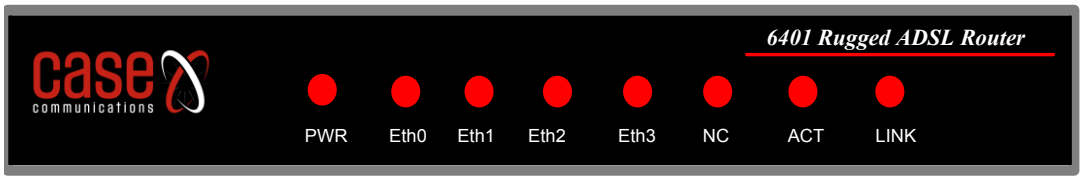
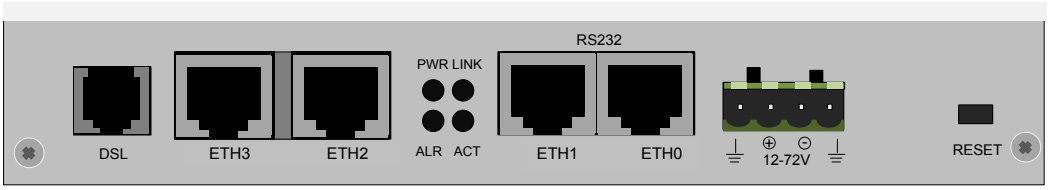
CASE COMMUNICATIONS





6401 RUGGED ADSL ROUTER

Revision 1.6

Sept 2013

CE Mark Warning

The Case Communications 6401 Rugged ADSL Router is an Industrial product which may cause radio interference in a domestic environment. In which case the user may be required to take adequate measures.

Copyright
Copyright © 2012 Case Communications Ltd. All rights reserved
This document contains information that is the property of Case Communications Ltd.
All or part of this document may not be copied, reproduced reduced to any electronic medium or machine readable form, or otherwise duplicated, and information herein may not be used, disseminated or otherwise disclosed, expect with the prior written consent of Case Communications Ltd

Version	Date	Notes
Rev 1.2	March 2012	First release of manual
Rev 1.3	June 2012	Removed Print Server and duplicate entries
Rev 1.4	July 2012	Note of Ethernet labelling error
Rev 1.5	June 2013	Appendix B – removal of Known Issues
Rev 1.6	Sept 2013	Ethernet WAN config added, correction of several errors

Case Communications
www.casecomms.com
0845 643 0800

CONTENTS

SECTION	TITLE	PAGE
1	6401 RUGGED ADSL ROUTER HARDWARE	1.1
2	GETTING STARTED	2.1
2.1	Connecting a PC to the Case 6401	2.1
3	DEVICE INFORMATION	3.1
3.1	SUMMARY INFORMATION	3.1
3.2	WAN INFORMATION	3.2
3.3	STATISTICS	3.2
3.3.1	STATISTICS LAN	3.2
3.3.2	STATISTCS WAN	3.2
3.3.3	STATISTICS xTM	3.3
3.3.4	STATISTICS xDSL	3.4
3.4	DEVICE ROUTE	3.6
3.5	DEVIVE INFO ARP	3.7
4	QUICK START GUIDE	4.1
4.1.1.	EQUIPMENT REQUIRED	4.1
4.1.2	STEP ONE A LAYER TWO INTERFACE	4.2
4.1.3.	STEP 2 – SELECT WAN SERVICE	4.2
4.1.4	CONFIGURING THE LAN	4.4
5	ADVANCED SET UP	5.1
5.1.1	INTRODUCTION	5.1
5.1.2	CONFIGURING A LAYER TWO ATM INTERFACE	5.2
5.1.3	CONFIGURING AN ATM INTERFACE	5.3
5.1.4	CONFIGURING AN ETHERNET INTERFACE	5.4
5.1.5	EXPLANATION OF OPTIONS	5.5
5.2	WAN SERVICES	5.7
5.2.1	INTRODUCTION	5.7
5.2.2	WAN SERVICE OPTIONS	5.7
5.2.2.1	CONFIGURING PPPoA	5.8
5.2.2.2	CONFIGURING IPoA	5.11
5.2.2.3	CONFIGURING PPP Over Ethernet	5.13
5.2.2.4	CONFIGURING IPoE	5.16
5.2.2.5	CONFIGURING BRIDGING	5.17
5.2.3	EXPLANATION OF WAN SERVICE OPTION	5.18
5.3	VPN	5.20
5.3.1	INTRODUCTION	5.20
5.3.2	L2TP CONFIGURATION	5.21
5.4	LAN CONFIGURATION	5.23
5.4.1	LAN SETUP	5.23

5.5 NETWORK ADDRESS TRANSLATION 5.25
5.5.1 NAT-VIRTUAL SERVER CONFIGURATION 5.25
5.5.2 NAT – PORT TRIGGERING 5.27
5.5.3 NAT – DMZ HOST 5.29

5.6 SECURITY 5.30
5.6.1 IP FILTERING 5.30
5.6.2 MAC FILTERING 5.32

5.7 PARENTAL CONTROL 5.34
5.7.1 TIME RESTRICTIONS 5.34
5.7.2 URL FILTER 5.35

5.8 QUALITY OF SERVICE 5.36
5.8.1 INTRODUCTION 5.36
5.8.2 CONFIGURING A LAYER TWO INTERFACE 5.37
5.8.2 QOS – QUEUE MANAGEMENT CONFIGURATION 5.37
5.8.4 QOS – QUEUE CONFIGURATION SETUP 5.38
5.8.5 CONFIGURING QOS CLASSIFICATION 5.39
5.8.7 DSCP OVERVIEW 5.42
5.8.8 CONFIGURATION EXAMPLES 5.43

5.9 ROUTING 5.45
5.9.1 DEFAULT GATEWAY 5.45
5.9.2 STATIC ROUTES 5.45
5.9.3 POLICY ROUTING 5.46
5.9.4 RIP 5.47

5.10 DNS 5.50
5.10.1 CONFIGURING A DNS SERVER 5.50
5.10.2 CONFIGURING DYNAMIC DNS 5.51

5.11 DSL CONFIGURATION 5.52

5.12 UPNP 5.54
5.12.1 INTRODUCTION TO UPnP 5.54
5.12.2 CONFIGURING UPnP ON THE 6401 RUGGED ROUTER 5.54
5.12.3 CONFIGURING UPnP ON A WINDOWS XP PC 5.54
5.12.4 CONFIGURING UPnP ON A WINDOWS 7 PC 5.55

5.13 DNS PROXY 5.56

5.15 INTERFACE GROUPING 5.57

5.16 IP SEC 5.59
5.16.1 HOW TO SET UP AN IP SEC TUNNEL 5.59
5.16.1.1 IPSec Tunnel over Ethernet WAN 5.62
5.16.2 TESTING THE IP SEC TUNNEL 5.63
5.16.3 ADVANCED SETTINGS 5.64
5.16.4 CONFIGURATION EXAMPLES 5.65
5.16.5 HOW IP SEC WORKS 5.66
5.16.6 ADVANCED IKE SETTINGS 5.67

5.17 CERTIFICATES 5.69
5.17.1 INTRODUCTION 5.69
5.17.2 CONFIGURING A CERTIFICATE OF AUTHORITY 5.69
5.18 MULTICAST 5.71
5.18.1 INTRODUCTION 5.71
5.18.2 CONFIGURING IGMP 5.72

6 DIAGNOSTICS 6.1
6.1 INTRODUCTION 6.1

7 MANAGEMENT 7.1
7.1 SETTINGS 7.1
7.1.1 BACKUP 7.1
7.1.2 UPDATE 7.1
7.1.3 RESTORE DEFAULT 7.1
7.2 SYSTEM LOG 7.2
7.3 SECURITY LOG 7.3
7.4 SNMP AGENT 7.3
7.5 TR069 CLIENT 7.4
7.6 INTERNET TIME 7.5
7.7 ACCESS CONTROL 7.6
7.8 UPDATE SOFTWARE 7.6
7.9 REBOOT ROUTER 7.7
7.10 WIPING 6401 FLASH 7.7

8 COMMAND LINE INTERFACE 8.1
8.1 ACCESSING CLI 8.1
8.2 COMMAND EXAMPLES 8.1

APPENDIX A PRODUCT SPECIFICATION

APPENDIX B KNOWN ISSUES

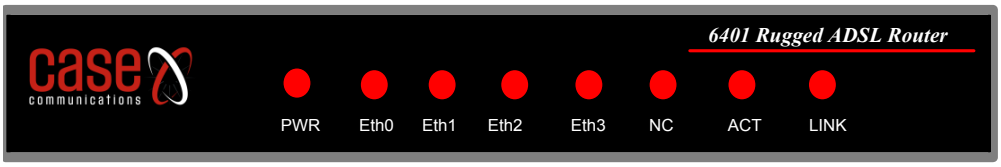
APPENDIX C SAFETY INFORMATION

APPENDIX D TECHNICAL ASSISTANCE

1 6401 RUGGED ADSL ROUTER HARDWARE

In the 6401 packing materials will contain the following items

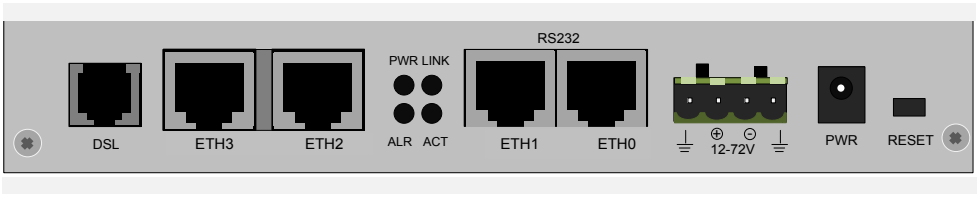
- The 6401 Rugged Router as shown below
- External Power Supply with mains lead.
- ADSL Line cord
- Option - manual – either CD or Hardcopy (NB. PDF versions of the 6401 manual are available from our web site on www.casecomms.com)



The indications on the front are

1. PWR – Indicates power is attached to the router and it is powered on.
2. Eth0 to Eth3- Ethernet ports 0 to 3. When a device is attached the port glows steady red with a slight flicker
3. NC – Reserved for future options
4. ACT - Link is Active when running PPPoE
5. Link –When flashing the 6401 is handshaking when steady the ADSL link is up.

The Back Panel has the following ports and functions



1. DSL – DSL port – attach line cord here.
2. Eth0 – Eth 3 – Ethernet ports
3. Cut outs for pwr – Link – ALR – ACT not used at this time.
4. Green strip 12v – 72v – DC power input. Attach DC supply here or use the AC to DC adapter with a plug to fit the PWR socket
5. PWR – Alternative DC power input source for use with alternate Power Adapter.
6. Reset – Reset switch to be operated via a pen or pin.

2 GETTING STARTED

2.1 CONNECTING A PC TO THE CASE 6401

Use a standard UTP Patch lead to connect a PC to the 6401 via any of the 4 Ethernet ports on the rear of the 6401. Using a standard browser (i.e. Firefox, Google Chrome, Internet Explorer etc.), enter the IP address of the router. It's possible some restrictions may have been configured within the router, therefore if one port does not allow access then move your PC to one of the other ports until the logon screen is retrieved.

If it's not possible to get a response from any of the Ethernet ports, press the 'reset' switch on the rear of the 6401 router in for 10 seconds which returns the 6401 to its default configuration.

The default IP Address of the Case 6401 router is **192.168.1.1**

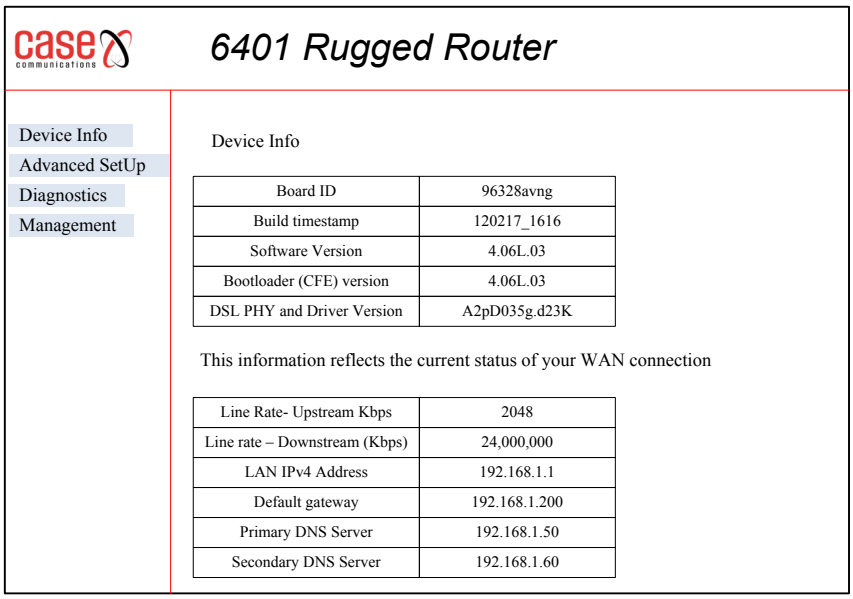
There are three operational modes, each with its own user 'Logon' name and password as shown below. The menu options available will vary depending on the logon status of the user

Management Level	**Admin level**	**Support Level**	**User Level**
User name	Admin (Local)	Support (remote)	User (Local)
Default Password	Admin	Support	User.
MENU OPTIONS	**Device Info**	**Device Info**	**Device Info**
	Advanced Set Up	**Advanced Set Up**	Not available
	Layer 2 Interface	Layer 2 Interface	Not available
	WAN Service	WAN Service	Not available
	VPN	VPN	Not available
	LAN	LAN	Not available
	NAT	Not available	Not available
	Security	Not available	Not available
	Parental Control	Not available	Not available
	Quality of Service	Quality of Service	Not available
	Routing	Routing	Not available
	DNS	DNS	Not available
	DSL	DSL	Not available
	UPnP	UpnP	Not available
	DNS Proxy	DNS Proxy	Not available
	Print Server	Print Server	Not available
	Interface Grouping	Not available	Not available
	IP Sec	Not available	Not available
	Diagnostics	**Diagnostics**	**Diagnostics**
	Management	**Management**	**Management**

If you enter an incorrect user name or password three times, the 6401 Router will close down your login session

Welcome Screen

When you first connect to the 6401 router you should see the following screen displayed on your PC. This is the 'Device Information' summary information page.



The 'device Information' page is explained below

Menu name	Value	Meaning
Board ID:	96328avng	The identification of the hardware used in this router
Build Timestamp:	120206_1817	The date (Year- Month-Day and time) the software was compiled
Software Version:	4.06L.03	Software revision of the board
Bootloader (CFE) Version:	1.0.37-106.24	The boot loader used by this board
DSL PHY and Driver Version:	A2pD035g.d23k	The DSL PHY and Driver version

This information reflects the current status of your WAN connection.

Menu name	Value	Meaning
Line Rate - Upstream (Kbps):	0	Upstream operating rate of the ADSL part of this router
Line Rate - Downstream (Kbps):	0	Downstream operating rate of the ADSL part of this router
LAN IPv4 Address:	192.168.1.1	IP v4 Address of the router
Default Gateway:		Default Gateway out of the subnet
Primary DNS Server:	0.0.0.0	Primary Data Name Server
Secondary DNS Server:	0.0.0.0	Secondary Data Name Server

To configure any parameters select from Advanced Set up (only showing if you have logged on as Admin or Support) and select from the menu tabs.

3 DEVICE INFORMATION

3.1. DEVICE INFO >SUMMARY INFORMATION

This page provides a quick summary of the 6401 Rugged ADSL routers status, and is divided into two parts, the first part being the hardware and software versions and the second part the operational status of the unit.

Board ID:	96328avng
Build Timestamp:	120206_1817
Software Version:	4.06L.03
Bootloader (CFE) Version:	1.0.37-106.24
DSL PHY and Driver Version:	A2pD035g.d23k

Board ID – The Hardware version used in this model

Build Timestamp – The time and date the software version was compiled

Software Version – The software version of the board

The Boot loader used for this router –

DSL PHY and Driver Version – used for this board

The second table reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	885
Line Rate - Downstream (Kbps):	18642
LAN IPv4 Address:	192.168.25.81
Default Gateway:	PPPoA
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

Line Rate Upstream **(Kbps)** Max 3.3Mbps (Annex M), Max 1.2Mbps standards ADSL2+)

Line Rate Downstream (KBPS) Up to a maximum of 24Mbps

LAN IPv4 Address 192.168.25.81

Default Gateway The port description of this routers Gateway. In this example we only have a single PPPoA WAN port going to the Internet therefore the Gateway is that port ID

Primary DSN Server 62.6.40.162

Secondary DNS 192.74.65.49

3.2. DEVICE INFO >WAN INFORMATION

This section provides an overview of the Wide Area Network information

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
pppoa	Pppoa_0_0_38	pppoA	Disabled	Disabled	Enabled	Enabled	Connected	81.136.19.67

Interface pppoa	This is the WAN interface being used
Description	Description given to the WAN Interface
Type	Reflects if this is IPoA, PPPoE, PPPoA etc.
VLAN Mux ID	Shows if enabled or disabled
IGMP	Shows if enabled or disabled
NAT	Shows if enabled or disabled (**N.B**. for some protocols it can't be disabled)
Firewall	Shows if enabled or disabled. (**NB**. for some protocols this can't be disabled)
Status	Connected, shows that the link is up
IPv4 Address	This is the WAN IP Address provided to you by your ISP

3.3. DEVICE INFO >STATISTICS

3.3.1. DEVICE INFO >STATISTICS > LAN

This option displays the Ethernet Interface statistics on the 6401 Rugged Router

Interface	**Received**				**Transmitted**			
	Bytes	**Pkts**	**Errs**	**Drops**	**Bytes**	**Pkts**	**Errs**	**Drops**
eth1	358893	2835	0	0	407710	1096	0	0
eth2	0	0	0	0	0	0	0	0
eth3	548407	4683	0	0	940061	2069	0	0
eth4	0	0	0	0	0	0	0	0

3.3.2. DEVICE INFO >STATISTICS > WAN

This option displays the Wide Area Network Interface statistics on the 6401 Rugged Router

Interface	**Description**	**Received**				**Transmitted**			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa	Pppoa_0_0_38	309560	2158	0	0	665133	1862	0	0
						Reset Statistics			

Select the 'reset statistics' to set the statistics back to zero

3.3.3. DEVICE INFO >STATISTICS > xTM (ATM)

This table shows the xTM statics for the 6401

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	146016	214438	873	809	0	0	0	0	0	0

The Extended Task manager provides additional information on the ports on the 6401 Rugged Router

Port Number: Shows the xTM (ATM) Port number

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received. . (Operational and Management)

Out OAM Cells: Number of OAM cells transmitted. (Operational and Management)

In ASM Cells: Number of ASM cells received. (Autonomous Status Messages)

Out ASM Cells: Number of ASM cells transmitted. (Autonomous Status Messages)

In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

Reset: Click to reset the statistics.

OAM Cells

If a communication problem occurs on a PVC (no traffic going one way or the other), the permanent virtual circuit (PVC) remains UP on the end-devices. Therefore, routing entries that were pointing to that PVC remain in the routing table for a certain time and as a result, packets will be lost. The solution to this problem is to use Operation and Maintenance (OAM) to detect such failures and allow the PVC to disconnect if it is disrupted along its path. At regular intervals, end-devices (such as routers) configured for OAM send loopback cells which must be looped in the network. This looping point can be the machine at the end of the PVC (end-to-end loopback cells) or equipment on the path (segment loopback cells)

3.3.4. DEVICE INFO >STATISTICS > xDSL

Statistics xDSL					
Mode	ADSL2+	Displays the DSL mode			
Traffic Type	ATM	Displays traffic type			
Status	UP	Displays status of the link (Disabled – Establishing- Linkup)			
Link Power State	L0	See Note below			
		Downstream	**Upstream**	**Downstream**	**Upstream**
Line Coding(Trellis):		On	Off	0	0
SNR Margin (0.1 dB):		117	243	0	0
Attenuation (0.1 dB):		265	130	0	0
Output Power (0.1 dBm):		208	120	0	0
Attainable Rate (Kbps): (Max you can obtain)		13024	1472	0	0
		Path 0		**Path 1**	
		Downstream	**Upstream**	**Downstream**	**Upstream**
Rate (Kbps): (Current Sync rate)		6653	448		
MSGc (#of bytes in overhead channel message		57	74		
B# (of bytes in mux data frame)		36	14		
M#(of Mux Data Frames in FEC Data Frame)		4	4		
T (Mux data frames over sync bytes)		4	1		
R# (of check bytes in FEC data frame)		16	14		
S (Ratio of FEC over PMD Data Frame Length)		0.1767	4.0		
L (# of bits in PMD Data Frame):		2399	148		
D (Interleaver depth)		160	2		
Delay (msec)		7.6	2.0		
INP (DMT symbol)		4.26	0.75		
Super Frames:		95843	53200		
Super Frame Errors:		0	5		
RS Words:		24152096	1067199		
RS Correctable Errors:		20	7		
RS Uncorrectable Errors:		0	0		
HEC Errors:		0	4		
OCD Errors:		0	0		
LCD Errors:		0	0		
Total Cells:		1674315	1121057		
Data Cells:		2123	4223		
Bit Errors:		0	215		
Total ES:		0	5		
Total SES:		0	0		
Total UAS:		23	23		

Status
This indicates the status of the connection. The link can be up but you're not connected to a service, in which case the Link Light on the front will be 'off', but the link will show up in the statistics.
The status goes through – Three stages – disabled – Establishing – Link up.

Link Power Status- The ADSL (G.992.3) and ADSL2+ (G.992.5) recommendations define a power management feature. Its primary application is to reduce the power consumption and the thermal dissipation of ADSL chip sets.

When there is no user traffic, the ADSL links can switch from a high power mode to a low power mode. If there is no user data for a long period of time, the link can switch further to a very low power, idle state. Once there is user data, the link will quickly return to the full power state.
The recommendations define three power states: L0, L2, and L3.

State	Name	Description
L0	Full On	This is the normal operating state. The system must be in this state in order to achieve the maximum data rate.
L2	Low Power	The ADSL link is active, but a low-power signal conveying background data is sent from the CO unit to the remote unit. Normal data is transmitted from the remote unit to the CO unit. This state is entered when there is little data to be transmitted. The reduced rate reduces the power consumption.
L3	Idle	When there is no user data to be transmitted, the system may enter the idle state. In this state there is no signal transmitted on the link. The unit may be without power.

SNR Margin
SNR Margin could be thought of as a "buffer zone" which is there to protect your connection against normal SNR fluctuations that can and do occur on a daily basis.
Once your SNR Margin starts to drop below 10dB on a traditional fixed rate line then you can experience problems.

Attenuation (0.1 dB):
Line attenuation is in relation to the "loop loss" on your line. The lower this figure the better, and the better chance you have of getting the faster speeds.
Attenuation is a term used to describe the reduction of the ADSL signal strength that occurs on the copper pair over distance and is measured in dB decibels. The further you are away from the exchange the higher your attenuation figure will be as the signal loss increases.

Output Power (0.1 dBm):
This is the upstream power used by your 6401 Rugged ADSL router on the copper circuit.

Super Frames: Total number of super frames.
Super Frame Errors: Number of super frames received with errors.
RS Words: Total number of Reed-Solomon code errors.
RS Correctable Errors: Total number of RS with correctable errors.
RS Uncorrectable Errors: Total number of RS words with uncorrectable errors.
HEC Errors: Total number of Header Error Checksum errors.
OCD Errors: Total number of out-of-cell Delineation errors.
LCD Errors: Total number of Loss of Cell Delineation.
Total Cells: Total number of cells.
Data Cells: Total number of data cells.
Bit Errors: Total number of bit errors.
Total ES: Total Number of Errored Seconds.
Total SES: Total Number of Severely Errored Seconds.
Total UAS: Total Number of Unavailable Seconds.
xDSL BER Test: Click this button to start a bit Error Rate Test.
Reset Statistics: Click this button to reset the statistics.

3.4. DEVICE INFO >ROUTE

Device Info -- Route
This page displays the routes currently in use within the router

The following symbols are used.

U This link is up

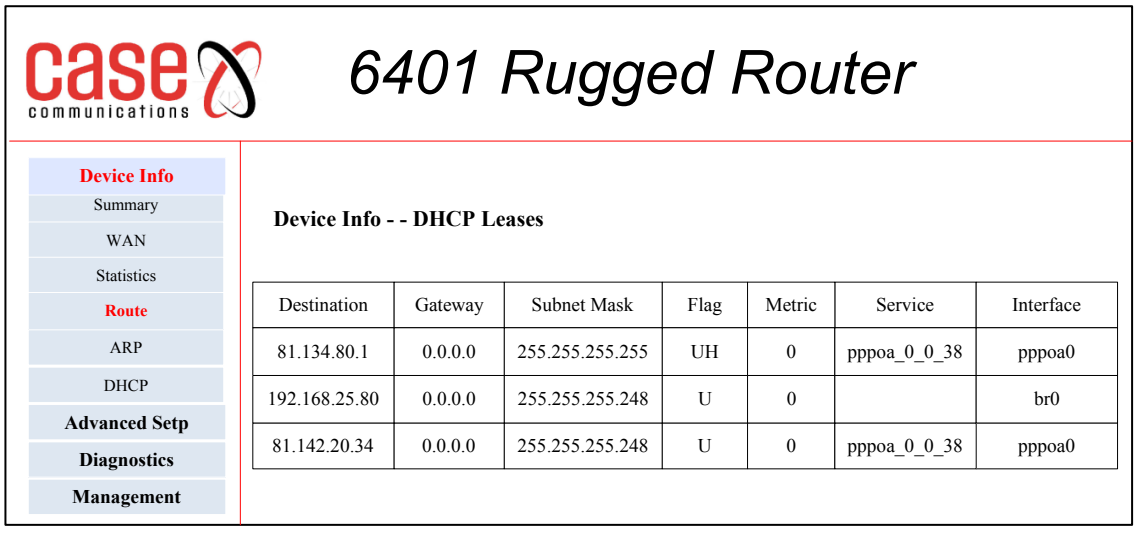
G This link is rejecting - Means that some other service incompatible with DSL is provisioned on the line.

H This link is the host

R Reinstate this link

D Dynamic (redirect) Dynamically re-directs requests for URL's

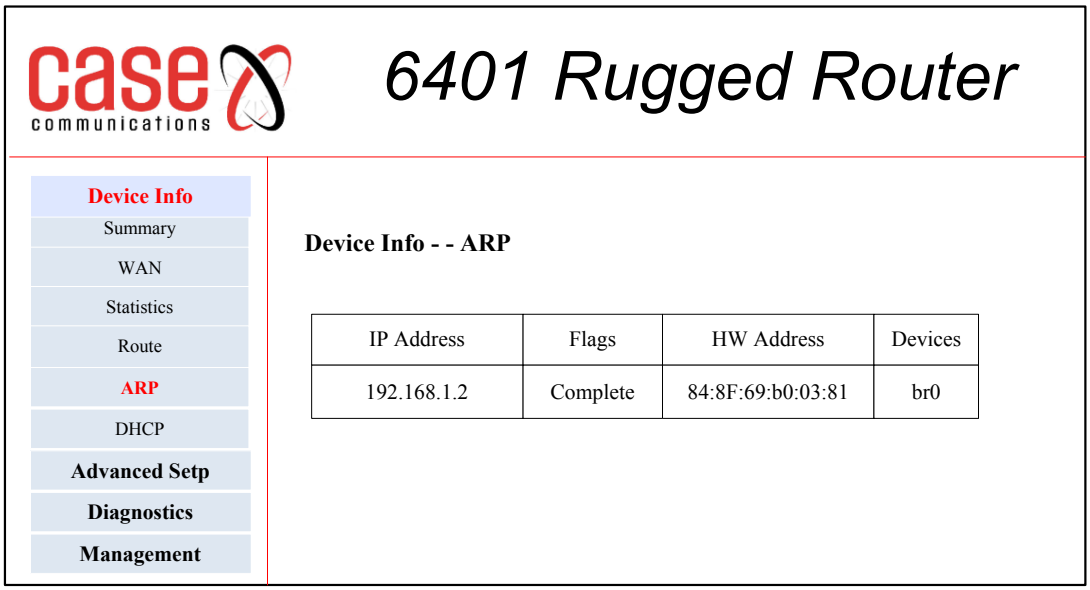
M Modified Redirect –What it does is break some TCP/IP utilities and it serves Search Pages with Ads on them if you mis-type a Domain Name



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
81.134.80.1	0.0.0.0	255.255.255.255	UH	0	pppoa_0_0_38	pppoa0
192.168.25.80	0.0.0.0	255.255.255.248	U	0		br0
81.142.20.34	0.0.0.0	255.255.255.248	U	0	pppoa_0_0_38	pppoa0

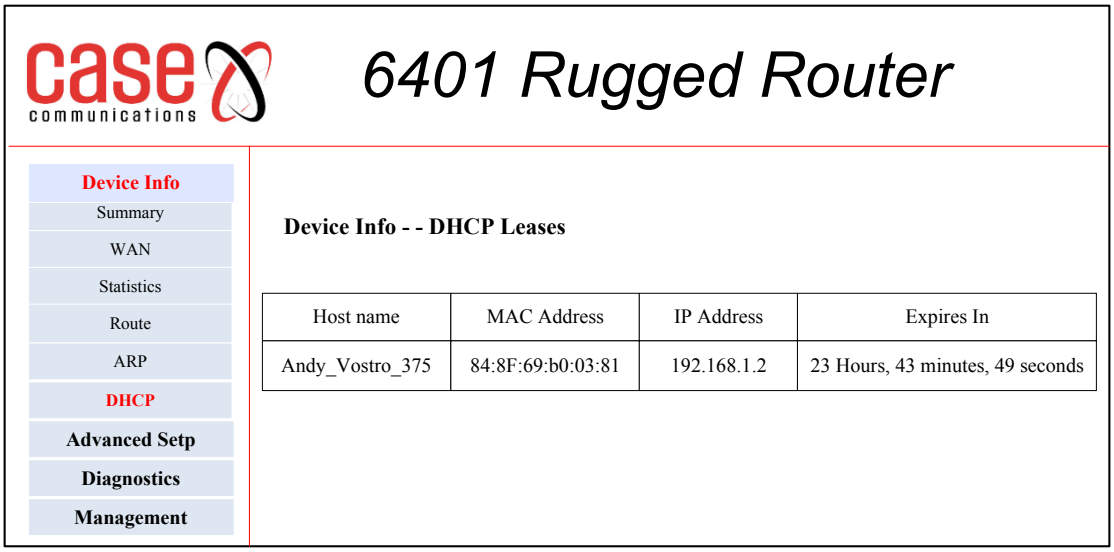
3.5. DEVICE INFO >ARP

The Address Resolution Protocol displays the MAC address of devices and their IP Addresses



3.6. DEVICE INFO >DHCP

The DHCP page displays the devices that the 6401 Rugged Router has issued with IP Addresses



Host name Name of the devices connected

MAC Address MAC Address of the device with the name 'Andy_Vostro_375'

IP Address The IP Address given to that device

Expires in The time that this IP Address will expire.

4 QUICK START GUIDE

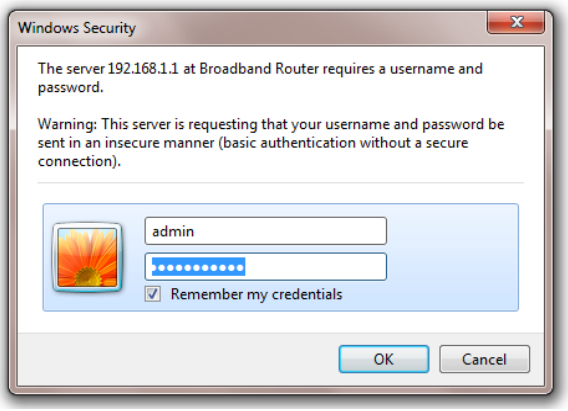
This Quick Start Guide gives you the minimum of information to allow you to get the router up and running quickly. It assumes that the 6401 Rugged Router is running default configuration.

4.1.1 EQUIPMENT REQUIRED

PC - with web browser and an IP address within the subnet of 192.168.1.xx (where xx is any address in the range apart from 1, which is the routers default address) use a subnet with a net mask of 255.255.255.0 or /24.

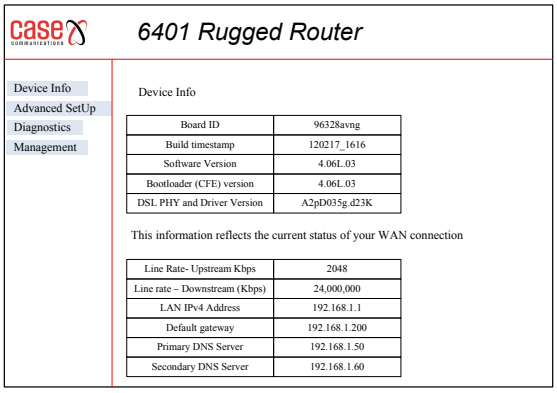
Standard Ethernet cable – straight or crossover (The Case 6401 router will auto-detect)

Login On the PC use the web browser to connect to IP 192.168.1.1
You should see the following screen



Note: If you're not able to obtain the logon screen try other Ethernet ports. If none of the Ethernet ports display the Logon screen you may find the router has been configured with a different IP Address. To ensure you have a connection to the port of the 6401 'Ping' the routers default IP address of 192.168.1.1. If no reply is received then use the reset switch on the rear of the router to 'default' the router back to its default settings.

On being asked for a login and password use **admin (or support)** for both entries
Having logged on the following page will displayed



On the left side select **Advanced Setup** to enter the configuration menu options.

4.1.2 STEP ONE CONFIGURE A LAYER TWO INTERFACE

1. Select **Layer 2 Interface**
2. Next you need to add an 'ATM' interface so select ' **Add'**

You will then be presented with the following page

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Configuration	Set to	Option
VPI [0 – 255]	0	Usual default for UK
VCI [32-65535]	38	Usual default for UK (This value will be used by the router to identify this path. This path will appear later as an option)
Select DSL Latency	Path0	The 6401 only has a single DSL path - select path 0
Select DSL Link Type	PPPoA	Select the service your ISP has provided, most common in the UK is PPPoA
Select Connection Mode	VC Mux	Select the mode of operation provided by your ISP, the most common is VC Mux in the UK
Service Category	UBR without PCR	Unless a specific service has been selected use UBR without PCR
Select IP QoS Scheduler Algorithm Strict Priority		Unless the router is on a network with QoS this option can be left as defaulted
Select		**APPLY / SAVE**

4.1.3 STEP 2 – SELECT WAN SERVICE

1. Select on **WAN Service**
2. Click **Add**
3. The following page is displayed

WAN Service Interface Configuration
Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

Atm0/0_0_38

SELECT THE WAN INTERFACE
Select the interface from the drop down menu. As its likely you're going to connect to an ADSL WAN Service the interface is the likely to be described by the VCI configured earlier (e.g. 38)

Atm0/0_0_38

If running PPPoA the link type (pppoa) and VPI / VCI will be displayed in the field. This can be changed to reflect a more meaningful name.

Enter Service Configuration	ppp0a_0_0_38

4. Click **Next**
   You will then see the following options

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password provided by your ISP .

PPP Username		Enter the username provided by your ISP
PPP Password		Enter the password supplied by your ISP
Authentication method	Auto	Select from drop down menu

☐ Enable Full Cone NAT	Leave un-checked
☐ Dial on demand (with idle timeout timer	Leave un-checked
☐ Use Static IPv4 Address	Leave un-checked
☐ Enable PPP debug mode	Leave un-checked
☐ Enable IGMP Multicast Proxy	Leave un-checked

APPLY / SAVE

Click Apply / Save

4.1.4 CONFIGURING THE LAN

In almost all circumstances the LAN IP address will have to be changed to suit the network. Please note that changing the LAN IP address of the router will result in loss of communication to the router until the PC can have its IP address set to match the new subnet and the new connection even run.

Select LAN from the Advanced Config menu. The following options will appear

Local Area Network (LAN) Setup
Configure the Broadband Router IP Address and Subnet Mask for LAN interface.
GroupName. [Default]

Option	Example	Meaning
IP Address	192.168.1.1	Configure the IP Address of the router on the LAN
Sub-Network Masks	255.255.255.0	Enter an appropriate sub network mask for the IP Address
☐ Enable IGMP Snooping		Leave unchecked unless required
☐ Enable LAN Side Firewall		Leave unchecked unless required
☒ Disable DHCP		Select to disable unless DHCP is required

1. Enter the required IP address and subnet mask for the Ethernet interface
2. Click **Disable DHCP Server (Unless DHCP is required)**
3. Click on **Apply/Save**
4. Change the IP address of the PC so that it is within the same subnet as the router
5. Log onto the router using its new IP address and enter the default **admin** username and password
6. Select **Advanced Setup**

You should now be able to connect to the Internet.
If not please go back over your settings to check they are correct. Here is a list of possible diagnostics.

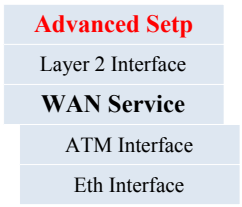
Indication	Status	Action
Power light	Off	Check power source
Link	Off	Check Line cord
Access to 6401	None	Check IP address, check cable – if unable to connect use reset button to default unit
Link Status		Check Statistics xDSL to see if 'up' If not check rate Please refer to the diagnostics section of this manual.
If up and no connection		Check ISP user name and password is as given

5. ADVANCED SET UP

5.1 LAYER TWO CONFIGURATION OPTIONS

5.1.1. INTRODUCTION

ADVANCED SETUP > LAYER2 INTERFACE



There are a maximum of two WAN paths out of the 6401, one via the ADSL / ATM interface and the other via one of the four the Ethernet Interfaces.

On entering the Layer 2 Interface screen a table showing any existing layer 2 interfaces is displayed, as shown below.

Interface	VPI	VCI	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler SP	Queue Weight	Group Precedence
Atm0	0	38	Path0	UBR	IPoA	Default Mode	Enabled	SP	1	8

DSL ATM INTERFACE CONFIGURATION

Choose, Add, or Remove to configure DSL ATM interfaces.

Interface	Shows the Interface configured
VPI	Virtual Path Identifier (In UK usually 0)
VCI	Virtual Circuit Identifier (In UK usually 38)
DSL Latency	Shows the DSL path, the 6401 only has a single DSL link = path0
Category	Traffic class for the interface here we see Unspecified Bit Rate
Link Type	Shows link type EoA (for PPPoE, IPoE & Bridging) or PPPoA, IPoA
Connection Mode	Single VC or VLAN Mux mode
IP QoS	Shows enabled or disabled
Scheduler	Strict priority or Weighted Fair Queuing
Queue Weight	1 to 64
Group or precedence	Select 1 - 8

ETH WAN INTERFACE DISPLAY

To View the Ethernet WAN ports Select **Advanced Setup >Layer 2 Interface > Eth Interface**

The following summary table is displayed.

Note Only one Ethernet port can be configured as a layer 2 WAN Port

Interface (Name)	Connection Mode	Remove
Eth0 / eth 0	Default Mode	

5.1.2. CONFIGURING A LAYER TWO ATM INTERFACE

ADVANCED SETUP > LAYER 2 INTERFACE>ATM INTERFACE

Device Info
Advanced Setp
Layer 2 Interface
ATM Interface
Eth Interface

Layer2 Interface and you can select WAN Service Interface (layer2 interface) over **ATM interfaces** or **ETH interface**.

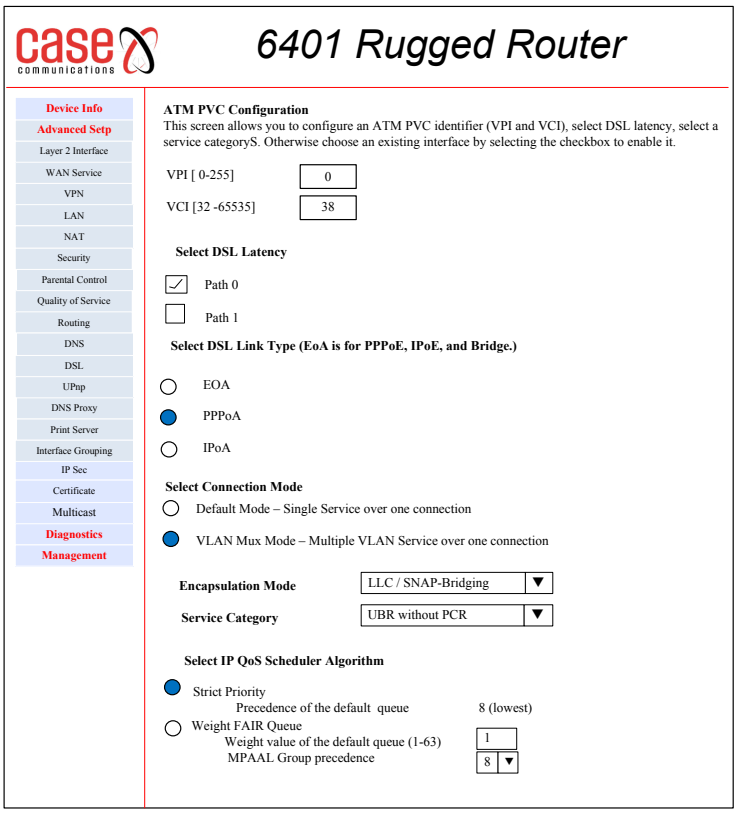
- **ATM Interface:** This configures a WAN port on the ADSL Link. ISP provides you VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings and the DSL Interface with RJ11 connector. (Figure 2-1)

- **ETH Interface:** This configures a WAN Interface over an Ethernet port

5.1.3 CONFIGURING AN ATM INTERFACE

ADVANCED SETUP >LAYER 2 INTERFACE> ATM INTERFACE

From layer 2 summary page, select ATM Interface and then '**add**' the following page will be displayed. Note this can be used as a reference configuration for most PPPoA ADSL connections.



Note;

If the interface is used by the WAN Service, you need to remove the corresponding WAN Service entry first before you can remove it here at layer 2.

The Table below explains the configuration options

LAYER 2 CONFIGURATION OPTIONS

On selecting add, a Layer 2 Interface the following page is presented. Here we see the option to configure 3 different layer 2 interfaces with the page appearing slightly different according to which of the three options has been selected;

1. Ethernet Over ATM
2. Point to Point Protocol Over ATM
3. IP Over ATM

Parameter	Value	Options
VPI [0- 255:]	0	Set according to ISP requirements
VCI 0 [0 – 65535] (UK =38)	38	Set according to ISP requirements (1-31 is generally reserved)
Select DSL Latency	Path 0	Select a Path0 or Path 1(6401 only has 1 path=0)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA		Select for PPPoE, IPoE or Bridging
PPPoA	PPPoA	Select for PPPoA – if that's ISP Service
IPoA		Select for IP over ATM

EOA CONFIGURATION OPTIONS

Select Connection Mode

Default Mode / VLAN Mux Mode	VLAN Mux	Single Service over one connection or Multiple VLAN Services over one connection.
Encapsulation Mode	VC Mux	Configure in accordance with ISP service. VC Mux LLC / SNAP – Bridging See note at end of this section for explanation

Service Categories see Service Category Table below

PPPoA CONFIGURATION OPTIONS

Select Connection Mode

Encapsulation Mode	VC Mux	Configure in accordance with ISP service. VC Mux LLC / SNAP-Routing See note at end of this section for explanation

Service Categories see Service Category Table below

IPoA CONFIGURATION OPTIONS

Select Connection Mode

Encapsulation Mode	VC Mux	Configure in accordance with ISP service. VC Mux LLC / Encapsulation See note at end of this section for explanation

Service Categories see Service Category Table below

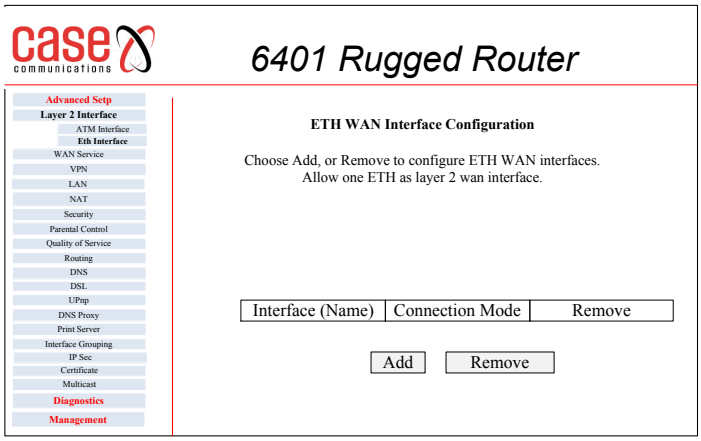
5.1.4 CONFIGURING AN ETHERNET INTERFACE

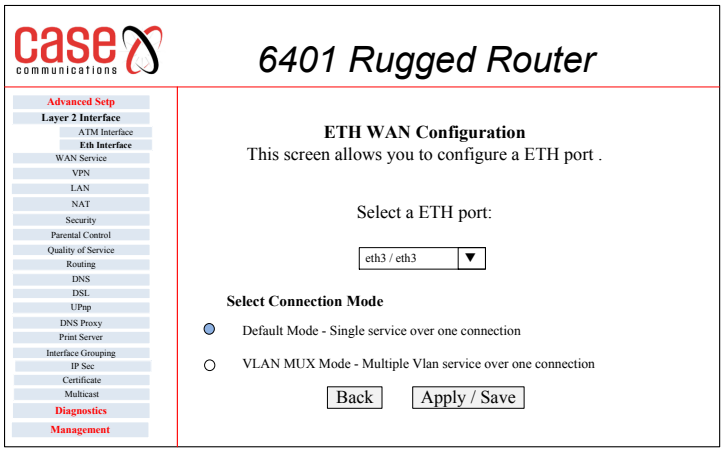
ADVANCED SETUP >LAYER2 INTERFACE>ETH INTERFACE

It's possible to configure one of the Ethernet ports on the router to work as a WAN port

Select Ethernet Interface' to enter the Ethernet WAN port configuration. Existing Ethernet ports that have been configured as WAN ports are displayed.

Select **'Add'** to configure a WAN interface via an Ethernet port.





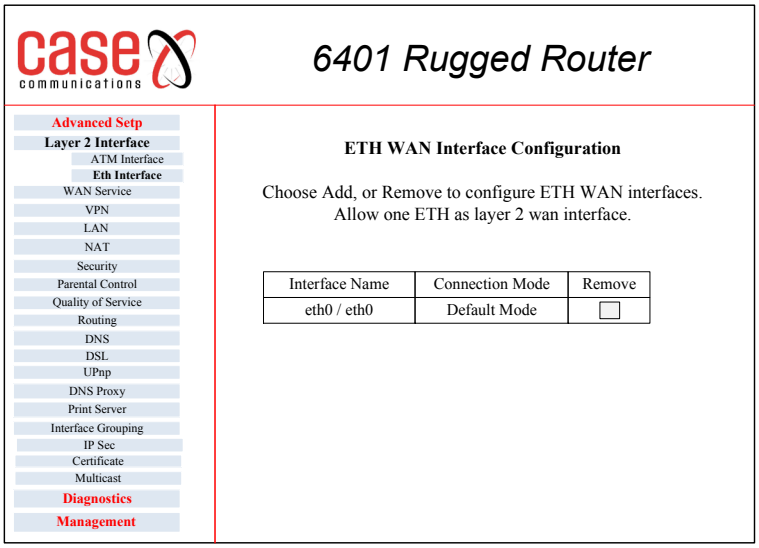
Select an **Ethernet port** from the drop down menu

Then **Select Connection Mode**

Default Mode – Single Service over one connection

VLAN MUX Mode – Multiple VLAN Service over one connection

Having selected 'Apply / Save' a page showing the configuration is displayed as shown below



5.1.5. EXPLANATION OF OPTIONS

ATM WAN INTERFACE OPTIONS
Under the ATM Interface we have the following options

EoA – Ethernet over ATM
Used for Point to Point Protocol over Ethernet, IP Over Ethernet or Bridging.

PPPoA – Point to Point Protocol Over ATM.
The Point-to-Point Protocol over ATM (PPPoA) is a network protocol for encapsulating PPP frames in AAL5. For more details on PPPoA please refer to PPPoA within the WAN Configuration

IPoA – IP over ATM
The use of Asynchronous Transfer Mode (ATM) technology and services creates the need for an adaptation layer in order to support information transfer protocols, which are not based on ATM. This adaptation layer defines how to segment and reassemble higher-layer packets into ATM cells, and how to handle various transmission aspects in the ATM layer. For more information on IPoA please refer to IPoA within the WAN Configuration part of this manual.

SERVICE CATEGORY TABLE
UBR Without PCR (Default)

Select IP QoS Scheduler Algorithm		
Strict Priority		Select strict or weighted
Precedence of the default queue		8 [Lowest]

Weighted Fair Queuing

Weight Value of the default queue: [1-63]	1	Enter value 1 to 63 (Default 1)
MPAAL Group Precedence:	8	Select value 1 to 8 (Default 8)

UBR With PCR

Peak Cell Rate: [cells/s]	Enter Peak Cell Rate Value (0 – 4095)

CBR

Peak Cell Rate: [cells/s]	Enter Peak Cell Rate Value (0-4095)

Non Real time VBR

Peak Cell Rate: [cells/s]	Enter Peak Cell Rate Value (0-4095)
Sustainable Cell Rate: [cells/s]	Enter Sustainable Cell Rate Value (0-4095)
Maximum Burst Size: [cells]	Enter Maximum Burst Size Value (0-4095)

Real time VBR

Peak Cell Rate: [cells/s]	Enter Peak Cell Rate Value (0-4095)
Sustainable Cell Rate: [cells/s]	Enter Sustainable Cell Rate Value (0-4095)
Maximum Burst Size: [cells]	Enter Maximum Burst Size Value (0-4095)

ENCAPSULATION MODES.
There are two main methods of Virtual circuit multiplexing.
VC-MUX is one of the two (the other being LLC encapsulation) mechanisms for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames specified by RFC 2684, Multiprotocol Encapsulation over ATM.

VC MUX
With virtual circuit multiplexing, the communicating hosts agree on the high-level protocol for a given circuit. It has the advantage of not requiring additional information in a packet, which minimizes the overhead. For example, if the hosts agree to transfer IP, a sender can pass each datagram directly to AAL5 to transfer, nothing needs to be sent besides the datagram and the AAL5

trailer. This tends to reduce fragmentation overhead (e.g., an IPv4 datagram containing a TCP ACK-only packet with neither IP nor TCP options exactly fits into a single cell). The chief disadvantage of such a scheme lies in duplication of virtual circuits: a host must create a separate virtual circuit for each high-level protocol if more than one protocol is used. Because most carriers charge for each virtual circuit, customers try to avoid using multiple circuits because it adds unnecessary cost.

It is commonly used in conjunction with PPPoE and PPPoA which are used in various xDSL implementations

LLC/SNAP Encapsulation—The user multiplexes multiple protocols over a single ATM VC. The protocol of a carried protocol data unit (PDU) is identified by prefixing the PDU with a Logical Link Control (LLC)/Sub network Access Protocol (SNAP) header.

ATM Service Categories:

Enabling packet level QoS for PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Real-time VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications

Within ATM traffic contracts form part of the mechanism by which "quality of service" (QoS) is ensured. There are four basic types (and several variants) which each have a set of parameters describing the connection.

1. **UBR** - Unspecified bit rate: traffic is allocated to all remaining transmission capacity.
2. **CBR** - Constant bit rate: a Peak Cell Rate (PCR) is specified, which is constant.
3. **VBR** - Variable bit rate: an average cell rate is specified, which can peak at a certain level for a maximum interval before being problematic. VBR has real-time and non-real-time variants, and serves for "bursty" traffic. Non-real-time is sometimes abbreviated to vbr-nrt.
4. **ABR** - Available bit rate: a minimum guaranteed rate is specified

Most traffic classes also introduce the concept of Cell Delay Variation Tolerance (CDVT), which defines the "clumping" of cells in time.

To maintain traffic contracts, networks usually use "shaping", a combination of queuing and marking of cells. "Traffic policing" generally enforces traffic contracts.

Traffic Parameters (Cell Rates)

Each ATM connection contains a set of parameters that describes the traffic characteristics of the source. These parameters are called source traffic parameters. They are:

Peak Cell Rate (PCR). The maximum allowable rate at which cells can be transported along a connection in the ATM network. The PCR is the determining factor in how often cells are sent in relation to time in an effort to minimize jitter. PCR generally is coupled with the CDVT (Cell Delay Variation Tolerance), which indicates how much jitter is allowable.

5.2 WAN SERVICES

5.2.1 INTRODUCTION

ADVANCED SETUP >WAN SERVICE

Having configured the layer 2 interfaces we now configure the Wide Area Network Interfaces from these menus. The configuration options are explained at the end of this section.

5.2.2 WAN SERVICE OPTIONS

The Layer 2 Configuration you have configured determines which WAN Services can be selected.

PPPoA – Point to Point Over ATM Only
IPoA – IP Over ATM

EOA WAN Options
Select WAN Service Type

- PPP over Ethernet (PPPoE)
- IP over Ethernet (IPoE)
- Bridging

Ethernet-

- IPoE
- PPPoE

The table below shows which services can be configured with which layer two services;

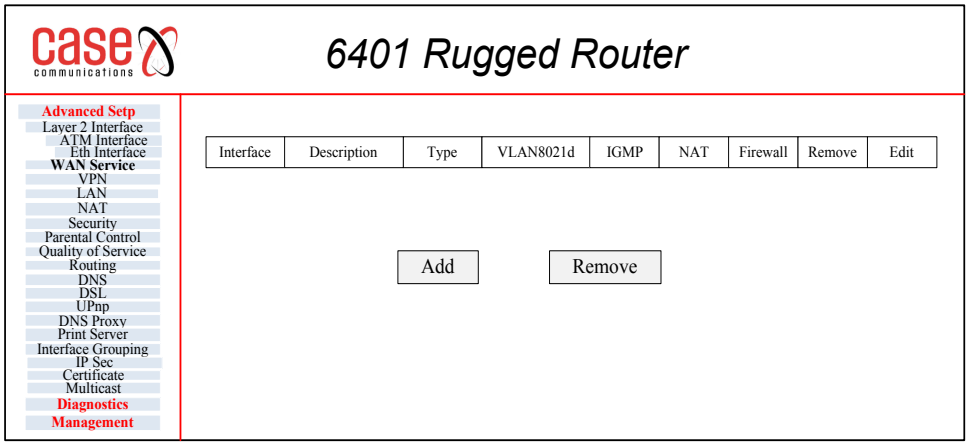
	Layer Two Service			
WAN Service	**EoA**	**PPPoA**	**IPoA**	**Ethernet**
PPP Over ATM (PPPoA)	No	Yes	No	No
PPP over Ethernet (PPPoE)	Yes	No	No	Yes
IP over ATM	No	No	Yes	No
IP Over Ethernet (IPoE)	Yes	No	No	Yes
Bridging	Yes	No	No	No

Having selected the WAN service then the sub services also provide different options, as shown below.

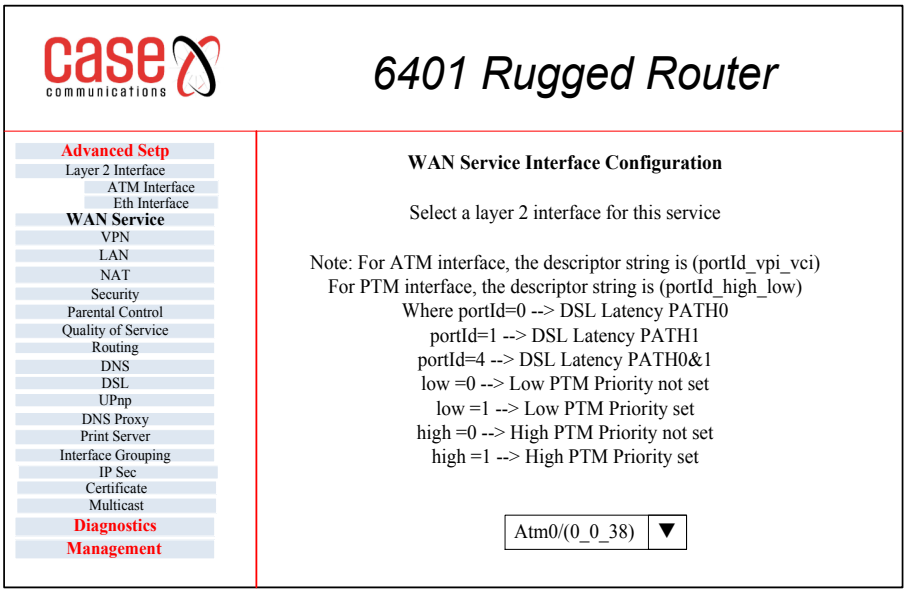
WAN Service Options	**PPPoA**	**PPPoE**	**IPoA**	**IPoE**	**Bridging**
NAT	Yes	Yes	Yes	Yes	N / A
Full cone NAT (enable/disable)	Yes	Yes	No	Yes	N / A
Dial on demand (idle timer)	Yes	Yes	No	No	N / A
Use PPP with IP Extension	Yes	Yes	No	No	N / A
Use Static IPv4 Address	Yes	Yes	Yes	Yes	N / A
Enable PPP debug Mode	Yes	Yes	No	No	N / A
Bridge PPPoE Frames between WAN and Local ports	No	Yes	No	No	N / A
Enable IGMP Multicast Proxy	Yes	Yes	Yes	IGMP	N / A
Firewall	Yes	Yes	Yes	Yes	Disabled
Quality of Service	Yes	Yes		Yes	Yes

5.2.2.1 CONFIGURING PPPoA (Layer 2 PPPoA)

Advanced setup>WAN Service
Select 'WAN set up' and you will be presented with the following table showing any existing WAN interfaces already configured. To add a new Interface select the 'ADD' button underneath the table



Select 'add' to add a new WAN Interface, the following screen will appear, with a drop down menu to select the Layer 2 interface.



Select the interface from the drop down menu. In our example we have configured an ATM layer 2 interface running VPI 0 and VCI 38 and this appears in our drop down box. This is the interface we want to use, so we leave this in place. If there was an Ethernet WAN Service configured then that would appear in the list and is configured identically as the ATM interface

Select 'next' and the following page appears

WAN Service Configuration

Enter Service description e.g. pppoA 0_0_38

Enter a description for the service or simply leave it as shown, and select 'Next'

You will then be presented with a series of forms to fill in these are explained below.

PPP Username and Password

PPP requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Configuration Options **Option**	**Example**	**Meaning**
PPP Username	Case	Enter the username provided by your ISP
PPP Password	Ca43XTZ	Enter the Password provided by your ISP
Authentication method	Auto	Select form the drop down menu • Auto • PAP • CHAP • MS Chap

☐ Enable full cone Nat (by default not enabled)

☐ Dial on demand (with idle timeout timer)

Note this option only appears if 'dial on demand is selected. Inactivity Timeout in minutes [1-4320) (default is 0)

☐ PPP IP Extension (not enabled by default)

☐ Use Static IP Address

NB. option below only appears if Static IP Address is selected.

IPv4 Address (enter your static IP Address if option selected) Example 172.16.40.23

☐ Enable PPP Debug Mode (not selected by default)

Multicast Proxy

☐ Enable IGMP Multicast Proxy (not selected by default)

Having selected your options select '**Next**' and the following page appears.

Routing -- Default Gateway

The Default Interface list can have multiple WAN Interfaces served as system default gateways but only one will be used according to the priority with the first being the highest, and the last one the lowest priority if the WAN is connected. The priority order can be changed by removing and re-adding the interfaces.

Select Default Gateway Interfaces		**Available Routed WAN Interfaces**
pppoA	▷ ◁	Note if only one interface has been configured it will be automatically added to the default gateway

Select Next to proceed to the DNS Server configuration

DNS Server Configuration

.

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, a Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again

◉ Select DNS Server Interface from available WAN interfaces

Selected DNS Server Interfaces		Available WAN Interfaces
pppoA	▷ ◁	

○ **Use the following Static DNS IP address**

Primary DNS Server	Enter IP Address of Primary Server
Secondary DNS Server	Enter IP Address of Secondary Server

Select ‘Next’ to see the WAN set up Summary

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type	PPPoA
NAT	Enabled
Full Cone NAT	Disabled
Firewall	Enabled
IGMP Multicast	Disabled
Quality of Service	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

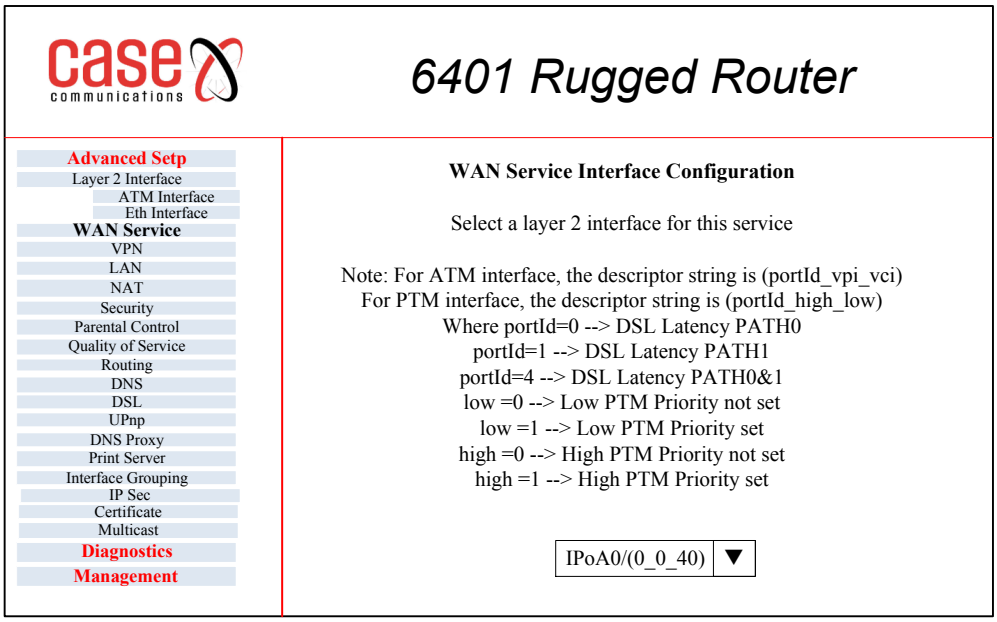
5.2.2.2 CONFIGURING IPoA (Layer 2 IPoA)

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit

Select Add to start configuring an IPoA Service, and then select the interface from the following drop down menu; The menu displays previously configured layer 2 interfaces.



WAN Service Configuration

Enter Service Description Ipoa_0_0_40

Either leave the description at the default or give the service a more meaningful description
Select **next** and the next page appears where the destination configuration is configured.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Menu Option	Example Value	Meaning
WAN IP Address	192.168.40.20	Add WAN IP Address of destination
WAN Subnet Mask	255.255.255.0	Add subnet mask for IP Address

Select Next and the following page appears

Select the options required, there are details on the meanings of these options at the end of this section.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

☐ Enable NAT (Default not enabled)

☐ Enable Full Cone NAT (Default not enabled)

☐ Enable Firewall (Default not enabled)

IGMP Multicast

☐ Enable IGMP Multicast (Default not enabled)

Select Next to be shown the 'Routing Default Gateway.

The Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select Default Gateway Interfaces		Available Routed WAN Interfaces
Ipoa0	▷ ◁	Note if only one interface has been configured it will be automatically added to the default gateway

Select Next to go to the DNS Server configuration

Select DNS Server Interface from available WAN interfaces		
Selected DNS Server Interfaces		Available WAN Interfaces
pppoA	▷ ◁	
Use the following Static DNS IP address		
Primary DNS Server	Enter IP Address of Primary Server	
Secondary DNS Server	Enter IP Address of Secondary Server	

If you are configuring an Ethernet WAN Interface you may be asked to configure a static DNS servers manually because there is no DHCP client on Ethernet WANs. This information can be provided by your ISP.

Select next

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	VLAN8021p	VLAN Mux ID	IGMP	NAT	Firewall
Ipoa0	Ipoa_0_0_35	N / A	N / A	Disabled	Disabled	Disabled

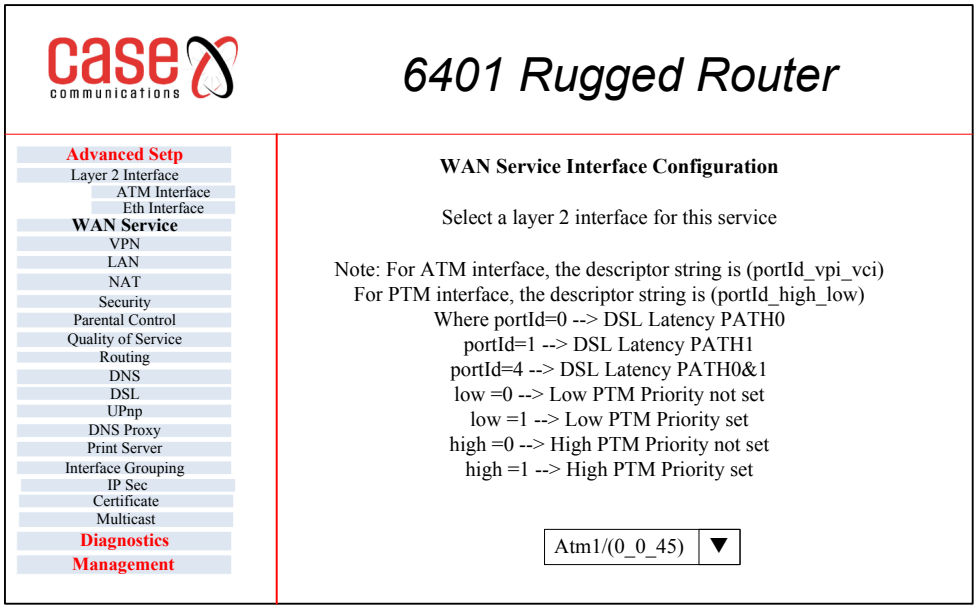
5.2.2.3 CONFIGURING PPP Over Ethernet (PPPoE - layer 2 EOA)

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit

Select Add to start configuring a PPPoE Service, and then select the interface from the following drop down menu;



WAN Service Configuration

Select WAN Service type:

[X] PPP over Ethernet (PPPoE) (Select this as we are configuring PPPoE)

[ ] IP over Ethernet

[ ] Bridging

Enter Service Description: Example – PPPoE_0_0_45

Select **next** to configure your ISP settings

Menu Option	Example	Meaning
WAN Service description	pppoe_eth0	Enter a free form name for this service or keep the default provided

PPP Username	Case	Enter the name provided by your ISP
PPP Password	6401ADSL	Enter the password provided by your ISP
PPPoE Service Name	Case_PPPoE	Enter free form name
Authentication Method	Auto	Select from drop down menu (Auto, PAP, CHAP, MSCHAP)

Menu Option	Default (for explanations please see end of this section)
☐ Enable Full Cone Nat	(Default not selected)
☐ Dial on demand with idle timer	(Default Not selected)
☐ PPP IP Extension	(Default Not selected)
☐ Use Static IPv4 Address (If selected field below opens)	(Default Not selected)
☐ IPv4 Address	Enter your static IPv4 Address
☐ Enable PPP Debug Mode	(Default Not selected)
☐ Bridge PPPoE frame between WAN and Local ports	(Default Not selected)

Multicast Proxy

☐ Enable Multicast IGMP Proxy	(Default Not selected)

Select Next to be shown the 'Routing Default Gateway.
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select Default Gateway Interfaces		Available Routed WAN Interfaces
Ppp0	▷ ◁	Note if only one interface has been configured it will be automatically added to the default gateway

Select Next to go to the DNS Server configuration

◉ Select DNS Server Interface from available WAN interfaces		
Selected DNS Server Interfaces		Available WAN Interfaces
ppp0	▷ ◁	
○ **Use the following Static DNS IP address**		
Primary DNS Server		Enter IP Address of Primary Server if not using option above
Secondary DNS Server		Enter IP Address of Secondary Server if not using the option above

Select next **Wide Area Network (WAN) Service Setup**

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	VLAN8021P	VLANMux ID	IGMP	Firewall
ppp0	ppp0e_eth0	PPPoE	N / A	N / A	Disabled	Enabled

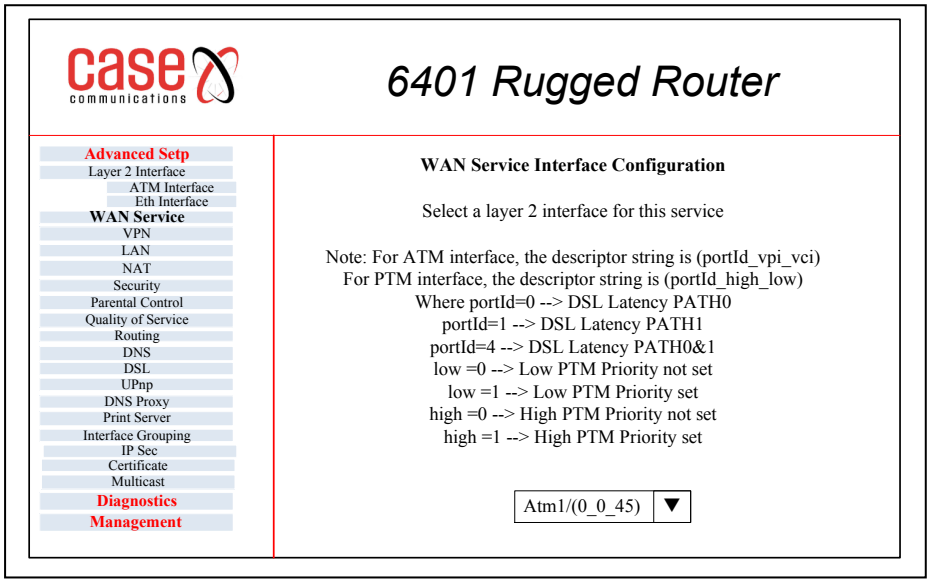
5.2.2.4 CONFIGURING IPoE (IP Over Ethernet – layer 2 EOA)

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit

Select Add to start configuring an IPoE Service, and then select the interface from the following drop down menu;



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway

X Obtain and IP Address Automatically (Default)

Option 60 Vendor ID

Option 61 IAID 8 hexadecimal digits

Option 61 DUID hexadecimal digits

Option 125 X Disable Enable

Use the following Static IP Address (Select if using a static IP Address)

WAN IP Address

WAN Subnet Mask

WAN Gateway IP Address

Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Menu Option	Default
☐ Enable NAT	Default not selected
☐ Enable Firewall	Default not selected

IGMP Multicast

☐ Enable IGMP Multicast	Default not selected

NB. Configure the Routing Default Gateway and DNS Server as per PPPoA
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Interface	Description	Type	VLAN 8021p	VlanmuxId	IGMP	NAT	Firewall
Atm0	ipoe_0_035	IPOE	N/A	N/A	Disabled	Enabled	Enabled

5.2.2.5 CONFIGURING BRIDGING – (layer 2 EOA)

There is very little configuration for Bridging, its only necessary to select an interface and provide it with a name, then the summary configuration table will be displayed as shown below.

Enter Service Description (example br_0_0_35)

Connection Type	Bridge
NAT	Disabled
Full Cone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Not Applicable
Quality of Service	Disabled

Interface	Description	Type	VLAN 8021p	VlanmuxId	IGMP	NAT	Firewall
armo	Br_0_035	Bridge	N/A	N/A	Disabled	Disabled	Disabled

5.2.3 EXPLANATION OF WAN SERVICE OPTIONS

PPPoA – Point to Point over ATM
Point-to-Point Protocol over ATM (PPPoA) is a network protocol for encapsulating PPP frames in AAL5. It is used mainly with DOCSIS and DSL carriers.
It offers standard PPP features such as authentication, encryption, and compression. If it is used as the connection encapsulation method on an ATM based network it can reduce overhead slightly (around 0.58%) in comparison to PPPoE. It also avoids the issues that PPPoE suffers from, related to having a MTU lower than that of standard Ethernet transmission protocols. It also supports the encapsulation types: VC-MUX and LLC based (as does PPPoE)

IPoA – IP over ATM
The use of Asynchronous Transfer Mode (ATM) technology and services creates the need for an adaptation layer in order to support information transfer protocols, which are not based on ATM. This adaptation layer defines how to segment and reassemble higher-layer packets into ATM cells, and how to handle various transmission aspects in the ATM layer.

The following ATM Adaptation Layer protocols (AALs) have been defined by the ITU-T. It is meant that these AALs will meet a variety of needs. The classification is based on whether a timing relationship must be maintained between source and destination, whether the application requires a constant bit rate, and whether the transfer is connection oriented or connectionless.

AAL Type 1- supports constant bit rate (CBR), synchronous, connection oriented traffic. Examples include T1 (DS1), E1, and x64 Kbit/s emulation.

AAL Type 2 - supports time-dependent Variable Bit Rate (VBR-RT) of connection-oriented, synchronous traffic. Examples include Voice over ATM. AAL2 is also widely used in wireless applications due to the capability of multiplexing voice packets from different users on a single ATM connection.

AAL Type 3/4 - supports VBR, data traffic, connection-oriented, asynchronous traffic (e.g. X.25 data) or connectionless packet data (e.g. SMDS traffic) with an additional 4-byte header in the information payload of the cell. Examples include Frame Relay and X.25.

AAL Type 5 - is similar to AAL 3/4 with a simplified information header scheme. This AAL assumes that the data is sequential from the end user and uses the Payload Type Indicator (PTI) bit to indicate the last cell in a transmission. Examples of services that use AAL 5 are classic IP over ATM.

Ethernet Over ATM Services.
PPPoE – Point-to-Point Protocol over Ethernet
The Point-to-Point Protocol over Ethernet is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.

IPoE – IP Over Ethernet
The most commonly used link layer protocol for Local Area Networks (LANs) is Ethernet and this is frequently used to support a range of network layer protocols, including IP. The IP datagrams are transmitted by encapsulation in Medium Access Control (MAC) frames (or LLC frames using MAC encapsulation). IPoE is also sometimes referred to as “DHCP” since that protocol plays a key role in the overall IPoE session.

Bridging
Bridging allows the network to appear as one flat network with devices at the remote site appearing on the local LAN.

NAT - Network Address Translation
The majority of NATs map multiple private hosts to one publicly exposed IP address. In a typical configuration, a local network uses one of the designated "private" IP address subnets (RFC 1918). A router on that network has a private address in that address space. The router is also connected to the Internet with a "public" address assigned by an Internet service provider. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address. The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply

Full-cone NAT, also known as *one-to-one NAT*

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
- *Any external host* can send packets to iAddr:iPort by sending packets to eAddr:ePort

IGMP snooping - is the process of listening to Internet Group Management Protocol, maintains a map of which links need which IP multicast streams.

IGMP snooping with proxy - reporting or report suppression actively filters IGMP packets in order to reduce load on the multicast router. Packets join and leave heading upstream to the router are filtered so that only the minimal quantity of information is sent.

Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again. (Default is the configured interface)

DNS Server Configuration
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again

5.3 VPN

5.31 L2TP INTRODUCTION

ADVANCED SETUP >VPN>L2TP

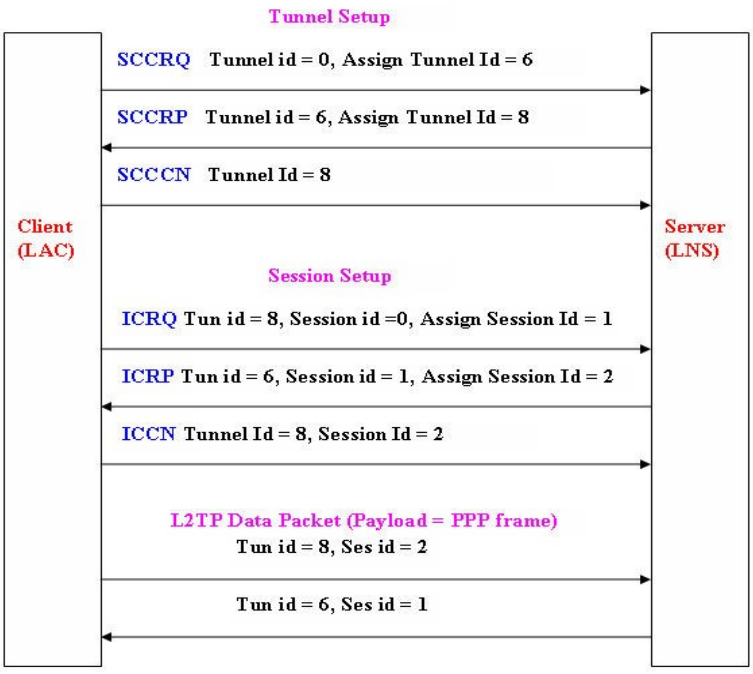
Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP session (or call) is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel.

The packets exchanged within an L2TP tunnel are categorised as either control packets or data packets. L2TP provides reliability features for the control packets, but no reliability for data packets.

DiagramL2TP Packet Exchange



L2TP Control and Data Packets

5.31.1 L2TP CONFIGURATION

ADVANCED SETUP > VPN>L2TP

This menu option allows you to configure an L2TP (Level 2 Tunnelling protocol) service.
On selecting the option the following page appears

L2TP Client Side PPP Connection

Choose Add, Remove to configure a PPP over L2TP WAN Service)

Tunnel name	LNS IP Address	Remove

Select 'Add' to add a new tunnel, this produces the following menu options.

Add a L2TP Client Side PPP Connection (PPPoL2TP WAN Service)

Menu Option	Example	Meaning
Tunnel name	Tunnel	Enter a freeform name
L2TP Server IP Address	80.80.16.240	Enter the IP Address of the remote server

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you

Menu Option	Example	Meaning
PPP Username	Case	Enter the name provided by your ISP
PPP Password	6401ADSL	Enter the password provided by your ISP

Authentication Method	Auto	Select from drop down menu (Auto, PAP, CHAP, MSCHAP)

☐ Enable Full Cone Nat (Default not selected)

☐ Dial on demand with idle timer (Default Not selected)

Use Static IPv4 Address (If selected field below opens) (Default Not selected)
☐ IPv4 Address Enter your static IPv4 Address

☐ Enable PPP Debug Mode (Default Not selected)

Multicast Proxy
☐ Enable Multicast IGMP Proxy (Default Not selected)

Select **Next** to see the WAN Set up Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Having selected 'Apply / save' we are taken back to the following Wide Area Service SetUp overview.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	VLAN 8021p	VLANMuxId	IGMP	NAT	Firewall	Remove	Edit
PPPoa0	Case_WAN	PPPoA	N/A	N/A	Disabled	Enabled	Enabled		
ppp1	PPPoL2tpAc	PPPoE	N/A	N/A	Disabled	Enabled	Enabled		

To Check the L2TP configuration return to the L2TP menu option and now you will see the following tunnel configured.

L2TP Client Side PPP Connection

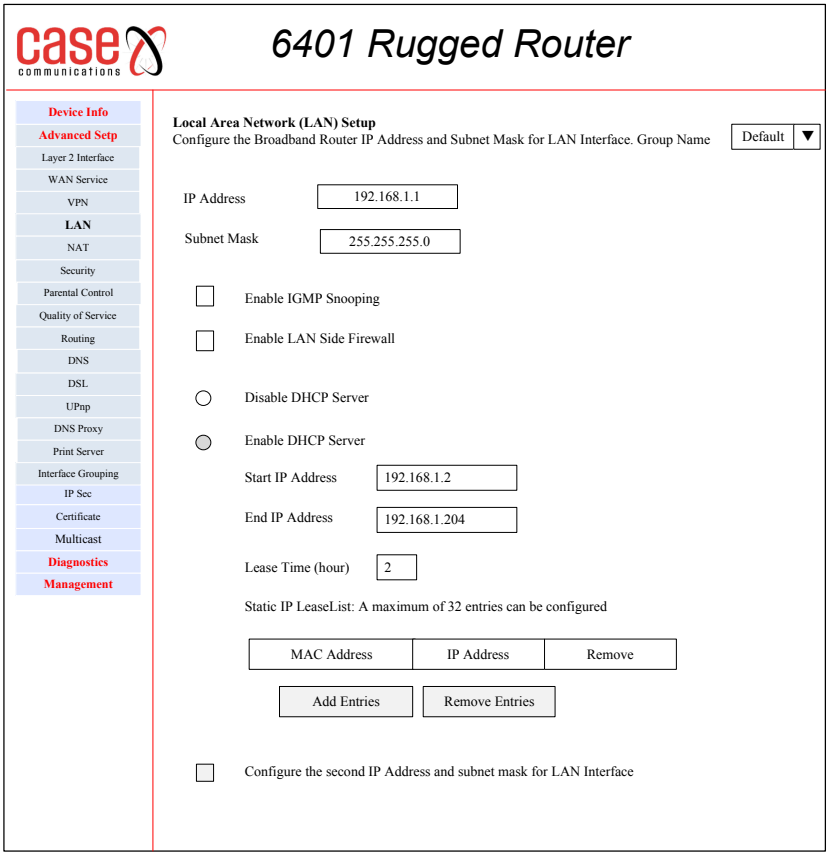
Choose Add, Remove to configure a PPP over L2TP WAN Service)

5.32 LAN CONFIGURATION

5.4.1 LAN SETUP

ADVANCED SETUP >LAN

This part of the menu allows the network manager to configure the LAN interfaces on the router. On entering this option we are presented with the following page.



Configure the Broadband Router IP Address and Subnet Mask for LAN interface.	(Default) (Ethernet 1)
IP Address: Configure an IP address for this routers MMI e.g. (The default IP Address is 192.168.1.1)	192.168.1.1
Subnet Mask: Configure the sub network mask for the port e.g. (The default sub network mask is 255.255.255.0)	255.255.255.0

Enable IGMP Snooping: Enable or disable IGMP Snooping. If you enable IGMP its necessary to select one of the follow modes

Standard Mode – In standard mode the multicast traffic, will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode – In blocking mode multi-cast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast groups.

Enable LAN side firewall; enable the routers firewall on the LAN ports.

Disable DHCP Server: Stop the router from issuing IP addresses to users connected to its LAN ports

Enable DHCP Server: Allows the router to issue IP Addresses to users connecting to its LAN ports. Enabling this option allows you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the Router's Ethernet LAN interface.
The DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the Router through the Ethernet port. When the Router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router, you must change the range of IP addresses in the pool used for DHCP on the LAN.

Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the default Start IP Address is 192.168.1.2, and the Start IP Address must be 192.168.1.2 or greater, but be equal to or smaller than 192.168.1.254.

End IP Address: End IP Address: Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is 192.168.1.254.

Leased Time (hour): The Leased Time is the amount of time in which a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is 24 hours**.**

Static IP Lease List: The function allows you to specify a reserved IP address for a PC on the LAN, that PC will always obtain the assigned IP address each time it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. Click the Add Entries button, and then you will set the rule in the screen as shown below

DHCP Static IP Lease
Enter the MAC address and Static IP address then click "Apply/Save". Up to 32 addresses can be configured.

MAC Address		The MAC address of the computer on the LAN for which you want to reserve an IP Address
IP Address		The IP address you want to reserve for this computer

Apply / Save

The addresses are displayed in a table as shown below

MAC Address	IP Address	Remove
00:25:86:c7:99:ab	192.168.1.20	

5.5 NETWORK ADDRESS TRANSLATION (NAT)

5.5.1 NAT – VIRTUAL SERVER CONFIGURATION

ADVANCED SETUP >NAT

Advanced Setp
Layer 2 Interface
WAN Service
VPN
LAN
NAT

Advanced Set up>NAT

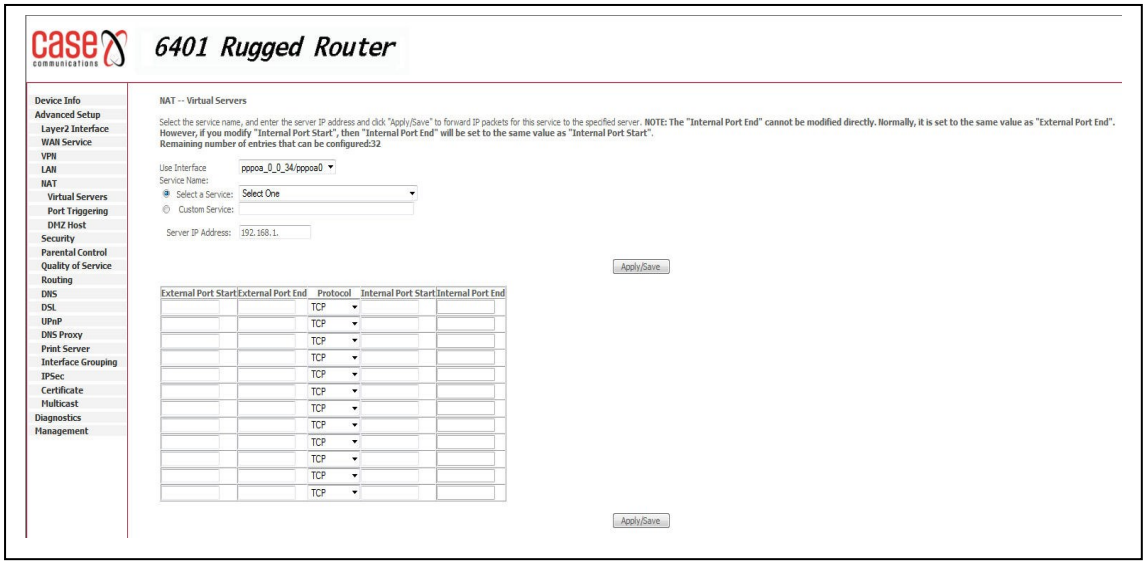
Virtual Server allows you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

A maximum of 32 entries can be configured

On entering the menu option there is a table showing any existing virtual servers, inviting the network manager to 'Add' a new service. Here we can see a configuration for an X-Windows terminal going out via WAN Interface ppp0

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface
X-Windows	6000	6000	TCP	6000	6000	192.168.1.175	Ppp0

To Add a new Interface select 'Add' and the following screen appears.



Adding a service

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
Remaining number of entries that can be configured: 32

NAT – Virtual Server Setup Options

User Interface: A drop down menu shows the interfaces available. These are the interfaces previously configured under the WAN Interface.

Service Name: Select a service name from the drop down list.

Custom Service. You can add your own service in this field

Server IP Address The IP Address of the server on the LAN side

The table below provides an example of a Virtual Server Configuration.

NAT – Virtual Server Setup Example – X-Windows

Menu Option	**Example**	**Meaning**
User Interface:	PPPoE_0_0_35/ppp0	Select an interface from the drop down list
Service Name:		
☐ **Select a service**		Select a pre-defined name form the drop down list or select 'custom service' and configure your own parameters
☐ **Custom Service.**		Use a free form name and configure your parameters.
Server IP Address	192.168.1.175	

The following table can allow mapping of internal to external ports and allows the network manager to configure whether the protocol should be TCP and UDP, TCP only or UDP only

External Port Start	External Port End	Protocol		Internal Port Start	Internal Port End
2611	2612	TCP	▼	2611	2612
6667	6667	TCP	▼	667	667
6500	6500	UDP	▼	6500	6500
27900	27900	UDP	▼	27900	27900
		TCP/UDP			
		UDP			

Having configured your options select 'Next' and the following summary display will be shown, allowing the network manager to view the options configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface
X-Windows	912	912	TCP	2912	912	192.168.1.230	pppoA

5.5.2 NAT – PORT TRIGGERING

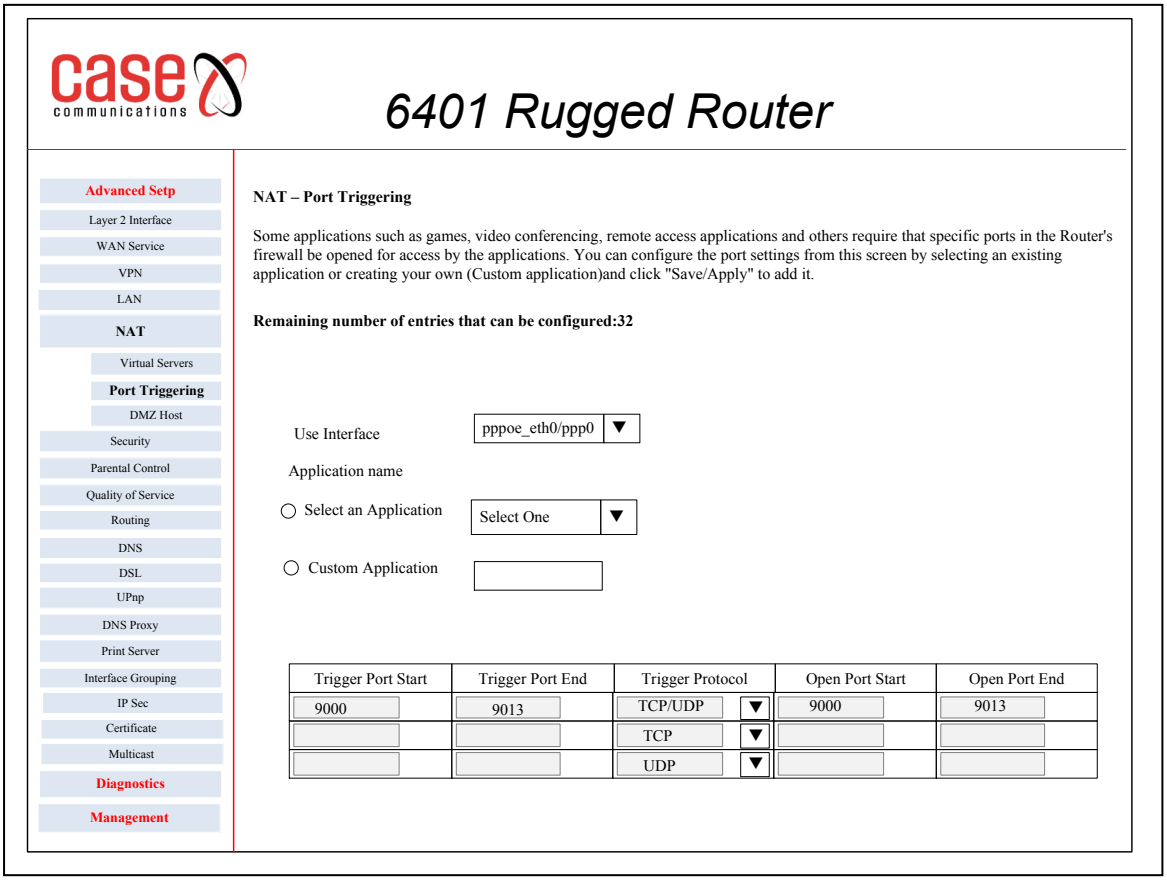
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

On entering the NAT - Port Triggering option the following screen appears.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port range		Protocol	Port Range			
		Start	End		Start	End		

To add ports select the 'Add' button and the following options can be configured.

On selecting 'Add' a new screen with the configuration parameters appears, this is shown below.



NAT -- Port Triggering – explanation of the options.

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.
Remaining number of entries that can be configured: 32

Use Interface: A drop down menu shows the interfaces available. These are the interfaces previously configured under the WAN Interface.

Service Name: Select a service name from the drop down list. If selecting a pre-defined service the 6401 will automatically complete the port and protocol values.

Custom Service. You can add your own service in this field

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
6801	6801	UDP	6801	6801	UDP

Trigger Port Start Enter the port range from wish to trigger to open the firewall. For example we may want to open the firewall for an application which uses ports 5400 to 5500, so we enter 5400 in this first column.

Trigger Port End Enter the last port in the range, for example 5400 to 5500.

Trigger Protocol: Enter the protocol that is to be operated via the port, the options are TCP and UDP, TCP only UDP only.

Open Port Start This is the protocol Start Value used to open the port. For example open port on 200000

Open Port End This is the protocol End Value used to close the port. For example close port on 20059

Open protocol Enter the protocol that is to open the port, the options are TCP and UDP, TCP only UDP only.

Having selected apply a summary of the configuration is provided as shown below

Application Name	**Trigger**			**Open**			**WAN Interface**	**Remove**
	Protocol	Port range		Protocol	Port Range			
		Start	End		Start	End		
Case_IP-Phone	UDP	6801	6801	UDP	6801	6801	PPPoA	

Note: If you select an application from the drop-down list, the fields will be automatically added for you.

5.5.3 NAT – DMZ HOST.

The Case Communications 6401 Rugged Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to a DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address: Enter the IP Address of your DMX host

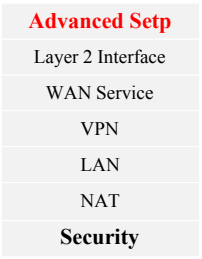
- To add a new DMZ Host:
- You can enter the computer's IP address and then click Save/Apply to activate the DMZ host you set on this page.

Note:
DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change while using the DHCP function.

5.6 SECURITY

5.6.1 IP FILTERING

ADVANCED SETUP > SECURITY>IP FILTERING



Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

On selecting this option the following table is displayed.

Filter Name	IP Version	Protocol	SrcIP/ Prefix Length	ScrPort	DstIP/ Prefix Length	DstPort	Remove

Choose Add or Remove to configure outgoing IP filters

Add IP Filter -- Outgoing
This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter name: Select a name for this filter

IP Version Select IP v 4 or IP v 6

Protocol Select the protocol this filter will apply to: TCP &UDP, TCP, UDP or ICMP only.

Source IP address [/prefix length]: Enter the IP Address

Source Port (port or port:port): Enter source the port number

Destination IP address [/prefix length]: Enter the IP Address of the destination

Destination Port (port or port:port): Enter the destination port details.

Select **'save'** and the following screen appears, giving a summary of the configuration.

Outgoing IP Filtering Setup
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Filter Name	IP Version	Protocol	SrcIP /PrefixLength	Src Port	DstIP/ PrefixLength	DstPort	Remove
Case_Test	4	TCP or UDP	192.168.2.30	23	80.26.45.200	23	

Advanced Setp
Layer 2 Interface
WAN Service
VPN
LAN
NAT
Security

Incoming IP Filtering Setup

When the When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be accepted by setting up filters.

On selecting this option the following table is displayed.

Filter Name	Interfaces	IP Version	Protocol	SrcIP /PrefixLength	Src Port	DstIP/ PrefixLength	DstPort	Remove
Case_Test	pppoa,br0	4	TCP or UDP	192.168.2.30	23	80.26.45.200	23	

Choose Add or Remove to configure incoming IP filters

Add IP Filter -- Incoming

This screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter name:	Select a name for this filter
IP Version	Select IP v 4 or IP v 6
Protocol	Select the protocol this filter will apply to: TCP &UDP, TCP, UDP or ICMP only.
Source IP address [/prefix length]:	Enter the IP Address
Source Port (port or port:port):	Enter source the port number
Destination IP address [/prefix length]:	Enter the IP Address of the destination
Destination Port (port or port:port):	Enter the destination port details.
WAN Interfaces	Tick the interfaces that the filter needs to be applied to

Select **'save'** and the following screen appears, giving a summary of the configuration.

NOTE: If the 6401 is to be managed using a SNMP management system like CaseView then you will have to enter the public (ADSL) IP address of the SNMP management system for both UDP/TCP and ICMP traffic but only if the access is over ADSL. If the access is via the Ethernet port (or via an IPSec tunnel) then an Incoming IP Filtering rule is not needed.

5.6.2 MAC FILTERING

Before the network manager can configure MAC Filtering Bridging must be configured.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another on an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

On entering the MAC Filtering page, if the 6401 Rugged ADSL Router has Bridging configured the following table will appear

Interface	Policy	Change
Atm0	FORWARD	

Choose 'Add' or 'remove' to configure MAC Filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Add Remove

Select 'Add' to display the following table

Add MAC Filter

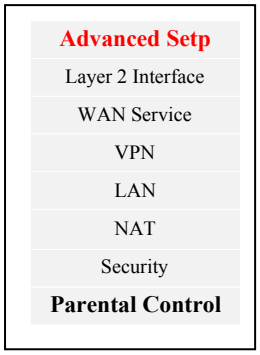
Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter

Menu Option	Example	Meaning
Protocol Type	NetBEUI	Select from drop down menu (PPoE, IPv4, IPv6, Apple Talk, IPX, NetBEUI, IGMP)
Destination MAC Address	00:25:86:c7:99:ab	Enter MAC Address of destination device
Source MAC Address	84:8F:69:b0:03:81	Enter MAC address of source device
Frame Direction	LAN>=<WAN	Select from drop down menu, LAN>=<WAN, WAN=>LAN, LAN=>WAN
WAN Interfaces (Configured in Bridge mode only)		
Select from drop down menu	Br_0_0_45	Select from drop down menu, (pppoe_eth0/ppp0, pppoe_eth4/ppp2 etc.)
		Save / Apply

5.7 PARENTAL CONTROL

5.7.1 TIME RESTRICTIONS

ADVANCED SETUP > PARENTAL CONTROL> TIME RESTRICTIONS



Choose - Advanced Setup>Parental Control>

Parental control provides two ways to control access to the Internet using Time Restrictions and a Url Filter. These are explained below.

Time Restriction allows you to control the Internet activities on the router by restricting the time of surfing. URL Filter limits every computer connected to the router to access certain websites. These two features work independently.

User Name	Enter the PC's user name
Browser's MAC Address	84:8f:69:b0:03:81
Other MAC Address	Enter other MAC Addresses to be restricted.

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select							

Select the days of the week the restrictions should apply.
Select ADD and a page is displayed which allows you to add restrictions as shown below/

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN devices, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name	Enter the PC's user name
Browser's MAC Address	84:8f:69:b0:03:81
(NB the router will detect a connected PC's MAC address)	
Other MAC Address	Enter other MAC Addresses to be restricted.

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select							

Select the times the restrictions should apply.
Note if the routers time has not been set this option will not be set and a warning given. To set the time go to **Management>Internet Time** and configure the region and time.

Start Blocking Time (hh:mm)	
End Blocking Time (hh:mm)	

Having configured time restriction click save and the following table will be displayed.

User name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop
Case-Test	84:8F:69:b0:03:81			X					10.00	11.00

5.7.2 URL FILTER

This feature allows you to configure the filter rules based on URL's to control all the computers in the LAN to access the specified port. This operates independently of the Time Restriction feature.
On entering this option a table is displayed showing any filters than have been configured and the rule applied to the filter
Note it's necessary to select the list type before entering the URL's of the sites. A Maximum of 100 entries can be configured..

If the port number is left blank the 6401 router will use port 80 by default.

URL List Type. **Exclude** **Include**

Address	Port	Remove
www.casecomms.com	80	Select to remove

There are two policies for the URL Filter.

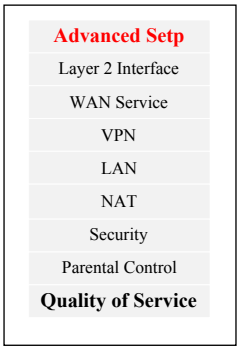
Exclude: Block the PCs to access the specified URL.

Include: Only allow the PCs to access the specified URL.

5.8 QUALITY OF SERVICE

5.8.1 INTRODUCTION

ADVANCED SETUP > QUALITY OF SERVICE



Choose - Advanced Setup>Quality of Service – To enable Quality of Service. Quality of Service helps to prioritise data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

With the 6401 Rugged Router traffic will generally enter the router from the Ethernet ports and will be marked for transmission over the WAN port or via other Ethernet ports. The order of configuration for Quality of Service should be;

1. Configure the interfaces – Ethernet and ATM
2. Enable - QoS Queue Management and Configuration
3. Configure the queues – QoS setup
4. Configure Traffic rules to match traffic and assign to the Queues.

Quality of Service is set up on three screens in the Quality of Service menu

Step 1 **Layer 2** Setup Interfaces If not already configured.	**Step 2** **Queue Management Configuration** Tick menu option to Enable QoS and assign default DSCP from drop down box	**Step 3** **Queue Configuration** Configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface	**Step 4** **QoS Classification** Create traffic class rules to classify upstream traffic, assign a queue which defines the precedence and interface and optionally overwrites the DSCP header. A rule consists of 1. Class Name 2. One condition matching the configuration

5.8.2. CONFIGURING A LAYER TWO INTERFACE

Generally these will have been configured before in the layer two interfaces settings.

It's possible to configure an Ethernet interface from the QoS menu, but to configure an ATM interface this must have been previously configured from the Layer Two menu option.

When configuring the layer two parameters for an interface select the menu options to configure the IP QoS Schedules for the interface. These options are

Strict Priority
Precedence of the default queue — Default 8 (lowest)

Weighted fair queuing
Weighted fair value of the default queue [1-63] — 1
MPAAL Group precedence — 1 to 8

5.8.3. QOS – QUEUE MANAGEMENT CONFIGURATION

If Enable the QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

If you enable QoS (tick box) you are presented with another menu option, and a drop down box where you can select your DSCP Mark.

Select Default DSCP Mark

Note: A default DSCP mark is used to mark all 'egress' packets that do not match any classification rules.

Enabling QoS then allows selection of the DSCP values from the drop down menu, which displays the following options. Note' No-Change (-1) and Auto Marking (-2) options are also displayed.

Assured Forwarding (AF) Behaviour Group				
Priority	**Lowest**			**Highest**
	Class 1	**Class 2**	**Class 3**	**Class 4**
Low Drop	AF11 (DSCP 10)	AF 21 (DSCP 18)	AF 31 (DSCP 26)	AF 41 (DSCP 34)
Med Drop	AF 12 (DSCP 12)	AF 22 (DSCP 20)	AF 32 (DSCP 28)	AF 42 (DSCP 36)
High Drop	AF 13 (DSCP 14)	AF 23 (DSCP 22)	AF 33(DSCP 30)	AF 43 (DSCP 38)

5.8.4. QOS QUEUE CONFIGURATION-SETUP

This screen allows the network manager to configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface.

- In ATM mode a maximum of 16 queues can be configured
- In PTM (Packet Transfer Mode) a maximum of 8 queues can be configured.
- For each Ethernet interface a maximum of 4 queues can be configured.

- If configuring an Ethernet interface its only possible to set precedence levels
- If configuring a WAN port the Precedence or weighting can be selected as well as DSL latency

If any interfaces are configured on entering this option we see a table as shown below, which displays the various queues configured.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable
Eth0_telnet	23	Eth0	SP	2				☑
Default	25	atm0	WFQ	4	1	Path0		☑
Voice	27	atm0	WFQ	4	12	Path0		☑

These fields have the following meanings

Note: For SP scheduling, queues assigned to the same Layer 2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others

Click 'Apply/Save' to save and activate the queue.

Name:	Provide a Name for this schedule
Enable	Enable or disable this service
Interface	This will be the Layer 2 interfaces or any of the LAN ports (Atm0, Eth0 WAN, Eth1, Eth2, Eth3, Eth4)
Precedence (NB1)	1 to 7 (For ATM WAN interface) 1 to 4 (for Ethernet Interface)
Queue Weight	1 to 63 (NB Lower value gives higher priority)
DSL Latency	Displays the DSL latency set for the interface if the schedule is set on a DSL interface.
PTM Priority	Packet Transfer Mode – alternative to ATM not currently enabled

Note 1
Lower integer values for precedence imply higher priority for this queue relative to others.
The queue entry configured here will be used by the classifier to place ingress packets appropriately.

QoS Queue Configuration – Example for interface with Precedence

Name	Voice
Enable	Enable
Interface	Select from the drop down menu of interfaces on the router
Precedence	1 (This rule has highest priority)

5.8.5. CONFIGURING QOS CLASSIFICATION

This screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte.
A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.
The Table below shows the Class Interfaces and where they may be used.

Class Interface	Available EtherType	Classification Queue (assuming Queues for all Ethernet ports are set)
LAN	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth0, eth1, eth2, eth3, eth4 or ATM
WAN	IP	eth0, eth1, eth2, eth3 or eth4
Local	IP	eth0, eth1, eth2, eth3, eth4 or ATM
Eth0	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth1, eth2, eth3, eth4 or ATM
Eth1	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth0, eth2, eth3, eth4 or ATM
Eth2	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth0, eth1, eth3, eth4 or ATM
Eth3	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth0, eth1, eth2, eth4 or ATM
Eth4	IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866 or 8021Q	eth0, eth1, eth2, eth3 or ATM
Configured ATM	IP	eth0, eth1, eth2, eth3 or eth4

QoS Classification Setup -- A maximum 32 entries can be configured..

The screen that will be displayed will depend on which options are set. Therefore we have provided a number of tables which show the options available. However there are too many combinations to include all within this menu.

Specify Classification Criteria							
	WAN	LAN, Local ATM, Ethernet					
Ether type	IP Only	IP	ARP	IPv6	PPPoE	8865/6	802.1Q
802.1p Priority Check							☑
Source MAC Address	☑	☑	☑	☑	☑	☑	
Source MAC Mask		☑	☑		☑	☑	
Destination MAC Address					☑	☑	
Destination MAC Mask		☑	☑			☑	
Source IP Address	☑	☑		☑			
Destination IP Address	☑	☑		☑			
DSCP Check	☑	☑		☑			
Protocol	☑	☑		☑			
TCP/UDP	☑	Port Nos		☑			
ICMP	☑	☑					
IGMP	☑	☑					
ICMPv6				☑			
Specify Classification Results							
Assign classify queue	☑	☑	☑	☑	☑	☑	☑
Mark DSCP	☑	☑	☑	☑	☑	☑	☑
Mark 802.1p Priority		☑	☑	☑	☑	☑	☑
TAG VLAN ID		☑	☑	☑	☑	☑	☑

The Network options available are described in the table below.

Traffic Class name Name given to this Profile

Rule Order The order this rule should be carried out in, the number will depend on the number of Traffic Class rules entered. If there are no previously configured rules in place the only option will be 'last.

Rule Status Enable or Disable

Specify Classification Criteria

Class Interface Select a list of available interfaces from the drop down menu. (e.g. LAN, WAN, Local, eth0, eth1, eth2, eth3, eth4, pppoa0/atm1)

Ether type Select from the drop down menu (IP, ARP, IPv6, PPPoE_DISC, PPPoE_SES, 8865, 8866, 802.1Q)

802.1p Priority Check The QoS technique, also known as **class** of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged **frames** as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to Differentiate traffic.

802.1P Priority levels						
Level	**Code**	**Application**		**Level**	**Code**	**Application**
0 Lowest	BK	Background		4	VI	Video, <100ms latency
1	BE	Best Effort		5	VO	Voice, <10ms latency
2	EE	Excellent Effort		6	IC	Inter-network control
3	CA	Critical Applications		7	NC	Network control

Source MAC Address Enter the Source (originating devices) MAC Address e.g. 00:1A:A0:93:A5:65

Source MAC Mask Type the mask for the MAC address. Enter the mask with periods Separating the three groups of four characters (112.334.556.778, for Example). Entering 255.255.255.255 as the mask causes the access Point to accept any IP address. If you enter 0.0.0.0, the access point Looks for an exact match with the IP address you entered in the IP Address field.

Destination MAC Address Enter the destination device (receiving devices) MAC Address e.g. 00:11:22:33:44:AA

Destination MAC Mask Type the mask for the MAC address. Enter the mask with periods separating the three groups of four characters (112.334.556.778, for example). Entering 255.255.255.255 as the mask causes the access point to accept any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.

Source IP Address Enter the IP Address for the source / originating device e.g. 192.168.1.20/24 (255.255.255.0)

Destination IP Address Enter the IP Address of the remote service the application is to reach. E.g. 172.16.20.1/ 16 (255.255.0.0)

Differentiated Services Code Point (DSCP) Check. Select from the drop down menu, the options within the DSCP Drop down menu are;

<0-63>	Differentiated services	codepoint value
AF11	Match packets with AF11	dscp (001010)
AF12	Match packets with AF12	dscp (001100)
AF13	Match packets with AF13	dscp (001110)
AF21	Match packets with AF21	dscp (010010)
AF22	Match packets with AF22	dscp (010100)
AF23	Match packets with AF23	dscp (010110)
AF31	Match packets with AF31	dscp (011010)
AF32	Match packets with AF32	dscp (011100)
AF33	Match packets with AF33	dscp (011110)
AF41	Match packets with AF41	dscp (100010)
AF42	Match packets with AF42	dscp (100100)
Af43	Match packets with AF43	dscp (100110)
CS1	Match packets with CS1(precedence 1)	dscp (001000)
CS2	Match packets with CS2(precedence 2)	dscp (010000)
CS3	Match packets with CS3(precedence 3)	dscp (011000)
CS4	Match packets with CS4(precedence 4)	dscp (100000)
CS5	Match packets with CS4(precedence 5)	dscp (101000)
CS6	Match packets with CS4(precedence 6)	dscp (110000)
CS7	Match packets with CS7(precedence 7)	dscp (111000)
Default	Match packets with default	dscp (000000)
ef	Match packets with EF	dscp (101110)

Protocol Select from drop down menu – TCP – UDP – ICMP-IGMP (where IPv6 ICMPv6 is displayed)

Specify Classification Results Assign Classify Queue Select the 'Classification Queues' previously configured under 'Queue Config. Note they will have been given 'key' numbers.

Mark Differential Service Code Point (DSCP) This is the same drop down menu as shown above and allows you to mark the traffic with a DSCP value.

Mark 802.1p Priority Provides a layer 2 802.1p priority to unassigned frames. Please refer to the table previously showing the 802.1p priority levels.

TAG VLAN ID IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

802.1Q does not actually encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType/Length fields of the original frame,

extending the minimum and maximum frame sizes from 64 and 1,518 bytes (octets) to 68 and 1,522 bytes. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, CFI, and VID.

802.1q operation
Enable 802.1q" in the WAN configuration WEB page if IEEE 802.1q VLAN header is to be inserted to the rfc2684 bridged encapsulated MAC frame in upstream direction.

In receiving downstream MAC frame, the 802.1q header will be stripped before it is forwarded to the IP or the bridge module.

If the 802.1p marking is configured in the packet Quality of Service, it will only be effective if the packet is forwarded to a PVC that has 802.1q VLAN enabled.

5.8.7. DSCP OVERVIEW

Quality of Service within the 6401 Rugged Router is provided by **Differentiated Services Code Point** (**DSCP**). DiffServ uses the 6-bit field in the IP header for packet classification purposes. DSCP replaces the outdated Type of Service (TOS) field.

Network traffic entering a DiffServ domain is subjected to classification and conditioning. Traffic may be classified by many different parameters, such as source address, destination address or traffic type and assigned to a specific traffic class. Traffic classifiers may honour any DiffServ markings in received packets or may elect to ignore or override those markings.

Differentiated Services Code Point (DSCP)
The DSCP is a number in the range 0 to 63 that is placed into an IP Packet to mark it according to the class of traffic it belongs in. Half of these values are earmarked for standardized services the other half are available for local definition

Assured Forwarding (AF) PHB group
Assured forwarding allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs.

The AF behaviour group defines four separate AF classes with Class 4 having the highest priority. Within each class, packets are given drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from AF11 through AF43 (see table below).

Assured Forwarding (AF) Behaviour Group				
Priority	**Lowest**			**Highest**
	Class 1	**Class 2**	**Class 3**	**Class 4**
Low Drop	AF11 (DSCP 10)	AF 21 (DSCP 18)	AF 31 (DSCP 26)	AF 41 (DSCP 34)
Med Drop	AF 12 (DSCP 12)	AF 22 (DSCP 20)	AF 32 (DSCP 28)	AF 42 (DSCP 36)
High Drop	AF 13 (DSCP 14)	AF 23 (DSCP 22)	AF 33(DSCP 30)	AF 43 (DSCP 38)

5.8.8. CONFIGURATION EXAMPLES

EXAMPLE 1 – LAN – TELNET TRAFFIC ENTERING FROM LAN

Parameter	Value	Options
Traffic Class Name	Telnet	Enter a name
Rule Order:	Last	Only option for this configuration
Rule Status	Enable	Enable / Disable

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	LAN	LAN, WAN, Local, eth1, eth2, eth3,eth4
Ether Type	IP (0x800)	Select from drop down list IP, ARP, IPv6, PPPoE_Disc, PPPoE_SES, 8865, 8866, 802.1Q
Source MAC Address:	Not reqd	Enter Source Device MAC Address
Source MAC Mask	Not reqd	Enter Source Device MAC Mask
Destination MAC Address	Not reqd	Enter Destination MAC Address
Destination MAC Mask	Not reqd	Enter destination MAC Mask
Source IP Address/Mask	192.168.1.20	Enter Source IP Address
Destination IP Address		Left blank to allow access to any remote IP address
DSCP Check	AF43(100110)	Assign priority
Protocol	TCP	TCP, UDP, ICMP, IGMP
UDP/TCP Source Port	23	Select port number for the application
UDP/TCP Destination Port	23	Select port number for the application

Specify Classification Results

Must select a classification queue.		A blank mark or tag value means no change
Assign Classification Queue:	Atm0 Key 56	Select from a drop down menu, these are previously configured Queues
Mark Differentiated Service Code Point (DSCP):	Auto-Marking	AF43
Mark 802.1p priority	1	Provides QoS at the MAC Layer. Select from drop down menu range 0 (Lowest) to 7 (Highest)
Tag VLAN ID [0-4094]:		Enter VLAN Tag ID if tagged VLANS are in use
Set Rate Control (kbps)	10000	Enter a data rate in Kbps

Having selected this click save and the following table will be displayed showing the configuration

CLASSIFICATION CRITERA											
Class Name	Order	Ether Type	SrcMAC /MASK	Dst MAC/ Mask	SrcIP/ Prefix Length	DstIP Prefix Length	Proto	Src Port	Dst Port	DSCP Check	802.1P Check
Telnet	1	IP			192.168.1.20	172.16.20.1	TCP	23	23	AF43	

CLASSIFICATION RESULTS						
Queue Key	DSCP Mark	802.1P Mark	VLAN ID tag	Rate Control Kbps	Enable	Remove
56	AF43	1		1200	☑	

EXAMPLE 2 – TRAFFIC ON ETH 0 USING 802.1Q

Parameter	Value	Meaning
Traffic Class Name	Eth-0	Name of the Traffic Class Rule
Rule Order:	Last	Last rule to be processed
Rule Status	Enable	Enable this rule

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	Eth0	We apply this rule to eth0
Ether Type	8021Q	
802.1p Priority Check	1	Drop down selection 0-7

Specify Classification Results

Assign Classification Queue:	Atm0&atm0path&key56&Pre8 (from drop down menu)	
Mark Differentiated Service Code Point (DSCP):	AF23 Low priority higher medium high drop rate	
Mark 802.1p priority	6	Select form drop down menu range 0 to 7
Tag VLAN ID [0-4094]:	N/A	Enter VLAN tag ID
Set Rate Control (kbps)	24	Enter bandwidth to assign for this QoS

	CLASSIFICATION CRITERA											
Class Name	Order	Class Intf	Ether Type	SrcMAC/MASK	Dst MAC/ Mask	SrcIP/ Prefix Length	DstIP Prefix Length	Proto	Src Port	Dst Port	DSCP Check	802.1P Check
Eth-0	1	Eth0	8021Q									1

CLASSIFICATION RESULTS						
Queue Key	DSCP Mark	802.1P Mark	VLAN ID tag	Rate Control Kbps	Enable	Remove
56	default	6		24	☑	

EXAMPLE 3 WAN - SNMP TRAPS ON WAN

Please note that using the WAN Interface for QoS requires at least one of the Ethernet ports configured as a Queue (see above)

Parameter	Value	Meaning
Traffic Class Name	SNMP-Trap	Enter a name
Rule Order:	Last	Only option for this configuration
Rule Status	Enable	Enable / Disable

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	WAN	LAN, WAN, Local, eth1, eth2, eth3,eth4
Ether Type	IP (0x800)	Only option allowed on WAN
Source MAC Address:	Not reqd	Enter Source Device MAC Address
Source IP Address/Mask	Not reqd	Enter Source IP Address
DSCP Check	default	Assign priority
Protocol	TCP	TCP, UDP, ICMP, IGMP
UDP/TCP Source Port	162	Select port number for the application
UDP/TCP Destination Port	162	Select port number for the application

5.9. ROUTING

5.9.1 DEFAULT GATEWAY

ADVANCED SETUP > ROUTING

- Advanced Setp
- Layer 2 Interface
- WAN Service
- VPN
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- **Routing**

On entering the Routing menu the first option is to select the Default Gateway, out of the router.
The default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
The router will automatically enter any configured WAN interfaces into the 'Default Gateway'.

5.9.2 STATIC ROUTES.

This menu allows the network manager to configure static routes on the 6401 router. Up to 32 Static routes can be configured in the 6401. On entering the menu option a table is displayed showing what static routes have been configured as shown below.

IP Version	DstIP/ PrefixLength	Gateway	Interface	Metric	Remove
IPv4	172.16.10.20/16		pppoa0	2	

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

Static Routing Menu options

IP Version	Select IPv4 or IPv6
Destination IP address/prefix length:	Enter the destination IP address with an address subnet mask using the CIDR format. For example 172.16.10.20/16 or 192.168.1.1/24
Gateway (Only if using Ethernet port as a WAN port)	Enter the Gateway address out of the local LAN
Interface	pppoa0
Metric	Select the maximum number of hops to the destination

5.9.3 POLICY ROUTING

In computer networking, **policy-based routing** (**PBR**) is a technique used to make routing decisions based on policies set by the network administrator.
When the 6401 Rugged Router receives a packet it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria. For example, a network administrator might want to forward a packet based on the source address, not the destination address. This should not be confused with source routing.
Policy-based routing may also be based on the size of the packet, the protocol of the payload, or other information available in a packet header or payload. This permits routing of packets originating from different sources to different networks even when the destinations are the same and can be useful when interconnecting several private networks.

Policy Routing Setup
A maximum of 8 policies can be added to the 6401 router.
Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.

Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name	Provide a name for this policy, a maximum of 8 letters, no spaces
Physical LAN Port	Select a LAN port from the drop down menu
Source IP	Enter the Source IP Address of the device setting up the connection.
Use Interface	Select the user interface from all the WAN interfaces that have been configured. For example. pppoa_0_0_38/pppoa0, this will be the WAN interface out of the Router
Default Gateway	Enter the IP Address of the Gateway out of the LAN

Having configured your routes and saved the configuration, a table will be displayed showing the configured routes.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
File_TFR	192.168.34.5	Eth2	Atm0		
Voice	192.168.1.24	Eth0	Pppoa0		
Video	192.168.1.42	Eth2	Atm0		

5.9.4 RIP

To configure RIP select the RIP option under Routing and you will see the RIP menu option.
RIP can only be configured on services which don't use Network Address Translation (**NAT**), and any invalid interface will not be displayed in the RIP table.

Layer 2 Service	Interface	WAN Service	RIP
EOA	Atm 0	Point to Point over Ethernet	Not Possible
EOA	Atm 1	IP Over Ethernet	Yes
EOA	Atm 2	Bridging	Yes
PPPoA	Atm 3	Point to Point Over ATM	No
IPoA	Atm 4	IP Over ATM	Yes
PPPoE	Eth 1	Point to Point over Ethernet	No
PPPoE	Eth 2	IP Over Ethernet	No

If a Service has been configured which can support RIP then when going to the RIP option in the menus, the interface will be displayed.

The following table will be displayed

Interface	Version	Operation	Enable
Selects a WAN interface	Select RIP version, 1, 2 or both	Select passive or Active	

Select 'Enable' to enable the configuration to be active.

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Having configured your WAN ports they will appear in a table showing the ports enabled for RIP, as shown below.

Interface	Version	Operation	Enable
Atm0	2	Active	
Atm4	1	Active	

Select enable to activate these ports.

Active or Passive RIP

RIP classifies routers as active and passive (silent).
Active routers advertise their routes (reachability information) to others;
Passive routers listen and update their routes based on advertisements, but do not advertise.
Typically, routers run RIP in active mode, while hosts use passive mode

RIP version 1

The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP version 2

RIP II includes the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remains.
RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* feature allows fine-grained interoperability adjustments.
In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 *multicasts* the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.
Some of the most notable RIP II enhancements are:

Next hop

The primary ones are the ability to advertise a next hop to use other than the router supplying the routing update. This is quite useful when advertising a static route to a dumb router that does not run RIP as it avoids having packets destined through the dumb router from having to cross a network twice. RIP I routers will ignore next hop information in RIP II packets. This may result in packets crossing a network twice, which is exactly what happens with RIP I.

Network Mask

RIP I assumes that all sub-networks of a given network have the same network mask. It uses this assumption to calculate the network masks for all routes received. This assumption prevents subnets with different net-masks from being included in RIP packets. RIP II adds the ability to explicitly specify the network mask with each network in a packet.

While RIP I routers will ignore the network mask in RIP II packets, their calculation of the network mask will quite possibly be wrong. For this reason, RIP I compatible RIP II packets must not contain networks that would be mis-interpreted. These networks must only be provided in native RIP II packets that are multicast.

Authentication

RIP II packets may also contain one of two types of authentication string that may be used to verify the validity of the supplied routing data. Authentication may be used in RIP I compatible RIP II packets, but be aware that RIP I routers will ignore it.

The first method is a simple password in which an authentication key of up to 16 characters is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.

CIDR blocks and number of Host IDs per segment:

How can I calculate the Subnet Mask from a CIDR-type address?

Write down the number of bits that are in the CIDR notation (in Binary notation), divide them into 4 octets, and convert them to decimal notation. For example:

CIDR address: 212.43.43.33/27

Write down 27 bits as 1 (one), and the rest (5) as 0 (zero): 11111111111111111111111111100000

Divide them into 4 octets: 11111111.11111111.11111111.11100000

Convert to decimal: 255.255.255.224

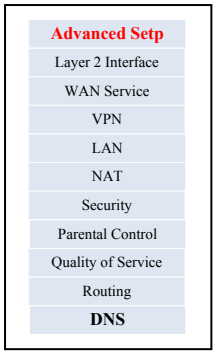
Remember that class A networks are followed by a /8, class B networks are followed by a /16, and class C networks are followed by a /24. The table below should allow a quick reference.

CIDR Length	Mask	Networks	Class	Hosts
/1	128.0.0.0	128	A	2,147,483,392
/2	192.0.0.0	64	A	1,073,741,696
/3	224.0.0.0	32	A	536,870,848
/4	240.0.0.0	16	A	268,435,424
/5	248.0.0.0	8	A	134,217,712
/6	252.0.0.0	4	A	67,108,856
/7	254.0.0.0	2	A	33,554,428
/8	**255.0.0.0**	**1**	**A**	**16,777,214**
/9	255.128.0.0	128	B	8,388,352
/10	255.192.0.0	64	B	4,194,176
/11	255.224.0.0	32	B	2,097,088
/12	255.240.0.0	16	B	1,048,544
/13	255.248.0.0	8	B	524,272
/14	255.252.0.0	4	B	262,136
/15	255.254.0.0	2	B	131,068
/16	**255.255.0.0**	**1**	**B**	**65,024**
/17	255.255.128.0	128	C	32,512
/18	255.255.192.0	64	C	16,256
/19	255.255.224.0	32	C	8,128
/20	255.255.240.0	16	C	4,064
/21	255.255.248.0	8	C	2,032
/22	255.255.252.0	4	C	1,016
/23	255.255.254.0	2	C	508
/24	**255.255.255.0**	**1**	**C**	**254**
/25	255.255.255.128	2 Subnets	C	124
/26	255.255.255.192	4 Subnets	C	62
/27	255.255.255.224	8 Subnets	C	30
/28	255.255.255.240	16 Subnets	C	14
/29	255.255.255.248	32 Subnets	C	6
/30	255.255.255.252	64 Subnets	C	2
/31	255.255.255.254	None	C	None
/32	255.255.255.255	1 / 256	C	1

A network is called a ‘Supernet, when the prefix boundary contains fewer bits than the network’s natural (i.e. Classful) mask. A network is called a subnet when the prefix boundary contains more bits than the networks natural mask

5.10 DNS

ADVANCED SETUP >DNS

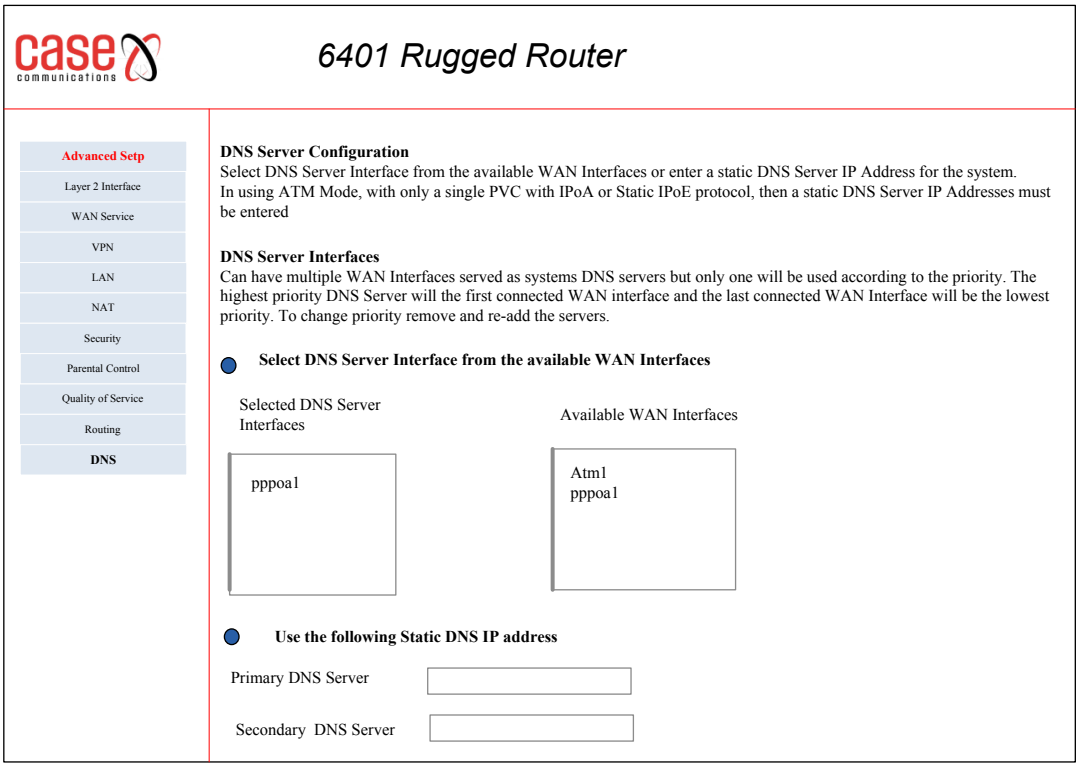


The Domain Name System (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

A Domain Name Service translates queries for domain names (which are meaningful to humans) into IP addresses for the purpose of locating computer services and devices worldwide.

5.10.1 CONFIGURING A DNS SERVER

Select DNS From the menu and the following page will be displayed



DNS Server Configuration

Select DNS Server Interface from the available WAN Interfaces or enter a static DNS Server IP Address for the system.

If using ATM Mode, with only a single PVC with IPoA or Static IPoE protocol, then a static DNS Server IP Addresses must be entered

DNS Server Interfaces

Can have multiple WAN Interfaces served as systems DNS servers but only one will be used according to the priority. The highest priority DNS Server will be the first connected WAN interface and the last connected WAN Interface will be the lowest priority. To change priority remove and re-add the servers.

5.10.2 CONFIGURING DYNAMIC DNS

Dynamic DNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers to keep the active DNS configuration of their hostnames, addresses and other information up to date.

In order to use the Dynamic DNS service it's necessary to subscribe to a Dynamic DNS Service.

Dynamic DNS providers offer a software client program that automates the discovery and registration of the client system's public IP addresses. The client program is executed on a computer or device in the private network. It connects to the Dynamic DNS provider's systems with a unique login name; the provider uses the name to link the discovered public IP address of the home network with a hostname in the domain name system. Depending on the provider, the hostname is registered within a domain owned by the provider, or within the customer's own domain name. These services can function by a number of mechanisms. Often they use an HTTP service request since even restrictive environments usually allow HTTP service.

The Dynamic DNS Server allows the network manager to alias a dynamic IP Address to a static host name in any of the domains, allowing the 6401 Rugged Router to be more easily accessed from various locations on the Internet

On entering the Dynamic DNS menu the following options are presented.

Configuration	Options
D-DNS Provider	Select from the drop down menu. In version of software 4.06L.03 the two service providers for dynamic DNS are; DynDNS.Org TZO (Different menu options appear when TZO has been selected)
Hostname	Enter the name of the host in this field - freeform
Interface	Select an interface from the drop down menu, e.g. ipoE_0_0_34/atm1
	Where DynDNS has been selected the following options are shown
DynDNS Setting	
Username	
Password	
	Or if TZO has been selected complete the following options
TZO Settings	
EMail	
Key	

Dyn DNS.Org - Dynamic DNS service used to connect remotely to your Network, Camera, PC or Domain. http://dyn.com/dns/

TZO - TZO is a leading provider of Static and Dynamic DNS services. Our easy to use Dynamic DNS (DDNS) is a simple way to run your own servers on a Dynamic IP address http://www.tzo.com/

5.11 DSL CONFIGURATION

ADVANCED SETUP>DSL

Advanced Setp
Layer 2 Interface
WAN Service
VPN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL

The following menu options will be show, simply select all that are required.

☑ G.DMT Enabled

☑ G.Lite Enabled

☑ T.1413 Enabled

☑ ADSL 2 Enabled

☑ Annex L Enabled

☑ ADSL2+ Enabled

Annex M Enabled (do not select unless your ISP supports Annex M)

Select the Phone Pair
Some equipment requires a signal on the "outer pairs" instead of the "inner pairs" of a telephone jack.

☑ **Inner Pair** – selecting the inside pair of wires

Outer pair – selects the outer pair of wires

Capability (see below for details on Bit Swap and SRA)

☑ Bit swap Enabled

SRA Enabled

DSL Options

G.DMT

In telecommunications, **ITU G.992.1** (better known as **G.DMT**) is an ITU standard for ADSL using discrete multi-tone modulation. G.DMT full-rate ADSL expands the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates up to 8 Mbit/s downstream and 1.3 Mbit/s upstream

G.LITE

In telecommunications, ITU G.992.2 (better known as G.Lite) is an ITU standard for ADSL using discrete multi-tone modulation. G.Lite does not strictly require the use of phone line splitters, but like all ADSL lines generally functions better with splitters.
G.Lite is a modulation profile which can be selected on a DSLAM port by an ADSL provider and provides greater resistance to noise and tolerates longer loop lengths (DSLAM to customer distances) for a given bandwidth. Most ADSL modems and DSLAM ports support it, but it is not a typical default configuration. Real life download speeds with this modulation is 2 Mbit/s.

ANSI T1.413
ADSL (T1.413) allows the provision of voice band services including plain old telephone service (POTS) and data services up to 56 Kbit/s, and a variety of digital channels.

ADSL 2
ITU G.992.3 is also referred to as ADSL2 or G.DMT.bis. It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream. ADSL2 uses the same bandwidth as ADSL but achieves higher throughput via improved modulation techniques.

Annex L
Increases the range of the DSL service enabling the link to work at a distance of 7 kilometres (23,000 ft)

ADSL 2+
ITU G.992.5 is an ITU standard, also referred to as ADSL2+ (or ADSL2Plus), is notable for its maximum theoretical download speed of 24 Mbit/s. ADSL2+ allows port bonding, also known as G.998.x or G.Bond

Annex M
Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream.

Bit Swapping
Bit Swapping is a way of keeping the line more stable by constantly monitoring the frequency bins (carriers) in use and reusing them if possible.
The bit swap process enables the connection to either change the number of bits assigned to each individual sub channel or if necessary increase/decrease the power level (gain) whilst still maintaining the data flow.
With bit swapping the Case 6401 Rugged router can swap the bits around and redistribute the bits to other channels by using any spare SNR at other frequencies or increasing the gain.
Without bit-swapping, your connection would lose sync every time there was a noise burst that meant any sub-channel wasn't able to transmit its allocated number of bits.

SRA - Seamless Rate Adaption
Seamless Rate Adaption is a method which dynamically adapts your line rate /sync speed on the fly depending upon the current condition of your line without having to perform a full retrain or resync.

With SRA, line conditions are constantly monitored and any increases/decreases in SNR result in an increase/decrease in the line connection speed without having to go through the initialisation process.

Line speed will always be at the highest possible rate depending upon your set target SNR, which is particularly useful if you have had a low synch and line conditions later improve, as SRA will ensure that your line speed will increase in line with the better conditions.
While the Case Communications 6401 Rugged Router supports SRA its necessary for the ISP's DSLAM to support SRA for it to be used. By default this will not be enabled.

5.12 UPnP

5.12.1 INTRODUCTION TO UPnP

ADVANCED SETUP > PGuP

Advanced Setp
Layer 2 Interface
WAN Service
VPN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnp

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise class devices.

Universal plug and play (UPnP) is architecture for pervasive peer to peer network connectivity of intelligent appliances and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public places, or attached to the Internet.

5.12.2 CONFIGURING UPnP ON THE 6401 RUGGED ROUTER

The 6401 Rugged Router has an option to select UPnP and to then apply

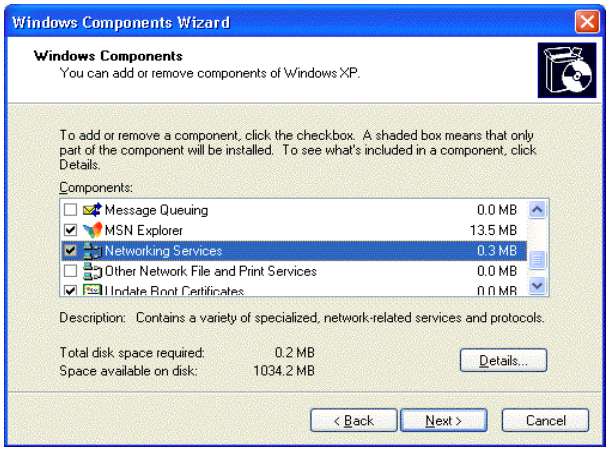
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled
Having selected UPnP click 'Apply / Save'

5.12.3 CONFIGURING UPnP ON A WINDOWS XP PC

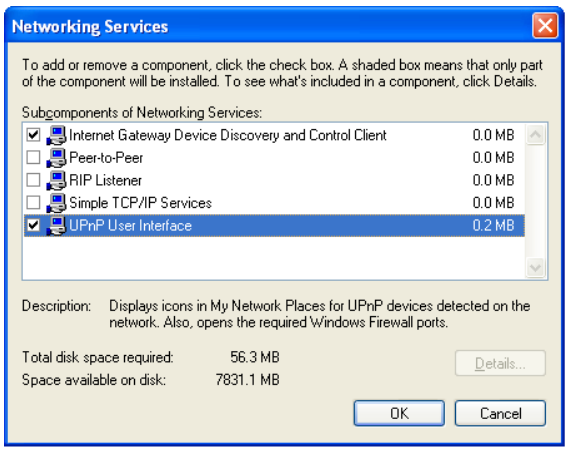
Windows XP supports UPnP function.
Please follow the steps below for installing UPnP components.

1. Click on the Start menu, point to Settings and click on Control Panel.

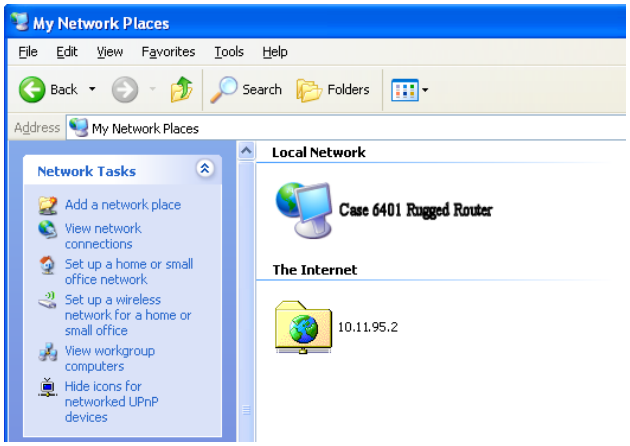
2. Select Add or Remove Programs > Add/Remove Windows Components to open Windows Components Wizard dialog box.



3. Select Networking Services and click Details. Click the UPnP User Interface check box.



4. Click OK. The system will install UPnP components automatically.



5. After finishing the installation, go to My Network Places. You will find an icon (e.g., Case 6401 Rugged Route) for UPnP function.

6. Double click on the icon, and the ADSL router will open another web page via the port for UPnP function. The IE address will be directed to the configuration main webpage as shown in the graphic.

7. Now, the NAT traversal function has already been provided. The ADSL router will create a new virtual server automatically when the router detects that some internet applications is running on the PC.

5.12.4 CONFIGURING UPnP ON A WINDOWS 7 PC

On newer versions of Windows UPnP has been changed to Network Discovery and on most installations of Windows 7 it is installed and enabled by default.

To enable Network Discovery:

1. Go to Control Panel and select “Network and Sharing Center”
2. Select “Change advanced sharing settings”
3. Under “Home or Work” ensure that Network Discovery is turned on.
4. Under “Public” ensure that Network Discovery is turned off (to prevent a possible network security issue)

5.13 DNS Proxy

ADVANCED SETUP > DNS PROXY

- Advanced Setp
- Layer 2 Interface
- WAN Service
- VPN
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnp
- **DNS Proxy**

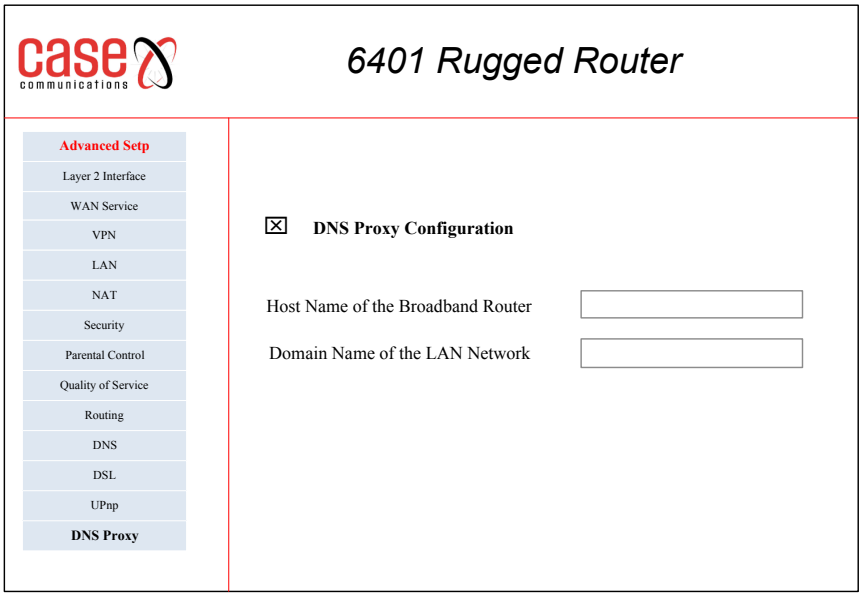
The Domain Name Service is a system designed to allow the identification of Internet servers to be based on names rather than IP addresses. Because Internet communication is based on IP addresses, all names must be translated into an IP address.

The 6401 Rugged Router has a built-in DNS proxy that can take DNS queries from devices on the local network and forward them to the 6401 Router, which in turn asks the DNS Servers provided by the ISP.

By default the DNS Proxy is enabled and 6401 Router will forward all requests to the servers detected by the operating system (usually assigned by your ISP).

Alternatively you can choose to forward DNS queries to specified servers.

✓ On entering the option the following page is displayed.



Select DNS Proxy Configuration – Configure a specific server.

Host name of the Broadband Router – Enter the name of this router

Domain Name of the LAN Network – Enter the Domain name of the Local Network

5.15 INTERFACE GROUPING

ADVANCED SETUP > INTERFACE GROUPING

- Advanced Setp
- Layer 2 Interface
- WAN Service
- VPN
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnp
- DNS Proxy
- Print Server
- **Interface Grouping**

Interface Grouping -- A maximum 16 entries can be configured

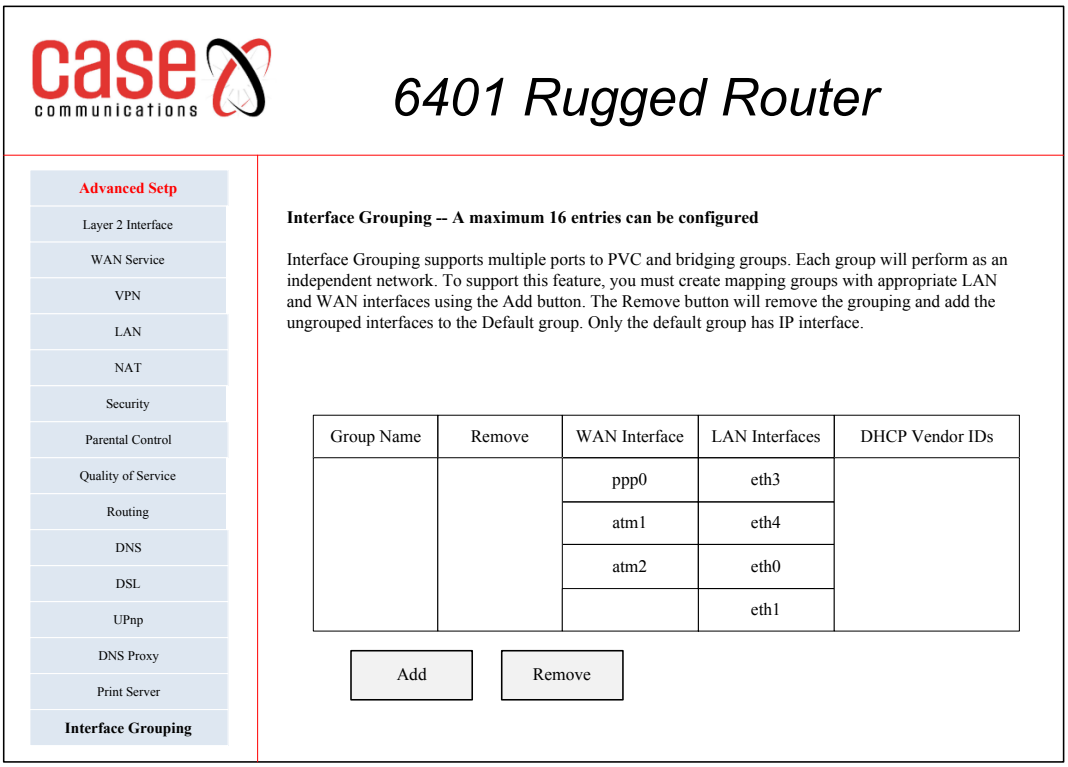
Interface Grouping supports multiple ports to PVC and bridging groups.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

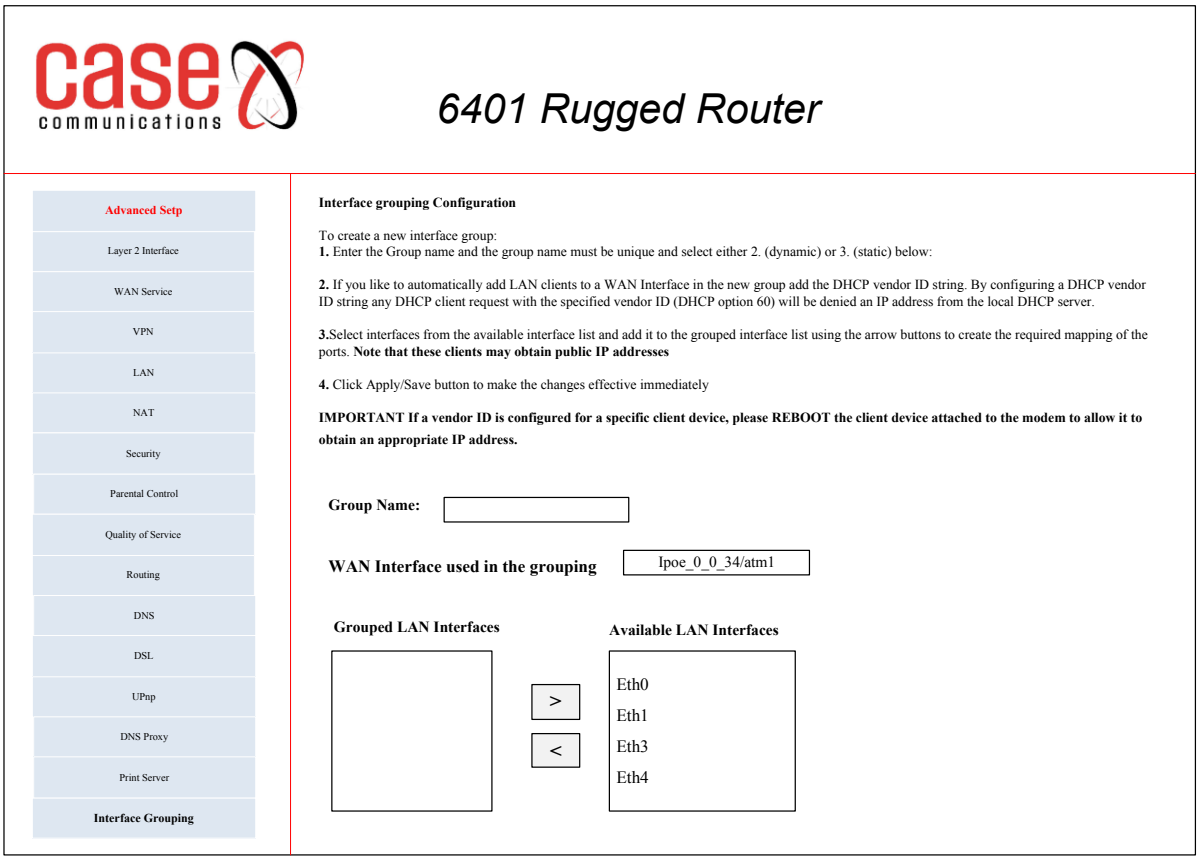
The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

On selecting the option the following page is displayed.

The table displays all available WAN and LAN Interfaces.



To add a new interface select ‘Add’ and to remove a group select ‘Remove’



Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either

(dynamic)
or
(static) below:

2. To automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses

4. Click Apply/Save button to make the changes effective immediately

IMPORTANT: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

5.16. IPSEC

ADVANCED SETUP > IPSEC (Only in Admin Mode)

5.16.1 HOW TO SET UP AN IPSEC TUNNEL

- Advanced Setp
- Layer 2 Interface
- WAN Service
- VPN
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnp
- DNS Proxy
- Print Server
- Interface Grouping
- **IP Sec**

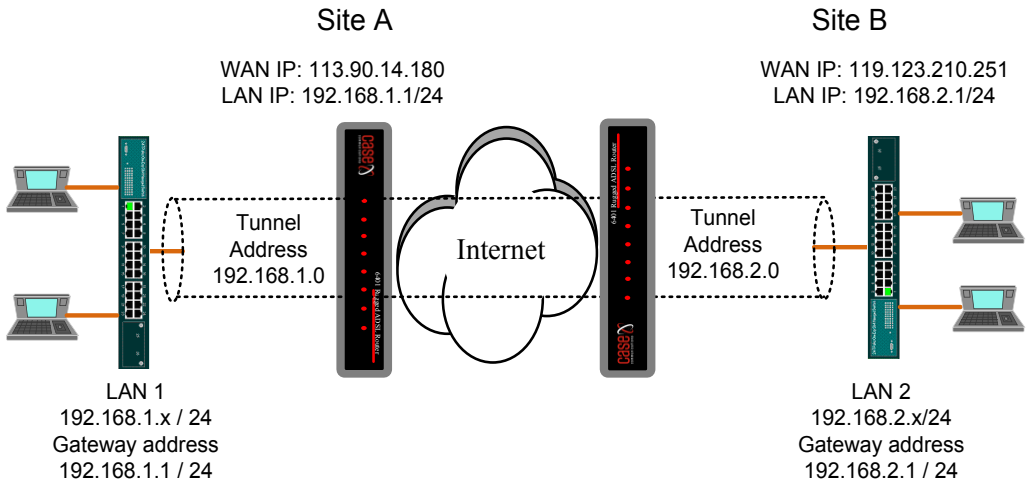
Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. We will use diagram below to provide an IP Sec example configuration. Here we can see two Local Area Networks connected via the Internet.

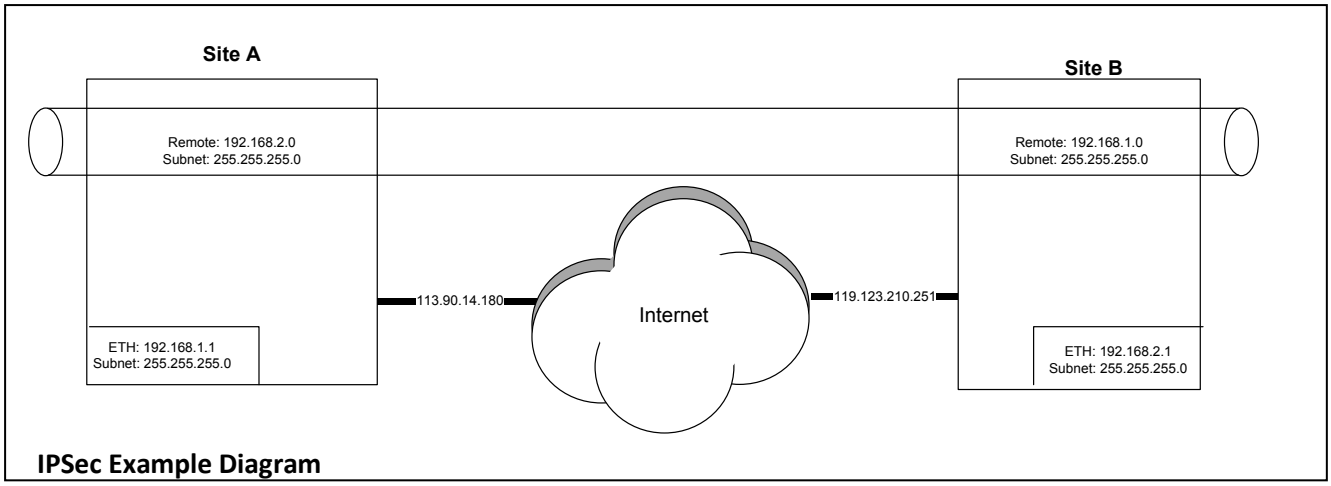
NB Please note that the IPSec tunnel will only establish when traffic is passed over it. Without that traffic the tunnel will not come up.

Site A - has a LAN IP Address of 192.168.1.1 / 24 with a WAN IP address of 113.90.14.180 and all devices at Site A should either be configured to use the LAN IP address of the Site A 6401 as the default gateway, or they can be configured with a static route to identify the Site A 6401 as the route to Site B

Site B - has a LAN IP Address of 192.168.2.1/24 with a WAN IP Address of 119.123.210.251 and all devices at Site B should either be configured to use the LAN IP address of the Site B 6401 as the default gateway, or they can be configured with a static route to identify the Site B 6401 as the route to Site A

IPSec Example

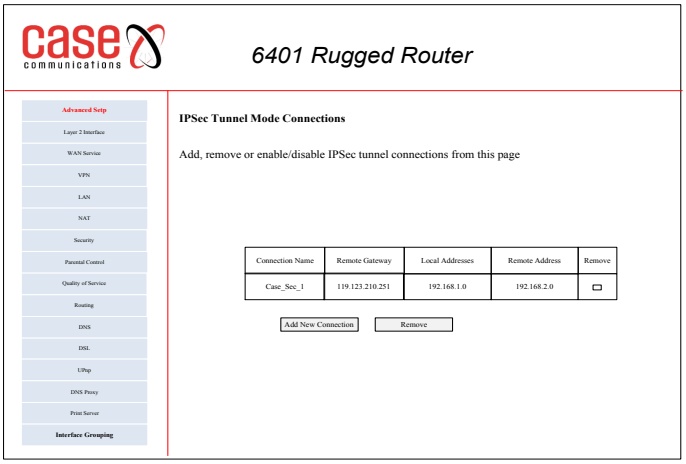




IPSec Example Diagram

Getting Started

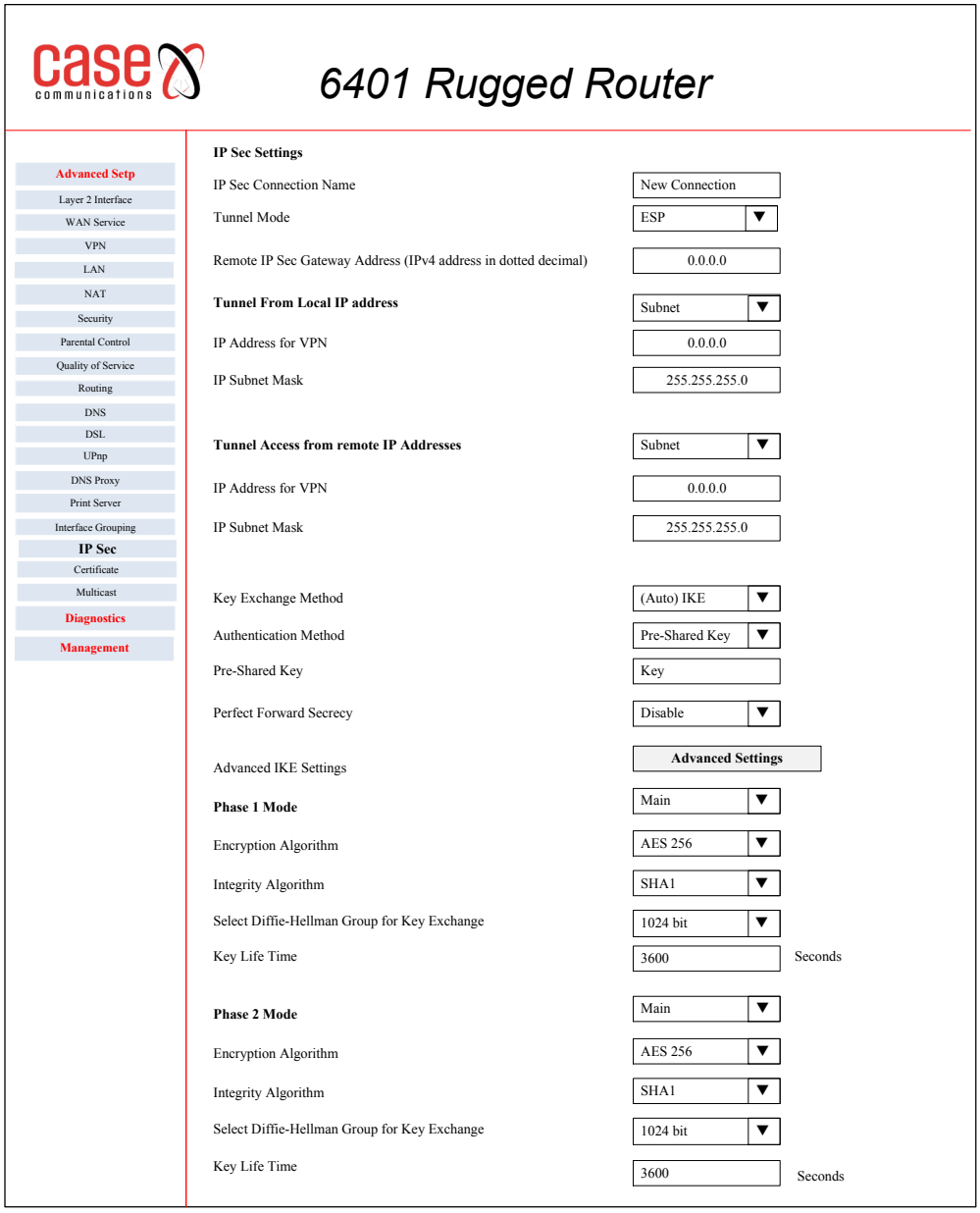
To configure the IPSec menu option go to the Advanced Setup and then select IPSec. The following screen will be displayed which shows any existing IPSec Tunnels already in use.
NB. This is option is only available at Admin level.



To create a new IP Sec Tunnel please click Add New Connection on the IP Sec page as shown below

On selecting 'add new connection' the following IPSec configuration page appears.

NB. This page shows the Advanced IKE settings



The following are explanations with examples of configuration settings for IPSec Tunnels

IP Sec Configuration Example Site A

	Parameter	Setting	Options
	IP Sec Connection Name	IPSecA	Free style name
	Tunnel Mode	ESP	Select ESP or AH
	Remote IP Sec Gateway Address	119.123.210.251	WAN IP address of site B
Site A	Tunnel Access from local IP Address	Subnet	Subnet or single address
	IP Address for VPN	192.168.1.0	Subnet ID for the Site A LAN
	IP Sub network mask – site A	255.255.255.0	Sub network mask for Site A
Site B	Tunnel Access from remote IP Address	Subnet	Subnet or single address
	IP Address for VPN	192.168.2.0	Subnet ID for the Site B LAN
	IP Sub network mask – site B	255.255.255.0	Sub network mask for Site B
	Key Exchange Method	Auto(IKE)	Auto or Manual
	Authentication method	Pre-shared Key	Pre-shared of certificate X509
	Pre-shared Key (Maxlength:128)	Key	
	Perfect Forward Secrecy	Disable	Disable or enable
	Advanced IKE Settings		Shows Advanced Settings
			Save / Apply

Having saved / applied this configuration the Case Communications 6401 Router will return you to the first IP sec page and display the Tunnel you have just configured, as shown below

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
IPSecA	119.123.210.251	192.168.1.0	192.168.2.0	

Add New Connections Remove

Configuration of Site B

1. Log onto the management page of the remote Case Communications 6401 rugged ADSL Router
2. On the left menu of the management page, please click Advanced Setup and then click IPSec.
3. On the IPSec main page, please click Add New Connection.
4. On the IPSec configuration page, please do configuration as follows:

IP Sec Configuration Example Site B

	Parameter	Setting	Options
	IP Sec Connection Name	IPSecB	Free style name
	Tunnel Mode	ESP	Select ESP or AH
	Remote IP Sec Gateway Address	113.90.14.180	WAN IP address of site A
Site B	Tunnel Access from local IP Address	Subnet	Subnet or single address
	IP Address for VPN	192.168.2.0	Subnet ID for the Site B LAN
	IP Sub network mask – site A	255.255.255.0	Sub network mask for Site B
Site A	Tunnel Access from remote IP Address	Subnet	Subnet or single address
	IP Address for VPN	192.168.1.0	Subnet ID for the Site A LAN
	IP Sub network mask – site B	255.255.255.0	Sub network mask for Site A
	Key Exchange Method	Auto(IKE)	Auto or Manual
	Authentication method	Pre-shared Key	Pre-shared of certificate X509
	Pre-shared Key (Maxlength:128)	Key	
	Perfect Forward Secrecy	Disable	Disable or enable
	Advanced IKE Settings		Shows Advanced Settings
			Save / Apply

Having saved / applied this configuration the Case Communications 6401 Router will return you to the first IP sec page and display the Tunnel you have just configured, as shown below

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
IPSecB	113.90.14.180	192.168.2.0	192.168.1.0	

Add New Connections Remove

5.16.1.1 IPSec Tunnel over Ethernet WAN

Running an IPSec tunnel over an Ethernet WAN link is similar to IPSec over ADSL. The addition of a 3rd party ADSL router requires some different configuration to the 6401. Instead of using an ADSL WAN the 6401 used an Ethernet WAN as the output to the internet.

There are basically two different ways for the 3rd party ADSL router to be configured to pass packets to the 6401.

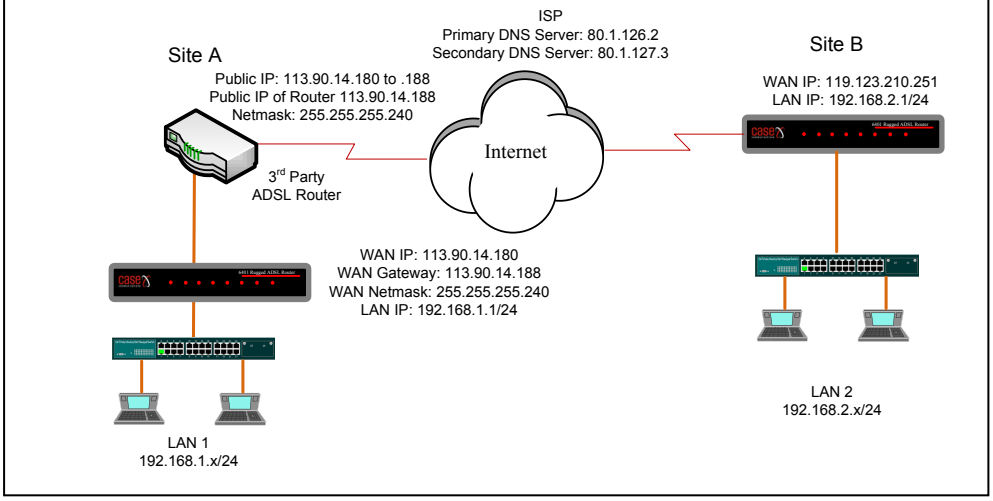
1. The first option is used when the ISP has provided multiple static IP addresses for the ADSL line. The 3rd party ADSL router can then be configured to pass one of the static IP addresses to the 6401.

   a) In the example below, at Site A all packets incoming from the internet destined for IP addresses 113.90.14.180 through to 113.90.14.188 enter the 3rd party router.

   b) The 3rd party router is configured to root all incoming packets from internet with the destination IP of 113.90.14.180 to the 6401

   c) On the 6401 the port configured as the Ethernet WAN port (IPoE) with the IP address of 113.90.14.180 is connected to the 3rd party router.

Diagram IPSec over Ethernet WAN Example 1



   d) The 6401 at Site A has to be configured with an IPoE Ethernet WAN port, see Section 5.1 (specifically 5.1.4) and 5.2 (5.2.2.4)

e) When configuring the Ethernet WAN IPoE port use the Static IP Address option and in this example set the WAN IP Address to 113.90.14.180 (WAN address passed through the 3rd party router), WAN Subnet Mask to 255.255.255.240 (Netmask assigned by the ISP for the ADSL line) and WAN gateway IP address to 113.90.14.188 (Public IP address of the 3rd party router)

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway

Obtain and IP Address Automatically (Default)

Option 60 Vendor ID		
Option 61 IAID		8 hexadecimal digits
Option 61 DUID		hexadecimal digits
Option 125	X Disable	Enable

X Use the following Static IP Address (Select if using a static IP Address)

WAN IP Address	113.90.14.180
WAN Subnet Mask	255.255.255.240
WAN Gateway IP Address	113.90.14.188

f) When configuring the WAN Service you will be asked to enter the DNS Server Configuration manually. Enter the DNS details supplied by the ISP as shown below (this information should be given to you by the ISP, if you do not have these details ask your ISP for them, you will be unable to proceed without this information)

DNS Server Configuration

Select DNS Server Interface from the available WAN Interfaces or enter a static DNS Server IP Address for the system. In using ATM Mode, with only a single PVC with IPoA or Static IPoE protocol, then a static DNS Server IP Addresses must be entered

DNS Server Interfaces

Can have multiple WAN Interfaces served as systems DNS servers but only one will be used according to the priority. The highest priority DNS Server will the first connected WAN interface and the last connected WAN Interface will be the lowest priority. To change priority remove and re-add the servers.

○ **Select DNS Server Interface from the available WAN Interfaces**

Selected DNS Server Interfaces	Available WAN Interfaces

● **Use the following Static DNS IP address**

Primary DNS Server	80.1.126.2
Secondary DNS Server	80.1.127.3

g) When the Ethernet WAN port has been configured then IPSec can be configured exactly as shown in Section 5.16.1

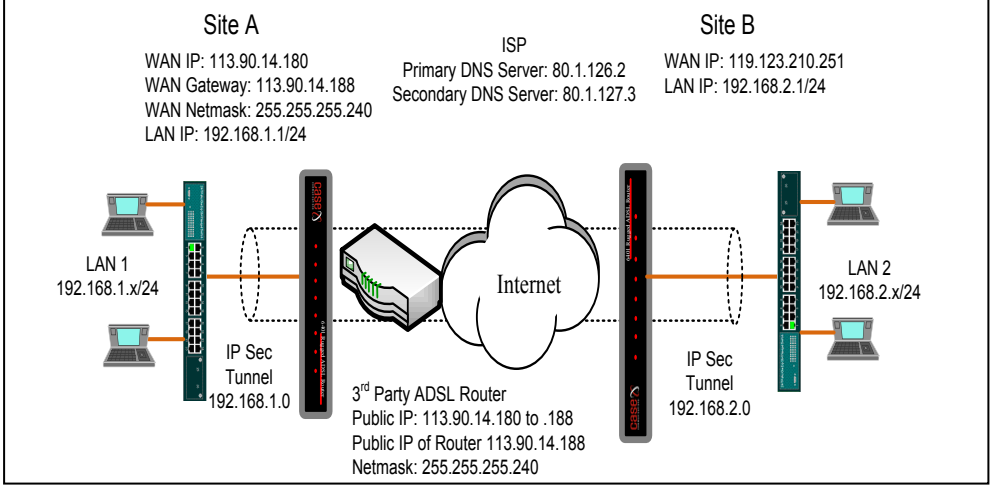
2. The second option is used when there is a single IP address on the ADSL line.

   a) At Site A all packets incoming from the internet destined for IP addresses 113.90.14.180 enter the 3rd party router.

   b) The 3rd party router is configured with an IP address for its LAN ports, in this example it is set to 192.1.1.1 with a netmask of 255.255.255.0

   c) Using port forwarding (if the 3rd party router is capable of this) it forwards the IPSec UDP packets and protocols (UDP port 500 and IP protocols 50 and 51) to the 6401. These are the only protocols and ports that are required for IPSec operation.

Diagram IPSec over Ethernet WAN Example 2



   d) The 6401 at Site A has to be configured with an IPoE Ethernet WAN port, see Section 5.1 (specifically 5.1.4) and 5.2 (5.2.2.4)

   e) When configuring the Ethernet WAN IPoE port use the Static IP Address option and in this example set WAN IP Address to 192.1.1.2 (an IP address in the LAN IP subnet of the 3rd party router), WAN Subnet Mask to 255.255.255.0 (Netmask of the 3rd party router) and WAN gateway IP address to 113.90.14.180 (Public IP address of the 3rd party router)

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway

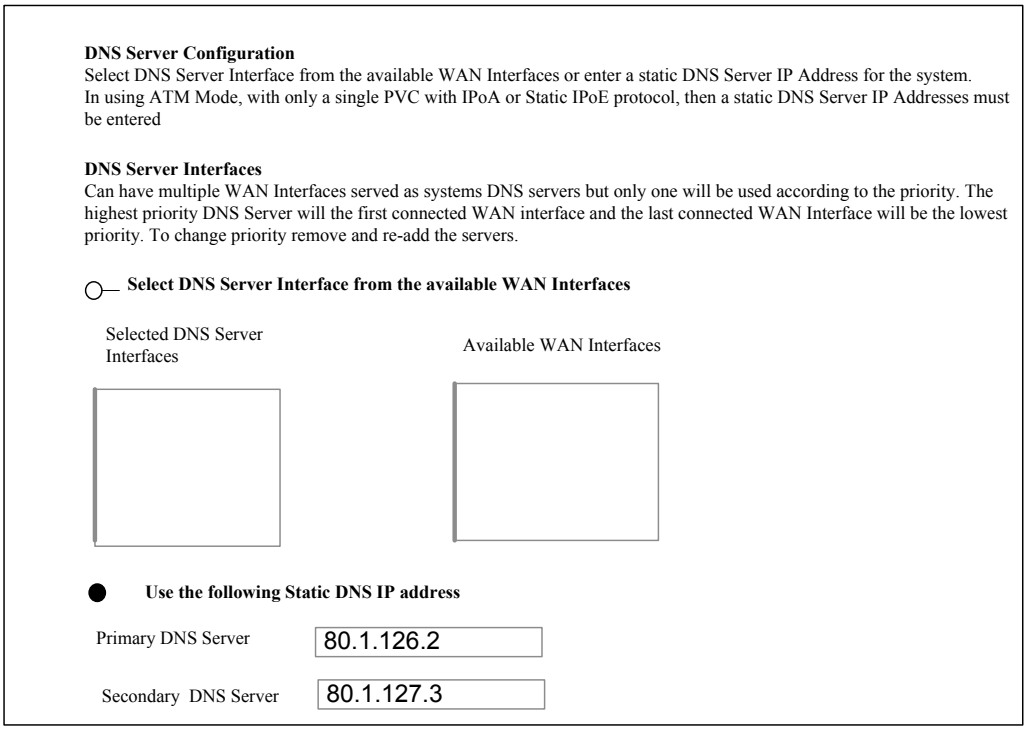
Obtain and IP Address Automatically (Default)

Option 60 Vendor ID		
Option 61 IAID		8 hexadecimal digits
Option 61 DUID		hexadecimal digits
Option 125	X Disable	Enable

X Use the following Static IP Address (Select if using a static IP Address)

WAN IP Address	192.1.1.2
WAN Subnet Mask	255.255.255.0
WAN Gateway IP Address	113.90.14.180

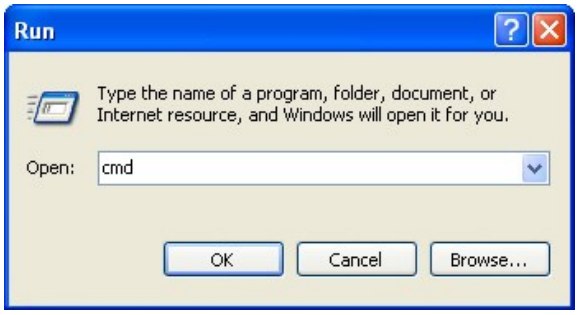
f) During configuration of the WAN Service you will be asked to enter the DNS Server Configuration manually. Enter the DNS details supplied by the ISP as shown below (this information should be given to you by the ISP, if you do not have these details to hand ask your ISP for them, you will be unable to proceed without this information)



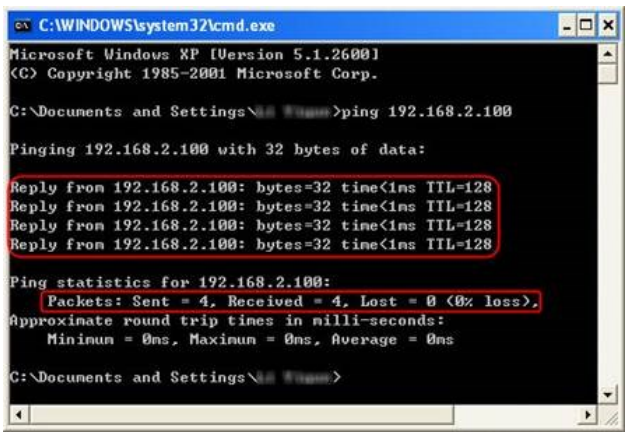
g) When the Ethernet WAN port has been configured then IPSec can be configured exactly as shown in Section 5.16.1

TESTING THE IP SEC TUNNEL

1. On the host in LAN1, press [Windows Logo] + [R] to open ***Run*** dialog. Input "cmd" and hit ***OK***.



2. In the CLI window, type in "ping 192.168.2.x" ("192.168.2.x" can be IP address of any host in LAN2). Then press [Enter].



If Ping proceeds successfully (gets replies from host in LAN2), the IPSec connection must be working properly now.

By default there is a 3600 second Life Timer on IPSec tunnels that will determine how often the IPSec tunnel needs to be re-negotiated. The IPSec tunnel will only re-negotiate if there is traffic running with a destination at the remote end of the tunnel. If currently there is no traffic then the tunnel will only re-establish the next time there is traffic and the Life Timer will be restarted.
There is no way to disconnect and reconnect IPSec tunnels without rebooting the 6401.
If one end drops, e.g. gets disconnected or loses power, then the IPSec tunnel will re-establish the next time there is traffic with a destination to the remote end of the tunnel.

Please note that the packet that establishes the IPSec tunnel can be sent from either end of the tunnel, i.e. in the examples above a device on LAN1 can ping or communicate to a device on LAN2 to establish the IPSec tunnel and vice versa.

5.16.2 ADVANCED SETTINGS

This is a dynamic page. It will change itself by showing and hiding options when different types or connections are chosen. User can select automatic key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.

When automatic key exchange method is used, click "Show Advanced Settings" will show more options towards the bottom of the screen. The advanced options are shown in the screen shot below.

This page allows manual configuration of the IP Sec parameters these are explained below.

Advanced IKE Settings
There are two Phases available and both can be edited to different settings if requires.

Mode: Recommendation
Select Main Mode to configure the standard negotiation parameters for IKE phase1.

Main - The Initiator send a proposal containing encryption methods used to and the Responder selects one and uses it. All further negotiation between the Initiator and Responder are encrypted. Select Main Mode to configure the standard negotiation parameters for IKE phase1.

Aggressive – Quicker negotiation method, but the Initiator and Responder's IDs are passed un-encrypted. Select Aggressive Mode to configure IKE phase1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended-Less Secure)

Encryption Algorithm: DES, 3DES, AES-128, AES-192 or AES-256 – This determines the algorithm used for encryption. Default is 3DES,

Integrity Algorithm: MD5, SHA1 – encryption techniques used by IPSec to make sure that a message has not been altered. Default is MD5, but SHA1 is used by Cisco.

Select Diffie-Hellman Group for Key Exchange: 768bit, 1024bit, 1536bit, 2048bit, 3072bit, 4096bit, 6144bit or 8192bit – a public key encryption method used by IPSec to establish a shared secret key.

Key Life Time: Enter the number of seconds for the IPSec lifetime. It is the period of time before establishing a new IPSec security association (SA) with the remote endpoint. Default value is 3600. (1 Hour) As the tunnel is re-started users will be disconnected and re-connected.

5.16.3 CONFIGURATION EXAMPLES

Example 1 – Connection to a PIX Firewall

Parameter	Setting	Meaning
IPSec Connection Name	To-Cisco	User definable
Tunnel Mode	ESP	Cisco default tunnel type
Remote IPSec gateway Address	182.12.1.200	IP address of the Cisco PIX WAN port
Tunnel Access from local IP address	Subnet	Use subnet to allow equipment connected to the routers to talk over the IPSec tunnel
IP address for VPN	192.168.1.1	Local VPN IP address, use this as default gateway for equipment
IP Subnet Mask	255.255.255.0	Class C subnet
Tunnel Access from remote IP address	Subnet	Use subnet to allow equipment connected to a Cisco PIX to talk over the IPSec tunnel
IP address for VPN	192.168.2.1	Remote VPN IP address
IP Subnet Mask	255.255.255.0	Class C subnet
Key Exchange Method	Auto (IKE)	
Authentication Method	Pre-Shared Key	
Pre-Shared Key	secret	Type in the secure PSK that the Cisco also uses
Perfect Forward Secrecy	Disable	
	ADVANCED IKE SETTINGS	
Phase 1 Mode	Main	send a proposal containing encryption methods used
Encryption Algorithm	3DES	DES, 3DES, AES-128, AES-192 or AES-256
Integrity Algorithm	SHA1	MD5 (default) , SHA1 (SHA1 used by Cisco PIX)
Select Diffie-Hellman Group	1024bit	768bit, 1024bit, 1536bit, 2048bit, 3072bit, 4096bit, 6144bit or 8192bit
Key Life Time	3600	determines when a new key is generated – see below.
Phase 2 Encryption Algorithm	2DES	
Integrity Algorithm	SHA1	
Select Diffie-Hellman Group	1024bit	
Key Life Time (60 – 3,000,000) 60 seconds to nearly 35 days	3600	Time before tunnel is broken and re-established using a new key. NB. Every tunnel break removes the users.

Example 2 – Manual Key Exchange Method

Parameter	Setting	Meaning
IPSec Connection Name	IPSec1	User definable
Tunnel Mode	AH	Cisco default tunnel type
Remote IPSec gateway Address	182.12.30.200	IP address of the Cisco PIX WAN port
Tunnel Access from local IP address	Subnet	Use subnet to allow equipment connected to the routers to talk over the IPSec tunnel
IP address for VPN	192.168.10.1	Local VPN IP address, use this as default gateway for equipment
IP Subnet Mask	255.255.255.0	Class C subnet
Tunnel Access from remote IP address	Subnet	Use subnet to allow equipment connected to the Cisco to talk over the IPSec tunnel
IP address for VPN	192.168.20.1	Remote VPN IP address
IP Subnet Mask	255.255.255.0	Class C subnet
Key Exchange Method	Manual	
Encryption Algorithm	DES	Options – DES, 3DES or AES
Encryption Key	1234567890abcdef	16 digit DES Key (48 for DES)
Authentication Algorithm	MD5	MD5 or SHA1
Authentication Key	1234567890abcdef1234567890abcdef	32 digit MD5 key (40 for SHA1)

SPI	101	User definable

5.16.4 HOW IP SEC WORKS

IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps:

1. "Interesting traffic" initiates the IPSec process. Traffic is deemed interesting when the IPSec security policy configured in the IPSec peers starts the IKE process.

2. IKE phase 1. IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.

3. IKE phase 2. IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers.

4. Data transfer. Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

5. IPSec tunnel termination. IPSec SAs terminate through deletion or by timing out.

TUNNEL MODE – (AH) AUTHENTICATION HEADER

Authentication Header guarantees connectionless integrity and data origin authentication of IP packets. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets.

In IPv4, the AH protects the IP payload and all header fields of an IP datagram except for mutable fields (i.e. those that might be altered in transit), and also IP options such as the IP Security Option (RFC-1108). Mutable (and therefore unauthenticated) IPv4 header fields are DSCP/TOS, ECN, Flags, Fragment Offset, TTL and Header Checksum.

In IPv6, the AH protects the most of the IPv6 base header, AH itself, non-mutable extension headers after the AH, and the IP payload. Protection for the IPv6 header excludes the mutable fields: DSCP, ECN, Flow Label, and Hop Limit. AH operates directly on top of IP, using IP protocol number 51.

TUNNEL MODE – (ESP) ENCAPSULATING SECURITY PAYLOAD

In IPSec Encapsulating Security Payload provides origin authenticity, integrity, and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure. Unlike Authentication Header (AH), ESP in transport mode does not provide integrity and authentication for the entire IP packet. However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header (including any outer IPv4 options or IPv6 extension headers) remains unprotected. ESP operates directly on top of IP, using IP protocol number 50.

REMOTE IP SEC GATEWAY ADDRESS

This is the WAN IP address of the remote device usually given by your ISP.

TUNNEL ACCESS FROM LOCAL IP

This is stipulates how device gain access into the IP Sec Tunnel. Selecting Subnet allows devices on the remote devices subnet to access the LAN. The other option is to simply configure one device (for example a PC) to have access to the tunnel.

IP ADDRESS FOR VPN

This is the local IP Address to access the IP Sec tunnel from the router at our local end.

IP SUBNET MASK
The sub network mask for the Local Tunnel Entrance's IP Address

KEY EXCHANGE METHOD (Set to Auto)
Auto Key (IKE)
When you need to create and manage numerous tunnels, you need a method that does not require you to configure every element manually. IPsec supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol. The Case 6401 software supports AutoKey IKE automated tunnel negotiation.

Manual Key
With manual keys, administrators at both ends of a tunnel configure all the security parameters. This is a viable technique for small, static networks where the distribution, maintenance, and tracking of keys are not difficult. However, safely distributing manual-key configurations across great distances poses security issues. Aside from passing the keys face-to-face, you cannot be completely sure that the keys have not been compromised while in transit.

AUTHENTICATION METHOD
Peer authentication is the process of ensuring that an IPSec peer is who it claims to be. By using peer authentication, IPSec can determine whether or not to communicate with another computer before the communication begins.

Pre-shared Key
IPSec can use preshared keys for authentication. Preshared means that the parties agree on a shared, secret key that is used for authentication in an IPSec policy. The use of pre-shared key authentication is not recommended because it is a relatively weak authentication method.

Certificate (X509)
X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm..
An organization's trusted root certificates can be distributed to all employees so that they can use the company PKI system. Browsers such as Internet Explorer, Netscape/Mozilla, Opera, Safari and Chrome come with root certificates pre-installed, so SSL certificates from larger vendors will work instantly; in effect the browsers' developers determine which CAs are trusted third parties for the browsers' users

PERFECT FORWARD SECRECY
If perfect forward secrecy (PFS) is specified in the IPSec policy, a new Diffie-Hellman exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost

5.16.5 ADVANCED IKE SETTINGS

MAIN MODE OR AGGRESSIVE MODE
Main Mode
Main mode has three two-way exchanges between the initiator and the receiver.

First exchange: The algorithms and hashes used to secure the IKE communications are agreed upon in matching IKE SAs (Security Association) in each peer.

Second exchange: Uses a Diffie-Hellman exchange to generate shared secret keying material used to generate shared secret keys and to pass nonces—random numbers sent to the other party and then signed and returned to prove their identity.

Third exchange: Verifies the other side's identity. The identity value is the IPSec peer's IP address in encrypted form. The main outcome of main mode is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds or kilobytes, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.

Aggressive Mode
In aggressive mode, fewer exchanges are made, and with fewer packets. On the first exchange, almost everything is squeezed into the proposed IKE SA values: the Diffie-Hellman public key; a nonce that the other party signs; and an identity packet, which can be used to verify identity via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange. The weakness of using the aggressive mode is that both sides have exchanged information before there's a secure channel.

ENCRYPTION ALGORITHM
The Case Communications 6401 has the ability to select the encryption algorithm used within IP Sec. The options are;

- DES 3 DES
- AES128 AES 192 AES 256

INTEGRITY ALGORITHM (SHA1 (default) or MD5)
The Authentication Header (AH) protocol provides a means to verify the authenticity /integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated through a Hash Message Authentication Code (HMAC) using a secret key and either MD5 or SHA-1 hash functions.

- **Message Digest 5 (MD5)**—An algorithm that produces a 128-bit hash (also called a *digital signature* or *message digest*) from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity.

- **Secure Hash Algorithm-1 (SHA-1)**—An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the ASIC, the performance cost is negligible.

SELECT DIFFE_HELLMAN GROUP (RANGE 768 – 8192 DEFAULT 1024)
The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
A Diffie-Hellman (DH) exchange allows the participants to produce a shared secret value. The strength of the technique is that it allows the participants to create the secret value over an unsecured medium without passing the secret value through the wire.

KEY LIFE TIME
Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).
A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected

5.17 CERTIFICATES

5.17.1 INTRODUCTION

ADVANCED SETUP > CERTIFICATES

Advanced Setp
Layer 2 Interface
WAN Service
VPN
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnp
DNS Proxy
Print Server
Interface Grouping
IP Sec
Certificate

In cryptography, a **certificate authority**, or **certification authority**, (**CA**) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.

Commercial CAs charge to issue certificates that will automatically be trusted by most web browsers (Mozilla maintains a list of at least 36 trusted root CAs, though multiple commercial CAs or their resellers may share the same trusted root).

The number of web browsers and other devices and applications that trust a particular certificate authority is referred to as ubiquity.
Aside from commercial CAs, some providers issue digital certificates to the public at no cost. Large institutions or government entities may have their own CAs.

The commercial CAs that issue the bulk of certificates that clients trust for email servers and public HTTPS servers typically use a technique called "domain validation" to authenticate the recipient of the certificate. Domain validation involves sending an email containing an authentication token or link, to an email address that is known to be administratively responsible for the domain. This could be the technical contact email address listed in the domain's WHOIS entry, or an administrative email like postmaster@ or root@ the domain. The theory behind domain validation is that only the legitimate owner of a domain would be able to read emails sent to these administrative addresses

5.17.2 CONFIGURING A CERTIFICATE OF AUTHORITY

Select Certificate > Local to select a local certificate.
This opens a page to configure a Local Certificate, with a Local certificate there are two options to choose from;

1. Create a new Certificate Request
Certificates are a digital means of ensuring the identity of a machine or individual and providing keys for encryption. These certificates also need to be certified by a root certification authority (CA).

2. Import a certificate
You can also import a certificate from another server instead of recreating the certificate on the current server. Having selected Local certificate the following table will be displayed showing any certificates already configured.

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

Create Certificate Request Import Certificate

Create new certificate request
To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name	Provide a name for this certificate
Common Name	
Organisation Name	Provide an organisation name
State / Province Name	
Country / Region Name	Select from the drop down menu

Select Certificate > Trusted Certificate Authority
When selecting a trusted certificate the only option is to import a trusted certificate.
Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. A Maximum 4 certificates can be stored.

Name	Subject	Type	Action

Import Certificate

Import CA certificate
Enter certificate name and paste certificate content.

Certificate Name:	Enter name for this certificate
Certificate	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

Apply

5.18 MULTICAST

5.18.1 INTRODUCTION

ADVANCED SETUP > MULTICAST

- Advanced Setp
- Layer 2 Interface
- WAN Service
- VPN
- LAN
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DNS
- DSL
- UPnp
- DNS Proxy
- Print Server
- Interface Grouping
- IP Sec
- Certificate
- **Multicast**

In computer networking, multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source creating copies automatically in other network elements, such as routers, only when the topology of the network requires it.

Multicast is most commonly implemented in IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media and Internet television. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for datagrams sent to a multicast destination address.

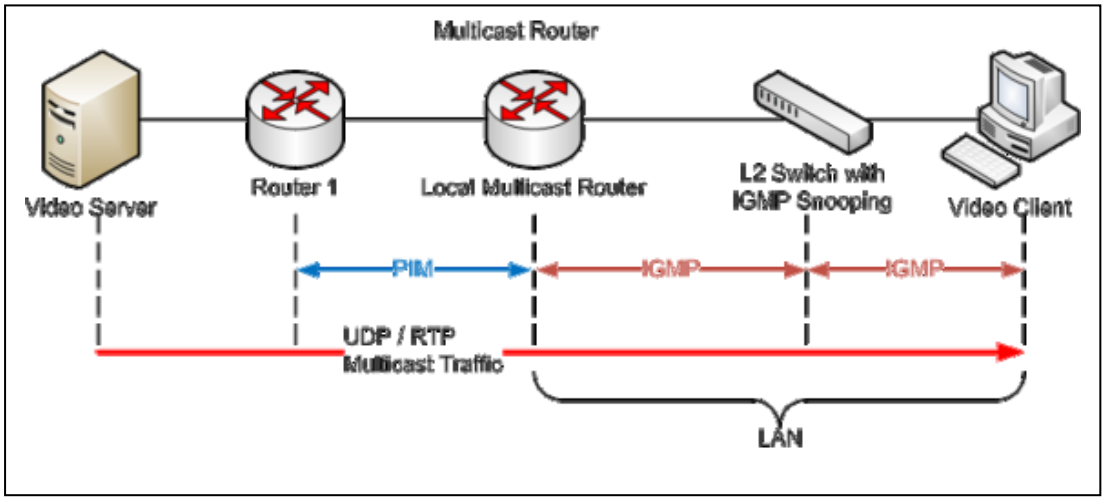
IGMP is an integral part of the IP multicast specification. It is analogous to ICMP for unicast connections. IGMP can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

There are basically 5 types of messages in the IGMP that must be implemented in IGMP for the IGMP v3 functional properly and be compatible with previous versions:

0x11: membership query
0x22: version 3 membership report
0x12: version 1 membership report
0x16: version 2 membership report
0x17 version 2 leave group

IGMP operates between the client computer and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from the multicast server to many multicast clients.

A network designed to deliver a multicast service using IGMP might use this basic architecture:



5.18.2 CONFIGURING IGMP

On entering the Multicast option the web page displays a table with default options.

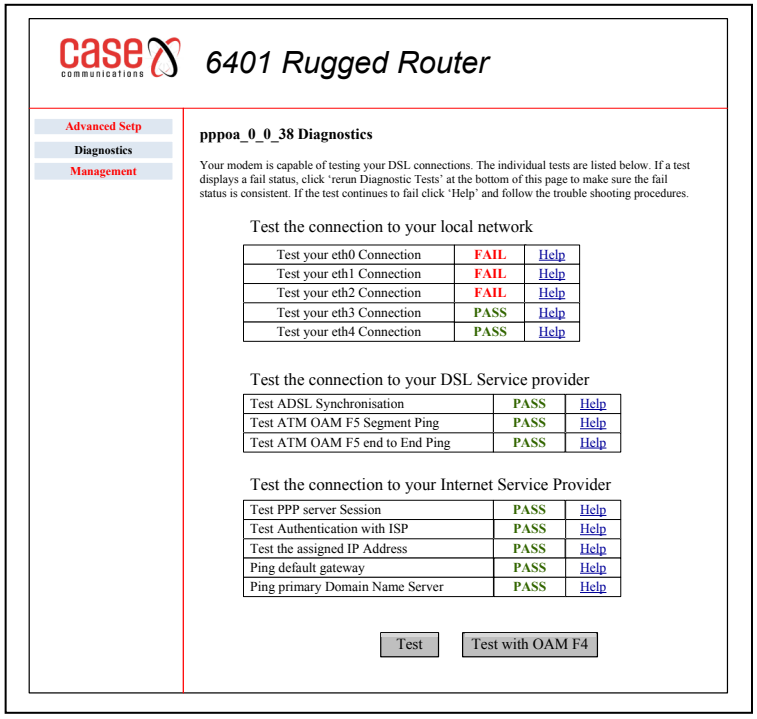
Configuring	Default	Options
Default Version	3	There are three versions of IGMP, V1, V2, and V3
Query Interval (In seconds)	125	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). You can also click the scroll arrows to select a new setting. The default query interval is 125 seconds
Query Response Interval (In Seconds)	10	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. You can also click the scroll arrows to select a new setting. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval (Seconds)	10	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.. The default last member query interval is 1 second
Robustness Value	2	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2
Maximum Multicast Data Sources for (IGMPv3) (1 -24)	10	This field specifies the number of source addresses present in the Query. For General and Group-Specific Queries, this value is zero. For Group-and-Source-Specific Queries, this value is non-zero, but limited by the network's MTU.
Maximum Multicast Group Members	25	The Maximum number of members allowed in the multicast group
Fast Leave Enable	Tick	Then the router will treat these groups as having single host member. After the reception of a Leave message, the router immediately removes the multicast forwarding state
LAN to LAN (Intra LAN) Multicast Enable	Tick	Tick to enable multicast

6. DIAGNOSTICS

6.1 INTRODUCTION

When you select diagnostics menu on the Case Communications 6401 Rugged ADSL Router, it automatically tests the local Ethernet ports and your WAN settings and produced a series of results. If the WAN is 'down' or disconnected then the only ports that will be tested are the Ethernet ports.

The page below shows the results of a 'Diagnostics 'test.



The tables over leaf explain these tests and their meanings.

Test the connection to your Local network	
Test eth0 – eth 1, eth 2, eth3, eth 4	
Pass	Indicates that the Ethernet interface from your computer is connected to the LAN port on your Case Communications 6401 Rugged ADSL Router
Fail	Indicates that your Case Communications 6401 Rugged ADSL Router does not detect an Ethernet Interface on your computer

Troubleshooting

Note. If this test fails, follow the trouble shooting procedures listed below and rerun diagnostics by selecting 're-run diagnostic Tests'

1. If you're not able to access the management page on the Case Communications 6401 Rugged ADSL Router verify that the Ethernet cable from your computer or your hub is connected to the LAN port on the router. Re-seat the cable by removing and replacing it to the same port.
2. Turn off your Case Communications 6401 Rugged ADSL Router wait 10 seconds and then power it on.
3. With the router on, press the reset button on your Case Communications 6401 Rugged ADSL Router for at least 5 seconds and release it. This resets the router to its default configuration. Wait for the router to initialise, then close and restart your browser. Then it will be necessary to re-configure the router.

Test the connection to your DSL Service provider	
Test ADSL Synchronisation	
Pass	Indicates that your 6401 Rugged ADSL Router has detected a DSL Signal from your DSL provider
Fail	Indicates that your 6401 Rugged ADSL Router has not detected a DSL Signal from your DSL provider

Troubleshooting

Note. This test will fail if the Test ADSL Synchronisation also fails, therefore test the ADSL Synchronisation first.

1. Make Sure your phone line is connected to the 6401 Router
2. After turning on your 6401 Router, wait for at least 1 minute to establish a connection. Run the diagnostic tests again, by selecting 'rerun Diagnostic test.
3. Make sure there is no DSL Micro filter on the phone cord connecting the 6401 Router to your phone socket
4. Make sure your using the correct phone cord with four copper wires visible in the plug.
5. If your DSL has been functioning properly for a long period of time and you suddenly experience problems, there may be a problem with the DSL network. It may be necessary to wait for 30 minutes to a couple of hours and to then call your ISP.
6. Turn off the power to the 6401 Router, wait 10 seconds then turn it back on. Wait at least one minute and retry.

Test OAM F5 segment Ping and OAM F5 End to End Ping	
Pass	Indicates that your 6401 Rugged ADSL Router can communicate with your DSL providers network
Fail	Indicates that your 6401 Rugged ADSL Router is unable communicate with your DSL providers network. This test may have an effect on your Internet Connectivity. Sometimes DSL providers may intentionally block this traffic. Therefore if the test fails but your still able to access the Internet, there is no need to troubleshoot this issue further
Disabled	Indicates no connection or not configured

Troubleshooting

Note. This test will fail if the Test ADSL Synchronisation also fails, therefore test the ADSL Synchronisation first.

1. Turn off the 6401 rugged ADSL Router, wait 10 seconds and power back on.
2. With the modem on, press the reset button (on the rear of the unit) and wait for 5 seconds. This resets the 6401 Rugged ADSL Router to its default settings. Wait for the 6401 to completely start, then close and restart your web browser. Reconfigure the unit.
3. If this is the first time the router has been used, you may need to reconfigure your VPI / VCI settings

Testing the connection to your Internet Service provider	
Test PPP Server Session	
Pass	Indicates that the PPP Server has established a valid PPP session with your 6401 Rugged ADSL Router
Fail	Indicates that the PPP Server cannot establish a valid PPP session with your 6401 Rugged ADSL Router
Disabled	Indicates not connected or configured
Test authentication with ISP	
Pass	Indicates that the username and password stored in your 6401 Rugged ADSL Router has authenticated with your ISP's network
Fail	Indicates that your 6401 Rugged ADSL Router was unable to verify your username and password with your ISP's network
Disabled	Indicates not connected or configured
Assigned IP Address	
Pass	Indicates that your 6401 Rugged ADSL Router has received a valid IP Address from the PPP Server
Fail	Indicates that your 6401 Rugged Router does not have a valid IP Address from the PPP Server
Disabled	Indicates not connected or configured
Ping Default Gateway	
Pass	Indicates that your 6401 Rugged ADSL Router can communicate with the first entry point to the network. This is usually your ISP's Edge router
Fail	Indicates that your 6401 Rugged ADSL Router was unable to communicate with the first entry point to the network. However if the connection is working do not brother trouble shooting further as your ISP's server may not respond to pings
Ping Primary Domain Name Server	
Pass	Indicates that your 6401 Rugged ADSL Router can communicate with the primary Domain Name Server (DNS)
Fail	Indicates that your 6401 Rugged ADSL Router is unable to communicate with the primary Domain Name Server (DNS). This may not have an effect on your primary connectivity. Therefore if this fails but you're still able to access the Internet, there is no need to troubleshoot the issue.

Differences between OAM F4 and OAM F5

OAM F4 cells operate at the VP level. They use the same VPI as the user cells; however, they use two different reserved VCIs, as follows:

VCI=3 Segment OAM F4 cells.
VCI=4 End-end OAM F4 cells.

OAM F5 cells operate at the VC level. They use the same VPI and VCI as the user cells. To distinguish between data and OAM cells, the PTI field is used as follows:

PTI=100 (4) Segment OAM F5 cells processed by the next segment.
PTI=101 (5) End-to-end OAM F5 cells which are only processed by end stations terminating an ATM link.

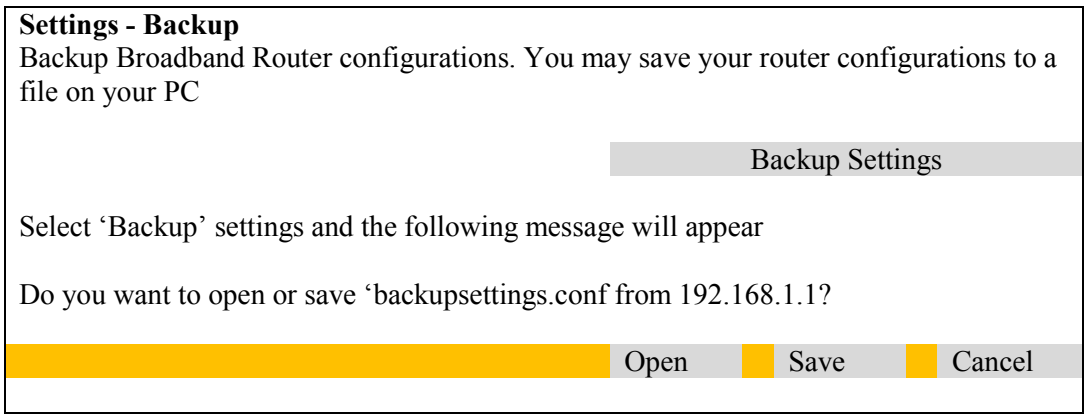
7. MANAGEMENT

7.1 SETTINGS

7.1.1 BACKUP

Management>Settings>backup

This option allows you to save your 6401 Routers settings to a file on your PC.
Once selected the following option appears



Back up files are generally titled 'backupsettings.conf and have a type file CONF File

Open - Select open to look at the file, generally open this with Notepad. Having viewed the file it can be saved on your PC.

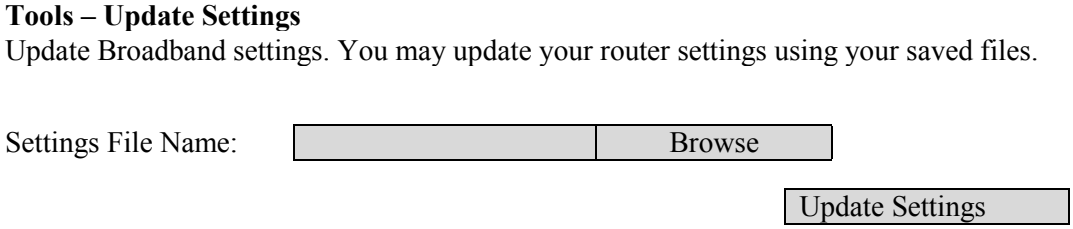
Save – Select 'Save' to save the configuration file to your PC, this will go to your usual download location, it's possible to then view where your PC has stored this file.

Save As – This is more useful option as it allows you to determine where the configuration files can be stored, in the same way 'Save As' can be used to save any PC file to a specific destination folder.

7.1.2 UPDATE

Management>Settings>Update

Update allows saved configurations to be loaded into the 6401 router. Select 'Update' and you will see the following option. Select 'Browse' to find the 'backup settings. Config file'



Once the file has been selected, click 'update' settings and the router will upload the configuration file. The message 'Uploading is in progress. The broadband Router will reboot upon completion. This process will take about 2 minutes.

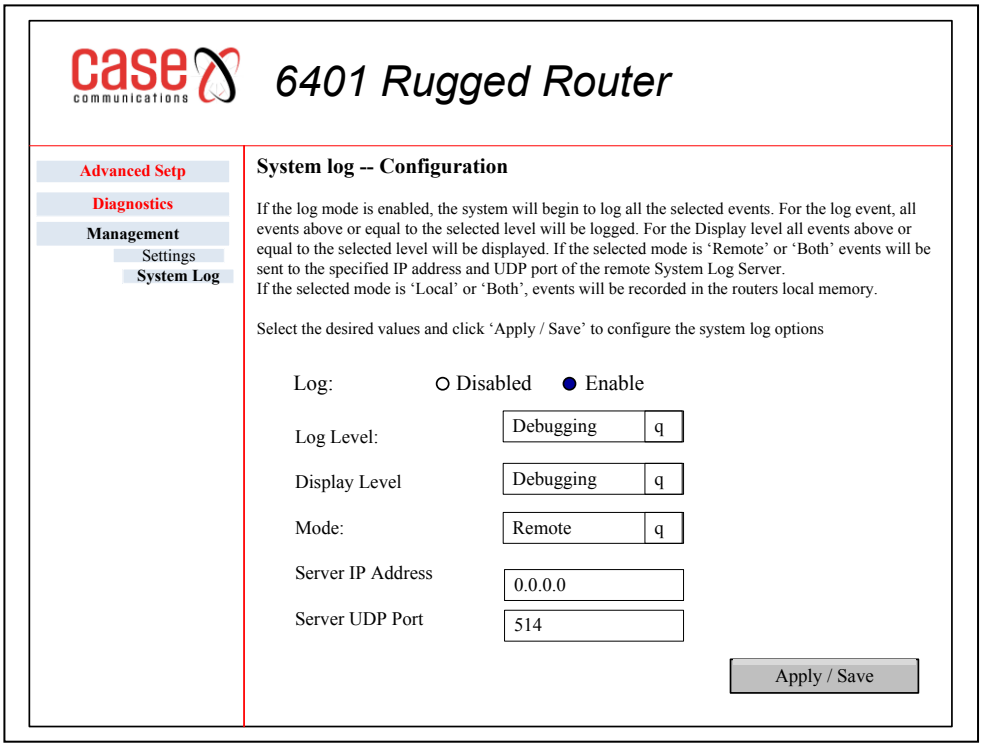
7.1.3 RESTORE DEFAULT

This option restores the 6401 Rugged Router to its default condition. Do not use this if you're connected to the 6401 Router remotely as it will take the router offline and deny you remote access.

7.2 SYSTEM LOG

MANAGEMENT > SYSTEM LOG

Selecting 'System Log' allows you to 'View the System Log' and to 'Configure The System Log. Select system log to see the following page



Option	Description
Log	Indicates whether the system is currently recording events. Users can 'enable' or 'disable' event logging. Having enabled the log, click on 'Apply'
Log Level	Allows the network manager to configure the event level and to filter out unwanted events below this level. The events ranging from highest critical level 'Emergency' level will be recorded into the 6401 routers RAM. When the system log buffer is full the 6401 will overwrite 'old' events with new events. By default the log is set to 'Debugging' which is the lowest level of alarm. The following levels can be set • Emergency – The 6401 is unstable • Alert – Action must be taken immediately • Critical – The 6401 is in a critical condition • Error – The 6401 has recorded an error • Warning – The 6401 has detected a significant event • Notice – the 6401 is issuing a notice. • Informational – The 6401 is providing general information • Debugging – this records all events
Display Level	Allows the user to select the logged events and displays them on the 'View System Log' events page. The level of events is as shown above. To display all events select 'debugging' to select only the more severe select 'Emergency'
Mode	Allows you to specify whether events should be stored in the local memory or be sent to a remote sys log server, or both simultaneously. If remote is selected, 'View System Log' will not be able to display events sent to the sys log server. When both or remote mode is selected, the 6401 will invite the network manager to enter the system log servers IP address and UDP Port Number.

7.3 SECURITY LOG

MANAGEMENT > SECURITY

The security Log dialog allows you to view the Security Log and configure the Security Log options

Click “View” to view the Security Log

Click “Reset” to clear and reset the Security Log

Right Click here to save the Security Log.

Security Log

Click “View” to view the Security Log

Click “Reset” to clear and reset the Security Log

Right Click here to save the Security Log.

Reset View

7.4 SNMP AGENT

MANAGEMENT > SNMP

This page allows configuration of the Routers SNMP parameters.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent	[X] Enable	[ ] Disable
Read Community	Public	
Set Community	Private	
System Name	Case_6401	
System Location	Unit_12	Enter Freeform Name
System Contact	John_Smith	Enter Freeform Name
Trap Manager IP	Enter IP Address of SNMP / Network Management System	

Save / Apply

7.5 TR 069 Client

MANAGEMENT > TR069 CLIENT

INTRODUCTION

TR-069 defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. The TR-069 standard was developed for automatic configuration of these devices with Auto Configuration Servers (ACS).

SOAP, Simple Object Access Protocol, is the communications protocol mandated by TR-069. The specification further mandates that all communications between the CPE (client) and ACS (server) are done via a persistent, bi-directional connection.

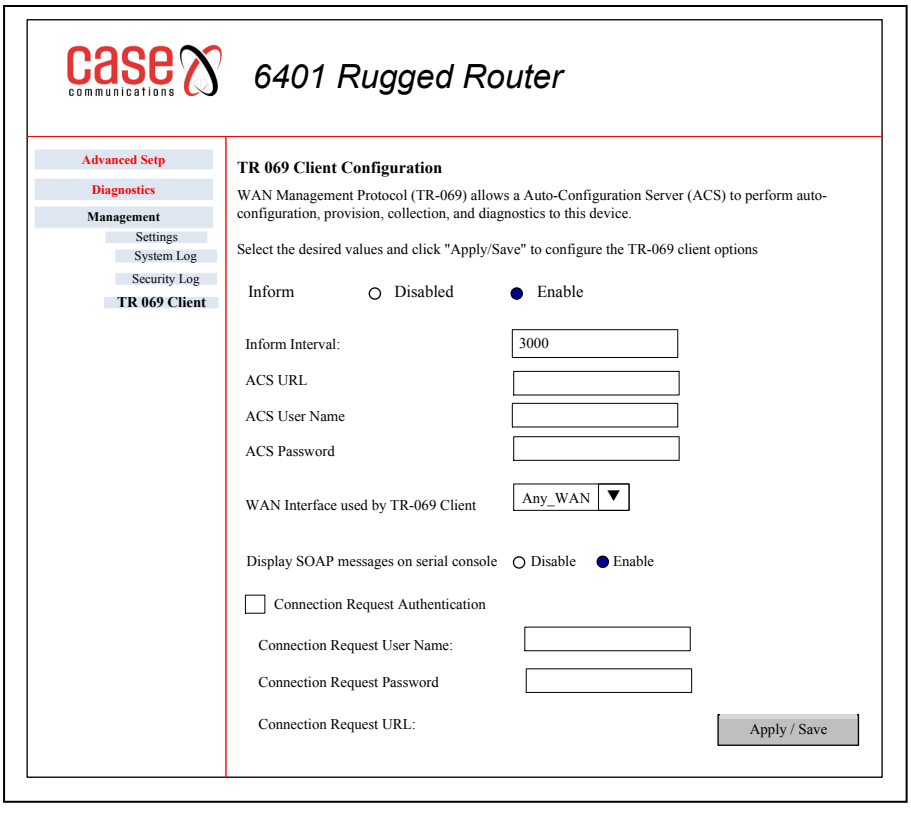
TR 069 Connection Request.

While the CPE always initiates a session, the ACS can stimulate it to do so, by issuing a "Connection Request" A Connection Request is a simple HTTPGet made on the CPE at an arbitrary URL/port set by the CPE which then tells the ACS what its CR URL is during the Inform

TR 069 Inform

The Inform RPC is a Remote Procedure Call made on the ACS by the CPE, which MUST be called FIRST in every session. It contains the reason(s) for the session (an Event) a list of parameters that are required by the Data Model to be included ("Forced Inform") Contains parameters that the ACS set to be notified upon changes. The ACS completes the RPC by sending an InformResponse.

Select the desired values and click "Apply/Save" to configure the TR-069 client options. The following screen will then appear.



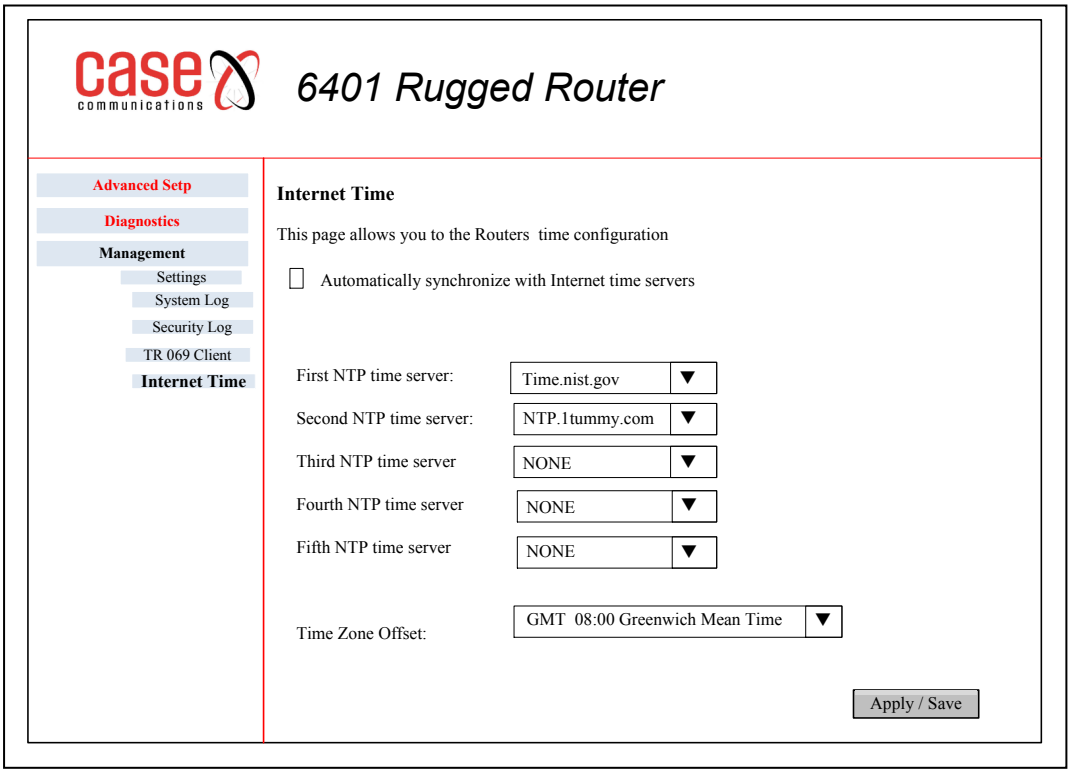
Option	Example	Meaning
Inform	☐ Enable ☐ Disable	Enable or disable the Inform Interval Timer
Inform Interval	3000	The interval between the client sending the request and the ACS Responding
ACS URL	http://www.casecomms.com	The web address of the ACS device
ACS User Name		Enter Auto Configuration Server -Name
ACS Password		Enter Auto Configuration Server -Name
WAN Interface Used by TR 069 Client		Select the path out from the drop down menu
Display SOAP messages on serial console		Enable or disable
☐ Connection Request Authentication		Enable Authentication for the connection request
Connection Request user name	Admin	ACS User Name
Connection Request Password		AS Password
Connection Request URL		

Apply Get RPCMethods

7.6 INTERNET TIME

MANAGEMENT > INTERNET TIME

Select this option to allow the 6401 to synchronise with a Network Time Server. Once the option to synchronise has been selected, an option with 5 drop down menus appears to allow selection of the NTP Servers.



7.7 ACCESS CONTROL

MANAGEMENT > ACCESS CONTROL

Access Control -- Passwords

Access to the Case Communications 6401 router is controlled through three user accounts:

1 **Admin** - Unrestricted access to change and view all configuration options.
2 **Support** – allows an ISP technician to access your Broadband Router for maintenance and to run diagnostics.
3 **User** – Allows a user to access the router to configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name	
Old Password	
New Password	
Confirm Password	

7.8 UPDATE SOFTWARE

MANAGEMENT > UPDATE SOFTWARE

Step 1: Backup configuration of the router as shown in Section 7.1.1, ensure that you know the location of the file so that it can be uploaded later.

Step 2: Obtain an updated software image file from Case Communications or your local Case Communications reseller.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file. The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Step 4: Configure your PC to either a DHCP Client or to an IP like 192.168.1.10 and use a web browser to access IP 192.168.1.1 and log on using the username and password **admin**

Step 5: Restore configuration of the router as shown in Section 7.1.2

Step 6: If you have changed the IP address of the PC change it back again

Software File Name: Browse

7.9 REBOOT ROUTER

MANAGEMENT > REBOOT ROUTER

To reboot the router select the reboot router page

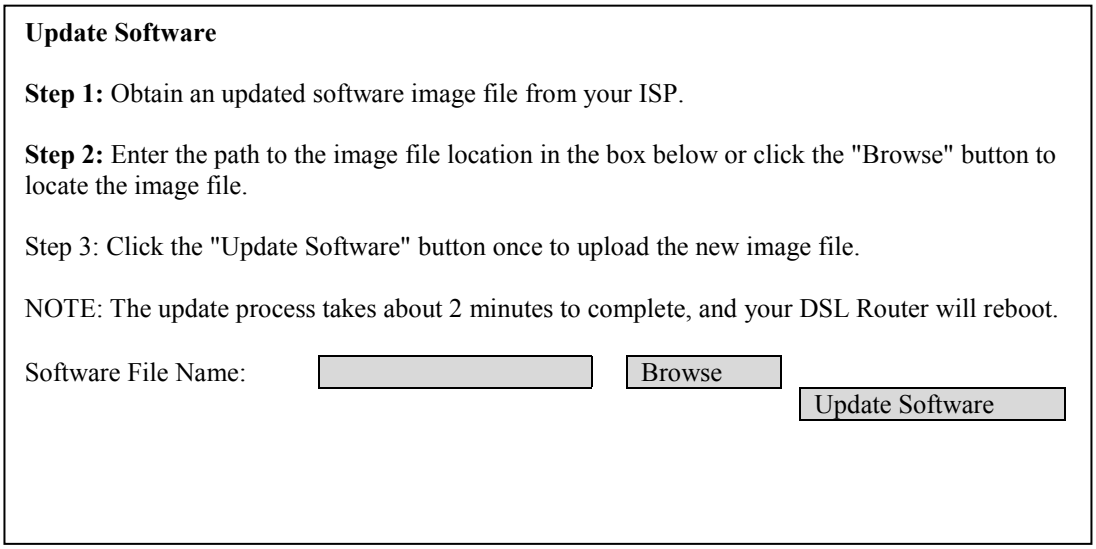
Click the button below to reboot the router

Reboot

7.10 WIPING 6401 FLASH

It is possible to wipe the flash onboard the 6401 and then reload the software. This is usually used in case of emergencies to get the 6401 back into a clean state. Examples of emergencies include forgetting the IP address of the 6401, misconfiguration that results in unable to access management to correct, or a bad configuration upload that resulted in the 6401 locking up.

Step 1: Power down the 6401.
Step 2: Gently press in and hold in the button on the rear of the 6401 using a small screwdriver or something similar.
Step 3: Power up the 6401 with the button pressed in.
Step 4: Release the button after approximately 10 seconds.
Step 5: On a PC set to an IP address 192.168.1.10 use a web browser to surf to IP 192.168.1.1 and you will see the following screen:



Step 6: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 7: Click the "Update Software" button once to upload the new image file. The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Step 8: After 2 minutes close down the again surf to IP 192.168.1.1 (i.e. ensure only that shows in the address bar and not 192.168.1.1/upload.cgi
Step 9: Logon as usual using the default username and password.

8 Command Line Interface

The CLI can only be accessed using a telnet session either through a Windows DOS Prompt (if enabled on the PC) or using a third party program like PuTTY that has telnet capability. Please note that it is strongly recommended that the CLI is not used for configuration as the web browser access that has been described above is vastly easier to use.
This section will not show how to configure using CLI, but will only give a brief overview of some of the useful commands that are available in the CLI that may be of some use.

8.1 Accessing the CLI

Step1: Start the DOS Prompt or third party program and access the IP address of the 6401 9by default this is 192.168.1.1)

Step 2: When prompted logon using the pre-set administrator logon and password (by default both set to **admin**), unless accessing remotely where you will have to use the support login using the username and password (by default set to **support**)

8.2 Command Examples

?: Shows a list of available commands
reboot: Reboots the 6401 immediately without any confirmation prompt
logout, exit, quit: To reboot the these command exit the telnet session immediately without any prompt.
ping 192.168.1.25: Produces 4 pings to the IP address set, in this example 192.168.1.25
syslog dump: Shows the syslog of the 6401, but only if it has been configured through the browser
lan show: Shows the LAN statistics as can be seen through the browser
route show: Shows the IP routing table on the 6401
adsl info --state: shows the status of the ADSL link

```
adsl: ADSL driver and PHY status
Status: Showtime
Last Retrain Reason:    8000
Last initialization procedure status:   0
Max:    Upstream rate = 1020 Kbps, Downstream rate = 3360 Kbps
Channel:        INTR, Upstream rate = 448 Kbps, Downstream rate = 3040 Kbps
```

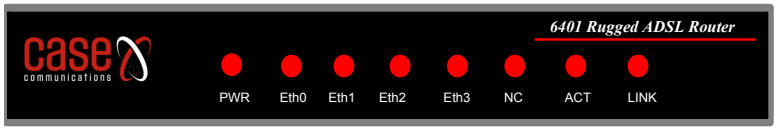
adsl info --SNR: Shows a history of the SNR value, please note that the result of this command will overflow the screen of most third party telnet programs.

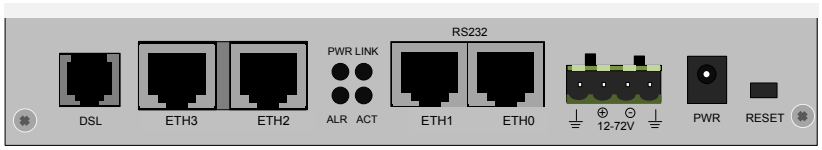
adsl info --show: More in depth status of the ADSL link including the SNR, attenuation and power.

```
adsl: ADSL driver and PHY status
Status: Showtime
Last Retrain Reason:    8000
Last initialization procedure status:   0
Max:    Upstream rate = 1020 Kbps, Downstream rate = 3360 Kbps
Channel:        INTR, Upstream rate = 448 Kbps, Downstream rate = 3040 Kbps

Link Power State:       L0
Mode:                   G.DMT
TPS-TC:                 ATM Mode
Trellis:                ON
Line Status:            No Defect
Training Status:        Showtime
                Down                    Up
SNR (dB):       15.2                    18.0
Attn(dB):       49.0                    31.5
Pwr(dBm):       17.9                    12.6
                        G.dmt framing
K:              96(0)                   15
R:              14                      16
S:              2.0000                  8.0000
D:              16                      4

                        Counters
                        Bearer 0
SF:             29558                   29558
SFErr:          1                       0
RS:             1004955                 250240
RSCorr:         44                      0
RSUnCorr:       5                       0

                        Bearer 0
HEC:            4                       0
OCD:            0                       0
LCD:            0                       0
Total Cells:    3602783                 0
Data Cells:     80                      0
Drop Cells:     0
Bit Errors:     0                       0

ES:             1                       0
SES:            0                       0
UAS:            729                     729
AS:             495

                        Bearer 0
INP:            1.00                    1.50
INPRein:        0.00                    0.00
delay:          8                       8
PER:            0.00                    0.00
OR:             32.00                   32.00

Bitswap:        0/0                     3/3
```

adsl info --stats: Shows the same information as **adsl info –show** but includes a history of the error counts

APPENDIX A
PRODUCT SPECIFICATION





Hardware Specifications

CPU	BCM63281T
RAM	128Mbyte
NOR FLASH	8Mbyte

Power

AC PSU	External in line 100-240vac
Power	20 Watts Max
DC PSU	(Internal) 12 -72 vdc

Input / Output Ports

WAN	ADSL 2 + Annex M (24Mbps)
Ethernet	4 x 10/100Mbps Rj 45

ADSL Features

Full-Rate ANSI T1.413 Issue 2
ITU-T G.992.1 (G.dmt) ITU-T G.992.2 (G.lite)
ITU-T G.994.1 (G.hs) ITU-T G.992.3 (G.dmt.bis)
ITU-T G.992.5 Supports Annex A/L/M
Max 6 kilometres

Environment

Operating Temp	-20 to +70 C
Storage Temp	-40 to +85 C
Humidity	10 to 90% RH

MTBF – (Calculated)

Main unit	800,000 Hrs

Housing

Die cast aluminium	105mm x 180mm x 31mm

Watchdog Timer – Hardware and Software

Software Specifications

WAN Services

- EoA (VC Mux / LLC SNAP bridging)
- PPPoA (VC Mux / LLC Encapsulation)
- IPoA (VC Mux / LLC Snap-Routing)
- PPPoE (Bridging)

Routing

- IPv4 & IPv6
- Static Routes
- RIP I and II
- Policy based routing

Tunnelling and security

- IP Sec VPN encrypted tunnels (3DES, 256 AES)
- L2TP v3
- Encryption 3DES, AES 256
- Authentication X509 or pre shared

Access Security

- Firewall
- NAT & Full Cone NAT
- Virtual Server (Protocol and external port no.)
- Port Triggering
- Forwarding to DMZ host
- IP and MAC Filtering mechanisms
- MAC Filtering (bridging mode)
- Access restriction by
  - User name
  - MAC Address
  - Date / Time
  - URL Filter

Quality of service and performance

- DSCP
- Queue set up ATM 16 modes, PTM 8 modes
- 4 Queues for Ethernet ports
- 32 classes of traffic
- IGMP Support

Management

- Web based
- SNMP

APPENDIX B

APPENDIX C

SAFETY INFORMATION

C1. Safety Information Warnings

- Install the equipment only as described within this manual
- Never Install equipment connected to telephone wiring during a lightning storm
- Never install telephone jack sockets in wet locations unless the jack is specifically designed for that environment.
- Use caution when installing or modifying telephone lines

APPENDIX D

TECHNICAL ASSISTANCE

D.1 Case Communications Technical Support

Case Communications Technical assistance can be contacted via e.mail address support@casecomms.com

D.2 Repair Return Address

Before you return a product you must contact case Communications and obtain a Repair Authorisation Number (RAN). This is available from the above e-mail address

Our web site address is www.casecomms.com

Case Communications

6401 Rugged ADSL Router

e-mail. admin@casecomms.com

www.casecomms.com