BLACK BOX Catalogue Ltd
The Source for Connectivity

VIPER
ISU9901-FXO (RJ-11FXO)
ISU9901-FXS (RJ-11 FXS)
ISU9901-EM (RJ-45 E&M)

VIPER Plus
ISU9901-PLUS-FXO (RJ-11)
ISU9901-PLUS-FXS (RJ-11)
ISU9901-PLUS-EM (RJ-45)

WAN Options
ISU9902-X21 (X.21 Interface)
ISU9902-V24 (V.24 Interface)
ISU9902-V.35 (V.35 Interface + Adapter Cable)

Software Upgrades
ISU9903-FR (Frame Relay)
ISU9903-AC15 (AC15)

VIPER
(Voice Over IP Exchange Router)

24 AUG 1999

TECHNICAL: (0118) 931 2233
SALES: (0118) 965 5100
FAX: (0118) 931 1727
ADDRESS: 15 Cradock Road, Reading, Berkshire RG2 0JT
WEB: www.blackbox.co.uk

Contents

1. Introduction

1.1 The VIPER

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

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, with the option of leased line to 2Mbps.

The VIPER provides Voice over IP facilities, with (2) independent voice ports supporting (3) different physical line interface options-
-E&M (for connection directly to or between PBX equipment)
-FXS (for the direct attachment of telephones), and
-FXO(for connection to telephone ports on a PBX).

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 4 provides essential information for the novice on network configuration, plus additional detail on the special features present on these routers.

Section 5 provides a complete description of the menu system used to configure all the features of the routers.

Section 6 describes the voice features available on the VIPER together with other optional features.

The last three sections provide additional technical information about the router, together with a glossary of terms used in this manual.

Words shown in **bold** in this manual are terms whose description appears in the Glossary section of the manual. The names of menus and other values that are entered into the menu system are shown in a `fixed width font`.

2. Installation

2.1 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 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 25-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.

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 flow control options on the Terminal or Terminal Emulation software that you are using. Switch on the mains power to the router. The router will go through a power up sequence, which can take up to a minute. During this period two 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.

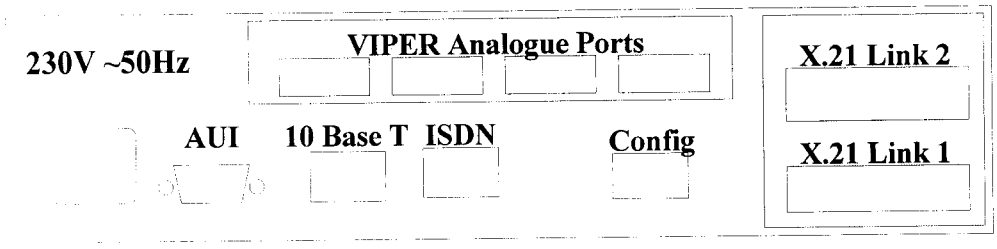
After basic configuration has been entered you may connect up the WAN and Ethernet links. The diagrams below show the locations of the ports on each of the products in the range.

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

2.2 Ports

The following are diagrams of the rear of the VIPER indicating the relative positions of the various connections.

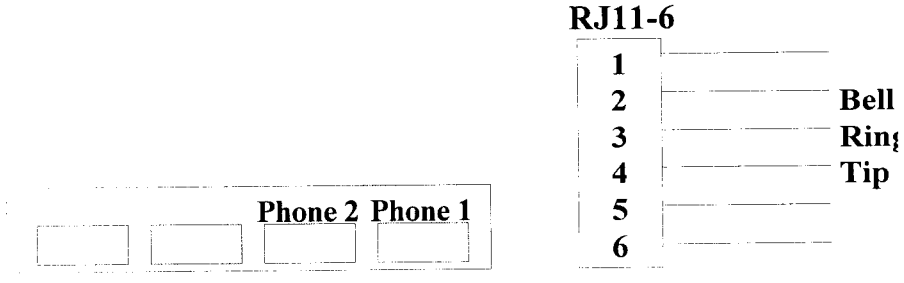
Diagram of VIPER rear panel



Depending on which of the 4 VIPER variants you are using, different sockets will be available in the area labelled VIPER Analogue Ports. Only two of these sockets will be available for use with the 2 unused positions blanked out.

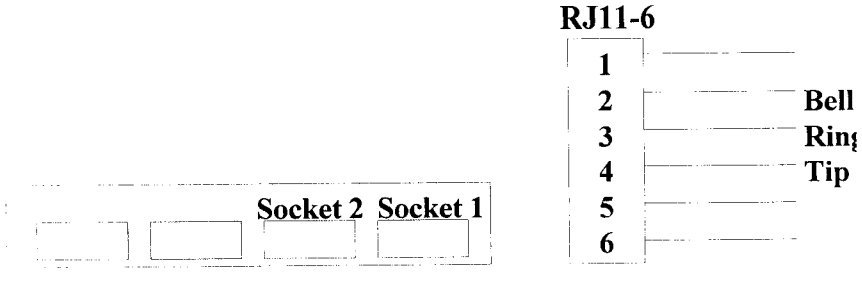
The following sections describe the various options. The pinouts of the VIPER analogue ports are provided. The connector pinouts are numbered with 1 on the left when looking at the end of the connector with the actual wire going away from you and with the lock tab at the top.

FXS



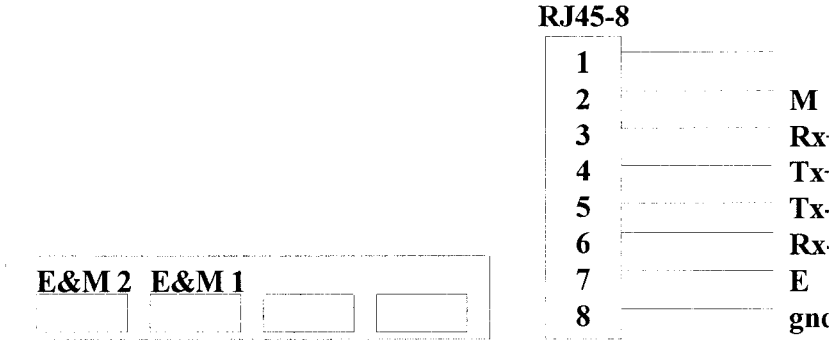
This option provides 2 RJ11-6 phone sockets, into which standard Phones/Fax Machines may be connected using the short conversion cables supplied. The sockets are Master Sockets and support both Tone and Pulse Dialling.

FXO



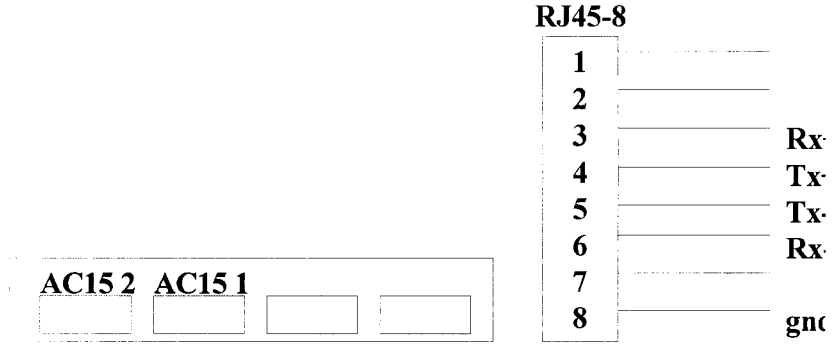
This option provides 2 RJ11-6 sockets that may be connected to a standard telephone exchange line. Cables are supplied for this purpose

E&M



This option provides 2 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.

AC15



This option provides 2 RJ45-8 sockets for connection to the AC15 ports of the PABX. Un-terminated cables are provided for this purpose.

.

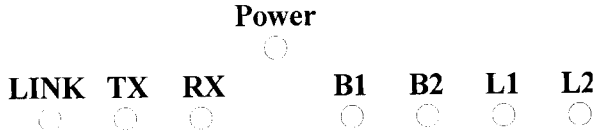
2.3 LEDs

The following sections describe the functions of the LEDs visible on the front of each of the units.

2.3.2 VIPER

The following diagram shows the arrangement of LEDs on the front on the VIPER units. The Power LED indicates that the unit is receiving power. The ENET TX and

ENET RX LEDs indicate activity on the Ethernet Interface. These 2 LEDS also flash alternately while the unit is going though its power up sequence. The Link light will illuminate when the unit is correctly connected to a 10BaseT network/hub, it will not operate when the 10Base5 AUI port is being used.



B1 and B2

These LEDs light to indicate that an ISDN B channel is in use. When a block of data is sent over the link they will briefly be extinguished to show the link activity.

L1 and L2

These LEDs light every time a frame is sent or received over the associated Leased Line channel. A correctly connected idle channel will cause the LED to flash once every second. A link that is receiving clock but not getting a response from the remote site will cause the LED to flash approximately every 3 seconds.

3. Basic Configuration

The following sections provide various basic configuration examples to get a basic configuration up and running as quickly as possible. Section 5 provides more details about the actual menus used in these examples.
For voice applications configure IP routing first, then enable the voice ports and create the phone list.

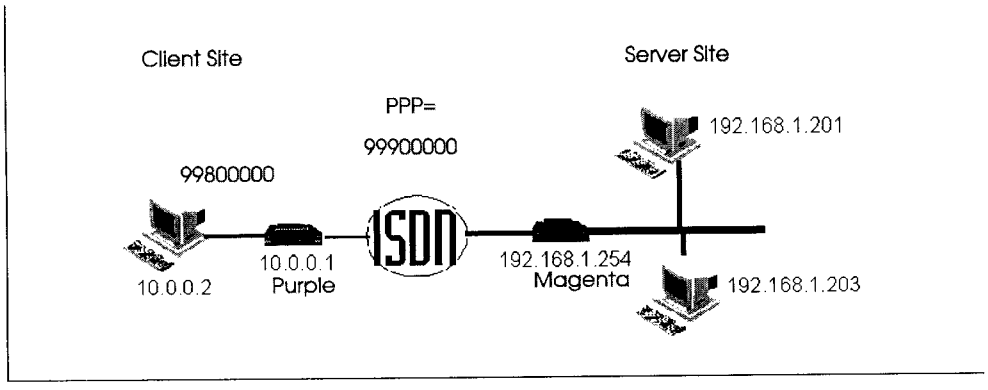
3.1 Quickstart

This section is intended to allow the user to set up a router with either an ISDN connection or leased line connection, as quickly and simply as possible using IP and/or IPX. It will use the Unnumbered Interface method that is considered easier. Before starting configuration, the following information must be either decided upon, or found from the Network Administrator. Example input has been provided.

3.1.1 General Required Information

1. Terminal Emulation Package with RS232 / V24 DTE running at 19,200 bps Hyperterminal)
2. Local Router Name = e.g. *purple*
3. Local Router ID = *purple* (For PAP negotiation, the global name is the default ID)
4. Local Router Password = e.g. *password* (For PAP negotiation)
5. Remote Router Name = e.g. *magenta* (For PAP negotiation)
6. Remote Router ID = *magenta* (For PAP negotiation, the WAN network name is the default ID).
7. Remote Router Password = e.g. *password* (For PAP negotiation)
8. Remote ISDN Phone Number (if appropriate) = e.g.*123456* (*magenta* ISDN no.)

Example Application



3.1.2 IP Required Information

1. Local Router IP address = e.g. *10.0.0.1* (Local IP address of *purple*)

2. Local Router sub-net mask = e.g. *255.0.0.0* (class A)
3. Remote Router IP address = e.g. *192.168.1.254* (Local IP address of *magenta*)
4. Remote Router sub-net mask = e.g. *255.255.255.0* (class C)

3.1.3 IPX Required Information

1. Unique IPX network number(s) for ethernet network (without server) = e.g.*99800000*
2. Arbitrary IPX network number for PPP network = e.g. *99900000*
3. IPX network numbers already in use on the LAN (needed so as not to conflict with them)

3.1.4 Configuration

The Configuration will lead the user through the required parameters that have to be set in the menu for their application. Any changes made to menus do not take affect until the user 'quits' from the screen.

Common Configuration Parameters

```
GLOBAL
└→    NAME Purple
NETWORK
└→    ADD
   └→    UNCONFIGURED
            └→    NAME eth
                  CHANNELS
                  └→    ETHERNET yes
      ADD
   └→    UNCONFIGURED
            └→    NAME magenta
```

The network menu must be 'quit' from to save the information. This configuration adds an ethernet network called eth and a Wide Area Network called magenta, which is the global name of the remote router.

To communicate with the remote router, the PAP passwords must be configured in the PPP protocol.

```
NETWORK
└→    magenta
   └→    PPP
      └→    PAP
         └→    PEERPASS password
               LOCALPASS password
```

IP CONFIGURATION

The IP Configuration must be configured for the two networks that have been added. This uses the unnumbered interface model. If the classical model is preferred refer to the manual.

```
NETWORK
└> eth
   └> IP
      └> LOCAL 10.0.0.1
         REMOTE 0.0.0.0
         MASK 255.0.0.0
   magenta
   └> IP
      └> LOCAL 0.0.0.0
         REMOTE 192.168.1.254
         MASK 255.255.255.0
      ISDN
      └> DIALLIST
         └> ADD
            └> NO
               ⊢> NUMBER 123456
```

IPX CONFIGURATION

For IPX configuration, there are two scenarios to be aware of:-

a) scenario 1 - one or more servers at each site
b) scenario 2 - one or more servers at only one site, with no servers at the other

Scenario 1 Configuration

The PRX router will learn the Ethernet IPX network numbers from the servers. It is, therefore, not necessary to configure the Ethernet IPX network numbers. However, the WAN link must still have an IPX network number that is **not** in the existing network configuration. This is configured under the IPX menu.

```
NETWORK
└> magenta
   └> IPX
      └> NETWORKS
         └> PPPNETWORK 99900000
```

Scenario 2 Configuration

The PRX router connected to the site without a server must have an Ethernet IPX network number chosen that does **not conflict** with the IPX network numbers already in use at the remote site.

```
NETWORK
└> eth
   └> IPX
      └> NETWORKS
         └> E8022NETWORK 99800000
```

Other Ethernet frame types may be configured at this stage but each must have a unique IPX network number. The PPP network number must also be configured on the WAN network similar as in Scenario 1.

LEASED LINE CONFIGURATION

If an ISDN line is not being used for the WAN connection, but a leased line is, the user must connect the cable to the back of the leased line interface card, and reboot the router. Providing the router has been configured correctly, it will automatically recognise the remote router. If the user wishes to connect the routers back-to-back, one of the routers must be set up to provide the clocking. Only Link 2 has the ability to provide the clocking.

```
HARDWARE
└→          X21L2
    └→              SPEED 64000
```

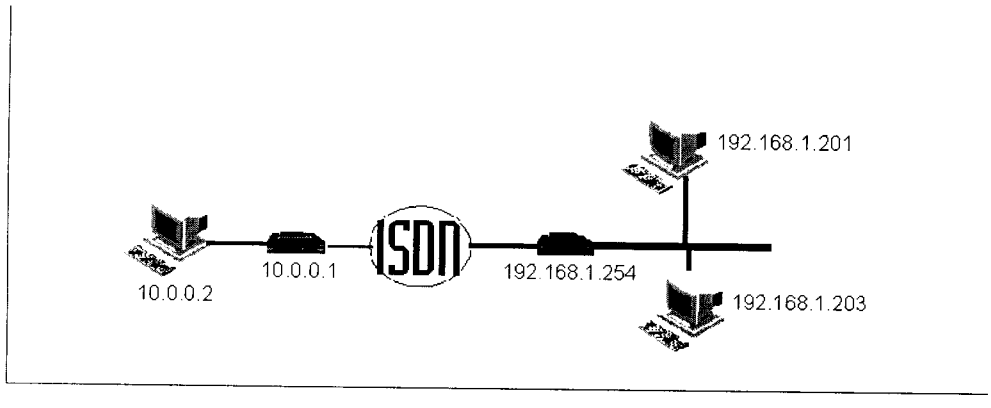
Remote Unit

The above sections have lead you through the configuration of one of the routers. To configure the second router, simply swap over all local names, IDs, IP addresses to the remote values.

3.2 Example IP Configuration - unnumbered interfaces

Below is a typical configuration, which configures everything necessary for IP routing between an Ethernet and an ISDN using two PRX routers. Each command is explained in detail in its own section of the manual. This example assigns addresses in accordance with the unnumbered interface scheme, as described in Section 4.? In comparison with the traditional addressing scheme, this is simpler, but not universally supported by older equipment.

Diagram of example network



Here, two routers are connected over the ISDN, providing routing between the two Ethernets 10.0.0.0 and 192.168.1.0. The following sequence describes the steps required to configure this network.

1. **GLOBAL NAME *PURPLE***
   You can choose any name you like for the router. The name will appear on most of the menus. It is also used as the default *Local User ID* within PAP negotiation for PPP links.

2. **NETWORK ADD**

3. **UNCONFIGURED NAME *ETH***
   You can choose any name you like for the network. The name will appear on various menus where it is necessary to identify a network. It is also used as the default *Peer User ID* within PAP negotiation on PPP links.

4. **NETWORK ETH IP LOCAL *10.0.0.1***
   This is a class A network from the range reserved for private use.

5. **NETWORK ETH IP MASK *255.0.0.0***
   This is the standard class A mask.

6. **NETWORK ETH CHANNELS ETHERNET *YES***
   Tell the router that this network uses the Ethernet port.

7. **NETWORK ADD**

8. **NETWORK UNCONFIGURED NAME *MAGENTA***

9. **NETWORK MAGENTA IP REMOTE *192.168.1.254***

10. **NETWORK MAGENTA IP MASK *255.255.255.0***

11. **NETWORK MAGENTA ISDN NUMBER ADD**

12. **NETWORK MAGENTA ISDN NUMBER I0 *<telephone number>***

13. **NETWORK MAGENTA PPP PAP PEERPASS *<password>***
    This is the password, which the remote router must send when it dials in to this one. The name it must send is MAGENTA because no PEERID is entered.

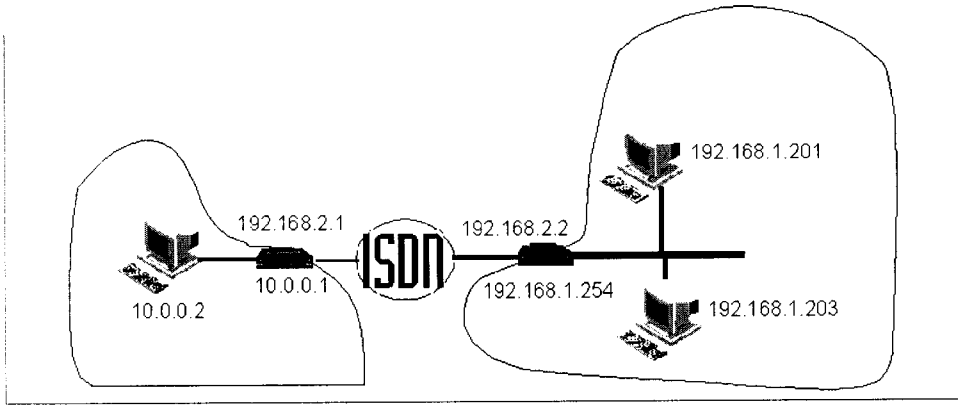
14. **NETWORK MAGENTA PPP PAP LOCALPASS *<password>***
    This is the password, which this router sends when it dials out to the remote router. The name sent will be the GLOBAL NAME because no LOCALID is entered.

Once the router has been rebooted, it is ready to dial the remote router MAGENTA, which has IP address 192.168.1.254.

3.3 Example IP Configuration - traditional numbering

Below is a typical configuration, which configures everything necessary for routing between an Ethernet and an ISDN using two PRX routers. Each command is explained in detail in its own section of the manual. This example assigns addresses in the traditional way, as described in Section 4.? In comparison with the unnumbered interface scheme, this is more complex, but universally supported by older equipment.

Diagram of example network



Here, two routers are connected over the ISDN, providing routing between the two Ethernets 10.0.0.0 and 192.168.1.0.

1. GLOBAL NAME *PURPLE*

2. NETWORK ADD

3. NETWORK UNCONFIGURED NAME *ETH*

4. NETWORK ETH IP LOCAL *10.0.0.1*

5. NETWORK ETH IP MASK *255.0.0.0*

6. NETWORK ETH CHANNELS ETHERNET *YES*

7. NETWORK ADD

8. NETWORK UNCONFIGURED NAME *MAGENTA*

9. NETWORK MAGENTA IP LOCAL *192.168.2.1*
   Here, the ISDN port is given an IP address. The ISDN port of the other router must have an IP address with the same network number.

10. NETWORK MAGENTA IP REMOTE *192.168.2.2*
    This is on the same network.

11. NETWORK MAGENTA IP MASK *255.255.255.0*
    This mask makes the LOCAL and REMOTE addresses be on the same network.

12. NETWORK MAGENTA IP ROUTES ADD
    This creates an entry for a static route. A static route is needed so that the IP network number assigned to the remote Ethernet is entered into the routing table. With the Unnumbered Interface model this is not necessary because the remote Ethernet's IP address is known.

13. NETWORK MAGENTA IP ROUTES IP:0.0.0.0 ADDRESS *192.168.1.0*

14. NETWORK MAGENTA IP ROUTES IP:192.168.1.0 MASK *255.255.255.0*

15. NETWORK MAGENTA ISDN DIALLIST ADD

16. NETWORK MAGENTA ISDN DIALLIST I0 *<telephone-number>*

17. NETWORK MAGENTA PPP PAP PEERPASS *<password>*
    This is the password, which the remote router sends when it dials in to this one. The name it must send is MAGENTA because no PEERID is entered.

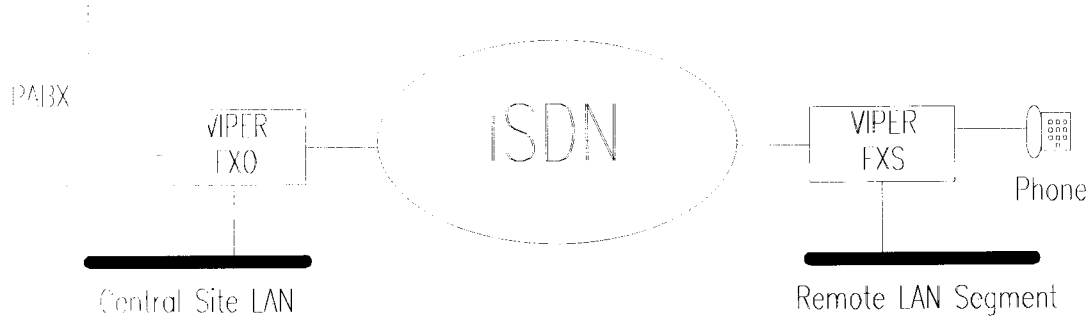
18. NETWORK MAGENTA PPP PAP LOCALPASS <password>

This is the password, which this router sends when it dials out to the remote router. The name sent will be the GLOBAL NAME because no LOCALID is entered.

Once the router has been rebooted, it is ready to dial the remote router MAGENTA, which has IP address 192.168.1.254.

3.4 Example Configuration- Voice over IP

In its simplest form a pair of units are connected to each other via a leased line or ISDN dial up connection. Usually an 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 configuration screens relating to voice features. The first allows the behaviour of the voice 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.

Lines of information are available on the Status screen for you to monitor the status of the voice features.

3.4.1 General Required Information

IP address of each VIPER in the network.
Telephone numbers for phones
User names
Port Types (Direct, numbered)

This example shows how an FXO/FXS pair of units can be used to move two extensions from a central site to a remote site. The Remote LAN is also connected to the Central Site using the same Line.

To achieve the above configuration you would first configure the IP Routing as necessary for the two networks 200.1.1.0 and 200.1.2.0, in each VIPER. IP Prioritisation should be enabled in each unit, and the options for the remote destination set to those shown in the previous section.

You should then select some consistent way of assigning phone numbers to each of the ports. We shall use the last digit of the network number plus the port number. This leads to numbers 11 and 12 for the LOCVIPER unit and 21 and 22 for the REMVIPER unit. Given this layout the VIPER menu for each unit and the common YPAGES list follow.

This screen shows the values in LOCVIPER (200.1.1.254)

```
                    LOCVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     21
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     22

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the values in REMVIPER (200.1.2.254)

```
                    REMVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     11
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     12

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the YPAGES entries, which should be identical at each end.

```
                          xxxVIPER YELLOW PAGES

   Index              Phone No.        IP Address        Port Number
-------------------------------------------------------------------------------
0  Y0                 11               200.1.1.254       1
1  Y1                 12               200.1.1.254       2
2  Y2                 21               200.1.2.254       1
3  Y3                 22               200.1.2.254       2

&  ADD                Add new item
%  DELETE             Delete item
.  QUIT               Previous menu
-------------------------------------------------------------------------------
```

For additional information on voice configuration see section 6.0

4. Features

4.1 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.

4.1.1 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.

4.1.2 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 bits, there is no benefit it doing so, and a lot of equipment does not support it.

4.1.3 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.

4.1.4 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.

4.1.5 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.

4.1.6 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.

4.1.7 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.

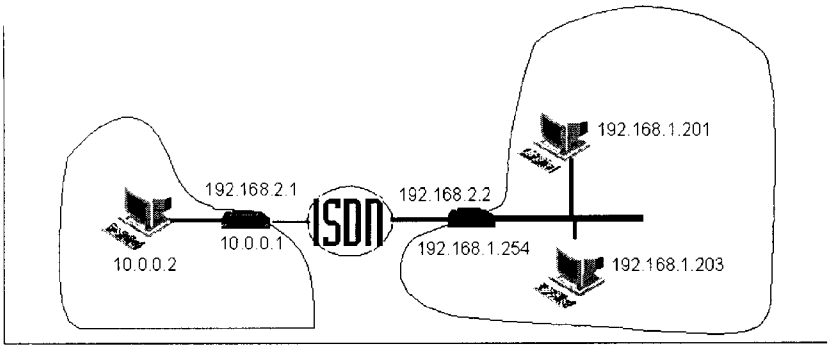
The traditional IP addressing scheme

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.

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:

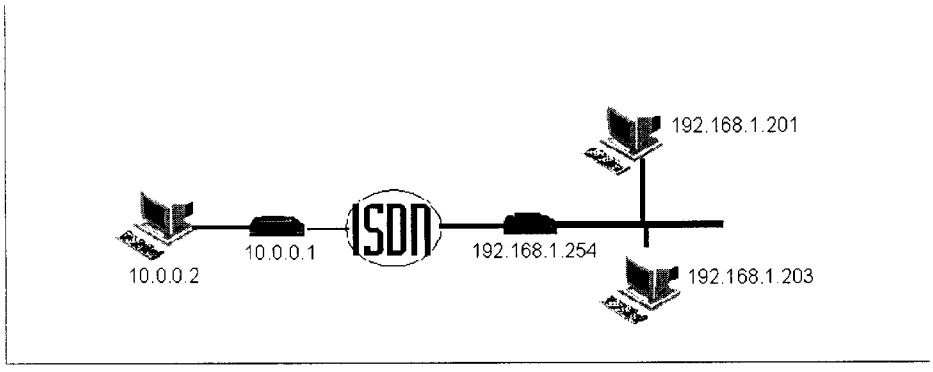
- Each broadcast (such as Ethernet) network needs a network number.
- Each router needs at least one IP address.
- Point-to-point links can reuse an address assigned to the router.

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 is 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



4.1.8 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.

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 4.1.9 - 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.

4.2 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.

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 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.

4.3.1 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".

4.3.2 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".

4.3.3 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.

4.4 Call Charge Limiting

All routers in the PRX 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 PRX 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 are 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.

4.5 ISDN Call Management

All routers in the PRX Range include an ISDN interface of some sort. On the WANHUB product this is optional and can take the form either of Basic Rate ISDN (ISDN2) or Primary Rate (ISDN30). On the other products this takes the form of a single Basic Rate (ISDN2) interface. This section describes the facilities in the routers that allow you to control use of this interface.

4.5.1 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
-------------------------------------------------------------------------------
```

There are also 4 options for the choice of interface on the Wanhub. On the Pluro, VIPER and Solo this option does not appear.

```
   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  BASICPRIMARY     Try basic, then primary if necessary <<<<<<
1  PRIMARYBASIC     Try primary, then basic if necessary
2  BASIC            Use basic rate interface only
3  PRIMARY          Use primary rate interface only

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

The default is shown here, and this will be sufficient for many purposes. They all have possible uses, for example one might use the primary interface for outgoing calls, leaving a basic rate line free for incoming calls.

4.5.2 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.

4.6 IP Express

This section describes the 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.

5. Menu System

All 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.

5.1 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 all the 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:

```
                        MAGENTA 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 MAGENTA
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 MAGENTA
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 MAGENTA
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

COMMAND: ADMIN IPROUTE
```

The heading contains the router name, here MAGENTA (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 IPROUTE` 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 <ENTER>. If you use the shortcut key or the command followed by <ENTER> 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.

5.2 Main Menu

```
                          MAGENTA 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
--------------------------------------------------------------------------------

COMMAND:
```

The main menu has these options:

GLOBAL - System Configuration

This leads to the GLOBAL menu, which configures 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.

5.3 GLOBAL Menu

MAGENTA

	Command	Description	Current Value
0	NAME	Router NAME	MAGENTA
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 (Not Solo/Solo Lite). 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.

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.

5.3.1 GLOBAL ISDN Menu

```
                                MAGENTA

   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 Dialback 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.

5.3.2 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 misconfiguration.

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. These calls are not covered by the charge limiter.

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 startup

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.

5.3.3 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             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.

5.3.4 GLOBAL ISDN MSN *item* Menu

```
                          MAGENTA 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 dialled.

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.

5.3.5 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.

5.3.6 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.

5.3.7 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.

5.3.8 GLOBAL SNMP Menu

```
   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  COMMUNITY        Name
1  MANIP            Manager IP Address                   0.0.0.0          /0
2  ACCESSTYPE       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 coldStart 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.

5.4 NETWORK Menu

```
                              MAGENTA NETWORKS

   Command            Description                          Current Value
-------------------------------------------------------------------------------
0  UNCONFIGURED       !! Invalid !!                        0.0.0.0
1  Eth                Ethernet Interface                   172.16.1.0
2  PURPLE             ISDN No: 01234567897                 158.152.1.0

&  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. It's 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.

5.4.1 NETWORK *name* Menu

```
                          MAGENTA NETWORKS

   Command          Description                          Current Value
--------------------------------------------------------------------------------
0  NAME             Name                                 PURPLE
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 PURPLE
```

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

Returns to the NETWORK menu.

5.5 NETWORK *name* IP Menu

```
                              MAGENTA

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  ENABLE           IP routing                           YES
1  LOCAL            Local IP address                     0.0.0.0
2  REMOTE           Remote IP address (if not Ethernet)  192.168.2.254
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            1in+3out
8  PIPE             IP Express                           disabled
9  FILTBROAD        Filter Directed Broadcast            NO

.  QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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. 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 un-reachable 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 which 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.

5.5.1 NETWORK *name* IP RIP Menu

```
                        MAGENTA 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           Age RIP entries - No IP RIP Spoofing YES
3  RIP-2            (2) Enable Transmission of RIP-2     NO

.  QUIT             Previous menu
-------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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.

5.5.2 NETWORK *name* IP ROUTES

```
                        MAGENTA 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 PURPLE 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 4.1 (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.

5.5.3 NETWORK *name* IP ROUTES *ip* Menu

```
                    MAGENTA 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 PURPLE 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.

5.5.4 NETWORK *name* IP TRANSLATE Menu

```
                              MAGENTA

   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 PURPLE 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 which 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.

5.5.5 NETWORK *name* IP TRANSLATE IN Menu

```
                              MAGENTA

   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 PURPLE 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 which deals with the translations which 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 which deals with the translations which apply to new UDP sessions coming from this network.

QUIT - Previous menu

Returns to the NETWORK *name* IP TRANSLATE menu.

5.5.6 NETWORK name IP TRANSLATE IN TCP Menu

```
                    MAGENTA 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 PURPLE 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.

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

```
                              MAGENTA 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 PURPLE 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 which 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 which defines the values of the address and port which 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.

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

MAGENTA 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 PURPLE 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.

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

```
                    MAGENTA 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 PURPLE 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.

5.5.9 NETWORK *name* IP TRANSLATE IN UDP Menu

```
                    MAGENTA 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 PURPLE 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.

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

```
                              MAGENTA UDP

   Command           Description                          Current Value
-------------------------------------------------------------------------------
0  PATTERN           Pattern to test against
1  NEW               Translated address and port          COPY:COPY

. QUIT              Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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 which 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.

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

```
                              MAGENTA 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 PURPLE IP TRANSLATE IN UDP I:0 PATTERN
```

MINADDR - Minimum address value

MAXADDR - Maximum address value

MINPORT - Minimum port value

MAXPORT - Maximum port value

QUIT - Previous menu

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

5.5.12 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 PURPLE 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.

5.5.13 NETWORK *name* IP PIPE PRIOR Menu

```
                    MAGENTA 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 PURPLE 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.

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

```
          MAGENTA IP PRIORITISATION

   Command           Description                     Current Value
-------------------------------------------------------------------------------
0  ADDRESS           IP Address                      192.16.1.1
1  PORT              Port number                     4000

.  QUIT              Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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.

5.6 NETWORK *name* PPP Menu

```
                                MAGENTA

   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
4  COMPRESS          Link Data Compression                -

.  QUIT              Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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 value 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.

COMPRESS - Link Data Compression

This leads to the NETWORK *name* PPP COMPRESS menu, which allows you to configure the link compression facilities.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

5.6.1 NETWORK *name* PPP PAP Menu

```
                              MAGENTA

   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 PURPLE 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 (*PURPLE* 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.

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.

5.6.2 NETWORK *name* PPP CHAP Menu

```
                                MAGENTA

   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 PURPLE 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 (*MAGENTA* 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 (*PURPLE* 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 PRX 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 PRX 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.

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 PRX 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 PRX 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.

5.6.3 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 PURPLE 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 PRX routers, which do not initiate additional calls.

QUIT - Previous menu

Returns to the NETWORK *name* PPP menu.

5.6.4 NETWORK *name* PPP COMPRESS Menu

```
   Command           Description                          Current Value
-------------------------------------------------------------------------
0  COMPRESSIN        Compression type inbound             None
1  COMPRESSOUT       Compression type outbound            None

.  QUIT              Previous menu
-------------------------------------------------------------------------

COMMAND: NETWORK PURPLE PPP COMPRESS
```

This menu allows you to control the use of Stac compression on each link and separately in each direction. A single compression history is negotiated to each destination and is shared across multiple links when multilink is in operation. Normally you would enable compression in both directions. Hardware Stac compression will be used if the hardware is available. The individual items on the menu are:

COMPRESSIN - Compression type inbound

This value enables Stac Compression on data flowing from this destination

COMPRESSOUT - Compression type outbound

This value enables Stac Compression on data flowing towards this destination

QUIT - Previous menu

Returns to the NETWORK *name* PPP menu.

5.7 NETWORK *name* IPX menu

```
                                MAGENTA

   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  LEARNSAPS         Learn static saps now

.   QUIT              Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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.

5.7.1 NETWORK *name* IPX NETWORKS Menu

MAGENTA

	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 PURPLE 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.

5.7.2 NETWORK *name* IPX ROUTES Menu

```
                    MAGENTA 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 PURPLE 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.

5.7.3 NETWORK *name* IPX ROUTES *route* Menu

```
                    MAGENTA 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 PURPLE 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.

5.7.4 NETWORK *name* IPX SAPS Menu

```
                    MAGENTA 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 PURPLE 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.

5.7.5 NETWORK *name* IPX SAPS *sap name* Menu

```
                      MAGENTA 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 PURPLE IPX SAPS sap name
```

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 cub-menu that allows the service type associated with this SAP to be selected.

QUIT - Previous menu

Returns to the NETWORK *name* IPX SAPS menu.

5.8 NETWORK *name* ISDN Menu

```
                              MAGENTA

   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 PURPLE 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.

5.8.1 NETWORK *name* ISDN DIALLIST Menu

```
                          MAGENTA 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 PURPLE 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 a ISDN number.

QUIT - Previous menu

Returns to the NETWORK *name* ISDN menu.

5.8.2 NETWORK *name* ISDN NUMBER Menu

```
                          MAGENTA 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  INTERFACE        Interfaces to use (ordered choice)   BASICPRIMARY
4  LASTFAILURE      Elapsed time since failed to connect -

.  QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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.

INTERFACE - Interfaces to use (ordered choice)

This option, only present on the WANHUB products, allows the choice of physical interface for dialling out to be controlled.

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.

5.8.3 NETWORK *name* ISDN CLILIST Menu

```
                          MAGENTA CLI LIST

                     Calling Number
-------------------------------------------------------------------------------
0  I0                <blank>
1  I1                0123456789

&  ADD               Add new item
%  DELETE            Delete item
.  QUIT              Previous menu
-------------------------------------------------------------------------------
NOTE: please select the blank entry and enter its value

COMMAND: NETWORK PURPLE 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.

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.

5.9 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).

```
                                MAGENTA

   Command            Description                          Current Value
-------------------------------------------------------------------------------
0  ETHERNET           Ethernet                             NO
1  X21L1              X.21/V.24 leased channel 1           NO
2  X21L2              X.21/V.24 leased channel 2           NO

.  QUIT               Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK PURPLE 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.

X21L1 - X.21/V.24 leased channel 1

This declares that the specified network is connected via port 1 on the optional X.21 or V.24 card.

X21L2 - X.21/V.24 leased channel 2

This declares that the specified network is connected via port 2 on the optional X.21 or V.24 card.

QUIT - Previous menu

Returns to the NETWORK *name* menu.

5.10 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.

```
                                MAGENTA

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  MSPEED           Management port speed                115200
1  ETHERNET         Configure Ethernet
2  VIPER            Configure VIPER Options
3  YPAGES           Configure VIPER Phone Book
4  X21L1            X21 leased line channel 1
5  X21L2            X21 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 which allows you to set the management post speed to one of the following speeds (9600, 19200, 38400, 57600 or 115200)

ETHERNET - Configure Ethernet

This leads to the HARDWARE ETHERNET menu, which allows you to configure the **Ethernet** port.

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 Dialled phone numbers and destination IP Addresses.

X21L*n* - X.21 leased line channel *n*

Each such item leads to a HARDWARE ... X21 menu for that serial line.

QUIT - Previous menu

Returns to the MAIN Menu.

5.10.9 HARDWARE ETHERNET Menu

```
                    MAGENTA 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 configure the Ethernet-specific parameters. The options here are:

ADDRESS - Ethernet address

This shows the Ethernet 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.

5.10.10 HARDWARE VIPER Menu

```
VIPER1 VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     32
2  PORT1OPTS        Port 1 Options                       2
3  PORT2TYPE        Port 2 Functionality                 RXONLY
4  PORT2NO          Port 2 Destination/Escape Prefix     9
5  PORT2OPTS        Port 2 Options                       2

.  QUIT             Previous menu
-------------------------------------------------------------------------

COMMAND: HARDWARE VIPER
```

This menu allows the functionality of the individual VIPER ports to be controlled. The meanings of the various fields alters slightly depending on the VIPER interface you are using. For a full description of these settings see Section 6.1.

PORTnTYPE

This field allows the way the port operates to be controlled. Depending on the type of VIPER interface card you have fitted a different selection of options will be presented. (See Section 6.1)

PORTnNO

Depending on the Option selected in the PORTTYPE field this field is either the Escape sequence to obtain an outside line, or the actual number to dial if a

direct connection has been selected. When the RXONLY option is selected this field is ignored.

PORTnFLAGS

This field allows further control on the features available on each of the ports. On those ports that are capable of dialling into another device (FXO, E&M, and AC15), an option is presented to Pulse Dial out of the port. By default tone dialling is normally used.

If you have an E&M Interface card installed you will be presented with a further option to select between a 2 and 4 wire interface.

5.10.11 HARDWARE YPAGES Menu

```
                          VIPER1 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
```

This menu allows a list of mappings between phone numbers, and IP Address and port numbers to be made.

The commands on this menu are:

An item Yn

This selects an item for you to modify.

ADD - Add new item

This menu creates a new mapping from phone number to IP Address and Port. It is initially blank. You should select the new entry and enter the number required.

DELETE - Delete item

This allows you to delete a mapping.

QUIT - Previous menu

Returns to the HARDWARE menu.

5.10.12 HARDWARE YPAGES Yn Menu

```
VIPER1 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
```

DNUMBER

The number to dial is the phone number that will be recognised.

DESTIP

This field is the IP address of the destination VIPER.

DESTCHAN

This field relates to the VIPER port number on the destination unit. A port number of 0 'zero' may be used if the destination router is an FXS units. In this case all free ports will ring.

5.10.13 HARDWARE ... X21 Menu

```
                    MAGENTA 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 that 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.

5.11 ADMIN Menu

```
                                MAGENTA

   Command           Description                          Current Value
-------------------------------------------------------------------------------
0  TELNET            Telnet Connection
1  PING              Ping
2  ARP               Examine ARP cache                    0 entries
3  IPROUTE           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.

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.

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.

5.11.1 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.

5.11.2 ADMIN ARP *ip* Menu

```
                          MAGENTA 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
5  AGE               time since last updated             (4s)
6  INTERFACE         name of associated interface        (!eth)

. 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).

INTERFACE - name of associated interface
The interface name given here will match the name of a network as defined on the `NETWORK` menu.

QUIT - Previous Menu
Returns to the `ADMIN ARP` menu.

5.11.3 ADMIN IPROUTE Menu

```
                        MAGENTA 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 PURPLE
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 PURPLE
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


COMMAND: ADMIN IPROUTE
```

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 IPROUTE 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

5.11.4 ADMIN IPROUTE ip Menu

```
                        MAGENTA 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 IPROUTE 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

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 IPROUTE 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 IPROUTE 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 IPROUTE menu.

5.11.5 ADMIN IPROUTE *ip* FLAGS Menu

```
                        MAGENTA IP ROUTE FLAGS

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  RIPTX            (T) advertise route via RIP          NO
1  RIPRX            (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 IPROUTE 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 IPROUTE *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.

RIPRX - 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 IPROUTE *ip* menu.

5.11.6 ADMIN IPXROUTE Menu

```
                    MAGENTA 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 MAGENTA
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

COMMAND: ADMIN IPXROUTE
```

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

5.11.7 ADMIN IPXROUTE *ipx* Menu

```
                          MAGENTA 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.

5.11.8 ADMIN IPXROUTE *ipx* ROUTER Menu

```
                        MAGENTA 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.

5.11.9 ADMIN IPXROUTE *ipx* FLAGS Menu

```
                        MAGENTA 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.

5.11.10 ADMIN SAP Menu

```
                          MAGENTA SAP TABLE

   Service Name      Sock Hop Age          Service Type
-------------------------------------------------------------------------------
0  SERVER_1          0451   1 57s          File Server (SLIST source)
1  PAXDATA           8104   2 20s          NetWare 386 or RSPX Remote Console
2  PAXDATA           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

5.11.11 ADMIN SAP *sap* Menu

```
                          MAGENTA SAP LIST
```

```
   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  SNAME            Server Name                          BLACK BOX
1  SADDR            IPX address of server        00000001:00-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 BLACK BOX
```

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 shows as the name of the service, while the value on this menu is shows 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.

5.11.12 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
```

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 form s.l where l indicates the link number in slot s. For the WANHUB, which has 2 slots - WAN Module 1 and WAN Module 2, the slot number may be 1 or 2. For the SOLO the slot number is M.

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.

5.12 STATUS Menu

```
                                Magenta STATUS

--------------------------------------------------------------------------------
   CODEVERSION         P2.196A
   UPTIME              55s
   RAMUSED             13%
   IOCARD              card: None
   DATE                Tuesday 16th December 1997
   TIME                08:31:09 GMT
   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. The items 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.

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 options fitted to the router. This item is repeated as necessary to describe all such lines.

DATE

The current date is shown if it is set, otherwise this line is blank.

TIME

The current time is shown if it is set, otherwise this line is blank.

Q921-?/ISAC-ISDN-BRI

The remaining lines give the status of all ISDN interfaces fitted to the unit.

5.13 STATISTICS Menu

```
                        MAGENTA 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.

5.13.1 WAN STATISTICS Menu

```
                        MAGENTA 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  ISDN2-1 B1       ISDN2-1 B1 Statistics
3  ISDN2-1 B2       ISDN2-1 B2 Statistics
4  ISDN2-2 B1       ISDN2-2 B1 Statistics
5  ISDN2-2 B2       ISDN2-2 B2 Statistics
6  X.21 Link 1      X.21 Link 1 Statistics
7  X.21 Link 2      X.21 Link 2 Statistics
8  X.21 Link 3      X.21 Link 3 Statistics
9  X.21 Link 4      X.21 Link 4 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. The values collected are the same as those reported in the SNMP IF Group.

5.14 DEBUG menu

```
                              MAGENTA

   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.

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.

5.14.1 DEBUG BOUNCE Menu

```
                        MAGENTA 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.

5.15 Menu Index

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
  9 ERASE - Erase all configuration

1 NETWORK - Configure networks, routes etc
 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
    5 RIPMETRIC - Advertised Metric when disconnected
    6 ROUTES - Associated static routes
    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
      1 CHAP - Challenge Handshake Authentication
      2 MPDMAX - No. of Dialup/Backup calls
      3 BANDWIDTH - Bandwidth on demand
      4 COMPRESS - Link Data Compression
  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
      4 ROUTES - Associated static routes
      5 SAPS - Associated static saps
      6 LEARNROUTES - Learn static routes now
      7 LEARNSAPS - Learn static saps now
  4 ISDN - ISDN configuration
      0 DIALLIST - List of numbers to dial
      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 SLOT1 - Select channels for slot 1
        1 TAX21 - Dual TA/X.21
      2 SLOT2 - Select channels for slot 2
        1 TAX21 - Dual TA/X.21

2 HARDWARE - Configure Hardware
  0 ETHERNET - Configure Ethernet
```

1 SLOT1 - Slot 1 configuration
  0 MSPEED - Management port speed
  2 TAX21 - Dual TA/X.21
2 SLOT2 - Slot 2 configuration
  0 MSPEED - Management port speed
  2 TAX21 - Dual TA/X.21

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

6 WANSTATS - Recent WAN Statistics

7 DEBUG - Debugging facilities

6. Optional Features

6.1 Voice Over IP

.

The VIPER unit is available in four variants, depending on the interface presented to the external telephonic equipment. Three variants (FXO, E&M and AC15) are for connection to the telephone exchange, while the fourth (FXS) is for the direct connection of telephones and fax machines.

In its simplest form a pair of units are connected to each other via a leased line or ISDN dial up connection. Usually an 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 the new features. 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.

6.1.1 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.

```
                              VIPER2 STATUS

--------------------------------------------------------------------------------
   CODEVERSION        V3.40A  27 Nov 14:31
   UPTIME             50m3s
   RAMUSED            14%
   IOCARD             card: None


   VIPER-PVM2         FXS (SLIC) Software Version 120
   VIPER-PVM2-CH 1    On Hook
   VIPER-PVM2-CH 2    On Hook
   Q.921-?            State: 4
+    NEXT PAGE

.  QUIT               Previous menu
--------------------------------------------------------------------------------


COMMAND: STATUS
```

6.1.2 Configuring the Ports

The following VIPER menu accessible from the HARDWARE menu allows the functionality of the individual ports to be controlled.

```
                     VIPER1 VIPER PORT CONFIGURATION

   Command            Description                          Current Value
--------------------------------------------------------------------------------
0  PORT1TYPE          Port 1 Functionality                 DIRECT
1  PORT1NO            Port 1 Destination/Escape Prefix     32
2  PORT1OPTS          Port 1 Options                       2
3  PORT2TYPE          Port 2 Functionality                 RXONLY
4  PORT2NO            Port 2 Destination/Escape Prefix     9
5  PORT2OPTS          Port 2 Options                       2


.  QUIT               Previous menu
--------------------------------------------------------------------------------


COMMAND: HARDWARE VIPER
```

The PORTnOPTS entry leads to the following screen, which allows various optional features to be enabled on the associated ports.

```
                    VIPER1 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       YES

.  QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: HARDWARE VIPER PORT1OPTS
```

The Single character shown in brackets is displayed in the Current Value of the Menu above to provide an abbreviated version of the options you have selected.

FXS

On the FXS the PORTOPTS field is not used. PORTTYPE field can be set to one of the following

```
                    VIPER2 VIPER PORT TYPE

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  RXONLY           Receive Calls Only
1  DIRECT           Permanently Mapped to Supplied Number
2  OUTSIDE          Permanently Mapped to ISDN Line
3  DIALOUT          Dial Out -  Esc to Outside Line      <<<<<<

.  QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: HARDWARE VIPER PORT1TYPE
```

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 dialtone. 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.

OUTSIDE - Permanently Mapped to ISDN Line

This option simulates the action of the phone ports on the current range of PRX routers. By enabling this option when the phone is picked up it is directly connected to a free ISDN channel. A call can then be placed over the ISDN network, maybe to a standard PRX router. No compression is used in this situation, the call will occupy the whole 64k bandwidth and the channel cannot be used for data while the call is up.

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.

FXO

On the FXO unit the PORTOPTS field can be used to select that numbers are pulse dialled into the exchange line, rather than the default tone dialling. The following options are available for the PORTTYPE field.

```
                    VIPER1 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 PORT1TYPE
```

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.

E&M - AC15

On the E&M and AC15 units the PORTOPTS field can be used to select that numbers are pulse dialled into the exchange line, rather than the default tone dialling. Also on the E&M unit there is also the option to present a 2 wire voice interface to the exchange rather than the usual 4 wire interface. 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.

```
                    VIPER1 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 of 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.

6.1.3 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.

```
                          VIPER1 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.

```
                      VIPER1 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.

6.1.4 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 done by using the IP Prioritisation mechanism already present in PRX routers. You should read Section 4.? (PRX 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.

```
                                VIPER1

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.

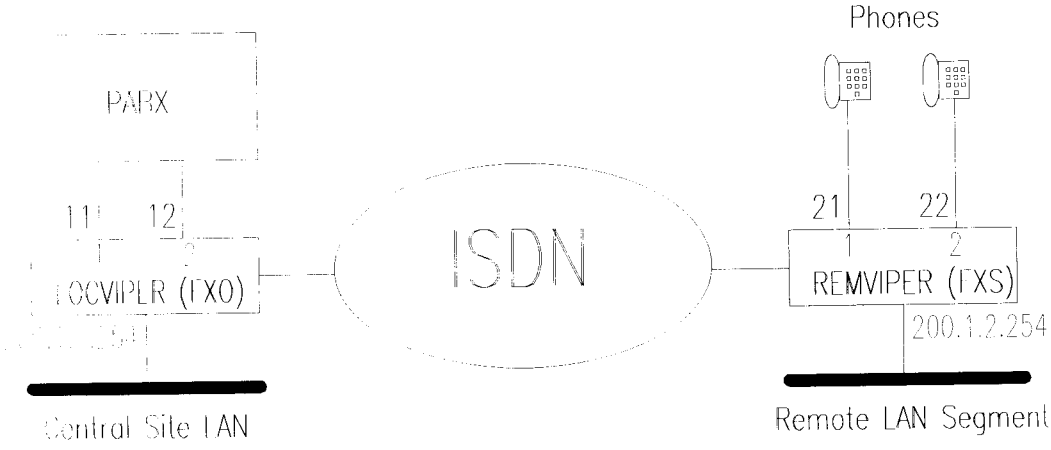
```
                              VIPER1 PRI

   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 VIPER3 IP PIPE PRIOR
```

If you are planning to route the voice traffic across Ethernet the same values should be used on the Ethernet port.

6.1.5 Example Configurations

Remote Office Operation

This first example shows how an FXO/FXS pair of units can be used to move two extensions from a central site to a remote site. The Remote LAN is also connected to the Central Site using the same Line.



To achieve the above configuration you would first configure the IP Routing as necessary for the two networks 200.1.1.0 and 200.1.2.0, in each VIPER. IP Prioritisation should be enabled in each unit, and the options for the remote destination set to those shown in the previous section.

You should then select some consistent way of assigning phone numbers to each of the ports. We shall use the last digit of the network number plus the port number. This leads to numbers 11 and 12 for the LOCVIPER unit and 21 and 22 for the REMVIPER unit. Given this layout the VIPER menu for each unit and the common YPAGES list follow.

This screen shows the values in LOCVIPER (200.1.1.254)

```
                    LOCVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     21
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     22

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the values in REMVIPER (200.1.2.254)

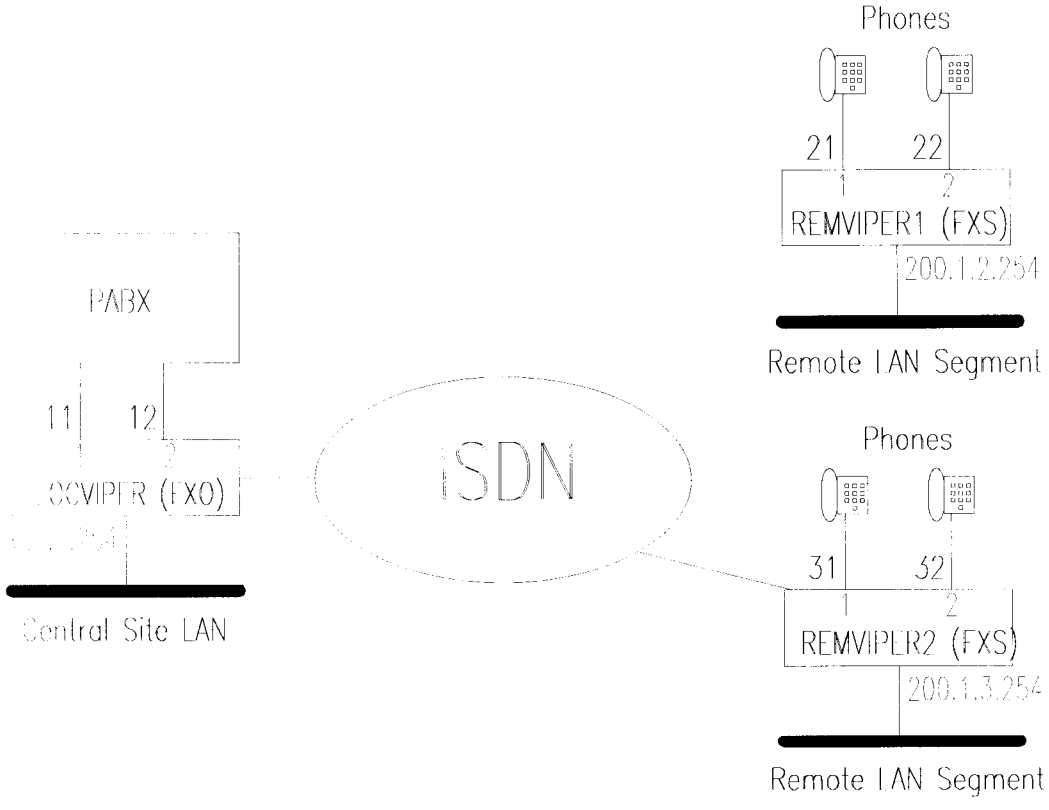
```
                    REMVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     11
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     12

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the YPAGES entries, which should be identical at each end.

```
                          xxxVIPER YELLOW PAGES

   Index                Phone No.        IP Address        Port Number
-------------------------------------------------------------------------------
0  Y0                   11               200.1.1.254       1
1  Y1                   12               200.1.1.254       2
2  Y2                   21               200.1.2.254       1
3  Y3                   22               200.1.2.254       2

&  ADD                  Add new item
%  DELETE               Delete item
.  QUIT                 Previous menu
-------------------------------------------------------------------------------
```

Multiple Remote Offices

This example shows a more complex set-up with two remote units and one central unit.



In this example 1 PABX extension will be routed to the first phone on each remote site. This leaves the second phone on each site available for other uses. Using the same phone numbering technique as in the last example the following configuration could be set up.

This screen shows the values in LOCVIPER (200.1.1.254)

```
                    LOCVIPER VIPER PORT CONFIGURATION

   Command           Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE         Port 1 Functionality                 DIRECT
1  PORT1NO           Port 1 Destination/Escape Prefix     21
2  PORT2TYPE         Port 2 Functionality                 DIRECT
3  PORT2NO           Port 2 Destination/Escape Prefix     31

.  QUIT              Previous menu
-------------------------------------------------------------------------------
```

This screen shows the values in REMVIPER1 (200.1.2.254)

```
                    REMVIPER1 VIPER PORT CONFIGURATION

   Command           Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE         Port 1 Functionality                 DIRECT
1  PORT1NO           Port 1 Destination/Escape Prefix     11
2  PORT2TYPE         Port 2 Functionality                 DIALOUT
3  PORT2NO           Port 2 Destination/Escape Prefix     9

.  QUIT              Previous menu
-------------------------------------------------------------------------------
```

This screen shows the values in REMVIPER2 (200.1.3.254)

```
                    REMVIPER2 VIPER PORT CONFIGURATION

   Command           Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE         Port 1 Functionality                 DIRECT
1  PORT1NO           Port 1 Destination/Escape Prefix     12
2  PORT2TYPE         Port 2 Functionality                 DIALOUT
3  PORT2NO           Port 2 Destination/Escape Prefix     9

.  QUIT              Previous menu
-------------------------------------------------------------------------------
```

This screen shows the YPAGES entries, which should be identical in all units.

```
                          xxxVIPER YELLOW PAGES

   Index             Phone No.        IP Address        Port Number
-------------------------------------------------------------------------------
0  Y0                11               200.1.1.254       1
1  Y1                12               200.1.1.254       2
2  Y2                21               200.1.2.254       1
3  Y3                22               200.1.2.254       2
4  Y4                31               200.1.3.254       1
5  Y5                32               200.1.3.254       2

&  ADD               Add new item
%  DELETE            Delete item
.  QUIT              Previous menu
-------------------------------------------------------------------------------
```

With this configuration the first phone at each remote site is directly connected to the central site. The second phone can be used for outside calls by dialling 9 and using the second ISDN channel. Alternatively it can call any of the numbers in its Yellow Pages list, providing you with a distributed PABX system.

A user who picks up the second phone on REMVIPER2 (200.1.3.254) would get the following when he dials each of the following numbers

11

Connected to the PABX extension that is reserved for REMVIPER1. In this way if the other remote site is not using its extension at the moment, this phone can use it. You will get an engaged tone if it is in use. (Actually doing this could prevent users at the other remote site using their VIPER system. In this case you may wish to remove the '11' entry from the YPAGES in REMVIPER2 and the '12' entry from the YPAGES in REMVIPER1 to prevent this from being allowed.)

12

Connected to the PABX extension that is reserved for the other phone at this site. You will get the engaged tone if the other phone is in use but otherwise you can use the phone line for the moment. In this way the two phones at the second remote site can share the central site extension.

21

Call up phone 1 on the other remote site. Depending on how the IP routing between the two remote sites is set up this call may go indirectly through the central site, or may go directly.

22

Call up phone 2 on the other remote site. This will work even while both phones 21 and 31 are connected to the central site, so that you get an additional line between the two remote sites for free.

31

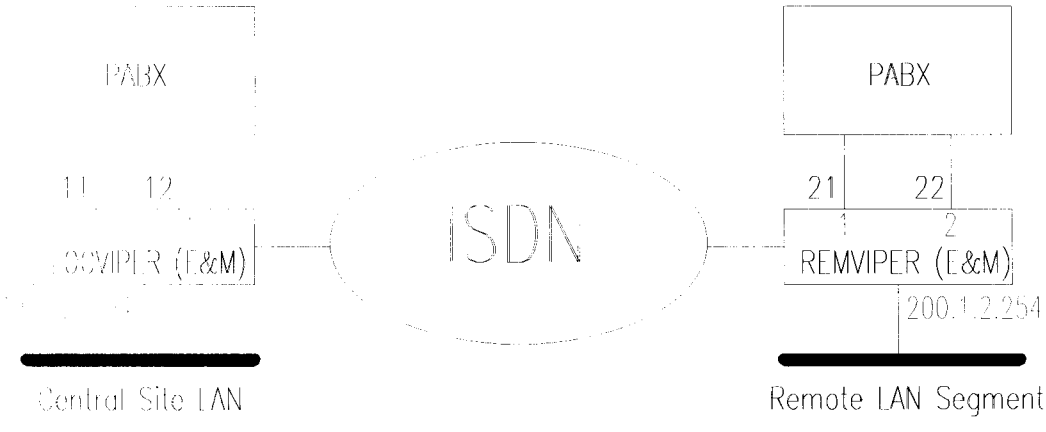
The other phone on the same site will ring if it is not busy.

32

You will get engaged tone since you have dialled yourself.

Connecting Remote E&M Exchanges

This final example shows how two exchange lines can be forwarded across a WAN link, connecting together two remote E&M Exchanges.



This screen shows the values in LOCVIPER (200.1.1.254)

```
                    LOCVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     21
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     22

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the values in REMVIPER (200.1.2.254)

```
                    REMVIPER VIPER PORT CONFIGURATION

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  PORT1TYPE        Port 1 Functionality                 DIRECT
1  PORT1NO          Port 1 Destination/Escape Prefix     11
2  PORT2TYPE        Port 2 Functionality                 DIRECT
3  PORT2NO          Port 2 Destination/Escape Prefix     12

.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

This screen shows the YPAGES entries, which should be identical at each end.

```
                          xxxVIPER YELLOW PAGES

   Index            Phone No.       IP Address        Port Number
-------------------------------------------------------------------------------
0  Y0               11              200.1.1.254       1
1  Y1               12              200.1.1.254       2
2  Y2               21              200.1.2.254       1
3  Y3               22              200.1.2.254       2

&  ADD              Add new item
%  DELETE           Delete item
.  QUIT             Previous menu
-------------------------------------------------------------------------------
```

6.2 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.

6.2.1 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.

6.2.2 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.

```
                                FR_LOCAL

    Command          Description                          Current Value
0   ETHERNET         Ethernet                             NO
1   X21L1            X.21/V.24 leased channel 1           NO
2   X21L2            X.21/V.24 leased channel 2           NO
3   FRL1             X.21/V.24 Frame Relay Address 1      17
4   FRCIR1           X.21/V.24 Frame Relay CIR 1          32000
5   FRL2             X.21/V.24 Frame Relay Address 2      0
6   FRCIR2           X.21/V.24 Frame Relay CIR 2          0

.   QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: NETWORK REMOTE 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.

6.2.3 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 don'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.

6.3 Hardware Compression

Viper *plus* units contain an additional co-processor to handle data compression. They also have additional RAM that allows the units to run much faster that there standard counterpart. In order to support the hardware compression two additional configuration items appear in the Hardware Menu, as shown below.

```
                                VIPER_PLUS

   Command          Description                          Current Value
-------------------------------------------------------------------------------
0  MSPEED           Management port speed                115200
1  ETHERNET         Configure Ethernet
2  VIPER            Configure VIPER Options
3  YPAGES           Configure VIPER Phone Book
4  STACPERF         Hardware Compression Performance     2
5  STACMIN          Minimum H/W Compression Size         64
6  X21L1            X.21/V.24 leased line channel 1
7  X21L2            X.21/V.24 leased line channel 2

.  QUIT             Previous menu
-------------------------------------------------------------------------------

COMMAND: HARDWARE
```

STACPERF - Hardware Compression Performance

This field controls the speed of the compression relative to its performance. Higher values will give improved compression ratio at the expense of speed. Lower values will return worse compression ratio, but introduce lower delays. Values in the range 1 to 16 are valid.

The default value 2 appears to give the best compromise and matches the value used by other units that use software compression.

STACMIN - Minimum H/W Compression Size

This field allows you to select what is the smallest frame that will be passed to the compression hardware. Since compression always adds additional delay to frames passing through the router you may choose to pass small frames uncompressed to improve response for traffic from Terminal Servers for example. You may also wish to adjust this value depending on the link speed you are using.

Frames using the IP Prioritisation feature will not be compressed. This reduces delays and would be a waste of time if the frames already contain compressed voice.

Status Information

Additional status information relating to hardware compression also appears on the Status Screen.

```
                              VIPER_PLUS

--------------------------------------------------------------------------------
   CODEVERSION        VP3.32     18 Dec 1998
   UPTIME             3h4m
   RAMUSED            5%
   IOCARD             card: Dual X.21
   DCC-9711           Stac Compression: 4 histories  2 performance


   VIPER-PVM2         E&M Software Version 120
   VIPER-PVM2-CH 1    Idle
   VIPER-PVM2-CH 2    Idle
+    NEXT PAGE

.  QUIT               Previous menu
--------------------------------------------------------------------------------

COMMAND: STATUS
```

The DCC-9711 information line relates the performance value you have set above, and the number of histories indicates the number of simultaneous links that hardware compression may be applied to. Since the Pluro can only support 3 links, all links may use hardware compression.

The 'P' in the CODEVERSION number indicates that you have a unit with the Hardware compression and Additional RAM features.

There is no separate option to enable hardware compression. When you enable Stac compression on a link, from PPP menu. If you have hardware compression fitted in your unit then it will be used. If not software compression will be used.

Hardware and Software compression will inter-work.

7. 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.

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.

Datagram
An 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 PRX 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.

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 though 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" if 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 and 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.

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".

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 PRX 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 PRX 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 PRX routers to support **RIP** and **SYSLOG**. UDP is defined in "RFC-768".

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.

WAN Wide Area Network

A network which covers a large area, usually at relatively low speed.

X.21

A standard type of serial port.

8. Upgrading and Diagnostics

8.1 Monitor Commands

? [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

cnitem object-id last-ptr
Get next config item in object **object-id** where **last-ptr** is 0 or the last value returned.

cnobject 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 **b**yte, **w**ord or **l**ong **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, ipxspoof, 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

8.2 Installing New Software in Routers

Firstly you will need a terminal communications package that is capable of 115200 bps. 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 you terminal package to 115200 bps. You should now see the menu screens correctly again.

Now go into the Monitor, using the DEBUG/MONITOR options. Once at the monitor '>' prompt type '+' to get into the debugger. You should now see a 'debug>' prompt.

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. The menus will now be presented at 115200. You can now go into the menus and reset the management port speed back to its original value, if you do not wish to continue operating at this high speed.

8.3 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.

9. Specification

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.