

CASE Multi Access Router Technical Manual.

1	Index	
2	Multi Access Router Application Examples	4
2.1	Introduction to application examples.	4
3	Unpacking your Multi-Access Router	8
4	Introduction	9
4.1	Platform hardware specification	9
4.2	Front panel	9
4.3	Rear panel	9
4.3.1	VGA screen & Keyboard	9
4.4	Power supply	10
4.4.1	Power up	10
4.4.1.1	Power up to prompt time	10
4.4.2	Power down	10
4.5	Software packages/Features	10
5	Management	11
5.1	Communications	11
5.1.1	By Local serial terminal	11
5.1.2	By IP Network device	11
5.1.2.1	Security	11
5.1.3	Logging on	11
5.1.4	Logging off	11
5.1.5	Changing password	11
5.1.6	Password rules	11
5.1.7	Configuration file	12
5.1.8	Configuration file execution	12
5.1.8.1	Package take up of changes	12
5.1.9	Remote configuration file loading	12
5.1.10	Configuration file editor	12
5.1.11	Configuration file syntax	12
5.1.11.1	File sections	12
5.1.11.2	Commands	12
5.1.12	Saving changes to flash	12
5.1.12.1	Controlling flash usage	13
5.1.13	Restoring default	13
5.2	Setting IP address	13
5.2.1	Example for dhcp	13
5.2.2	Example for static	13
5.2.2.1	Gateway	13
5.3	Setting date & time	13
5.4	Man pages	13
6	Hardware Option installation	14
6.1	RS232 synchronous ports	14
6.1.1	Channel identity	14
6.1.2	LEDS	14

6.1.3	RJ48 Pin-out	14
6.1.4	D25 Pin-out	14
6.1.5	External clock	14
6.1.6	Data rates	14
6.2	HDLC RS422 (X21) & RS232 synchronous ports	15
6.2.1	RS232 RJ48 Pin-out	15
6.2.2	X21 RJ48 Pin-out	15
6.2.3	HDLC Data rates	15
6.3	TDM RS422 (X21) & RS232 synchronous ports	15
6.3.1	TDM Data rates	15
6.4	PCI ADSL	16
7	Software options	17
7.1	Basic configuration	17
7.2	HDLC over IP	17
7.2.1	Synchronous ports	17
7.2.2	Functional description	17
7.2.3	Performance	17
7.2.4	IP Port number	17
7.2.5	Diffserv	17
7.2.6	BIST	17
7.2.7	Configuration file syntax	18
7.2.7.1	Examples	18
7.2.7.2	Configuration operation	18
7.2.8	IP link overhead	18
7.2.9	Status	19
7.2.10	Ifconfig / SNMP Status	19
7.2.11	DCX Extended Window Mode	19
7.3	TDM over IP	20
7.3.1	Synchronous ports	20
7.3.2	Functional description	20
7.3.2.1	Clocking	20
7.3.2.2	Interface card LED's, IP link performance	20
7.3.3	Performance	20
7.3.4	IP Port numbers	20
7.3.5	Configuration file syntax	21
7.3.5.1	Examples	21
7.3.6	Status	21
7.3.7	Ifconfig / SNMP Status	22
7.3.8	IP link overhead	22
7.4	PCI ADSL	23
7.4.1	Configuration	23
7.4.2	Status	23
7.4.3	Console Messages	23
7.5	SNMP Agent	23
7.5.1	Configuration	23
7.5.1.1	Enterprise Number	23
7.6	IPTables (Firewall) & NAT	23
7.6.1	Configuration	23
7.6.1.1	File image	23
7.6.1.2	Command lines	23
7.6.1.3	Script files	24
7.6.2	NAT Configuration	24
7.6.2.1	Incoming from public	24
7.6.2.2	Outgoing to public	24

7.6.3	Mangle for TOS	24
7.6.4	Firewall	24
7.7	VLANS	25
8	Ancillary packages	25
8.1	IProute2	25
8.1.1	Configuration	25
8.2	Quagga	25
8.2.1	Configuration	25
8.3	OpenVPN	25
8.3.1	Configuration	25
8.4	L2TPD	25
8.4.1	Configuration	25
9	Software maintenance	26
9.1	Identification	26
9.2	Flash drive replacement	26
9.3	Updates	26
9.3.1	Update files	26
9.3.1.1	Copying files	26
9.3.2	Changes to configuration file	26
10	Appendix A useful commands	27
11	Appendix B CMOS settings	28
12	Appendix C Example configuration file	29

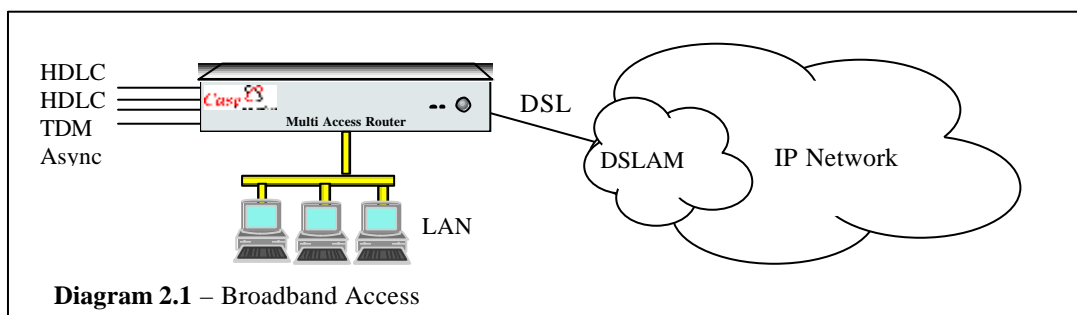
2 Multi Access Router Application Examples

2.1 Introduction to application examples.

The Multi-Access Router is a powerful router platform, which supports a wide range of option cards and a comprehensive software suite. In its basic form the Multi Access Router is a router with the ability to route IP over Wan service Broadband services or Ethernet. When Case Communications cards are installed the Multi-Access Router is also capable of supporting HDLC over IP or TDM Over IP.

2.2 The Multi-Access Router as a broadband router.

The Multi Access Router has the option of being fitted with internal DSL cards, allowing it to connect to a Broadband service. Within the UK most current broadband services are provided via ADSL, however as the Broadband card is a sub-module of the Multi Access Router it may also be possible to integrate other forms of DSL, such as ADSL 2 Plus, G.SHDSL, G.SHDSL bis and V.SHDSL as these systems emerge. Diagram 2.1 below shows the Multi Access Router connecting to an IP network via broadband.



2.3 The Multi-Access Router using MLPPP and multiple broadband links

The Multi-Access Router has the ability to run Multi-Link Point to Point Protocol (MLPPP) to aggregate bandwidth over the broadband connection. This requires the end system to also support MLPPP. The end system could be another Case Communications Multi-Access Router or a third party device, which supports MLPPP, such as a router or server. Some Internet Service providers support MLPPP, therefore it is possible to increase your Internet rates by using multiple Broadband Links to your ISP.

Diagram 2.2 below shows the Multi Access Router running MLPPP to communicate with a second Multi Access Router over an IP network

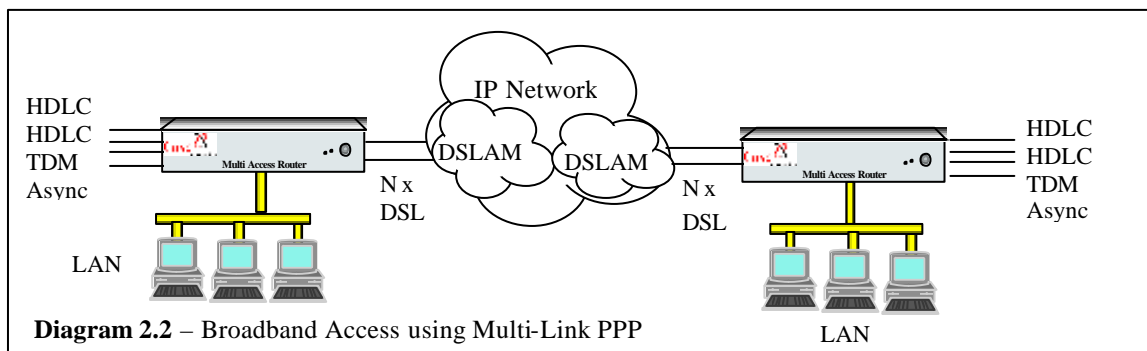
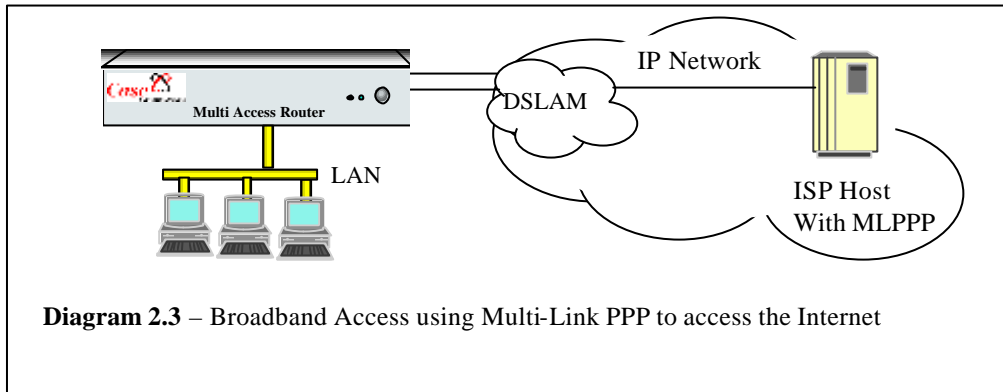
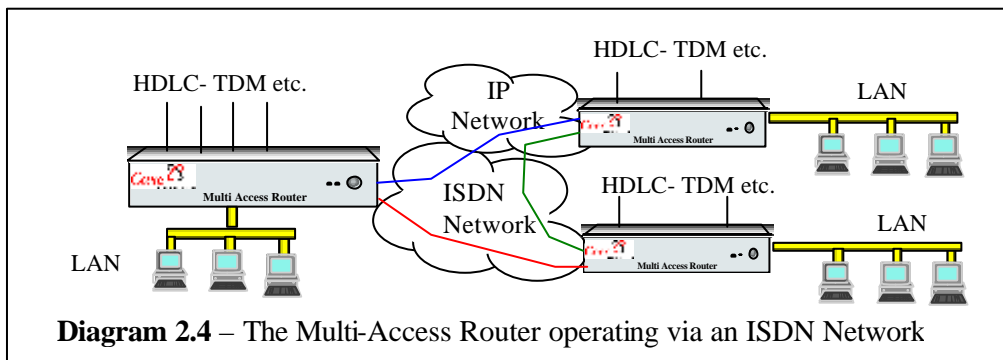


Diagram 2.3 below shows the Multi Access Router being used to communicate with an Internet Service providers server, using Multi-Link PPP. This provides N x the standard data rate with N being the number of DSL links in use. Up to 4 DSL links maybe fitted to the Multi Access Router.



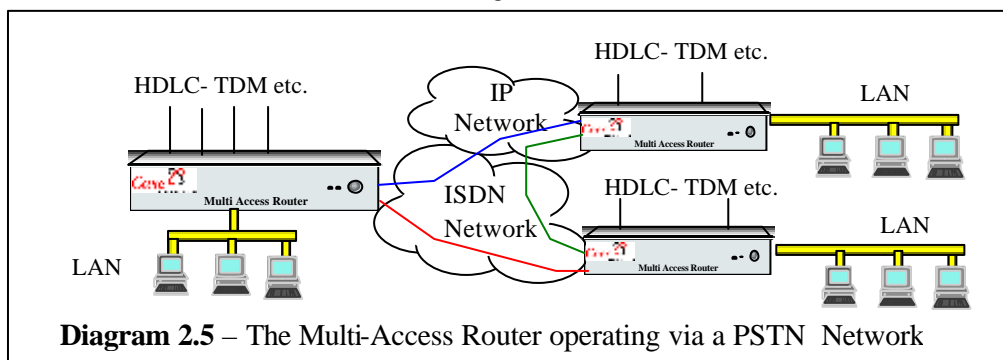
2.4 The Multi Access Router using ISDN.

The Multi Access Router can be fitted with a Basic rate ISDN card, making it into an ISDN Router. The MAR can connect to the Internet via ISDN or to other routers. Diagram 2.4 shows the MAR connected to another MAR via an ISDN connection.



2.5 Multi Access Router using dial up modems

The Multi-Access Router can use the PSTN (Public Switched Telephone Network) to connect to the Internet or to another router as shown in diagram 2.5 below.



2.6 Wide Area Network options.

The Multi-Access Router can also support a range of Wide Area cards from the Case Communications IS range. These include E1 / T1 and serial cards. For more information please contact your Case Communications office or local reseller.

2.7 Additional Ethernet ports

It is also possible to install additional Ethernet ports into your Multi-Access Router. Please contact your local Case Communications office or reseller for more details of the additional Ethernet cards.

2.8 HDLC Over IP

The Multi Access Router supports the Case Communications Quad HDLC cards, which allow the Router to transport HDLC Over an IP network. In order to transmit HDLC Over IP its necessary to install a Case Communications 4 port HDLC card in one of the Multi Access Routers two PCI slots.

The card may be installed in either slot, while the second slot can be used to support any of the other option cards, such as ISDN, ADSL, WAN or modem etc.

2.8.1 Models of QHDLC cards

Note at this time the Multi Access Router currently only support one HDLC card.

There are two flavours of the Quad HDLC card

- PCIQHDLC232 – 4 port RS 232 fixed port configuration (X6000 230205)
- PCIQHDLC232/422 – 4 port card supporting both RS 232 & 422. (X6000-230207)

Each card has its type silk screen printed on the card.

Each HDLC port can go to a different destination on the IP Network, therefore its possible to build fully meshed networks using the Multi Access Router and HDLC card. The HDLC card operates in a master / slave relationship, with the Master being designated the 'server' and the slave being the 'client'

A 'Client' port can only talk to a 'Server' port, but each quad card can support both client and server ports.

2.8.2 Fixed Ip Address

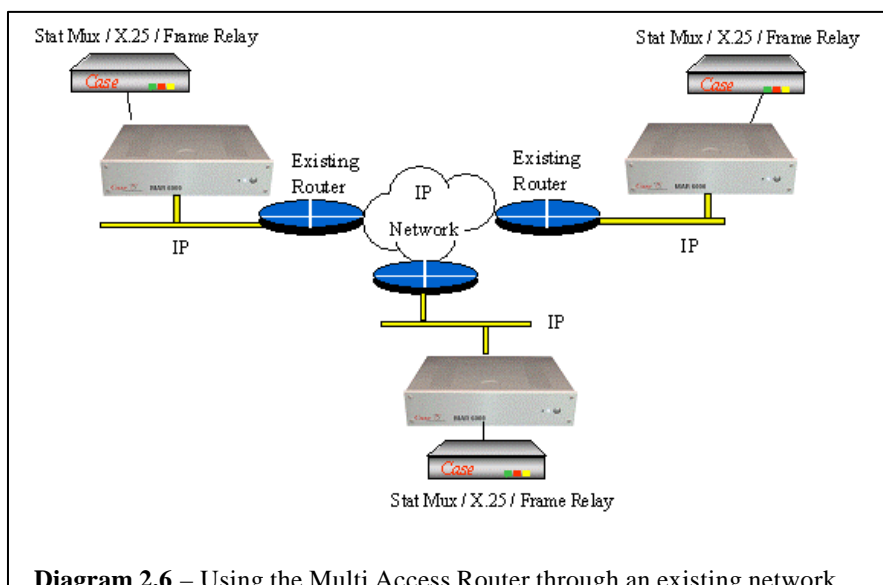
It is necessary for the Server port to be on a fixed IP address in order for the client to be able to find that port on the network. If using the Multi-Access Router via the Internet then your ISP (Internet Service Provider) must provide you with a fixed IP Address for your host site.

You should work with an ISP that's able to provide you with a guaranteed Quality of Service, in order to ensure your HDLC traffic is given priority over less time critical traffic.

2.8.3 HDLC Over IP Application Examples.

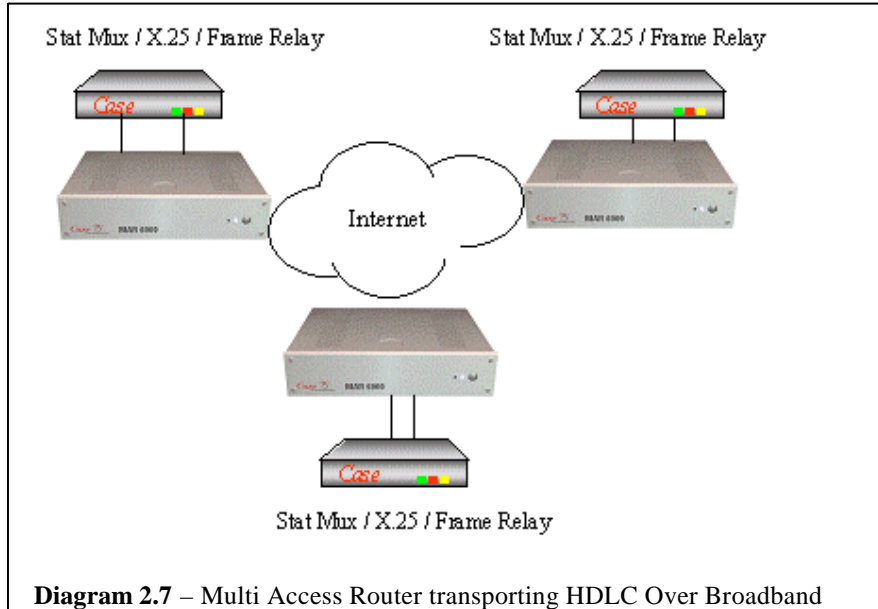
There are multiple ways in which you're Multi Access Router can be used to transmit HDLC Over IP. If you have an existing IP network the easiest way to use the Multi Access Router is to use the Multi Access Router as a outgoing port into your existing network.

Diagram 2.6 below provides an overview the Multi Access Router operating via an existing IP Network.



NB. When operating through third party routers do not forget to configure the local area networks outgoing address in the Multi-Access Router

Its also possible to connect to a network using 'Broadband' and to use the Multi Access Router as a Broadband Router as well as a transport product. Diagram 2.6 below shows three Multi Access Routers being used to connect HDLC based services over the Internet.

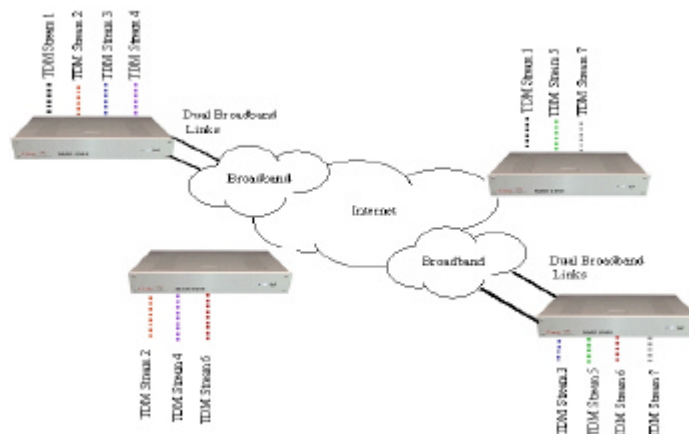


2.9 Time Division Multiplexing Over IP

The Multi Access Router supports the Case Communications Quad cards, which allow the Router to transport any serial protocol Over an IP network using transparent Time Division Multiplexing technology. In order to transport the serial devices over the Multi Access Router requires CQHDLC 232/422 card fitted with different firmware. The CQHDLC RS232 is not suitable for TDM Over IP.

As with HDLC over IP, TDM over IP requires one port to be designated as a server and the other end of the link has to be designated as a client. Clients make 'calls' to Servers, therefore servers must be on fixed IP Addresses. If operating via the Internet and an ISP, your ISP must assign you a fixed IP address and guarantee your Multi Access Router Quality of Service.

Within the Quad Card any port can be designated as a Client or Server. Diagram 2.8 below provides an example of TDM Over Broadband and IP



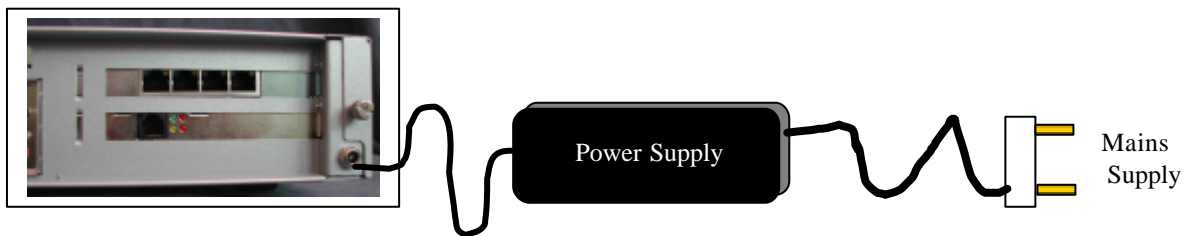
3 Unpacking your Multi-Access Router

Unpack your Multi Access Router and inspect the contents of the package. The following items should be present.

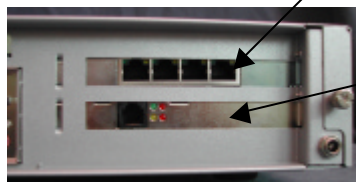
- **Multi Access Router Chassis** – Black or Silver



- **Power Supply Brick** – This may be 230 Vac mains or 24 volt DC. This has a flying lead which connects to the Multi Access Router, at the right hand side of the rear.



- **Option card** – HDLC or TDM or WAN, Broadband or Ethernet



ADSL card, Ethernet card, Modem card, WAN card or ISDN card

- Product documentation
- Option card leads – HDLC or TDM

4 Introduction

The product is able to provide a variety of functions depending on what interface cards are fitted and how the software is configured. For this reason the manual is divided into a generic section first that describes features common to all options then later there are sections for the different hardware & software options.

4.1 Platform hardware specification

- PCI slots 2
- Processor Via C3 (x86) 600Mhz convection cooled
- Memory 256Mbytes PC133 DRAM & 256Mbytes IDE flash drive
- Power Universal AC < 50 Watts
- Cooling Single chassis fan with monitor
- Performance Approx. 30Mbit/sec forwarding rate from Ethernet to Ethernet

4.2 Front panel

The front panel has the following components

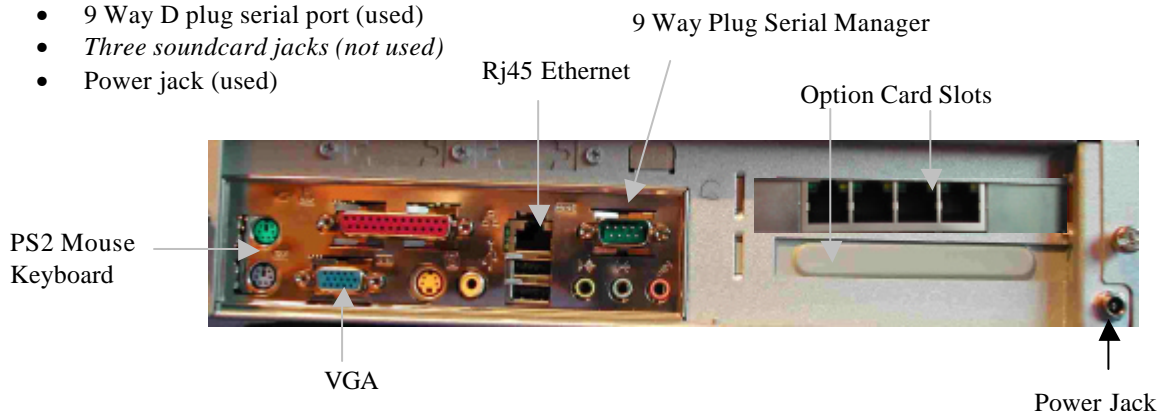
- Power on pushbutton
- Blue power led
- Orange storage activity LED



4.3 Rear panel

The rear panel has the following connectors from rear left to right

- PS2 Mouse & Keyboard (see below)
- VGA screen (see below)
- Parallel printer port (*not used*)
- Svideo & Phono Video (*not used*)
- RJ45 10/100 Ethernet (used)
- Two USB ports
- 9 Way D plug serial port (used)
- Three soundcard jacks (*not used*)
- Power jack (used)



4.3.1 VGA screen & Keyboard

The MAR will support the connection of these devices though they are non-preferred, in particular the keyboard can be used to re-boot the system without being logged on. Also when running at high bit rates updates to the VGA screen can cause link errors.

4.4 Power supply

The power supply (external) is fitted with a UK 13 Amp plug and able to operate over the range 100 to 240V AC 50/60Hz. Connect the output lead of the power supply to the input jack of the MAR located on the rear panel. The connector is not rated for use as a power switch. Alternatively a fully floating 24VDC input PSU module is available connected to the MAR in the same manner.

4.4.1 Power up

Press the button on the front panel, the blue light should come on. Normally this will not be necessary assuming the BIOS is configured according to the appendix the unit will power up immediately on application of power.

4.4.1.1 Power up to prompt time

Assuming DHCP with a fast server it takes approximately 85 (or 105 if DHCP fails) seconds from power up to boot prompt, routing operations will also be restored in this time.

4.4.2 Power down

Press the button on the front panel for several seconds until the blue light extinguishes or remove the supply.

If the button is used to power down it will have to be used again to power up, removal/restoration of the supply will not cause an automatic power up if the button has been used to power down.

4.5 Software packages/Features

- SSH & SCP Provides secure means of management
- HDLC over IP Provides transport for HDLC protocols including X25 over IP networks
- TDM over IP Provides transport for bitstream over IP networks
- SNMP agent Provides support for SNMPv1,2&3 MIBII
- IPtables Provides stateful firewall & Network Address Translation
- VLANS Provides virtual interfaces
- IProute2 Provides bandwidth control
- Quagga Provides OSPFv2, OSPFv3, RIP v1 and v2, RIPv3 and BGPv4 routing
- OpenVPN Provides encrypted tunnels
- L2TPD Provides PPP over IP networks

5 Management

Management options are controlled by a single configuration file, called 'configuration' located in the Case users home directory. This file may either be edited interactively on the MAR or downloaded using SCP (Secure CoPy). It is important to explicitly save changes (see Saving changes section).

5.1 Communications

Communications may either be local by attachment of a local terminal or remote over a network.

5.1.1 By Local serial terminal

A local terminal may need to be attached in order to configure the Ethernet address before configuration can be performed via the Ethernet. In this case a suitable device may be attached to the 9 way D-type plug on the rear panel. This presents an RS232 DTE interface with the same pin-out as a PC.

Communications parameters are 9600Bps no parity. If a PC is used as the terminal a crossover cable will be required and a software package such as "Terminal" used.

5.1.2 By IP Network device

A terminal session may be initiated using the SSH (Secure Shell) protocol, however the IP address of the MAR may need to be set with a local terminal first. As supplied the MAR will use DHCP by default. If the network device is a Windows PC then a package such as Putty (freeware) will be required to support SSH and WinSCP3 (freeware) to support SSH. By default the IP Address of the units is 192.168.0.10 with a sub net mask of 255.255.255.0

5.1.2.1 Security

By using SSH all data including the username & password is encrypted preventing unauthorised access by the use of network monitoring equipment. Security may be further enhanced by restricting access to a predefined list of hosts, see "man hosts_access" for details.

5.1.3 Logging on

At the logon prompt the user and password are both case for non-privileged access or user root & the root password for privileged access (not normally required).

5.1.4 Logging off

At the case user prompt type exit.

5.1.5 Changing password

The password controlling access to the CASE account may be changed using the passwd command. Type passwd at the prompt and you will be asked for the old password once then the new password twice.

5.1.6 Password rules

The default password of case is very insecure and the system will not let you use anything that simple again. The rules for an acceptable password are at least 8 characters with no spaces.

5.1.7 Configuration file

5.1.8 Configuration file execution

The system reads and executes the contents at system boot. In addition the configuration file is re-read every 30 seconds and its contents compared against the system settings, if any configuration parameters have changed they are also changed in the system. Due to this the configuration file should be edited with care to ensure the version saved is always consistent and without errors. One method of ensuring this is to make a copy, edit it, check it then copy it back.

5.1.8.1 Package take up of changes

All packages will take up the new configuration following a re-boot BUT if deliberately re-booting after a change 30 seconds must be allowed for the change to have reached the individual files and an "wru" should be done after this period to ensure those files new contents are saved. The only package where this is not necessary is "HDLC over IP" that reconfigures itself without a re-boot excepting if client ports are commented out.

5.1.9 Remote configuration file loading

The path for the configuration file is "/home/case/configuration". Simply use this command in an SCP command to either read or write the file.

5.1.10 Configuration file editor

To access the configuration file interactively logon as user 'case' then type "nano c*" at the prompt. To leave the editor type ctrl-x, if you wish to save changes type ctrl-o.

The cursor can be moved around with the arrow key's, page-up/down moves faster.

Backspace deletes characters & new characters are inserted.

Ctrl-k cuts lines & ctrl-u restores however many lines are in the cut buffer.

It is strongly recommended when working on the live configuration file (rather than a copy) that the file is only saved when each section is complete as otherwise the system will possibly corrupt other files, this is due to the configuration file being read and executed every 30 seconds.

5.1.11 Configuration file syntax

The configuration file is in human readable text format.

All lines starting with # are treated as comment lines.

The file is divided into sections used by different options and a default is supplied with the product that shows many examples, option specific sections of this manual will cover individual sections in detail.

5.1.11.1 File sections

It is possible to embed whole files within the configuration file that will cause the files within the system to be overwritten. The syntax is a block of text (the file) preceded by a line "casefilestart path" and terminated with the line "casefileend".

5.1.11.2 Commands

It is possible to embed command lines within the configuration file.

Any line beginning with the ; character will be executed at root privilege however this is limited to those commands outlined in the individual package sections. Execution will only occur once at system boot.

5.1.12 Saving changes to flash

After any changes have been made to the configuration area they need to be saved in non-volatile memory (flash) to ensure they are restored after a power cycle or reboot. To save the changes simply type "wru" at the command prompt, a series of dots will be printed whilst the process is in progress followed by OK when it has finished.

5.1.12.1 Controlling flash usage

It is possible to create so many files and directories that the flash space is used up or becomes insufficient for potential upgrades. The amount of space used can be found when at the case home directory (“cd ~case”) by using the command “du -sh”. It is recommended that no more than 250Kbytes be used.

5.1.13 Restoring default

A read only copy of the default configuration file is stored as “default.configuration”. To restore the active configuration file to default use the command “cp default.configuration configuration”, this change will need saving to flash with the “wru” command.

5.2 Setting IP address

This should be done by editing the appropriate section of the configuration file, examples for DHCP & static are given but just in case they become lost here they are again.

5.2.1 Example for dhcp

```
iface eth0 inet dhcp
```

5.2.2 Example for static

```
iface eth0 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    broadcast 192,168.0.255
```

5.2.2.1 Gateway

If the unit is connected to the IP network via an external router then that routers IP address will have to be added as the gateway address as shown in the configuration file, i.e. the line “gateway 192.168.0.100” must be added after the line containing “broadcast” in the above example.

5.3 Setting date & time

To set the date & time in the system two commands are needed. 1st “date MMDDhhmm” then “hwclock -w”. To just examine the current date & time use “date”. Other options for changing year & seconds available, see man page. These commands can only be used by user root.

5.4 Man pages

The system is shipped with a set of Linux man (manual) pages to provide on-line assistance. The man pages are accessed by using the command “man” at the prompt followed by the command that you want help on, e.g. “man ls”. To exit the man page use q, to scroll down use the spacebar.

6 Hardware Option installation

Normally the MAR will be supplied with the correct cards installed. If this is not the case then the unit should only be opened with the power removed and both it and the operator grounded to prevent any static damage (appropriate clothing should also be worn). The lid is removed with two rear thumbscrews & pushing the lid rearwards before attempting to lift from the rear, refitting is the reverse. It is assumed the operator will be familiar with the removal & installation of PCI cards.

6.1 RS232 synchronous ports

The Case Quad Synchronous PCI (CQHDL232) card is entirely software configured. The rear panel is fitted with an 4 way RJ48 connector with two indicator leds per channel.

6.1.1 Channel identity

The channels are numbered upwards from 0. Channel 0 is the connector nearest the power connector of the MAR or the rightmost when viewed from the rear. If more than one CWAN232 card is fitted, channel 0 will be on the lowest card.

6.1.2 LEDES

Two leds are fitted per channel, green being receive & orange transmit. The leds are triggered by an HDLC frame transmitted or received and in the case of single frames remain lit for ½ a second per frame, frame events occurring more frequently than 2Hz will cause the led to be permanently lit.

6.1.3 RJ48 Pin-out

On each connector the pins have the following functions

1 Brown, Signal Ground	2 Red, Ext clock, In	3 Orange, TXD, In	4 Yellow, DTR, In	5 Green, RXD, Out
6 Blue, DSR, Out	7 Violet, Rxclock, Out	8 Grey, Txclock, Out	9 White, RTS, In	10 Black, CTS, Out

Wire colours are derived from CASE standard RJ48 open cable assembly's.

6.1.4 D25 Pin-out

When using the standard case adapter cable to an D25 female the pins of the D25 female have the following functions

1 No Connection	2 TXD, In	3 RXD, Out	4 RTS, In	5 CTS, Out
6 DSR, Out	7 SignalGround	8 No Connection	9 No Connection	10 No Connection
11 No Connection	12 No Connection	13 No Connection	14 No Connection	15 Txclock, Out
16 No Connection	17 Rxclock,Out	18 No Connection	19 No Connection	20 No Connection
21 No Connection	22 No Connection	23 No Connection	24 Ext clock, In	25 No Connection

6.1.5 External clock

If an external clock is connected to the Extclock pin & selected in the software configuration it will be reflected onto the TX & Rxclock output pins.

6.1.6 Data rates

The lowest selectable internal rate is 75bps. An external clock has no low limit. The upper limit of the external & internal clocks is determined by the nature of the cable and the RS232 transceivers at both ends. On short (< 1 foot, 300mm) loopback cables 768Kbps can be achieved. On long 50 foot (15 Metre) cables rates can be limited to <= 19.2Kbps. Rates of 256Kbps are achievable on lengths < 6 feet (2 Metres). For higher speeds & longer lengths it is better to use an RS422 interface (see next section).

6.2 HDLC RS422 (X21) & RS232 synchronous ports

PLEASE NOTE AT THE TIME OF WRITING THIS INTERFACE IS HARD CONFIGURED, PLEASE CONTACT OFFICE FOR FURTHER DETAILS.

The X21 capable card (CQHDL232/422) has a soft selectable interface defined by options in the configuration file. The RS232 RJ48 interface of this card is **different** to the RS232 only card described previously but the D25 pin-out, clocking & data rates are the same.

6.2.1 RS232 RJ48 Pin-out

On each connector the pins have the following functions

1 Brown, Signal Ground	2 Red, CTS, Out	3 Orange, TXD, In	4 Yellow, DTR, In	5 Green, RXD, Out
6 Blue, DSR, Out	7 Violet, Txclock, Out	8 Grey, Rxclock, Out	9 White, RTS, In	10 Black, Ext clock, In

Wire colours are derived from CASE standard RJ 48 open cable assembly's.

6.2.2 X21 RJ48 Pin-out

On each connector the pins have the following functions

1 Screen, Signal Ground	2 N.C.	3 Wht/Ora, TXDb, In	4 Orange, TXDa, In	5 Wht/Grn, C/Ib, In/Out
6 Green, C/Ia, In/Out	7 Wht/Blu, TEb, In/Out	8 Blue, TEa, In/Out	9 Wht/Brn, RXDb, Out	10 Brown, RXDa, Out

Wire colours are derived from CASE standard RJ48 open cable assembly's.

The direction of TE (Timing Element) is determined by the internal/external clock selection.

The Direction of C/I (combined Control or Indication) is determined by the configuration file, it is not possible to support both Control & Indication simultaneously, presently these pins are always an input & there condition is ignored.

6.2.3 HDLC Data rates

When in RS232 mode these are as for the RS232 only card (see previous section). When in RS422 mode the same minimum's apply (as RS232) but the maximums assuming correct specification twisted pair 100ohm cables are very much higher.

The maximum internal clock rate is 4.8Mbps. At higher internal data rates speeds supported are integer divisions of 9.6Mbps e.g. 4.8, 3.2, 2.4, 1.92, 1.6, 1.37, 1.2, 1.06, 0.96, 0.87, 0.8, 0.738, 0.685 Mbps etc.

The maximum external clock rate is 4.8Mbps.

Assuming good quality cable 24awg 100r pairs 10Mbps is achievable at up to 5Mtrs.

Maximum distance is 1Km at 50Kbps.

Intermediate data is given by Mbps*Metres = 50 e.g 50/100Metres = 500Kbps.

6.3 TDM RS422 (X21) & RS232 synchronous ports

This is exactly the same card as the HDLC version above but with different firmware for TDM operation. All physical characteristics are the same however the internal clock source is different.

6.3.1 TDM Data rates

The maximum internal clock rate is 4.8Mbps. At higher internal data rates speeds supported are integer divisions of 16.384Mbps e.g. 4.096, 3.072, 2.048, 1.536, 1.024 Mbps etc.

The maximum external clock rate is 4.8Mbps.

6.4 PCI ADSL

A single PCI ADSL card may be fitted, the rear panel has a single RJ11 socket that should be connected to the ADSL side of the filter/splitter with the supplied cable (RJ11 to RJ11).

The only supported card type is the Traverse Pulsar. The four-rear panel LEDs are

- Orange Power
- Green Line synchronised
- Reds Transmit & receive data

7 Software options

7.1 Basic configuration

All of these options will require the setting up of the Ethernet address even if the Ethernet port is not in use as this address is also the identity of the unit that may have to be used in relation to some options.

7.2 HDLC over IP

7.2.1 Synchronous ports

These are provided by a four channel PCI card supporting RS232 only (CQHDLC232) or both RS232 and X21 (CQHDLC232/422) described in the hardware options section.

7.2.2 Functional description

In order to better understand the meaning of configurations & statuses this is a brief description of operation.

The IP transport model used in the MAR consists of clients & servers, clients initiate connections across the IP network whilst servers passively listen for incoming connections. A completed connection capable of transporting data consists of a client at one end and a server at the other that have mutually accepted a connection.

In the MAR individual WAN (synchronous) ports may be configured to be either a client or server port and a single MAR may contain any mixture. Within the overall network topology a given HDLC connection must consist of a client at one end and a server at the other. In the simple case of two nodes supporting 4 HDLC links then all four ports in one node could be configured as clients whilst all four in the other node could be configured as servers.

A servers port configuration need only consist of the parameters required for the WAN port (e.g. bit rate) whilst a client port needs to know what the server IP address is and what the WAN port number within the server it is to connect to. Within a given node client ports may connect to multiple server nodes and any mapping of WAN port numbers is permissible within the constraints of no collisions, the ports physically exist and they are configured as servers.

7.2.3 Performance

Aggregate rates of 3Mbits/sec have been verified without using secondary features such as firewalling, NAT or IPSec.

7.2.4 IP Port number

The MAR HDLC bridge application uses IP port number 15001.

7.2.5 Diffserv

Outgoing packets are marked with a TOS/DSCP/ECN field value of 0xFF. This is nominally the highest priority however the meaning of this field/s has been altered by many RFC's and most routers furthermore have vendor dependant treatments of the field. If other values are required IPtables may be used to modify the value 0xFF to something else using the mangle table with `-set-tos` option.

7.2.6 BIST

The software has a Built In Self Test feature that is intended to be used in conjunction with Client ports. The BIST software generates traffic as fast as possible (controlled by bit rate) out of the Client synchronous port where it is intended to be looped back via a physical loopback cable.

Data received from the Client synch port will be forwarded as normal to the server synch tx port where another loopback cable should be fitted. Data received from the server synch port will then be forwarded to the client as normal, however when it reaches the client it will not be transmitted on its synch port, instead it will be thrown away.

This allows the exercising of the whole network at the chosen bit rate, statistics gathered and ping used simultaneously to determine the network performance under load.

BIST is enabled by adding the token “test” onto the end of a port configuration (see configuration file syntax), normally the HDLC packet size is 4096 bytes but this can be reduced by adding the required size after the test token e.g. “test1024”.

7.2.7 Configuration file syntax

The configuration for a port must be completely contained on one line, the line must begin with the package identifier “chdlcip” (for Case HDLC over IP), spaces are used to separate tokens.

The tokens and their meanings are

- * “portNN” Where NN is in the range 00-31
- * “typeserver” or “typeclient”
- * “clockNNNN” NNNN is required bit rate (range 75 – 5000000) or “ext”
- * “linev24” or “linex21”
- “x21ciout” makes c/I pair an output (default is input).
- * for client “targetpipNNN.NNN.NNN.NNN” Client only primary IP address of server
- * for client “targetppportNN” Client only primary port on server (00-31)
- client only “testNNNN” Sets BIST mode, NNNN optionally sets HDLC packet size (else 4096 bytes).

Tokens marked with * are mandatory & must occur.

The actual bit rate will be as close as possible to the setting, RS232 boards cannot run > ~512Kbps.

7.2.7.1 Examples

```
“chdlcip port10 typeclient linev24 clock9600 targetpip192.168.17.3 targetppport12”
```

```
“chdlcip port10 typeclient linev24 clock9600 targetpip192.168.17.3 targetppport12 test10”
```

```
“chdlcip port10 typeserver linev24 clock9600”
```

7.2.7.2 Configuration operation

The port statements in the configuration file are checked every 30 seconds against the current port configuration. If a change is detected the change is made and the port restarted. If a port is commented out then it will continue operation as before until the next reboot as comment lines are ignored hence no change is detected.

7.2.8 IP link overhead

Each HDLC frame is wrapped up in an TCP packet with an 80 byte overhead.

If the transport link is ADSL then a further 10% overhead is incurred by the ATM formatting.

The following example shows some permutations on an 256Kbps ADSL link.

Raw rate 256Kbps – ATM overhead = 225Kbps.

512 byte HDLC rate = $225 / (512 + 80) * 512 = 195\text{Kbps}$.

256 byte HDLC rate = $225 / (256 + 80) * 256 = 171\text{Kbps}$.

128 byte HDLC rate = $225 / (128 + 80) * 128 = 94\text{Kbps}$.

7.2.9 Status

The command “sbstat” display’s the following menu

```
Case Synchronous Bridge sbstat4, (c)2005,2006,2007
Port Status Menu
```

```
Enter port number to display
Preceed with c to clear
or x to exit
```

Once a channel is selected, assuming it has a configuration the following will be displayed

```
Port 0 Type ,Clock      ,Line ,Synch stat ,IP stat
HDLC Server ,64000      ,V24  ,Up         ,Up

Tdlinkpkts,Tulinkpkts,Trestarts ,Abt      ,CRC      ,Orun
0           ,0           ,0       ,0        ,0        ,0
```

The first two lines confirm the configuration and display the link statuses, the most important being the IP status that is the link between the two ends, Synch stat refers to the local WAN card only (not the link between it & external equipment).

IP Down can simply mean no client configured to connect. In a Client Down will always be automatically retried but if persistent there may be a configuration or network problem.

The second two lines display the statistics (T = Total). Downlink is from server to client. Abt = local HDLC receiver abort frames, CRC = local HDLC receiver CRC error, Orun = local HDLC receiver overrun.

7.2.10 Ifconfig / SNMP Status

When viewing the status using the “ifconfig” command or remotely via SNMP the synchronous port identities are “cqhdlc0-n” and look like this

```
cqhdlc0  Link encap:AMPR NET/ROM HWaddr
         inet addr:169.254.254.200 Mask:255.255.255.255
         UP NOARP MTU:0 Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

Valid fields are

RX-packets, RX-bytes, RX-errors(CRC), RX-overruns(FIFO overflow), RX-frame(Abort).

TX-packets, TX-bytes, TX-errors(CRC), TX-overruns(FIFO underflow).

If using “ifconfig -s” the Flg R (Running) flag shows whether the link is up.

7.2.11 DCX Extended Window Mode

The CASE DCX ARQ uses a very short frame (<128 bytes) and normally only uses an modulo 8 sequence number, hence it is easy for this number to wrap causing errors given the amount of data that can be buffered within the IP stacks at each end of the link. For this reason the ARQ configuration should be changed to use “Extended Window Mode” that increases the modulo of the sequence number to 64.

7.3 TDM over IP

Most of the functionality is identical to HDLC over IP so only the differences are documented here.

7.3.1 Synchronous ports

Only the CQHDLC232/422 card described in the hardware options section is capable of TDM mode (when fitted with the appropriate firmware).

7.3.2 Functional description

Data from the serial port is assembled into blocks of bytes according to the configured block-size (32-512 bytes) prior to being transmitted across the IP network together with a 4 byte sequence number in an UDP packet. At the far end UDP packets are re-assembled the sequence number discarded and the data delivered to the serial port.

A TCP connection on port 15001 is used to manage the connection however data is transported by UDP packets using a range of port numbers from 15000 to 15100.

7.3.2.1 Clocking

The serial clocks at the two ends must be exactly the same frequency else data corruption will occur. The necessary accuracy can be achieved in a variety of ways depending on network topology

- External network clock (e.g. kilo-stream) provided to both ends (so both ends configured for external clock)
- MAR1 slaved to MAR2 where MAR1 is either internally clocked or externally from high stability source

Only one channel should be selected to slave mode as there is only one clock source on the interface card that can be slaved, the other channels set to internal clock will be derived from the same source and hence automatically slaved to the same distant end. It is not possible on one interface card to slave to more than one distant source.

7.3.2.2 Interface card LED's, IP link performance

These are not used to indicate channel activity as that has no meaning in TDM.

They are used as an 8 position bar meter to indicate the expected vs actual next packet sequence number and time for channel 0. Normally the centre led will be lit, leds to the left indicate early arrival and to the right late, jitter results in several leds being lit simultaneously.

Once the number of leds lit together exceeds 4 it likely that errors will occur, possible remedial action includes increasing the block-size, reducing the data rate or improving the IP link.

7.3.3 Performance

This will vary according to the block-size and quality of the IP link, the following results were obtained over 100Mbps Ethernet. The aggregate may be spread across 1, 2, 3, or 4 channels.

Block size bytes	Aggregate rate Kbps
512	4096
256	1024
128	TBA
64	TBA
32	TBA

It should be noted these limits do not include packet jitter from external IP causes.

7.3.4 IP Port numbers

The MAR TCP bridge application uses TCP port number 15001 & UDP port numbers in the range 15000 to 15100.

7.3.5 Configuration file syntax

In TDM mode the BIST feature is not supported but will be ignored if present on the line.

New tokens (for TDM) and their meanings are

- “clockslvNNNNNN” Clock is slaved to MAR at other end of IP link
- “blockNNN” Block-size in bytes, 512, 256, 128, 64 or 32

7.3.5.1 Examples

```
“chdlcip port10 typeclient linex21 clock1024000 targetpip192.168.17.3 targetpport12 block512”
```

```
“chdlcip port10 typeclient linex21 clockslv1024000 targetpip192.168.17.3 targetpport12 block512”
```

7.3.6 Status

The command “sbstat” displays the following menu

```
Case Synchronous Bridge sbstat4, (c)2005,2006,2007
Port Status Menu
```

Enter port number to display

Precede with c to clear

or x to exit

Once a channel is selected, assuming it has a configuration the following will be displayed

```
Port 0 Type ,Clock      ,Line ,Synch stat ,IP stat,Block
TDM Server ,64000      ,V24 ,Up          ,Up      ,256

Tdlinkpkts,Tulinkpkts,Trestarts ,TSyncErrors ,InSync
2789      ,2790      ,0      ,1      ,Yes
```

The first two lines confirm the configuration and display the link statuses, the most important being the IP status that is the link between the two ends, Synch stat refers to the local WAN card only (not the link between it & external equipment).

IP Down can simply mean no client configured to connect. In a Client Down will always be automatically retried but if persistent there may be a configuration or network problem.

The second two lines display the statistics (T = Total). Downlink is from server to client, note that TsyncErrors cannot be reset with the c command. If the link is not InSync it will not pass error free data, some SyncErrors are to be expected each time the link restarts. If there are no SyncErrors the TDM circuit should be error free.

7.3.7 Ifconfig / SNMP Status

When viewing the status using the “ifconfig” command or remotely via SNMP the synchronous port identities are “cqhdlc0-n” and look like this

```
cqhdlc0  Link encap:AMPR NET/ROM  HWaddr
         inet addr:169.254.254.200  Mask:255.255.255.255
         UP NOARP  MTU:0  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Valid fields are

RX-packets, RX-bytes, RX-errors(CRC), RX-overruns(FIFO overflow).

TX-packets, TX-bytes, TX-errors(CRC), TX-overruns(FIFO underflow).

If using “ifconfig -s” the Flg R (Running) flag shows whether the link is up.

7.3.8 IP link overhead

The TCP traffic is very low (~30*80bytes/sec or 19.2Kbps).

Each TDM block has a 4 byte sequence number added followed by an 40 byte UDP header.

If the transport link is ADSL then a further 10% overhead is incurred by the ATM formatting.

The following example shows some permutations on an 256Kbps ADSL link.

Raw rate 256Kbps – ATM overhead = 225Kbps – TCP data = 205Kbps.

512 byte TDM rate = $205/(512+4+40)*512 = 189\text{Kbps}$.

256 byte TDM rate = $205/(256+4+40)*256 = 175\text{Kbps}$.

128 byte TDM rate = $205/(128+4+40)*128 = 152\text{Kbps}$.

7.4 PCI ADSL

7.4.1 Configuration

The ADSL interface is configured in the ADSL section of the configuration file (see appendix) where your ISP details should be added. There are two types of authentication, most ISP's use CHAP, in both cases the username must be entered in the provider file. Also add the username and password into the CHAP or PAP section (it doesn't matter if its in both).

7.4.2 Status

The status of the ADSL interface (if fitted) can be determined by using ifconfig, e.g "ifconfig ppp0", if the interface is up this word will appear together with the IP addresses determined by your IP. In the event of connection difficulty's additional information can be found using the command "tail /var/log/syslog".

7.4.3 Console Messages

Both interfaces generate console messages when the link is not up that can be annoying when editing files.

7.5 SNMP Agent

An SNMP agent supporting MIBII is provided and may be enabled/configured in the configuration file. The Agent supports SNMP V1, 2 or 3 protocols (fully configurable) and is able to generate traps.

7.5.1 Configuration

The Agent is configured using appropriate sections of the CASE configuration file. By default it is commented out so the agent will be disabled for enhanced security. The default configuration if uncommented will provide an SNMPV1 read only agent. The "man snmpd" command is helpful for further information.

7.5.1.1 Enterprise Number

The Case Communications Enterprise Number is 144.

7.6 IPTables (Firewall) & NAT

The Linux IPTables package is used to provide a fire-walling capability (if required) together with NAT (Network Address Translation) facilities that would be required when using the ADSL or other public network interface.

Most IPTables commands are privileged so the root password is required to use them except when they are part of the configuration file.

7.6.1 Configuration

A section of the case configuration file is used to configure IPTables. Several different methods may be used

7.6.1.1 File image

The IPTables package has a save & restore function whereby its entire configuration may be dumped to or reloaded from a file. An image of this file (iptables.conf) is stored in the configuration file and an IPTables restore command. Consequentially changes in the configuration file IPTables image will be reflected in the IPTables configuration following the next re-boot. This is the default method used by the supplied configuration file.

7.6.1.2 Command lines

Direct IPTables command lines may be stored in the configuration file (syntax is ":command line") and the entire package may be configured this way or it may be used in a complimentary fashion with the restore command, placed either before or after it depending on the desired execution sequence. These commands are executed once only at system boot.

7.6.1.3 Script files

Many script files for configuring Iptables as a firewall are available on the web. These may be employed by copying them to the ~case directory and then entering a command line “:./scriptname” in the configuration file. After copying the script file into the ~case directory it needs to be made executable using the command “chmod a+x scriptname”.

7.6.2 NAT Configuration

NAT (Network Address Translation) is part of Iptables so uses the configuration methods outlined above. If the product uses a public (as opposed to a private) network NAT will almost certainly be required because public addresses are in a completely different range to those allocated for local use.

7.6.2.1 Incoming from public

When packets arrive from the public network the destination address will be the public address allocated to your organisation and might be something like 200.200.10.1. None of the nodes on your local network should have an address like this (they should be 192.168.x.y for example) so NAT has to be configured to translate the destination address. It does this by assuming different local nodes provide different services and is configured to associate incoming port numbers to local IP addresses.

7.6.2.1.1 HDLC over IP server

To configure NAT to route incoming connection attempts from the public network (assumed to be device ppp0) to the local server (using the port number) the following command line is required. “iptables -t nat -A PREROUTING -i ppp0 -p tcp -dport 15001 -j DNAT --to-destination 192.168.10.1:15001” 192.168.10.1 is an example address of the server. This line is in the case configuration file and may be uncommented and edited as required.

7.6.2.2 Outgoing to public

Packets being sent to the public network would without NAT have a source address of the local node originating the packet (e.g. 192.168.x.y). This would result in reply packets having this address in their destination which is unreachable within the public network. Outgoing NAT simply replaces the source address with the public address allocated to your organisation and might be something like 200.200.10.1. This ensures reply packets are correctly routed back to you by the public network.

7.6.2.2.1 HDLC over IP client

To configure NAT to replace the source address with that allocated by your ISP the following is required (assumes ppp0 is public network). For static IP allocation “iptables -t nat -A POSTROUTING -o ppp0 -j SNAT --to-source 200.200.10.0” (200.200.10.0 is an example static ip address) or for dynamic allocation “iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE”. These lines are in the case configuration file and may be uncommented and edited as required.

7.6.3 Mangle for TOS

Mangle may be used to change the TOS field in outgoing packets from the HDLC over IP application. To do so add the line “iptables -t mangle -A OUTPUT -p tcp -dport 15001 -j TOS --set-tos Minimise-Delay” in the configuration file.

7.6.4 Firewall

The firewall configuration is very product application dependent but the configuration file contains some examples. A Case document entitled “Case Firewall Application Note” is available for further explanation.

In the case of the HDLC over IP product a firewall is superfluous as the node will only accept SSH & SCP connections together with its own protocol on port 15001 where anything foreign (to its own protocol) will be ignored.

7.7 VLANS

Ethernet VLANS are supported on the product. To configure them use the “vconfig” command (see “man vconfig”, these can be added to the configuration file. The virtual interfaces created can be referenced in IPtables.

8 Ancillary packages

These are used to provide further IP routing and security capabilities.

8.1 IProute2

This is a sophisticated bandwidth control system, useful when services of different priority’s must share a relatively low bandwidth WAN or DSL pipe. The manual pages are “ip” & “tc” and much documentation is available on the web e.g. <http://lartc.org/howto/index.html> also a very good document called “Linux Advanced Routing & Traffic Control HOWTO”.

8.1.1 Configuration

This package does not have an configuration file as such so must be configured using command lines embedded in the case configuration file (lines beginning with ; character) that will be loaded when the system starts up. Because rules will be loaded every time the system starts the rule load must be preceded by a rule flush.

8.2 Quagga

Quagga is a routing software suite, providing implementations of OSPFv2, OSPFv3, RIP v1 and v2, RIPv3 and BGPv4 for Unix platforms. The man pages are zebra, ripd, ospfd, ospf6d, ripngd, bgpd & isisd. Quagga has a website at <http://www.quagga.net/> where there are many usage illustrations and more documentation.

8.2.1 Configuration

Either individual command lines, a configuration file or mixture of the two may be embedded within the case configuration file.

8.3 OpenVPN

OpenVPN is a full-featured SSL VPN solution which can accomodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls

8.3.1 Configuration

Either individual command lines, a configuration file or mixture of the two may be embedded within the case configuration file.

8.4 L2TPD

L2TP (layer two tunneling protocol) encapsulates PPP connections. See “man l2tpd” for details.

8.4.1 Configuration

The /etc/l2tpd/l2tpd.conf & /etc/l2tpd/l2tp-secrets files may be embedded in the case configuration file.

9 Software maintenance

9.1 Identification

Two pieces of information identify the software in your product. The first is the product name and revision date given in the welcome text when you login. The second is the “Linux line also given when you login immediately after the password.

9.2 Flash drive replacement

Most maintenance should be possible without the replacement of this component, however if it becomes damaged or too small it may require replacement, in this event your configuration will be lost so it is advisable to maintain a backup of your configuration elsewhere.

To replace the drive the same comments about static apply given in the hardware option installation section. The drive is under an additional cover retained by three screws, replace the drive in the IDE socket nearest the front panel also swapping the polarised power cable, do not attempt to run without the power cable fitted.

9.3 Updates

These updates are incremental so every update from that immediately following your systems revision date to the current must be applied strictly in date order. You must be root to execute these scripts. The revision date is given in the welcome text immediately after login.

9.3.1 Update files

Each update consists of a file named “ddmmy.tar” where dd is day, mm is month & yy is year.

Each file should be copied to the case home directory (cd ~case) using scp.

Once the update is present uncompress it by typing “tar xvzf ddmmy.tar” then execute (as root) it by typing “./script”. If you forgot to logon as root, do so and perform the procedure again.

9.3.1.1 Copying files

From an external server type “scp ddmmy.tar [root@192.168.0.25:~case/](#)” where 192.168.0.25 represents the MAR IP address, password will be for user root on MAR.

9.3.2 Changes to configuration file

If necessary wherever possible these are appended to the end of the existing file and commented out, this avoids disturbing the existing configuration. However it is strongly advised the existing configuration file is backed up prior to any updates being applied.

10 Appendix A useful commands

Several commands that have not been mentioned may be executed by the case user, this list also includes commands already used as a quick reminder.

- “cd d” Change directory to d
- “cd ..” Change directory to one level up
- “cd ~case” Change directory to user case home
- “cp a b” Copy file a to file b
- “date” Display or set system date & time (root only)
- “du -sh” List size of this and all it’s sub-directories
- “exit” Logoff
- “hwclock -w” Transfer date & time to hardware (root only)
- “ifconfig” Provides status & configuration of network interfaces
- “iptables” Manipulate IPTables configuration
- “ls” List files in current directory
- “man command” List help on command e.g. “man ls”
- “mkdir d” Create directory called d
- “nano file” Text editor, “ctrl-x” to exit
- “netstat -i” List interface status in tabular format
- “ping 192.168.0.1” Network test utility, “ctrl-c” to exit
- “/proc/pci” File to nano or cat to view PCI device configuration
- “rebootu” Reboot system
- “rm a” Remove file a
- “rmdir d” Remove directory d
- “route” Display list of known routes
- “scp” Secure copy file (e.g. configuration)
- “tail /var/log/syslog” Most recent reports of internal activity
- “tcpdump” Display packet headers on interface
- “tracpath” Alternative to traceroute, non-privileged
- “traceroute” Trace path through internet taken by packets
- “vconfig” Manipulate VLAN configuration
- “wru” Save configuration to flash

11 Appendix B CMOS settings

In the unlikely event your CMOS becomes corrupt or if you wish to change the power up behaviour use the delete key during power up to access the settings menu.

Loading the “optimised defaults” will enable the system to operate but it will not automatically start after power failure. To enable this feature in “Power Management Setup” change “AC Loss Auto Restart” to Enabled.

To increase boot speed you may also wish to disable “Full Screen Logo Show” in “Advanced BIOS Features”. In all cases save changes at exit.

Also 1st time unit is booted the network boot feature will have to be disabled, watch for the message after self test to enter the network boot menu with the esc key. Then enter 1 (to boot from drives) this change is saved in CMOS so it won't try & network boot again.

12 Appendix C Example configuration file

```
#####
#####
# Default configuration file for CASE Multi Access Router      #
# Uncomment lines (remove #) to activate                      #
#####
# Synchronous Bridge configuration                            #
# In this example the 1st 2 ports are clients & the other 2 servers #
# Clients are set to call loopback IP address & hence these server ports#
#####
#chdlcip port0 typeclient clock64000 linev24 targetpport0 targetpip192.168.0.20
#chdlcip port1 typeclient clock64000 linev24 targetpport1 targetpip192.168.0.20
#chdlcip port2 typeclient clock64000 linev24 targetpport2 targetpip192.168.0.20
#chdlcip port3 typeclient clock64000 linev24 targetpport3 targetpip192.168.0.20
#chdlcip port0 typeserver clock64000 linev24
#chdlcip port1 typeserver clock64000 linev24
#chdlcip port2 typeserver clock64000 linev24
#chdlcip port3 typeserver clock64000 linev24
#####
#####
# This is an example system configuration section              #
# The first sets up the network interfaces                      #
# Select eth0 to be DHCP or static by commenting/uncommenting sections #
# To activate remove one # from all the lines from casefilestart to casefileend
# In all interface configurations the sections for cqhdlc0-7 must remain#
#####
casefilestart /etc/network/interfaces
# This is a network interfaces file for MAR
# Loopback interface
auto lo
iface lo inet loopback
#
# 1st ethernet interface
auto eth0

# comment out next line if eth0 not DHCP
#iface eth0 inet dhcp

# comment out next 4 lines if eth0 not static, use gateway if required
iface eth0 inet static
    address 192.168.0.10
    netmask 255.255.255.0
    broadcast 192.168.0.255
#    gateway 192.168.0.100

# 1st ppp interface, leave commented out unless fitted
#auto ppp0
#iface ppp0 inet ppp
#    provider provider

# cqhdlc devices, do not change unless addresses clash with your network
# leave netmask at 255.255.255.255 to ensure no routing table entry's
iface cqhdlc0 inet static
```

```

        address 169.254.254.200
        netmask 255.255.255.255
iface cqhdlc1 inet static
        address 169.254.254.201
        netmask 255.255.255.255
iface cqhdlc2 inet static
        address 169.254.254.202
        netmask 255.255.255.255
iface cqhdlc3 inet static
        address 169.254.254.203
        netmask 255.255.255.255
iface cqhdlc4 inet static
        address 169.254.254.204
        netmask 255.255.255.255
iface cqhdlc5 inet static
        address 169.254.254.205
        netmask 255.255.255.255
iface cqhdlc6 inet static
        address 169.254.254.206
        netmask 255.255.255.255
iface cqhdlc7 inet static
        address 169.254.254.207
        netmask 255.255.255.255
#
casefileend
#####
#####
# This section configures ADSL with your ISP details #
#####
casefilestart /etc/ppp/peers/isp0
# skeleton peer file for ADSL
user yourlogin
plugin pppoatm.so 0.0.38
casefileend
casefilestart /etc/ppp/peers/isp1
# skeleton peer file for ADSL
user yourlogin
plugin pppoatm.so 1.0.38
casefileend
casefilestart /etc/ppp/peers/isp2
# skeleton peer file for ADSL
user yourlogin
plugin pppoatm.so 2.0.38
casefileend
casefilestart /etc/ppp/peers/isp3
# skeleton peer file for ADSL
user yourlogin
plugin pppoatm.so 3.0.38
casefileend

##### associate user names & passwords (up to 4)
casefilestart /etc/ppp/chap-secrets
# Secrets for authentication using CHAP
yourlogin0 * yourpassword0 *
yourlogin1 * yourpassword1 *

```

```

yourlogin2 * yourpassword2 *
yourlogin3 * yourpassword3 *
casefileend
casefilestart /etc/ppp/pap-secrets
# PAP authentication, won't work with MLPPP
* yourpassword
casefileend

#####
#####
# This section enables or disables SNMP (disabled by default)           #
# Please ensure SNMP is configured correctly before enabling             #
# as otherwise the security of your system may be compromised           #
# To activate remove one # from all the lines from casefilestart to casefileend
#####
#casefilestart /etc/default/snmpd
#SNMPDRUN=yes
#casefileend
#####
#####
# This section is for the SNMP configuration                             #
# This default allows read only access to allcomers                     #
#####
casefilestart /etc/snmp/snmpd.conf
sysdescr CASE Multi Access Router
com2sec readonly default public
group myROgroup v1 readonly
view all included .1 80
access myROgroup "" any noauth exact all none none
casefileend
#####
#####
# This section is for the IPTABLES configuration                         #
# It contains a series of command lines executed once at boot           #
# If you make changes you must re-boot to invoke after using wru       #
#####
# First dissable all input & flush the tables
;iptables -F
;iptables -F
# Enable common services
# PING out
;iptables -A INPUT -s any/0 -p icmp --icmp-type echo-reply -j ACCEPT
# PING in
;iptables -A INPUT -s any/0 -p icmp --icmp-type echo-request -j ACCEPT
# DHCP on eth0
;iptables -A INPUT -i eth0 -p udp --dport 67:68 --sport 67:68 -j ACCEPT
# SSH or SCP in
;iptables -A INPUT -s any/0 -p tcp --dport 22 -j ACCEPT
# SSH or SCP out
;iptables -A INPUT -s any/0 -p tcp --sport 22 -j ACCEPT
# Cheap & nasty products that need to fragment packets
;iptables -A INPUT -s any/0 -p icmp --icmp-type fragmentation-needed -j ACCEPT
# SMTP left dissabled
#;iptables -A INPUT -s any/0 -p tcp --dport 25 -j ACCEPT
#HDLC/TDM over IP

```

```

;iptables -A INPUT -s any/0 -p tcp --dport 15001 -j ACCEPT
;iptables -A INPUT -s any/0 -p tcp --sport 15001 -j ACCEPT
# TDM over IP
;iptables -A INPUT -s any/0 -p udp --sport 15000:15100 --dport 15000:15100 -j ACCEPT
# Enable services used by attached PC's
#HTTP (Web) left dissabled
#;iptables -A INPUT -s any/0 -p tcp --dport 80 -j ACCEPT
#POP3 (Mail) left dissabled
#;iptables -A INPUT -s any/0 -p tcp --dport 110 -j ACCEPT
#DNS (nameserver) left dissabled
#;iptables -A INPUT -s any/0 -p tcp --dport 53 -j ACCEPT
#;iptables -A INPUT -s any/0 -p udp --dport 53 -j ACCEPT
#OPENVPN
#;iptables -A INPUT -i eth0 -p udp --dport 1194 --sport 1194 -j ACCEPT

#Network Address Translation
#These are suggested entry's for HDLC/TDM over IP via ppp, see manual.
#;iptables -t nat -A PREROUTING -i ppp0 -p tcp -m tcp --dport 15001 -j DNAT --to-
destination 192.168.10.1
#;iptables -t nat -A PREROUTING -i ppp0 -p udp -m udp --dport 15000:15100 -j DNAT --to-
destination 192.168.10.1

#;iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
#;iptables -t nat -A POSTROUTING -o ppp0 -j SNAT --to-source 200.200.10.0

#Logging (normally dissabled)
#;iptables -A INPUT -j LOG

#HDLC over IP changing the TOS/DSCP feild value
#;iptables -t mangle -A OUTPUT -p tcp --dport 15001 -j DSCP --set-dscp-class EF

#VLAN configuration
#;ifconfig eth0 0.0.0.0 up
#;vconfig add eth0 2
#;ifconfig eth0.2 192.168.0.240/24 up

#openVPN configuration file
casefilestart /etc/openvpn/case.conf
#Simple openvpn configuration
#remote 192.168.0.240
#dev tun
#ifconfig 10.4.0.1 10.4.0.2
#verb 4
#secret /etc/openvpn/static.key
casefileend

# Start OPENVPN
#;openvpn /etc/openvpn/case.conf

#####
#####

```