Minimum Call Duration's
 - 6 WEEKENDTIMES - Weekend Minimum Call Duration's
- 8 SNMP - SNMP Configuration
 - 0 COMMUNITY - Community Name
 - 1 MANIP - Manager IP Address
 - 2 ACESSTYPE - SNMP Access Type
 - 0 None - No SNMP Access
 - 1 ReadOnly - Read Only SNMP Access
 - 3 TCOMMUNITY - Trap Community Name
 - 4 TRAPIP - Trap IP Address
 - 5 TRAPTYPE - Trap Types to Send
 - 0 None - No Traps Generated
 - 1 Auth - Generate Authorisation Traps
 - 2 Ord - Generate Ordinary SNMP Traps
 - 3 All - Generate All SNMP Traps
 - 6 CONTACT - Contact Name to Report
 - 7.LOCATION - Location to Report
- 9 ERASE - Erase all configuration

1 NETWORK - Configure networks, routes etc

- 0 N - Network Name
 - 0 NAME - Name
- 1 IP - IP configuration
 - 0 ENABLE - IP routing
 - 1 LOCAL - Local IP address
 - 2 REMOTE - Remote IP address (if not Ethernet)
 - 3 MASK - IP address mask
 - 4 RIP - RIP
 - 0 DISCARD - (D) Discard RIP from this network
 - 1 RIPTX - (T) Send RIP updates to this network

- 2 RIPAGE - (A) Age RIP entries, No RIP Spoofing
- 3 RIP-2 - (2) Enable Transmission of RIP-2

5 RIPMETRIC - Advertised Metric when disconnected

6 ROUTES - Associated static routes

- R - Route name
- 0 ADDRESS - Target IP network
- 1 ROUTER - IP address of next router
- 2 MASK - IP mask (0=default route)
- 3 METRIC - Cost of route

7 TRANSLATE - Address translation rules

- 0 IN - Rules for incoming sessions
- 0 TCP - Rules for incoming TCP sessions
- 0 PATTERN - Pattern to test against
- 1 NEWSRC - Translated source details
- 2 NEWDST - Translated destination details
- 1 UDP - Rules for incoming UDP sessions
- 0 PATTERN - Pattern to test against
- 1 NEW - Translated address and port
- 1 OUT - Rules for outgoing sessions
- 0 TCP - Rules for outgoing TCP sessions
- 0 PATTERN - Pattern to test against
- 1 NEWSRC - Translated source details
- 2 NEWDST - Translated destination details
- 1 UDP - Rules for outgoing UDP sessions
- 0 PATTERN - Pattern to test against
- 1 NEW - Translated address and port
- 2 USETCP - Use TCP Rules for all sessions

8 PIPE - IP Express

- 0 RESBAN - Reserved bandwidth (bytes/sec)
- 1 FRAGSIZE - Fragment size
- 2 PRIOR - IP Prioritisation

9.FILTBROAD - Filter Directed Broadcast

2 PPP - PPP configuration

0 PAP - Password Authentication Protocol

- 0 PEERID - Peer user id
- 1 PEERPASS - Peer password to check against
- 2 LOCALID - Local user id
- 3 LOCALPASS - Local password to send to peer

1 CHAP - Challenge Handshake Authentication

- 0 PEERID - Peer user id
- 1 PEERCALLX - Secret for checking when calling
- 2 PEERANSX - Secret for checking when answering
- 3 LOCALID - Local user id when calling
- 4 LOCALCALLX - Secret for responding when calling
- 5 LOCALANSX - Secret for responding when answering
- 6.REPINT - Challenge repeat interval (seconds)

2 MPDMAX - No. of Dialup/Backup calls

3 BANDWIDTH - Bandwidth on demand

- 0 MAXCHANS - Maximum Channels to Open
- 1 OPENTHRESH - Threshold to open first extra link
- 2 OPENDURATION - Duration to open extra link
- 3 CLOSETHRESH - Threshold to close extra link
- 4 DIRECTION - Direction to test thresholds against OUT

3 IPX - IPX configuration

0 ENABLE - IPX Routing

1 IPXUPDATES - Always update IPX Routing Tables

2 IPXLEARN - Initial IPX Learning Period

3 NETWORKS - IPX Networks

- 0 EIENABLE - Ethernet II enable
- 1 EIINetwork - Ethernet II network number
- 2 SNAPENABLE - SNAP enable
- 3 SNAPNETWORK - SNAP network number
- 4 E8022ENABLE - 802.2 enable
- 5 E8022NETWORK - 802.2 network number
- 6 E8023ENABLE - 802.3 enable
- 7 E8023NETWORK - 802.3 network number
- 8 PPENABLE - PPP enable
- 9 PPPNETWORK - PPP network number

4. ROUTES - Associated static routes

N - Name of IPX route

0 REMOTE - Remote network

1 LOCAL - Network number for next hop

2 NODE - Node number of next hop router

3 HOPS - Hop count

4 TICKS - Route length

5 FRAMETYPE - Ethernet frame type for next hop

5 SAPS - Associated static saps

N - Name of SAP

0 SNAME - Server Name

1 SADDR - IPX address of server

2 SOCK - server socket number

3 TYPE - service type

6 LEARNROUTES - Learn static routes now

7.LEARNSAPS - Learn static saps now

4 ISDN - ISDN configuration

0 DIALLIST - List of numbers to dial

P - ISDN phone number

0 NUMBER - Number to dial

1 PRIORITY - Priority of number

2 CHARGERATE - Charge rate for this number

0 LOCAL Local rate

1 REGIONAL Regional rate

- 2 NATIONAL National rate
- 3 INTERNATIONAL International rate
- 4 LASTFAILURE - Elapsed time since failed to connect

- 1 CLILIST - List of acceptable calling numbers
- 2 CLIACTION - Dialback on CLI Match
- 3 ACCESS - Use access control
- 4 MINCALL - Control Minimum Call Lengths
- 5 CLEAR - Cleardown time
- 6 DAY CLEAR - Daytime cleardown time
- 7 EVE CLEAR - Evening cleardown time
- 8 WKEND CLEAR - Weekend cleardown time

- 5 CHANNELS - Select channels to use
 - 0 ETHERNET - Ethernet
 - 1 ETHERNET2 - Secondary Ethernet
 - 2 X21L1 - Leased Line channel 1
 - 3 X21L2 - Leased Line channel 2
 - 4 FRL1 - Frame Relay Address 1
 - 5 FRCIR1 - Frame Relay CIR 1
 - 6 FRL2 - Frame Relay Address 2
 - 7 FRCIR2 - Frame Relay CIR 2

2 HARDWARE - Configure Hardware

- 0 MSPEED - Management port speed 19200
 - 0 9600 bps
 - 1 19200 bps
 - 2 38400 bps
 - 3 57600 bps
 - 4 115200 bps

- 1 ETHERNET - Configure Ethernet

- 2 FRELAY - Configure Frame Relay
 - N - Frame Relay entry
 - 0 FRADDRESS - Address of Frame Relay Channel
 - 1 PORT1 - First Port to Connect Not Set
 - 2 PORT2 - Second Port to Connect Not Set
 - 3 BITRATE - Committed Information Rate of Channel

- 3 VIPER - Configure VIPER Options
 - Menu options differ with Voice option card fitted

- 4 YPAGES - Configure VIPER Phone Book
 - Y - Phone Book entry
 - 0 DNUMBER - Number to Dial
 - 1 DESTIP - IP Address of Destination
 - 2 DESTCHAN - Port to Call on Destination Unit

- 5 X21L1 - Leased Line channel 1
 - 0 SPEED - External clock
 - 1 EXTSPEED - External clock speed
 - 2 IFTYPE - External Interface Type

- 6 X21L2 - Leased Line channel 2
 - 0 SPEED - External clock
 - 1 EXTSPEED - External clock speed
 - 2 IFTYPE - External Interface Type

3 ADMIN - Administration of running system

- 0 TELNET - TELNET Connection
- 1 PING - Ping
- 2 ARP - Examine ARP cache
- 3 IPROUTE - Examine IP routing table
- 4 IPXROUTE - Examine IPX routing table
- 5 SAP - Examine IPX SAP table
- 6 PHYSICALS - Examine Physical table

4 STATUS - Current Status

5 STATISTICS - Recent Statistics

- 0 IP - IP Statistics
- 1 ICMP RECEIVE - ICMP RECEIVE Statistics
- 2 ICMP SEND - ICMP SEND Statistics
- 3 TCP - TCP Statistics
- 4 UDP - UDP Statistics
- 5 SNMP1 - SNMP1 Statistics
- 6 SNMP2 -SNMP2 Statistics
- 7 ETHERNET - ETHERNET Statistics

6 WANSTATS - Recent WAN Statistics

- 0 X.21 Link 1 - X.21 Link 1 Statistics
- 1 X.21 Link 2 - X.21 Link 2 Statistics
- 2 ISDN2 B1 - ISDN2 B1 Statistics
- 3 ISDN2 B2 - ISDN2 B2 Statistics

7 DEBUG - Debugging facilities

- 0 MONITOR - Debugging monitor
- 1 BOUNCE - Action on error
- 2 REBOOT - Reboot Now

Appendix B Vipers Cables

The following tables show the pin out of the various cables that are used on the Viper and VLINE unit.

X.21 V.11 Male to Female X.21 V.11 - Straight

Sig	15W D Type Male	15W D Type Female	Sig
	1	1	
Ta	2	2	Ta
Ca	3	3	Ca
Ra	4	4	Ra
Ia	5	5	Ia
Sa	6	6	Sa
Xa	7	7	Xa
Gnd	8	8	Gnd
Tb	9	9	Tb
Cb	10	10	Cb
Rb	11	11	Rb
Ib	12	12	Ib
Sb	13	13	Sb
Xb	14	14	Xb
	15	15	

X.21 V.11 Female to Female X.21 V.11 – Cross Over

Sig	15W D Type Female	15W D Type Female	Sig
	1	1	
Ta	2	4	Ra
Ca	3	5	Ia
Ra	4	2	Ta
Ia	5	3	Ca
Sa	6	7	Xa
Xa	7	6	Sa
Gnd	8	8	Gnd
Tb	9	11	Rb
Cb	10	12	Ib
Rb	11	9	Tb
Ib	12	10	Cb
Sb	13	14	Xb
Xb	14	13	Sb
	15	15	

BRI Cable - Straight

Sig	RJ45 8W		RJ45 8W	Sig
TX+	3	_____	4	RX+
RX+	4	_____	3	TX+
RX-	5	_____	6	TX-
TX-	6	_____	5	RX-

BRI Cable – Cross Over

Sig	RJ45 8W		RJ45 8W	Sig
TX+	3	_____	3	TX+
RX+	4	_____	4	RX+
RX-	5	_____	5	RX-
TX-	6	_____	6	TX-

V.35 34 Way MRAC Plug to Female V.35

34 W		15W D
MRAC		Type
Plug		Female
C	_____	1
P	_____	2
H	_____	3
R	_____	4
Y	_____	5
V	_____	6
U	_____	7
B	_____	8
S	_____	9
		10
T	_____	11
AA	_____	12
X	_____	13
W	_____	14
F	_____	15

PRI Cable - Straight

Sig	RJ45 8W	RJ45 8W	Sig
RX(a)	1 _____	1	RX(a)
RX(b)	2 _____	2	RX(b)
TX(a)	4 _____	4	TX(a)
TX(b)	5 _____	5	TX(b)

PRI Cable – Cross Over

Sig	RJ45 8W	RJ45 8W	Sig
RX(a)	1 _____	4	TX(a)
RX(b)	2 _____	5	TX(b)
TX(a)	4 _____	1	RX(a)
TX(b)	5 _____	2	RX(b)

RJ11 to BT603A conversion – For FXO and FXS

Sig	RJ11 6W	BT603	Sig
Bell	2 _____	4	Bell
Ring	3 _____	5	Ring
Tip	4 _____	2	Tip

Manager Cable

RJ45 8W Plug	9 D Type Female	Sig
4 _____	5	GND
5 _____	3	TXD
6 _____	2	RXD