TECHNICAL MANUAL: CPVA 500 - SIP

RESIDENTIAL ACCESS GATEWAY
THE MOST COMPLETE OFFER

MT500--SIEN12

telsey
telecommunications

to enable the future

CPVA500 Residential Gateway

Tecnical Manual Code MT500--SIEN12

Telsey S.p.A. reserves the right to make changes in specifications and other information contained in this manual without prior written notice.
In no event shall Telsey be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out or related to this manual or the information contained herein, even if Telsey has been advised of, known, or should have known, the possibility of such damages.

Main Index

Main Index

Main Index

Main Index

Tables

Tables

Chapter 1

Introduction

CPVA 500

CPVA500 is the new Telsey Integrated Access Device which sets a reference for the roll out of broadband ADSL services to the residential market segment. Its cutting edge technology, combined with the well-known Italian design, makes CPVA500 the enabler for ADSL broadband operators for the mass deployment of integrated voice, data and video services.

CPVA500 connects end user equipment such as PCs, Set Top Box and analog telephones to the ADSL network through:

- 1 Ethernet 10/100BaseT
- 1 USB
- 2 FXS ports

It integrates voice and signalling gateway capability while providing direct access to VoIP services and data routing functionalities. These features allow Service Providers to massively deploy innovative services like Video On Demand, Video Telephony, Fast Internet Access and VoIP services to residential users.

Innovative autoinstalling optional solutions, such as the automatic switch of the end user's telephones to the VoIP service when the cut over is detected, completely remove installation costs and enable Service Providers to directly send CPVA500 to end users.

This product reinforces Telsey as a valuable and experienced partner for providers aggressively catching the broadband mass market roll out. Our extensive experience in this industry with about 300.000 gateways installed in FTTH/ETTH-ADSL networks, combined with our dynamic and aggressive R&D and a complete gamma of products for the residential and SOHO market are other important advantages that position Telsey as the ideal partner for new customers approaching the broadband communication market.

Moreover our CPVA500 is easily customizable according to the network strategy and topology chosen by any provider. Both the physical interfaces and the required protocols could be tailored according to specific needs.

Introduction

Chapter 2

External Interfaces and Connectors

CPVA 500 LED DESCRIPTION

Fig. 1 Front View

CPVA 500 is equipped with a signaling LED set showing its operation status. Namely signaling LEDs, listed from left to right, behave as the following table explains.

Tab. 1: CPVA 500 - Led Indication

Ref.	Led Denomination	Led Colour	Indication
1	PHONE 1	Green	It indicates activity on Phone 1 line [VoIP] **On** = LINE 1 is off-hook **Slow Blinking** = LINE 1 is registered on gatekeeper **Fast Blinking** = LINE 1 is receiving a telephone call **Off** = No registration (line out of service)
2	PHONE 2	Green	It indicates activity on Phone 2 line [VoIP] **On** = LINE 2 is off-hook **Slow Blinking** = LINE 2 is registered on gatekeeper **Fast Blinking** = LINE 2 is receiving a telephone call **Off** = No registration (line out of service)
3	LINK	Amber	ADSL Uplink active on the port towards network **On** = ADSL Link avaliable (solid ON) **Off** = ADSL Link not avaliable (device out of service) **Slow Blinking** = Seeking Phase **Fast Blinking** = Training Phase **Blinking** = Traffic activity
4	POWER	Red	Power On/Off

External Interfaces and Connectors

CPVA 500 CONNECTORS DESCRIPTION

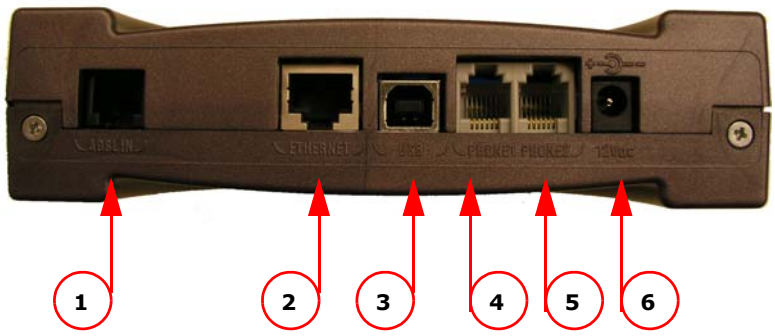


Fig. 2 CPVA 500 Connectors description

Tab. 2: CPVA 500 - Connection Indication

Port Number	Function	Indication	Remarks
1	**ADSL IN**	ADSL Uplink Port with RJ11 connector	To ADSL WAN Uplink
2	**ETHERNET**	ETHERNET 10/100 BaseTX with RJ45 connector	Connect to user device [PC] through CAT5 cable
3	**USB**	USB B type port - v. 1.1, 12Mbps	Connect to user device [PC] through USB cable
4	**PHONE 1**	FXS with RJ11 connector	Connect to user analogue telephone through phone cable
5	**PHONE 2**	FXS with RJ11 connector	Connect to user analogue telephone through phone cable
6	**12 Vdc**	Power Supply Input	Use the provided Power Supplier

Chapter 3

Installation

GENERAL ADVICES AND SECURITY RULES

Install the Access Gateway in a room with a temperature ranging between 5°C and 45°C, and a relative humidity ranging from 5% to 85%. It is recommended to avoid abrupt changes of temperature and humidity.

Leave a 10-15 cm of space around the Access Gateway in order to allow correct aeration. Do not expose to direct sunlight. The device has to always be connected to the electrical network. In order to avoid fire or electrical shock, do not install it in a wet or humid environment.

Do not defuse any parts of the Access Gateway. Do not execute operations on the internal parts for security reason. Do not insert any object into the Access Gateway. Use only the wall adapter present in the package and the original spare parts. The socket outlet shall be installed near the equipment and shall be easily accessible.

Ask for experienced assistance for any type of repair.

Do not cover the Serial Number and Mac Address label. The Serial Number and the Mac Address will be requested during any call to the Customer Service.

Installation

CPVA 500 PLACEMENT

CPVA500 can be positioned in a place compatibled with cable length and where the airflow is enough to cool off the equipment.

CPVA500 can be installed either on a flat or on a vertical surface (wall placement).

In case of **table placement**, use the provided vertical or horizontal support.

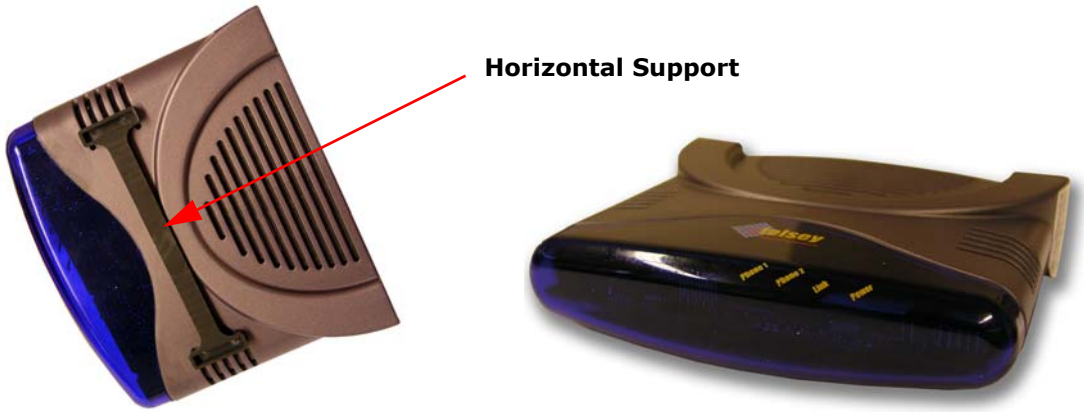


Fig. 3 Table Placement - Horizontal Support

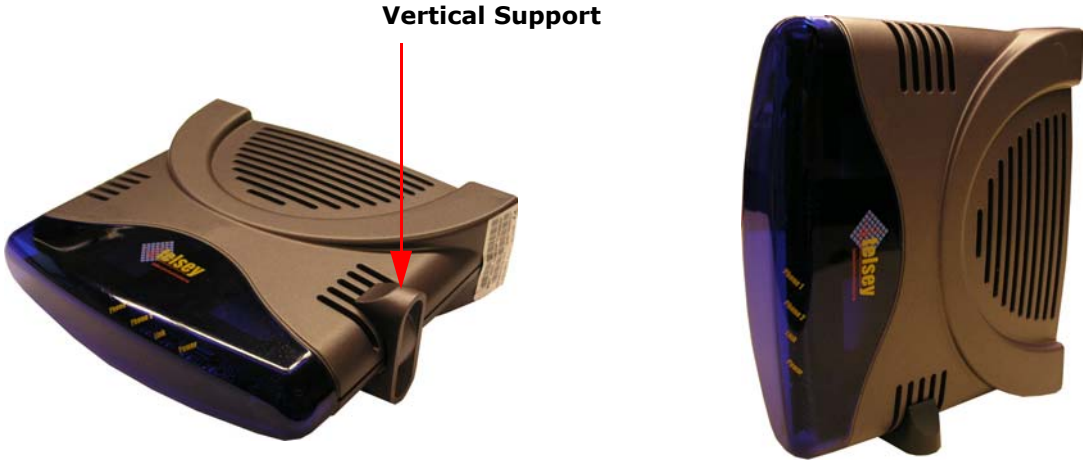


Fig. 4 Table Placement - Vertical Support

Installation

It is possible to place the Access Gateway on the wall by using the appropriate support (provided) and screw-anchors (not provided, we suggest to use two Fischer S4 screw anchors).

Wall Support

Fig. 5 Wall Placement: Wall Support

Installation

Chapter 4

SIP Protocol

INTRODUCTION

The Session Initiation Protocol (SIP) is a signalling protocol used for establishing sessions in an IP network. A session could be a simple two-way telephone call or it could be a collaborative multi-media conference session.

Since SIP is part of a IETF (*Internet Engineering Task Force*) specification, it extends the open-standard spirit of the Internet to messaging, enabling remote computers, phones, televisions and software to communicate.

Members in a session can communicate via multicast or via a mesh of unicast relations, or via a combination of these. SIP supports session descriptions that enable participants to agree on a set of specific media types. SIP is not tied to any particular conference control protocol. In essence, SIP has to provide or enable the following functions:

- **Name translation and user location:** ensuring that the call reaches the called party wherever it is located. Carrying out any mapping of descriptive information to location information. Ensuring that details of the nature of the call are fully supported.
- **Feature negotiation**: this allows the group involved in a call to agree on the features supported, recognizing that not all the parties can support the same level of features.
- **Call participant management**: during a call, a participant can bring other users onto the call or cancel connections to other users. Besides, users could be transferred or placed on hold.
- **Call features changes**: a user should be able to change the call characteristics during the course of the call. For example, a call may have been set up as 'voice-only', but the users may need to enable a video function.

SIP fulfils these functions and re-uses other web elements to make it flexible and scalable.

Rather than defining a new type of addressing system, SIP addresses users by an email-like address. Each user is identified through a hierarchical URL that is built around elements such as a user's phone number or host name (for example, `sip:user@telsey.com`). This means that it is just as easy to redirect someone to another phone as it is to redirect someone to a webpage.

SIP Protocol

In this sense, SIP borrows from the email model, using the Domain Name System, to deliver requests to the server that can appropriately cope with them. This also simplifies the integration of voice and email.

SIP is also transport layer indipendent. Therefore, the underlying transport could be IP over ATM. SIP uses the User Datagram Protocol (UDP) as well as the Transmission Control Protocol (TCP), flexibly connecting users independent of the underlying infrastructure.

SIP provides the necessary protocol mechanisms so that end systems and proxy servers can provide services:

- User location
- User capabilities
- User avaliability
- Call setup
- Call handling
- Call forwarding
- Callee and calling number delivery
- Personal mobility, i.e. the ability to reach a called party under a single, location-independent address regardless the change of terminal by the user
- Terminal type negotiation and selection
- Terminal capability negotiation
- Caller and callee authentication
- Blind and supervised call transfer
- Invitation to multicast conferences.

Protocol Components

There are four basic components within SIP:

1) SIP user agent

2) SIP network server

3) SIP Registration service

4) SIP Event and Presence server

The user agent is the end system component for the call and the SIP server is the network device that handles the signalling associated with multiple calls. The user agent itself has a *client element*, the User Agent Client (UAC) and a *server element*, the User Agent Server (UAS). The client element initiates the calls and the server element answers the calls. This allows peer-to-peer calls to be made using a client-server protocol.

The main function of the SIP servers is to provide name resolution and user location, since the caller is unlikely to know the IP address or host name of the called party, and to pass on messages to other servers using next hop routing protocols.

SIP servers can operate in three different modes:

- Stateful proxy mode

SIP Protocol

- Stateless proxy mode
- Re-direct server

The difference between these modes is that a *server in a stateful mode* remembers the incoming requests it receives, along with the responses it sends back and the outgoing requests it sends on.

A *server in a stateless mode* forgets all information once it has sent a request. These stateless servers are likely to be the backbone of the SIP infrastructure while stateful-mode servers are likely to be the local devices close to the user agents, controlling domains of users.

A *re-direct server* receives the request, but instead of passing it onto the next server, it sends a response to the caller party, indicating the address for the called user. This method enables the provisioning of the address for the caller, in order make it possible to contact the called party directly at the next server.

The *SIP Registration Service* provides a means for a particular device to register to use a SIP address. As seen at the beginning of this chapter, SIP addresses use 'URLs' based on the same addressing scheme used in the web and similar in form to an email address. The SIP address provides a single address of record for the user that delivers a one number service for all communications applications. Users can dynamically register the devices through which they may be contacted for all types of applications. As a result, people will no longer have to hand out multiple contact addresses as the system will automatically handle the distribution of all types of calls appropriately through the proxy and redirect servers.

SIP Event and Presence Servers allow the effective sharing of information about and between users and/or applications.

SIP Signalling

Here is reproduced a simple procedure of a call set-up:

a) The caller (User Agent Caller) sends a request with the SIP URL of the called party.

b) If the client knows the location of the other party, is sends the request directly to its IP address. If the location is unknown, the client can send it to a SIP network server, which has been locally configured.

c) The server will try to resolve the called user's location and sends the request to them. There are many ways it can do this: searching the DNS or accessing databases. Alternatively, the server may be a redirect server that may return the called user location to the calling client for it to try directly. During the course of locating a user, one SIP network server can proxy or redirect the call to additional servers until it arrives at one that definitely knows the IP address where the called user can be found.

d) Once found, the request is sent to the user. In the simplest case, the user's telephony client receives the request, that is, the user's phone rings. If the user takes the call, the client responds to the invitation with the designated capabilities of

SIP Protocol

the client software and a connection is established. If the user declines the call, the session can be redirected to a voice mail server or to another user.

SIP has two additional significant features.

1) A stateful SIP server's ability to split an incoming call so that several extensions can be rung at once. The first extension to answer takes the call.
2) SIP's unique ability to return different media types within a single session.

SIP Methods

The commands that SIP uses are called methods. SIP defines the following methods:

SIP Method	Description
INVITE	Invites a user to a call
ACK	Used to facilitate reliable message exchange for INVITEs
BYE	Terminates a connection between users or declines a call
CANCEL	Terminates a request, or search, for a user
OPTIONS	Solicits information about a server's capabilities
REGISTER	Registers a user's current location
INFO	Used for mid-session signalling

Protocol Header Structure

The protocol is composed of:

a) A start line
b) A message header
c) An empty line
d) An optional message body.

Request Messages

The format of the Request Packet header is shown in the following figure:

Method	Request URI	SIP Version

SIP Protocol

Method - It is the method to be performed on the resource. All the possible methods are listed in the previous table

Request URI - A SIP URL or a general Uniform Resource Identifier. It represents the user or service to which this request is being addressed.

SIP Version - The SIP version being used.

Response Message

The format of the Response Message header is shown in the following figure:

SIP Version - The SIP version being used.

Status Code - A 3-digit integer code of the attempt to understand and satisfy the request.

Reason Phrase - A textual description of the status code.

SIP Protocol

Chapter 5

Web Interface

USING THE WEB-BASED USER INTERFACE

To configure the CPVA500 for the first time, the configuration PC must have a static IP address within the 192.168.1.x subnet.
Perform the following steps to bring up the Web User Interface:

1) Connect an Ethernet cable between the CPVA500 and a PC configured to use subnet 192.168.1.x.

2) To configure the PC to use subnet 192.168.1.x, right click on the **Local Area Connection** under the Network and Dial-Up connection window and select **Properties**.

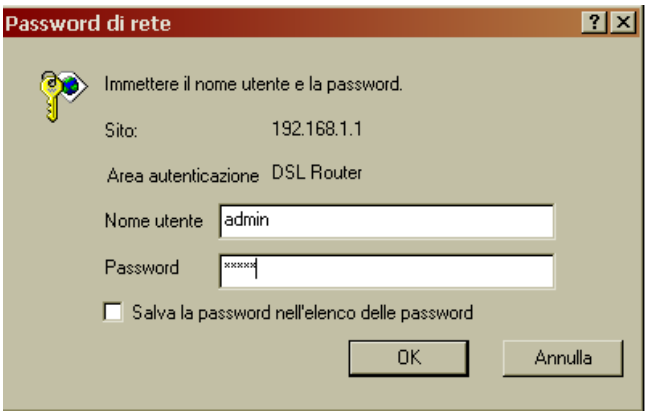
3) Select **Internet Protocol (TCP/IP)** and then click on the Properties button.

4) Select the **Use the following IP address** option and then enter the IP address as 192.168.1.x[1], where x is some number between 2 and 254. Click the tab button to select the subnet mask as 255.255.255.0.

5) If the CPVA500 has not been turned on, turn on the power. Wait about one minute.

6) In a Web browser on the PC, connect to **http://192.168.1.1/** to enter the router's configuration program. The browser should connect and you should see the Enter Network Password screen shown in the following figure. If the browser does not connect, the router may not have an image. In this case, follow the instructions on page 69 to update the CPVA500 image.

7) Type **admin** in the User Name and Password fields, and click OK. These values can be changed later in the Web User Interface.



1. Note that Ethernet and USB interface share the same subnet, since they are bridged within the router.

Web Interface

USB Drivers Installation

In order to use USB port, it is necessary to install Microsoft Windows Remote NDIS USB drivers.

Follow these steps to complete the installation:

1) On Windows 98, Windows Me, Windows 2000 or Windows XP PC, enter "`mkdir \temp\usb`" to create a temporary directory.
2) Enter "`cd \temp\usb`" to change to the temporary directory.
3) Copy the **tlsID_cpva500_winusbrndis.zip** file to the Windows PC.
4) Unzip tlsID_cpva500_winusbrndis.zip into the temporary directory.
5) Connect a USB cable between the PC and the CPVA500.
6) The first time that this is done, the Windows PC displays the "New Hardware Found" dialog. When prompted for the location of the driver, specify the temporary directory, \temp\usb.
7) On Windows 98 and Windows Me, you will need to reboot the Windows PC.
8) The CPVA500 Windows USB driver looks like a network adapter card to Windows. It is bound to TCP/IP. Configure TCP/IP appropriately for your environment.

The driver is now operational.

Web Interface

Factory Default Configuration

During Power on initialization, the CPVA500 initializes all configuration attributes to default values. It will read in the configuration profile from the permanent storage section on the flash memory. The default values are overridden when identical attributes with different values are configured.

The configuration profile in the permanent storage can be created via Web User Interface or Telnet User Interface, or the other management protocols.

The factory default configuration can be restored in the following method:

- Via *Web page*, by clicking the **Restore Default Settings** option in the Restore Default screen;
- Via *Telnet* with `restoredefault` command.
- Via *Phone*, when the unit becomes unreachable. Refer to page 71 for futher information.

The default parameters of the device are the following:

- LAN port IP address: **192.168.1.1**
- LAN port Netmask: **255.255.255.0**
- Local Administrator[1] account name: **admin**
- Local Administrator account password: **admin**
- Local Non-Administrator[2] account name: **user**
- Local Non-Administrator account password: **user**
- Remote WAN access[3]: **enabled all service**
- Remote WAN access account name: **support**
- Remote WAN access account password: **support**
- DHCP server on LAN interface: **disabled**

Note **The parameters not included in the previous list are not set.**

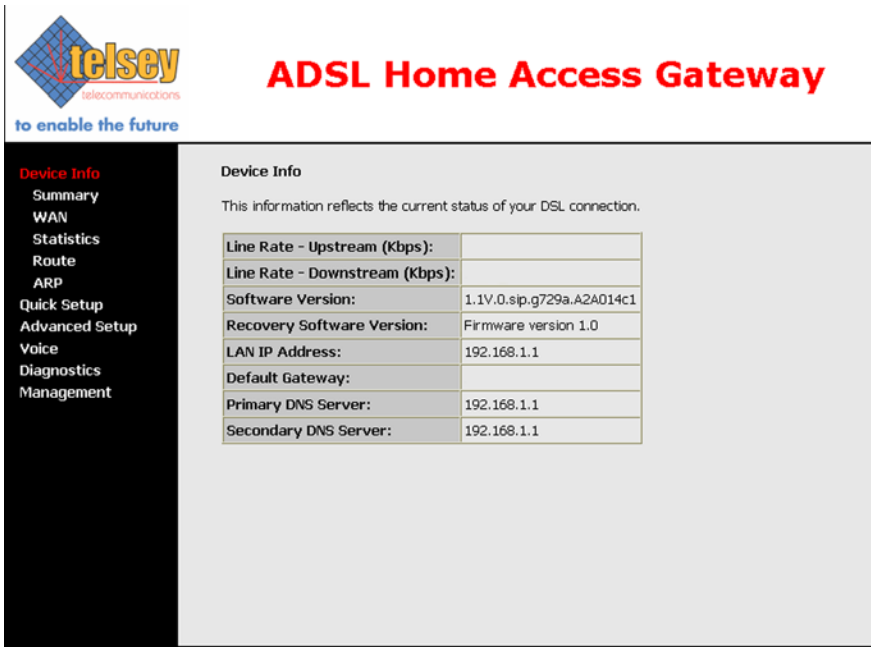
1. The Local Access screen allows you to set and confirm "admin" unrestricted access to change the configuration of the router, but cannot obtain access from WAN. Both username and password have a maximum length of 15 characters.
2. The User Access screen allows you to set and confirm "user" access to view the configuration, statistics, and to update the router software via LAN, but not via WAN. Both username and password have a maximum length of 15 characters.
3. The Remote technical support account allows the local administrative user to explicitly enable a remote technician to access Telsey Router user interface and allows it to send ping response packet. This account allows you to set and confirm "support" access for router maintenance and diagnostics. The remote support access will not work in bridge mode since there is no public IP address assigned to the router. Both username and password have a maximum length of 15 characters.

Web Interface

DEVICE INFO

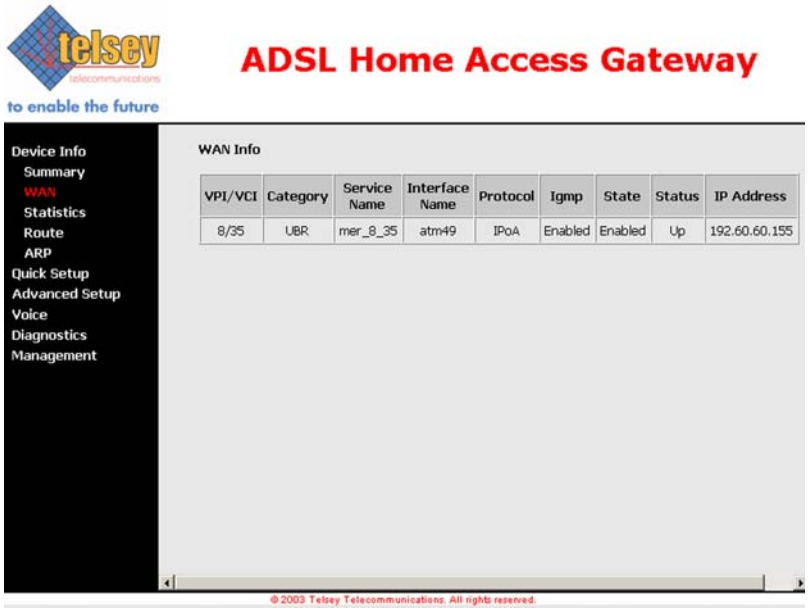
Summary

After login, the Device Info screen appears as shown in the following figure.



WAN

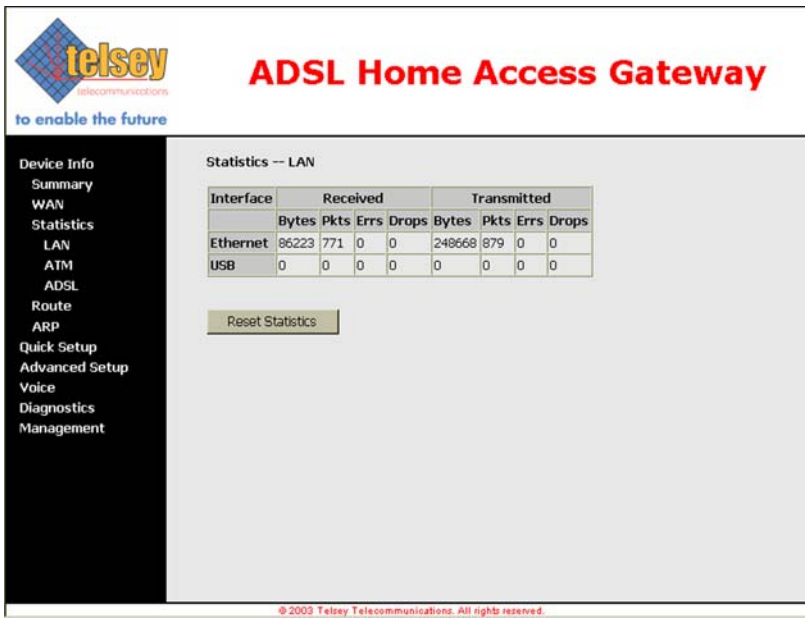
The following page shows the settings currently configured in the WAN setup (Advanced Setup section).



Web Interface

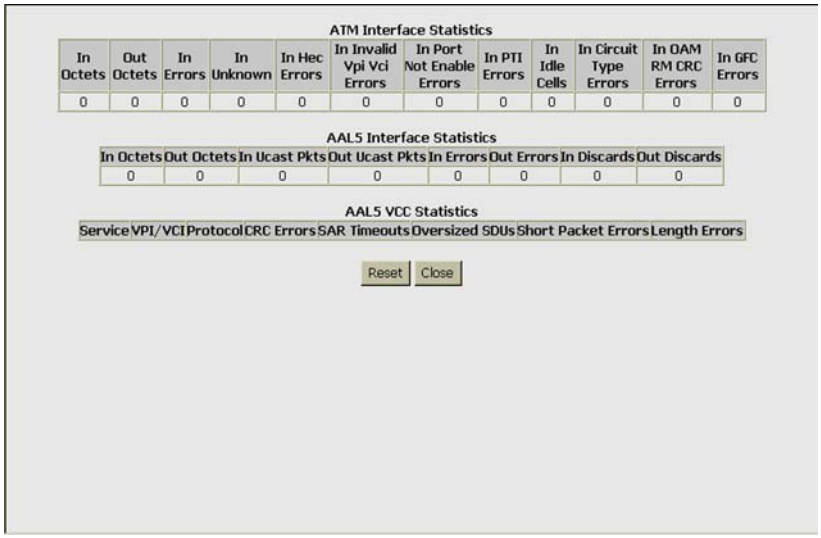
Statistics LAN

The LAN Statistics screen shows interface statistics for Ethernet and USB interfaces.



ATM Statistics

The following figure shows the ATM statistics screen.



Web Interface

Tab. 3: ATM Layer Statistics over ADSL interface

Field	Description
InOctets	Number of received octets over the interface
OutOctects	Number of transmitted octets over the interface
InErrors	Number of cells dropped due to uncorrectable HEC errors
InUnknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
InHecErrors	Number of cells received with an ATM Cell header HEC error.
InInvalidVpiVciErrors	Number of cells received with an unregistered VCC address.
InPortNotEnabledErrors	Number of cells received on a port that has not been enabled.
InPtiErrors	Number of cells received with an ATM header Payload Type Indicator (PTI) error.
InIdleCells	Number of idle cells received.
InCircuitTypeErrors	Number of cells received with an illegal circuit type.
InOamRmCrcErrors	Number of OAM and RM cells received with CRC errors.
InGfcErrors	Number of cells received with a non-zero GFC.

Tab. 4: ATM AAL5 Layer Statistics over ADSL interface

Field	Description
InOctets	Number of received AAL5/AAL0 CPCS PDU octets.
OutOctets	Number of AAL5/AAL0 CPCS PDU octets transmitted.
InUcastPkts	Number of received AAL5/AAL0 CPCS PDUs passed to a higher-layer.
OutUcastPkts	Number of AAL5/AAL0 CPCS PDUs received from a higher-layer for transmission.
InErrors	Number of AAL5/AAL0 CPCS PDUs received that contain an error. The types of errors counted include CRC-32 errors, SAR timeout errors and oversized SDU errors.
OutErrors	Number of AAL5/AAL0 CPCS PDUs that could not be transmitted due to errors.
InDiscards	Number of AAL5/AAL0 CPCS PDUs discarded due to an input buffer overflow condition.
OutDiscards	This field is not currently used.

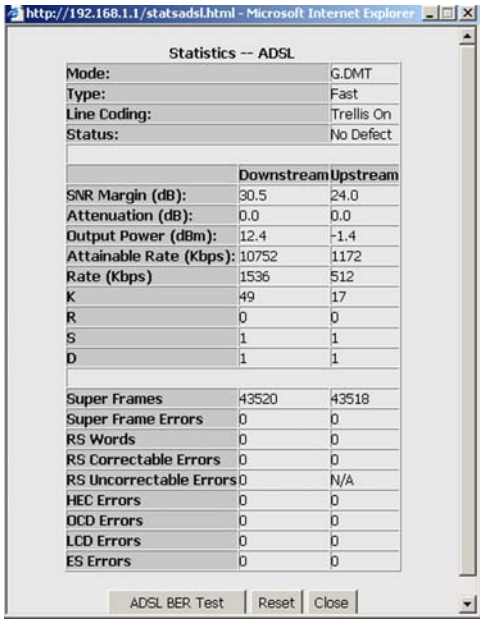
Web Interface

Tab. 5: ATM AAL5 Layer Statistics for each VCC over ADSL interface

Field	Description
CrcErrors	Number of PDUs received with CRC-32 errors.
SarTimeOut	Number of partially re-assembled PDUs which were discarded because they were not fully re-assembled within the required time period. If the re-assembly timer is not supported, then this object contains a zero value.
OverSizedSDUs	Number of PDUs discarded because the corresponding SDU was too large.
ShortPacketError	Number of PDUs discarded because the PDU length was less than the size of the AAL5 trailer.
LengthErrors	Number of PDUs discarded because the PDU length did not match the length in the AAL5 trailer.

ADSL Statistics

The following figure shows the ADSL statistics screen.



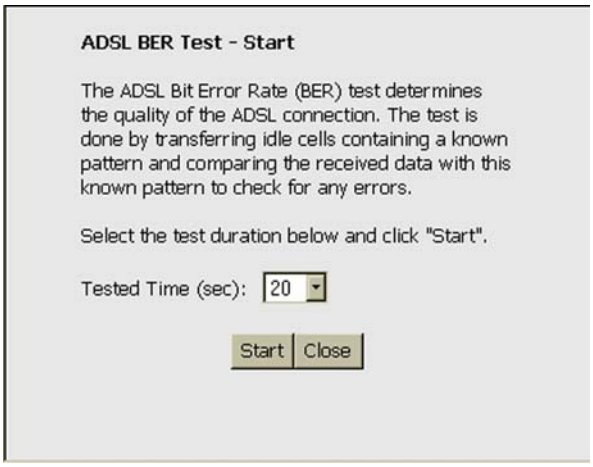
Tab. 6: ADSL Statistics field

Field	Description
Mode	Modulation protocol G.DMT or T1.413
Type	Channel type, Interleave or Fast
Line Coding	Trellis coding on/off
Status	Link Status
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin

Web Interface

Tab. 6: ADSL Statistics field

Field	Description
Attenuation (dB)	estimate of average loop attenuation in the downstream direction
Output Power (dBm)	total upstream output power
Attainable rate (Kbps)	maximum achievable downstream rate
K	number of data bytes in ADSL data frame (DMT symbol)
S	length of Reed-Solomon code word in data frames
R	number of redundant check bytes per Reed-Solomon code word
D	interleaver depth
Super Frames	total number of super frames
Super Frames Errors	number of super frames received with errors
RS Words	total number of Reed-Solomon code words
RS Correctable Errors	number of RS words with correctable errors
RS uncorrectable Errors	number of RS words with uncorrectable errors
HEC Errors	total number of Header Error Checksum errors
LCD Errors	total number of Loss of Cell Delineation



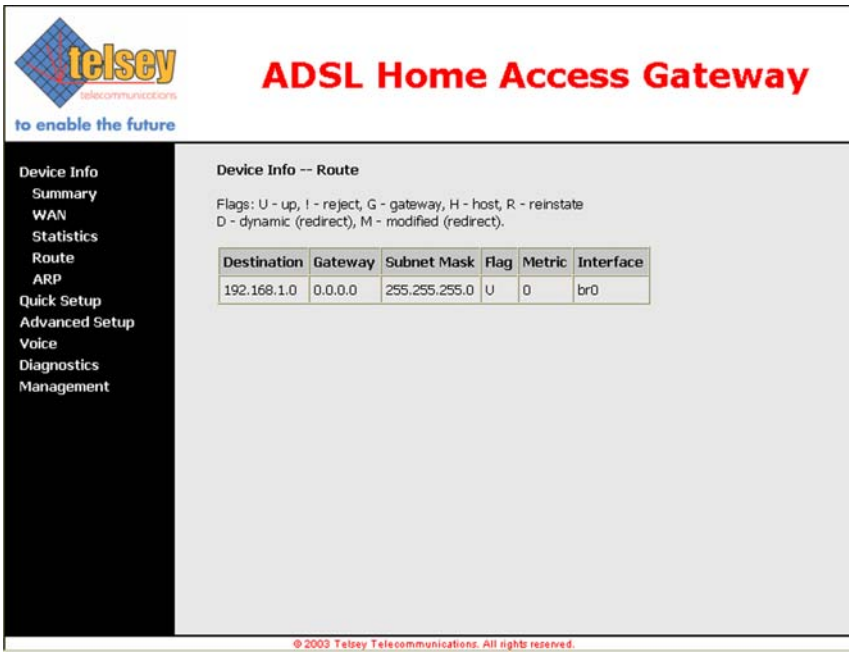
With the ADSL Statistics window, a Bit Error Rate Test can be started using the **ADSL BER Test** button. The windows associated with this test include a start/ configuration window, and in-process window and a results window.

Select the Tested Time (in seconds) and press Start.

Web Interface

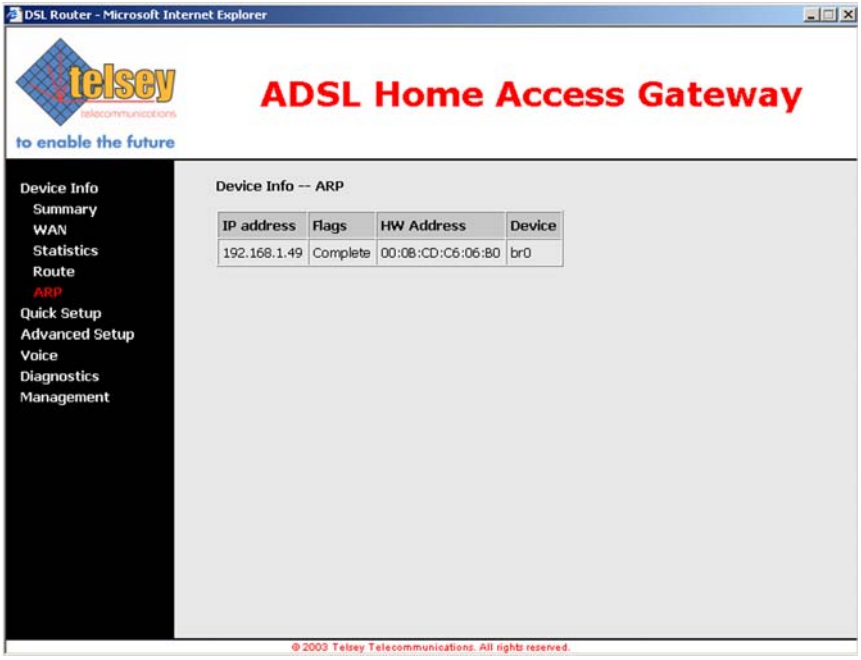
Route

The following page shows the routing information.



ARP

The following page shows the ARP configuration.

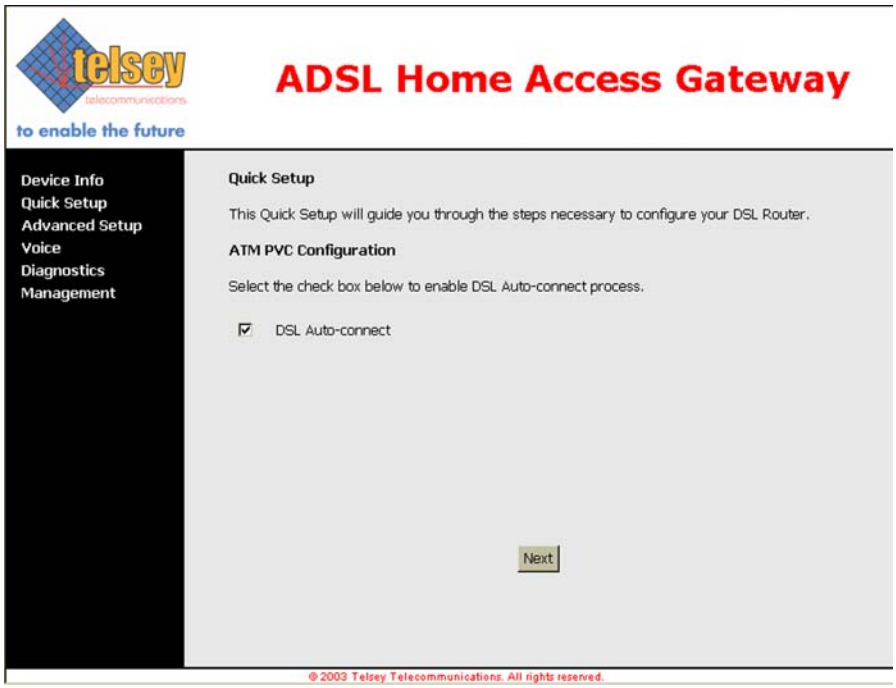


Web Interface

QUICK SETUP

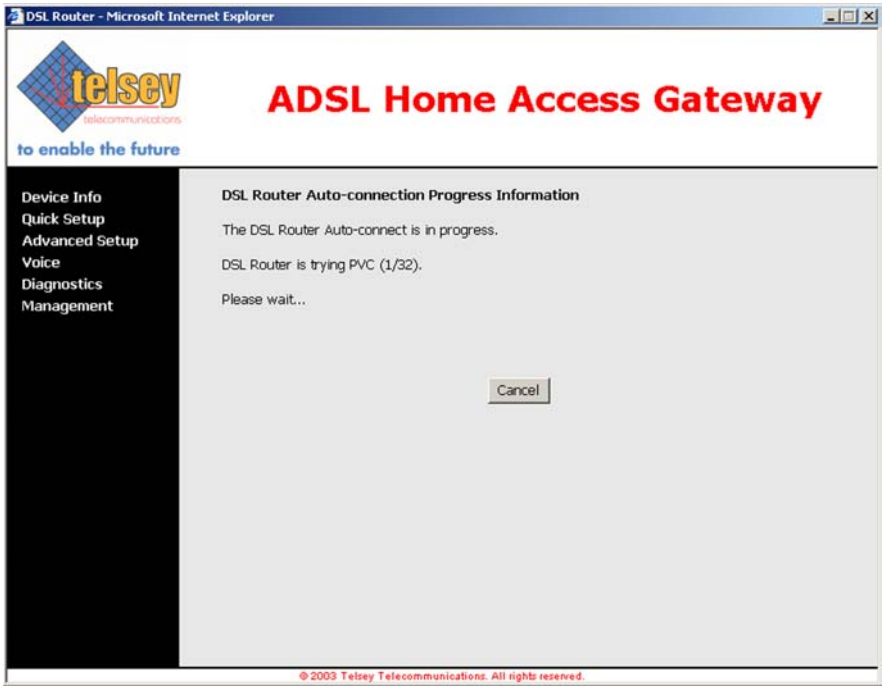
Quick Setup enables a user-friendly interface to configure CPVA500.

DSL Auto-connect is a feature that automatically scans PVC and tries to estabilish an ADSL connection. This feature, though, takes a long time, especially for the VPI/VCI scanning. We suggest to obtain the correct network settings from the ISP and then manually configure the CPVA500, by deselecting "DSL Auto-Connect" check box.

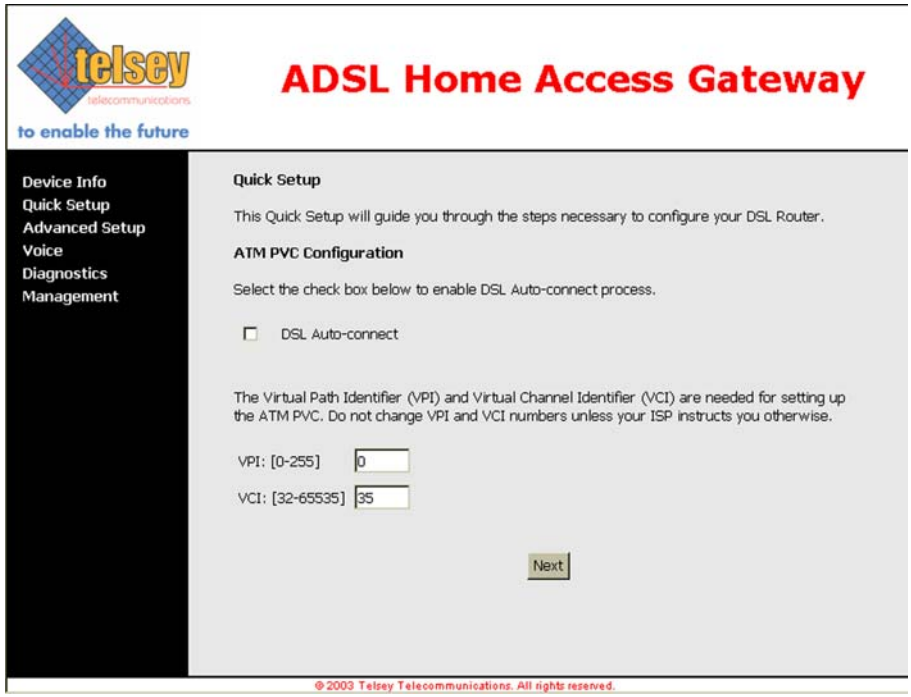


An example of DSL Auto-Connect configuration page is shown in the following figure:

Web Interface

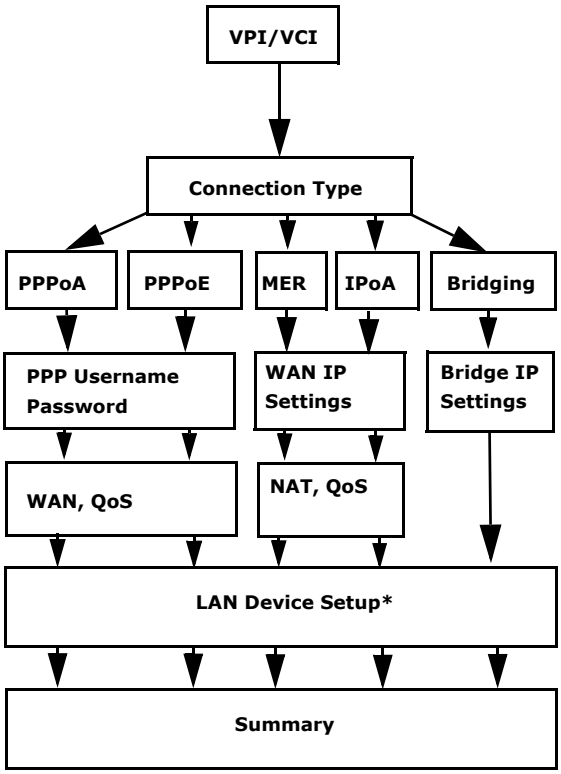


If DSL Auto-Connect is not selected, then it is possible to manually configure VPI/VCI, Connection Type, WAN IP Settings. For all the information regarding these settings, please refer to the Advanced Setup section starting from page 28.

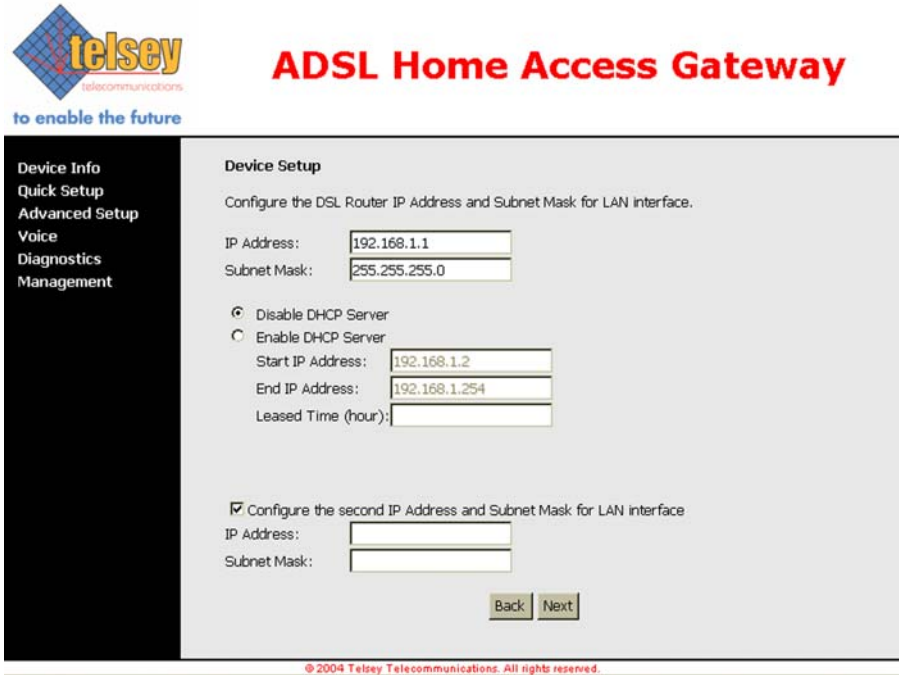


Web Interface

Quick setup navigation menu can be represented in the following diagram.

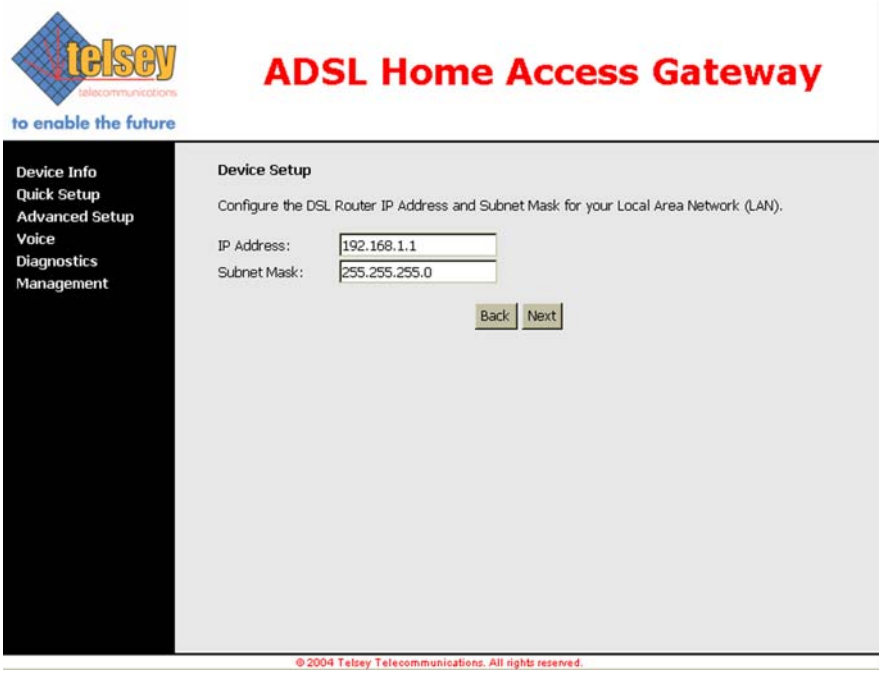


* In case of configuration via "Quick Setup", **Device Setup for LAN interface** can be configured by setting the following page (for *PPPoA, PPPoE, MER, IPoA*):



Web Interface

LAN Device Setup for *Bridging mode* is represented in the following page.



Web Interface

ADVANCED SETUP

WAN

WAN Setup

By clicking on **WAN** in the **Advanced Setup** menu it is possible to begin the configuration of WAN interfaces. The following screen shows the inital situation, when no WAN interface is present.

By clicking on **Add** button, it is possible to begin the setup.

ATM PVC Configuration

The first page to configure is **ATM PVC Configration.** These settings are usually given by Internet Service Providers.

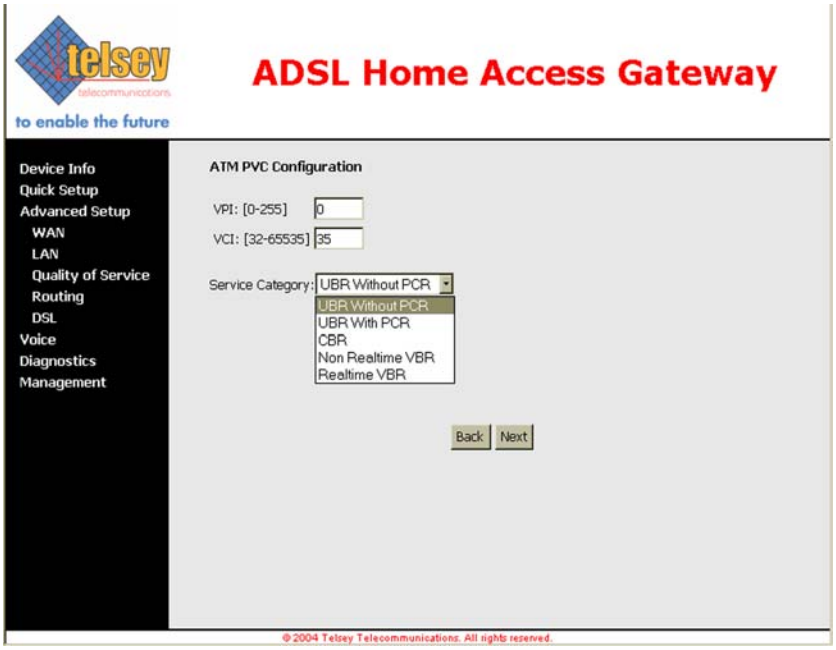
In this page it is possible to set VPI, VCI and Service Category.

Avaliable Service Categories are:

- UBR (Unspecified Bit Rate) without PCR (Peak Cell Rate)
- UBR with PCR
- CBR (Constant Bit Rate)
- Non Realtime VBR (Variable Bit Rate)
- Realtime VBR

The following figure shows the ATM PVC Configuration Page

Web Interface



In case of UBR with PCR and CBR, it is possible to set *Peak Cell Rate* [cells/s] value.
In case of Non Realtime VBR, it is possible to set values for:

- Peak Cell Rate [cells/s]
- Sustainable Cell Rate [cells/s]
- Maximum Burst Size [cells]

Click on Next to set Connection Type.

Connection Type

The **Connection Type** page allows to select the type of encapsulation protocol and encapsulation mode over the ATM PVC that has been selected in the previous page.

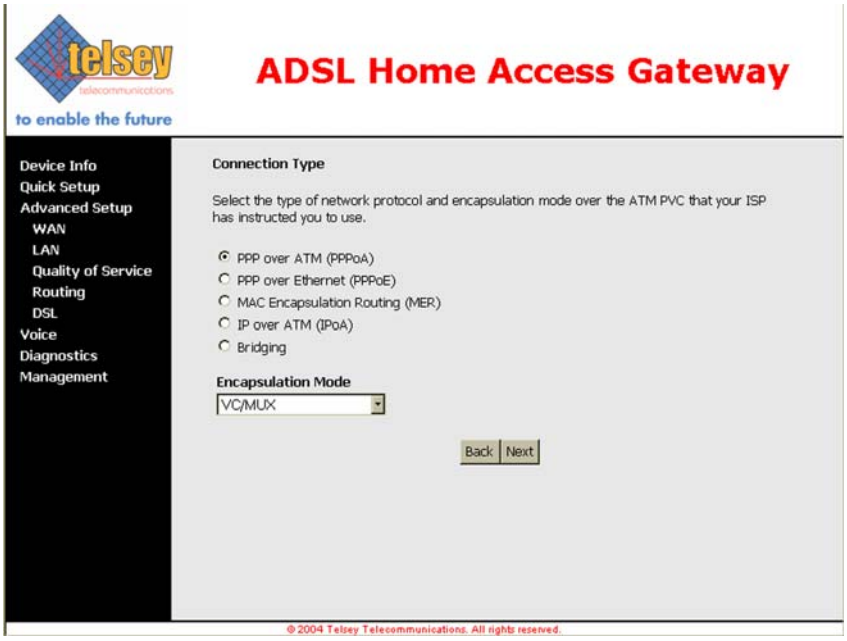
Avaliable connection types are:

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IPoA)
- Bridging

Depending on the selected network protocol, it is then possible to choose an appropriate encapsulation mode (VC/MUX, LLC/ENCAPSULATION, LLC/SNAP BRIDGING, VC/MUX, LLC/SNAP ROUTING).

Web Interface

The following figure shows the Connection Type page.



The following table shows all the encapsulation modes avaliable for each network protocol.

Tab. 7: Network Protocol and Encapsulation Mode

Protocol	Encapsulation Mode
PPP over ATM	VC/MUX, LLC/ENCAPSULATION
PPP over Ethernet	LLC/SNAP BRIDGING, VC/MUX
MAC Encapsulation Routing	LLC/SNAP BRIDGING, VC/MUX
IP over ATM	LLC/SNAP ROUTING, VC/MUX
Bridging	LLC/SNAP BRIDGING, VC/MUX

Each Network Protocol needs further configurations, which can be set by clicking on Next.

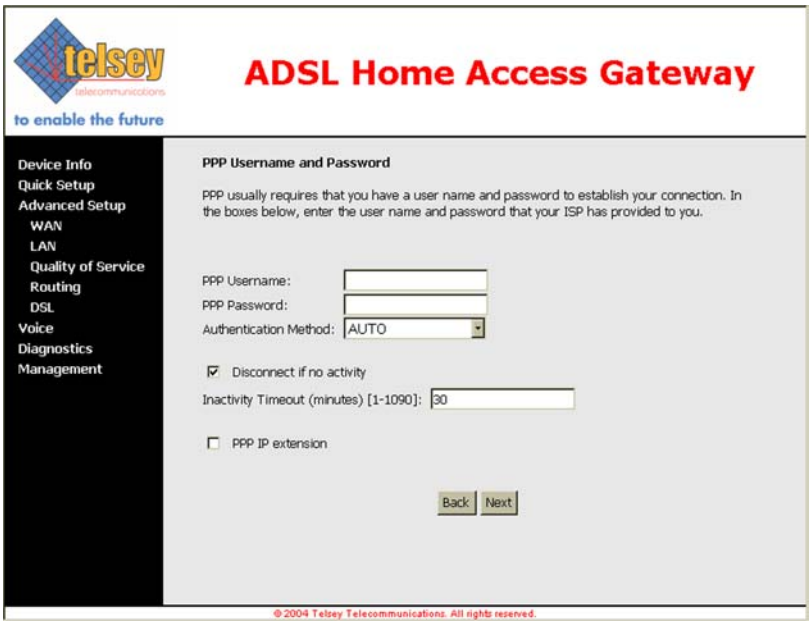
PPPoA

If **PPP over ATM** is chosen, regardless of the selected encapsulation mode, the following screen requires to set PPP Username and Password. The Password requirement is dependent on the particular requirements of the ISP or ADSL Service Provider.

PPP Username max. length is 256 characters, PPP Password max. length is 32 characters.

Web Interface

The following figure shows PPP Username and Password page.



CPVA500 can be configured to disconnect if there is no activity for a period of time by selecting the **Disconnect if no activity** box. Default time is 30 minutes.

As **Authentication Method**, either "PAP", or "CHAP" can be used. If "AUTO" is selected, then the authentication protocol is automatically selected.

PPP IP extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

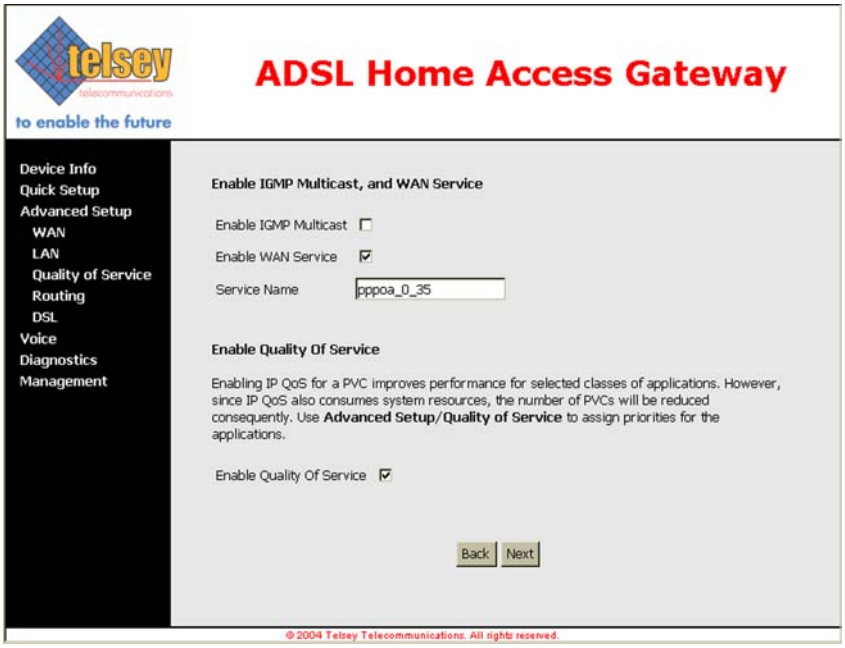
- Allows only one PC on the LAN
- The public IP address assigned by the remote using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote since the DHCP server within the ADSL router has only a single IP address to assign to a LAN device.
- NAPT and firewall are disabled when this option is selected.
- The ADSL router becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The ADSL router extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The ADSL router bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the router's LAN IP address.

By clicking on Next, it is then possible to enable or disable WAN service (and assign a service name), IGMP multicast (not supported yet) and Quality of Service. QoS can be activated and then controlled by means of the relative menu (Advanced Setup --> Quality of Service). Note that enabling QoS for a

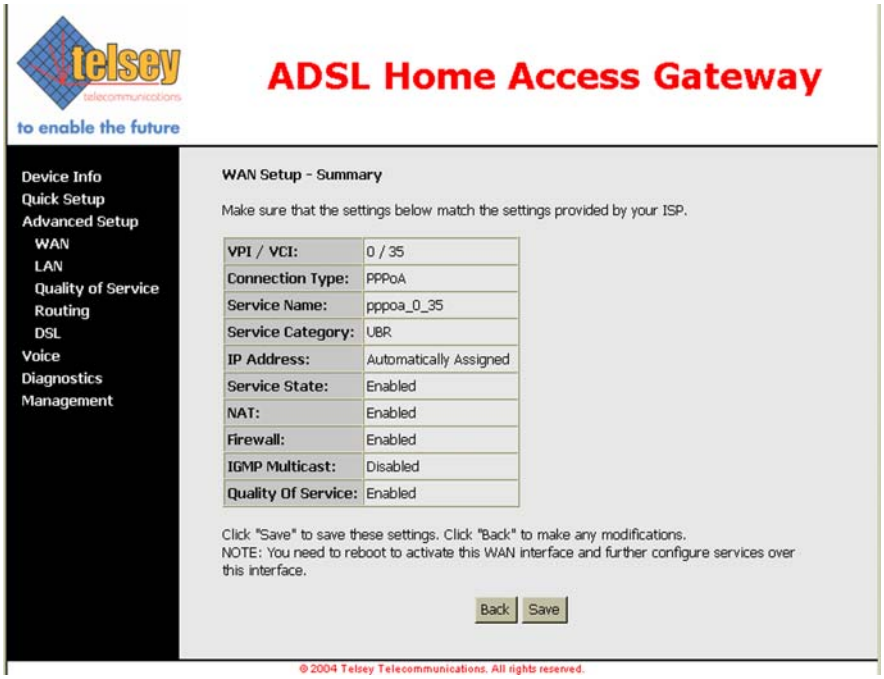
Web Interface

selected PVC improves performance for selected classes of applications, but also reduces the number of available PVC's.

The following figure shows the relative page.



By clicking on Next, the WAN Setup Summary shows up.

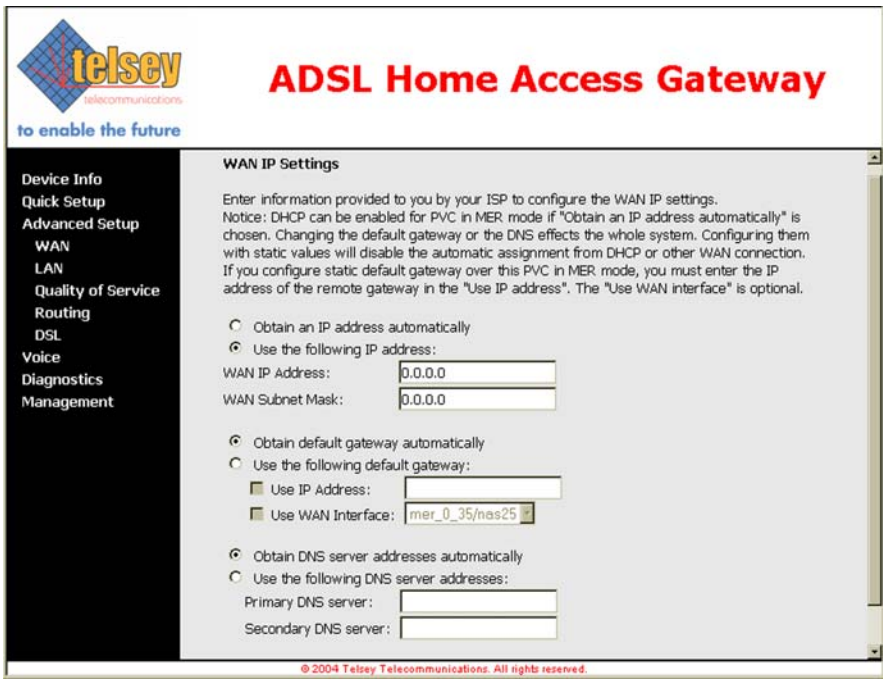


Web Interface

PPPoE If **PPP over Ethernet** is chosen, regardless of the selected encapsulation mode, the configuration pages are identical to PPP over ATM. All the considerations explained in the PPPoA section remain valid.

MER If **MAC Encapsulated Routing** is chosen, it is then necessary to configure WAN IP Settings.

The following figure shows WAN IP Settings page for MER protocol.



The **IP Address**, **Default Gateway** and **DSN Server** can be obtained automatically through the DHCP client in the CPVA500.
Otherwise, the user must enter static values in the appropriate fields.

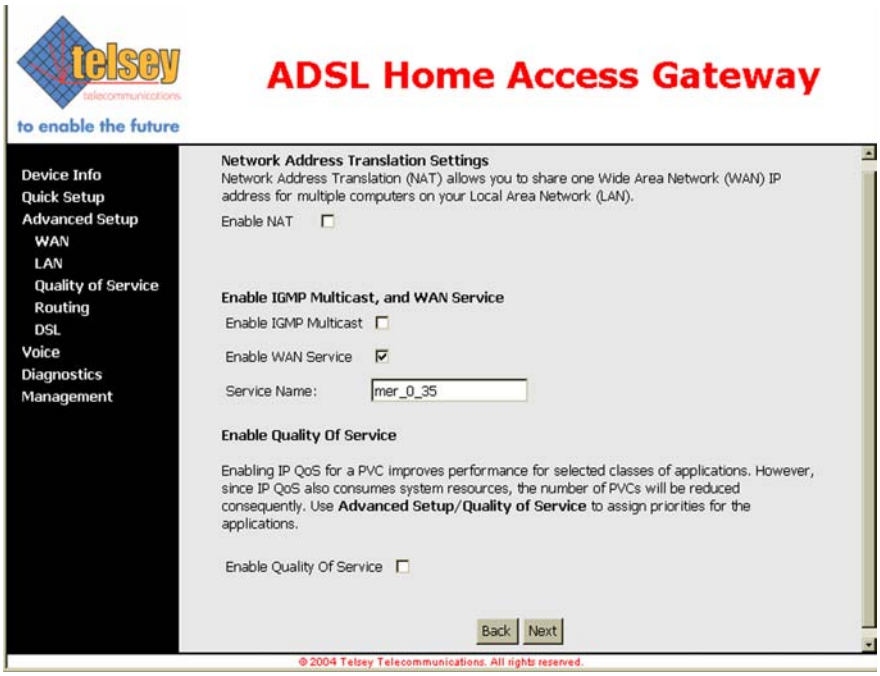
After that, by clicking on Next, it is possible to enable Network Address Translation (**NAT**). If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be deselected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

Refer to page 37 in order to configure NAT features.

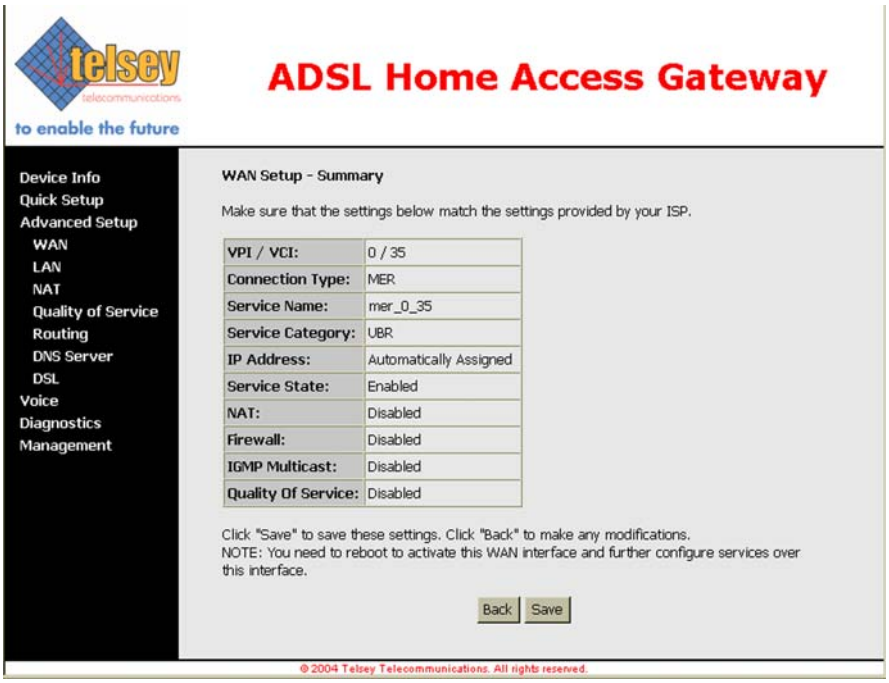
Besides NAT, from this page it is possible to enable WAN service (and assign a service name), IGMP multicast (not supported yet) and Quality of Service. QoS can be activated and then controlled by means of the relative menu (Advanced Setup --> Quality of Service). Note that enabling QoS for a selected PVC improves performance for selected classes of applications, but also reduces the number of available PVC's.

The following figure shows NAT, WAN Service, IGMP and QoS page.

Web Interface

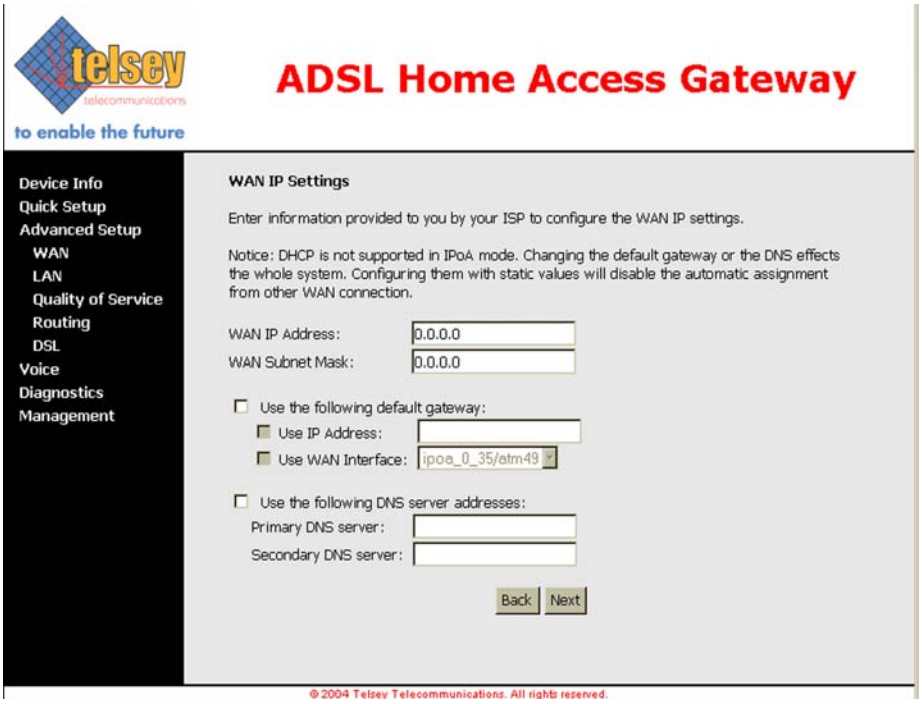


By clicking on next, the setup summary will be displayed. Click on Save to apply the settings.



Web Interface

IPoA If **IP over ATM** is chosen, it is then necessary to configure WAN IP Settings.



Enter WAN IP Address, Subnet Mask, Default Gateway and DNS Servers. Note that DHCP is not supported, meaning that automatic provisioning is not available when using IPoA.

After that, by clicking on Next, it is possible to enable Network Address Translation (**NAT**). If the LAN is configured with a private IP address, the user should select this checkbox. The NAT submenu on the left side main panel will be displayed after reboot. The user can then configure NAT-related features after the system comes up. If a private IP address is not used on the LAN side, this checkbox should be deselected to free up system resources for better performance. When the system comes back after reboot, the NAT submenu will not be displayed on the left main panel.

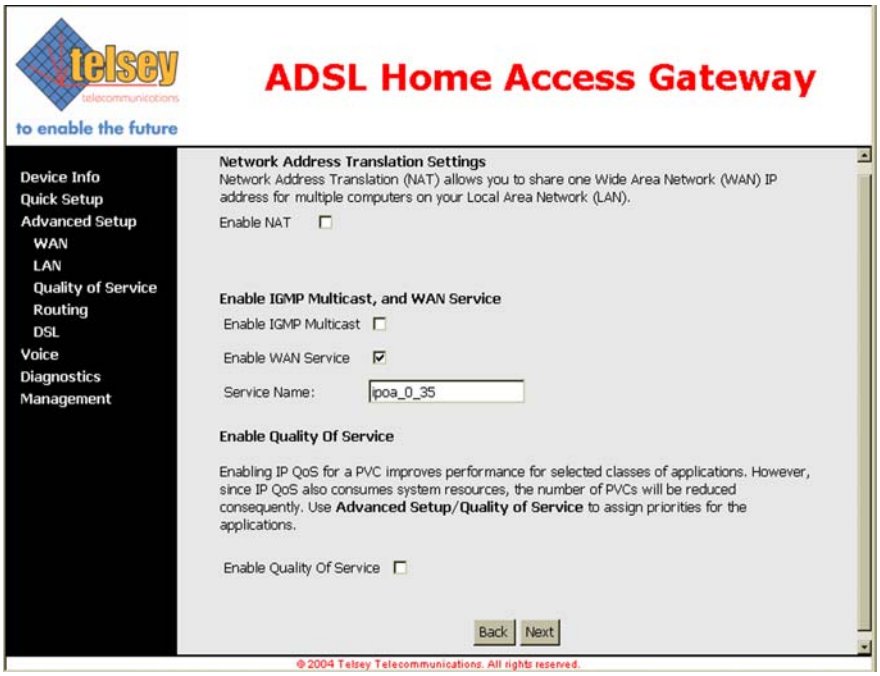
Refer to page 37 in order to configure NAT features.

Besides NAT, from this page it is possible to enable WAN service (and assign a service name), IGMP multicast (not supported yet) and Quality of Service. QoS can be activated and then controlled by means of the relative menu (Advanced Setup --> Quality of Service). Note that enabling QoS for a selected PVC improves performance for selected classes of applications, but also reduces the number of available PVC's.

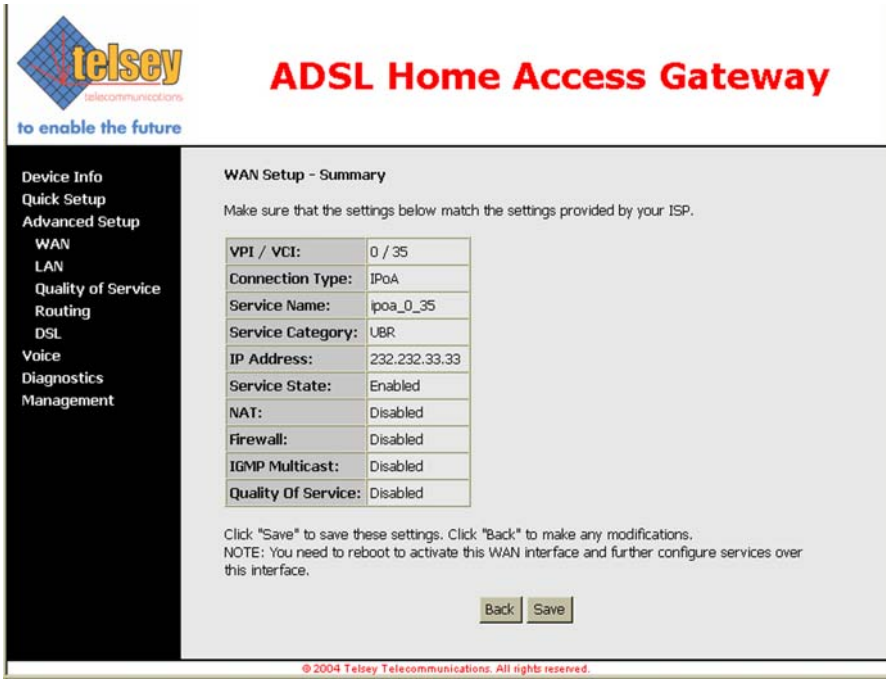
The following figure shows NAT, WAN Service, IGMP and QoS page.

Web Interface

The following figure shows Network Address Traslation Settings page.



By clicking on next, the setup summary will be displayed. Click on Save to apply the settings.



Web Interface

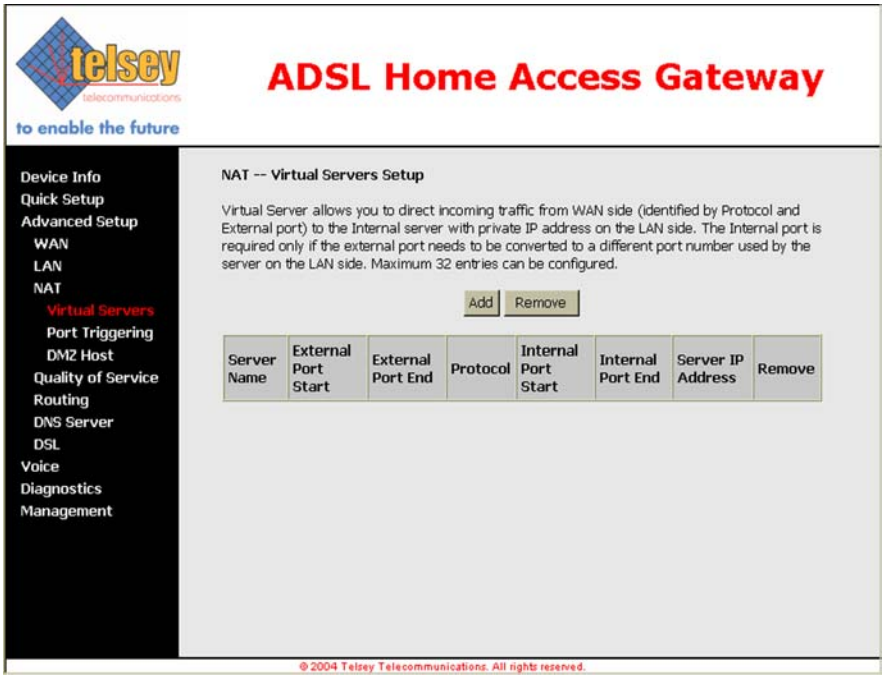
NAT Configuration

After enabling NAT (for MER, IPoA, PPPoA, PPPoE) and rebooting, on the left side menu a new NAT submenu comes up. Network Address Translation (NAPT) allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.

Implementing dynamic NAPT automatically creates a firewall between your internal network and outside networks, or between your internal network and the Internet. NAPT only allows connections that originate inside the sub domain. Essentially, this means that a computer on an external network cannot connect to your computer unless your computer has initiated the contact. You can browse the Internet and connect to a site, and even download a file; but somebody else cannot latch onto your IP address and use it to connect to a port on your computer. Under the NAPT environment, all computers behind the NAPT are not accessible from outside (i.e., the WAN). However, if public services, such as web servers, ftp servers or email servers, are needed from your private network, a virtual server can be configured to set up permit secured access. A virtual server setup enables a connection from outside to be redirected to a host running the services on the private subnet. This host running the services is called a virtual server (a virtual server is synonymous with IP forwarding).

The NAT dialog box allows you to configure Virtual Servers and DMZ Host settings by adding, removing and saving.

The following figures show the NAT configuration pages.



The first page is **NAT Virtual Servers**. Virtual server allows you to direct incoming traffic from WAN side (identified by Protocol and External Port) to the Internal server with private IP address on the LAN side. The internal port is

Web Interface

required only if the external port needs to be converted to a different port number used by the server on the LAN side.

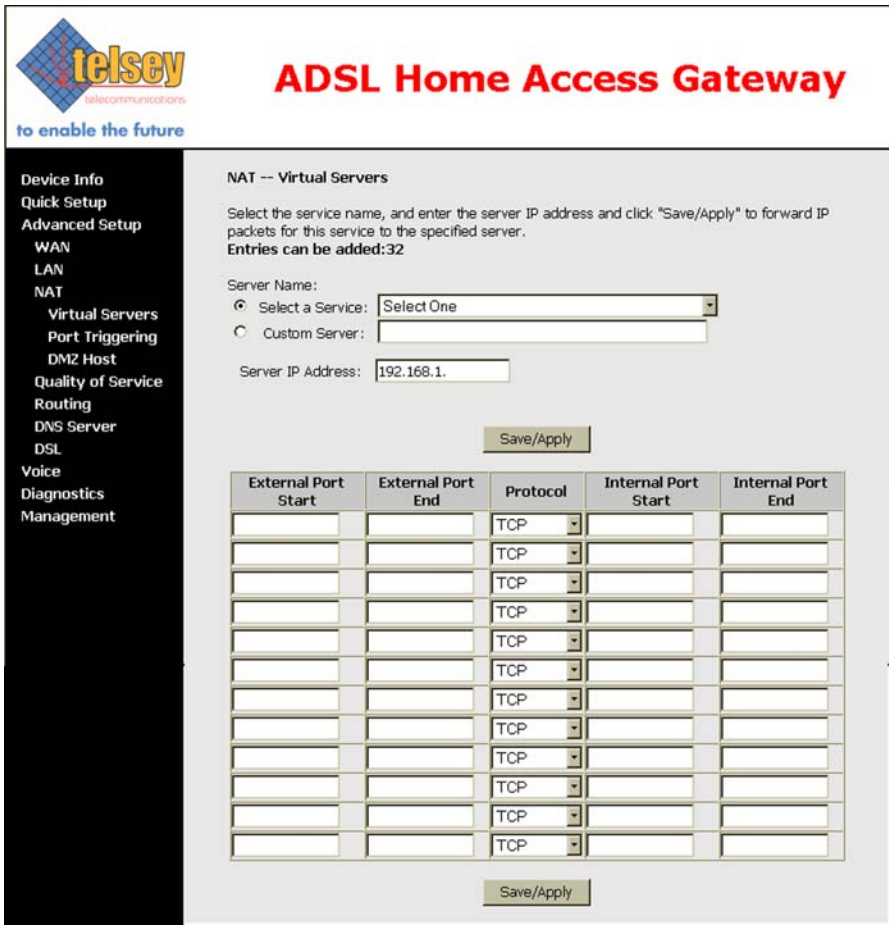
Tab. 8: NAT Virtual Servers main page

Option	Description
Server Name	The service the virtual server will provide (web, ftp, email).
Protocol	The protocol (UDP,TCP or both) used by the service.
External Port	The port or port range that an outside connection will use.
Internal Port	The port or port range that the virtual server will use to listen to the connection from outside.
Server IP Address	The internal (private) IP address of the virtual server.

Click on Add to add a Virtual server and display the following page.

Click on Remove, after selecting the Virtual Server, to delete the Virtual Server.

After clicking on Add, it is possible to select the service name and IP address in order to forward IP packets for this service to the specified server.



Web Interface

Tab. 9: NAT Virtual Server fields

Option	Description
Service Name	Allows the selection of an existing service from a drop-down-menu, or an entry of a custom service entry is the name is known, but not listed in the existing list.
Protocol	Allows the selection of a transport protocol (UDP,TCP or both).
External Port (Start/End)	Allows the entry of an individual external port, or range of ports.
Internal Port (Start/End)	Allows the entry of an individual internal port, or range of ports.
Server IP address	Allows the entry of an internal server IP address.

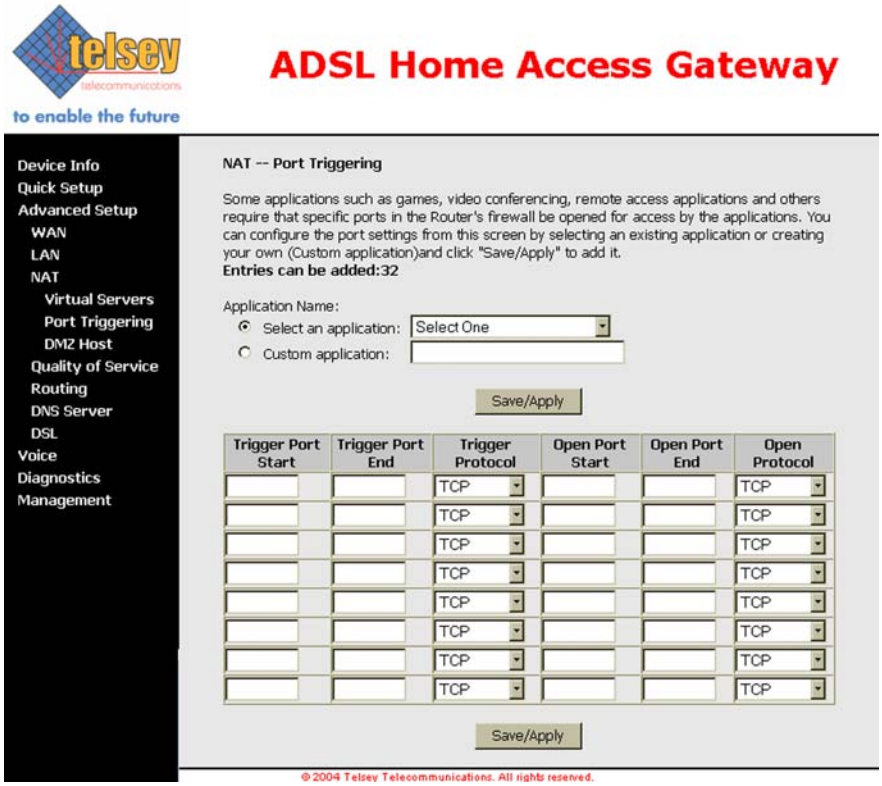
By clicking on **Port Triggering** in the NAT menu, you will enter NAT Port Triggering configuration page.

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Triggering 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 parties from the WAN side to estabilish new connections back to the application on the LAN side using the "Open Ports".

The following figure shows NAT Port Triggering main page.

Web Interface

By clicking on Add, the following page shows up.



Select an application from the drop down menu, or type in a custom application name.

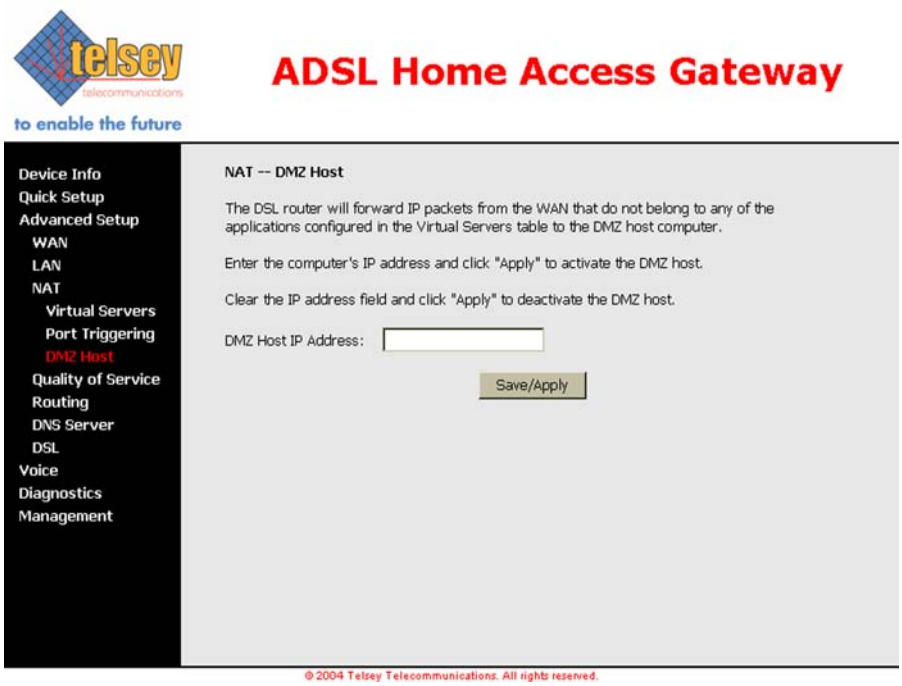
Enter the trigger port range (Trigger Port Start --> Trigger Port End) and the Trigger Protocol (TCP, UDP, TCP/UDP). Then, enter the open port range (Open Port Start --> Open Port End) and the Open Protocol (TCP, UDP, TCP/UDP).

By clicking on **DMZ Host**, you will enter the DeMilitarized Zone Host options page.

The DeMilitarized Zone Host option is used to forward IP packets from the WAN that do not belong to any of the applications configured in the virtual servers table, to the DMZ host computer. While virtual server can only forward (redirect) a limited number of services (ports), DMZ hosting allows all the services (ports) running on the DMZ host, to be accessible externally.

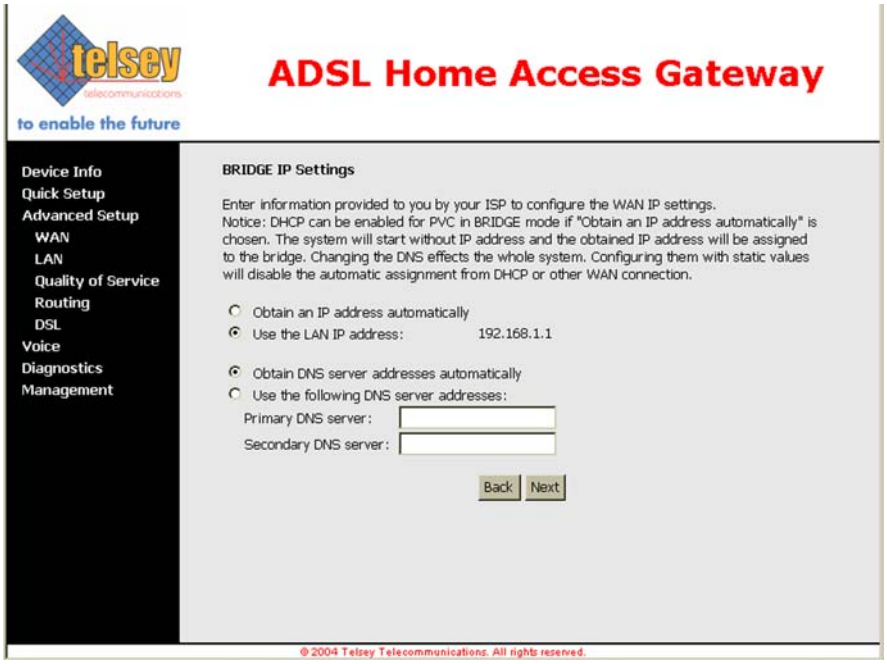
The following figure shows the DMZ Host page.

Web Interface



To configure the DMZ, type in the computer's IP address in the DMZ Host IP Address field and click on Save/Apply. Clear the IP address field and click on Save/Apply to deactivate the DMZ host.

Bridging If **Bridging** is chosen, by clicking on Next, it is then possible to set the following page (BRIDGE IP Settings).

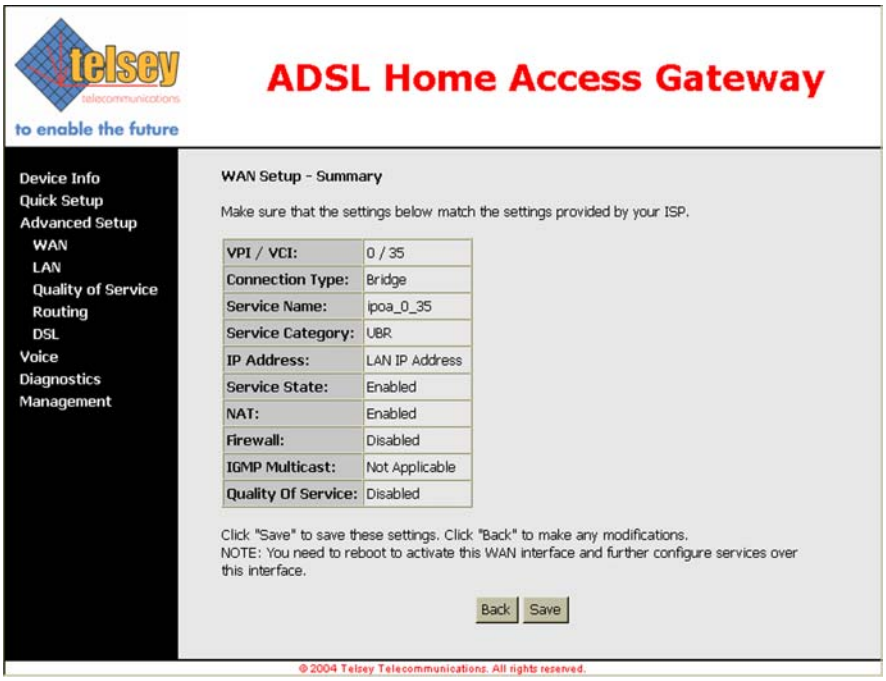


Web Interface

Enter information provided by the ISP to configure the WAN IP Settings. Note that DHCP can be enabled for PVC in Bridge mode if "Obtain an IP address automatically" is chosen. The system will start without IP address and the obtained IP address will be assigned to the bridge. Changing the DNS effects in the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
The next page allows to disable a WAN service indicated in the "Service Name" field.

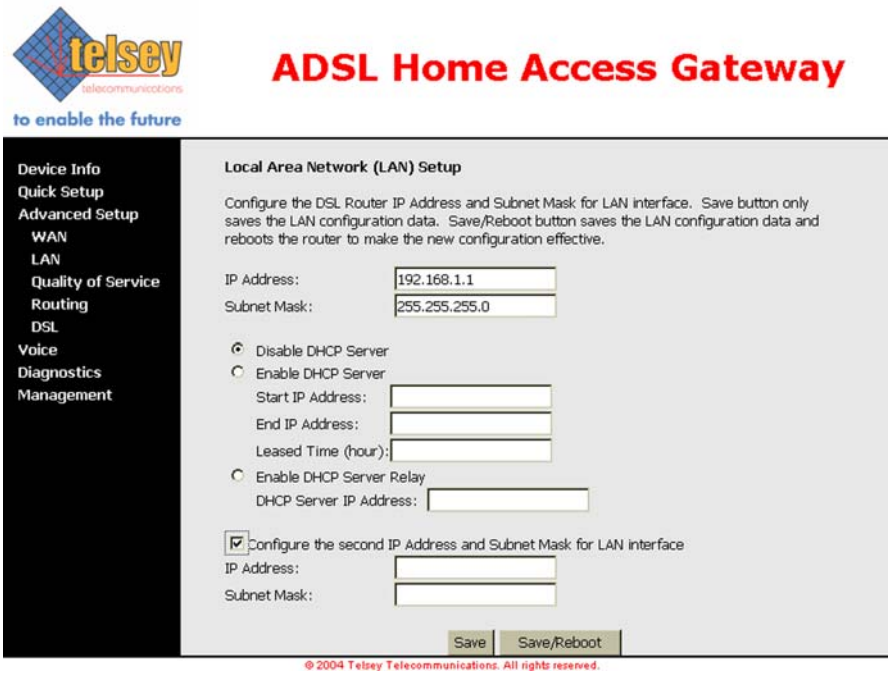
Web Interface

After that, by clicking on Next the setup summary will be displayed. Click on Save to apply the settings.



LAN

By clicking on LAN in the Advanced Setup menu, the following page will show up.



Web Interface

Configure the DSL Router IP address and Subnet Mask for LAN interface. It is also possible to enable DHCP server on the LAN, by defining the IP address range and leased time. A second IP address and Subnet Mask for LAN interface can be enabled by selecting the last checkbox.

Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

Quality of Service[1]

By clicking on **Quality of Service** in the Advanced Setup menu, it is possible to configure network traffic classes.QoS button will only be displayed to a qualified PVC when all of the following conditions are met:

- PVC is not in bridge mode (i.e. the WAN protocol can be PPPoA, PPPoE, IPoA, MER);
- PVC is in set to one of the following ATM service category: UBR with PCR, UBR without PCR, non realtime VBR;
- There are enough ATM TX queues left in the System.

If no traffic class is set, then it is possible to configure QoS by clicking on Add. If a class has already been set, then it is possible to remove it by selecting "remove" checkbox and clicking on Remove.

Each QoS-enabled PVC will consume 3 ATM TX queues. QoS consumes 1 TX queue for transmitting OAM F5 cells for all PVC's[2]. The overall number of ATM TX queues for the whole system is 8. Setting up the first PVC with QoS enabled

1. Quality of Service is currently not supported in ADSL AnnexB software release.
2. This restriction is temporary and will be removed in the future.

Web Interface

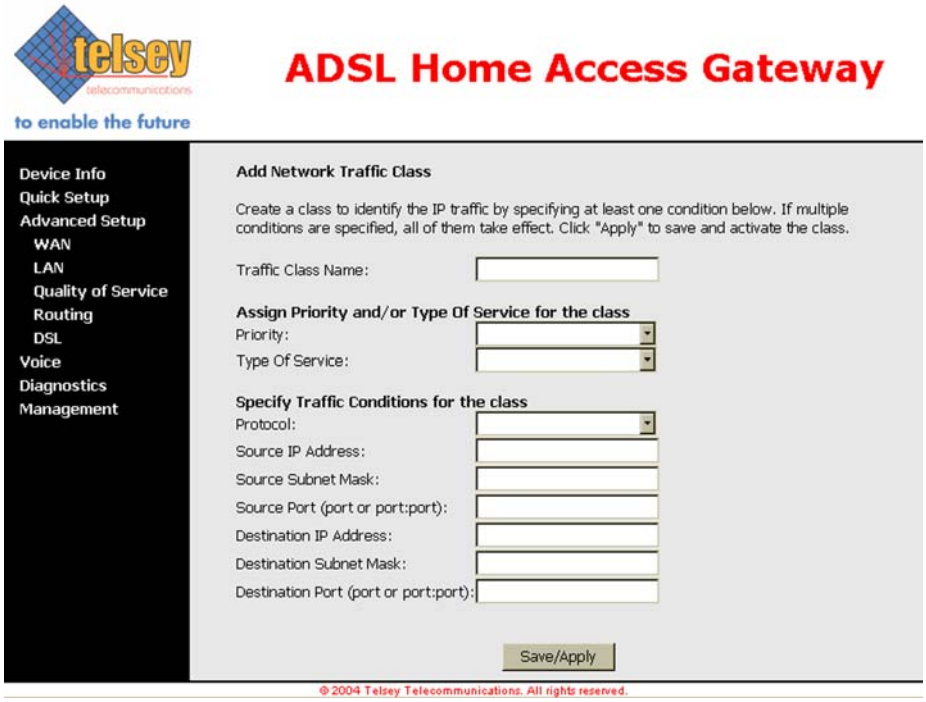
requires 4 TX queues. Setting up the second PVC with QoS enabled needs 3 TX queues.

The following table shows the system capacity for maximum number of PVC's, with or without QoS enabled:

Tab. 10: System capacity - PVC/QoS

Maximum Configurations	Number of PVC's with QoS enabled	Number of PVC's with QoS Disabled
Configuration #1	2	1
Configuration #2	1	4
Configuration #3	0	8

By clicking on Add, then the following page shows up.



IP QoS is executed in the IP layer. It will classify traffic according to the classification rule. Each rule may contain a combination of the following conditions: protocol (TCP, UDP, ICMP), source IP address/subnet mask, destination IP address/subnet mask, source port (one or range), destination port (one or range). The result of matching a classification rule will produce a priority (high, medium, low) and a Type of Service (don't care, Normal Service, Minimum Cost, Maximum Reliability, Maximum Throughput, Minimum Delay). Note that the original IP header TOS and PRECEDENCE values are not used in the classification.

Web Interface

The Type of Service (TOS) of the matching rule will overwrite the original IP header TOS field if "don't care" is not selected.

The priority of the matching rule determines which ATM TX queue to send over this PVC if the packet is routed to this PVC. The ATM SAR scheduler transmits the packet according to the following order:

1) ATM service category from the highest to the lowest order: CBR, rt-VBR, nrt-VBR, UBR
2) For the same service category: Proirity level from high to medium to low
3) For the same priority level: round robin.

IP QoS will only take effect if the packet is routed to a QoS-enabled PVC. If it is routed to a regular QoS-disabled PVC, it will be transmitted at the same priority level as the low priority of a QoS-enabled PVC of the same ATM service category.

Click on Save/Apply to store the QoS setting.

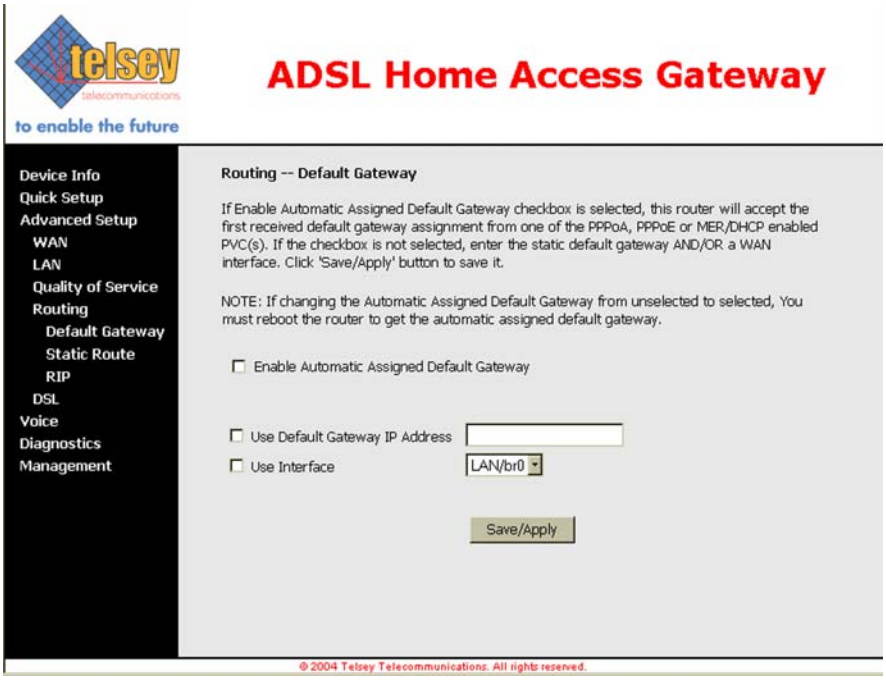
Routing

By clicking on **Routing** in the Advanced Setup menu, it is possible to configure:

- *Default Gateway*
- *Static Route*
- *RIP*

Default Gateway

The following figure shows Default Gateway page, accessed by clicking on **Default Gateway** on the Advanced Setup --> Routing menu.

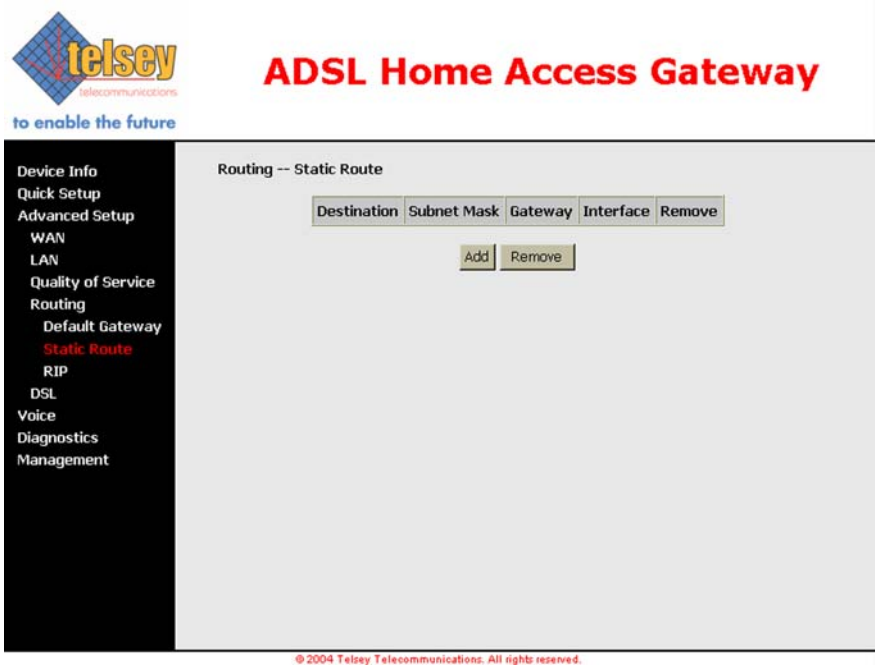


Web Interface

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway IP address and/or a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

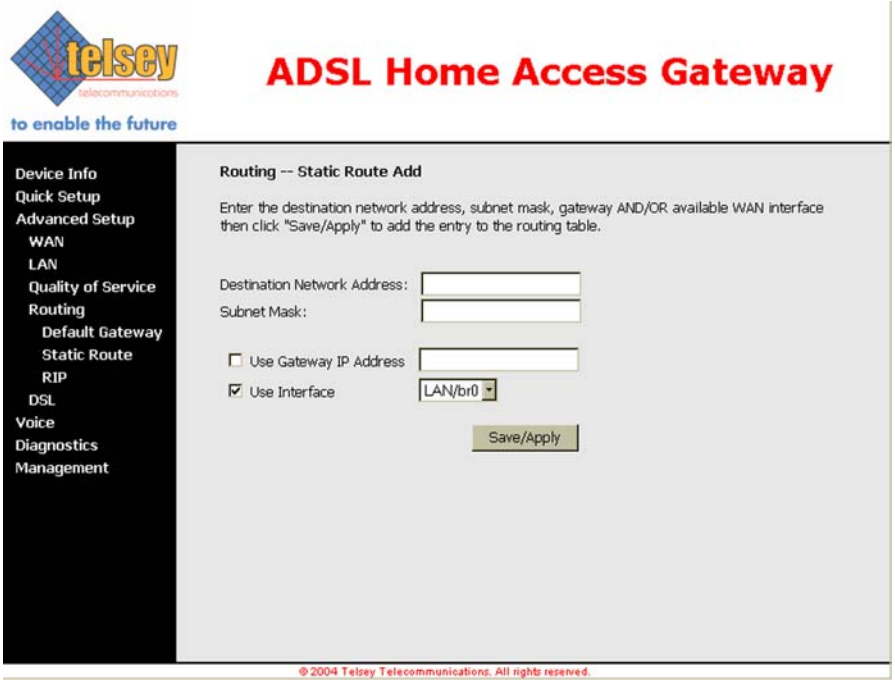
Static Route Click on Add in the following page to configure static route entry.



In case a static route entry is already present, then select it and click on Remove to delete it.

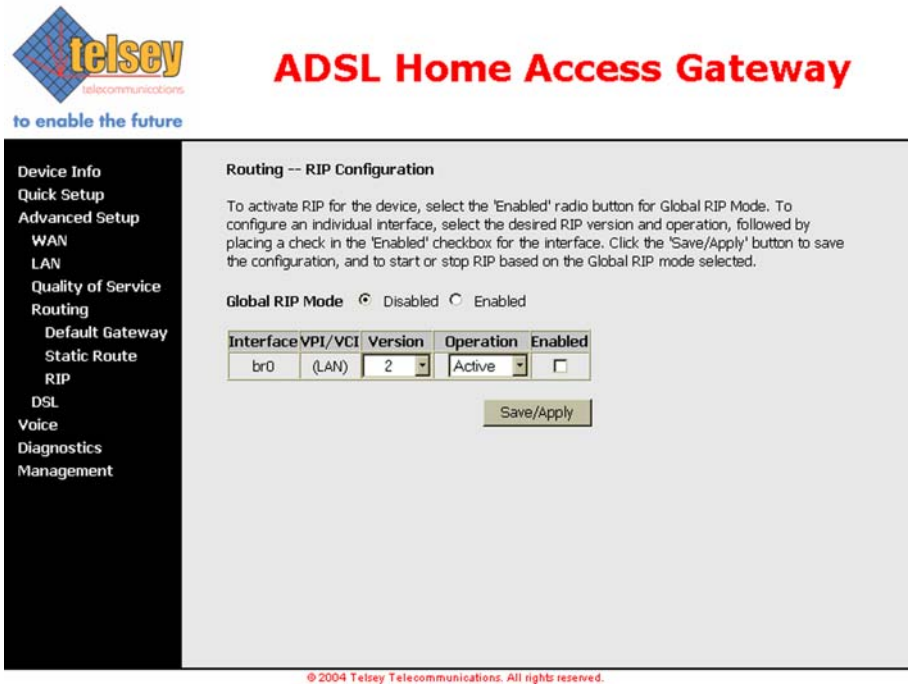
The following figure shows the Static Route Add page.

Web Interface



Enter the destination network address, subnet mask, gateway address and/or avaliable WAN interface. By clicking on Save/Apply, the entry is included in the routing table.

RIP By clicking on **RIP**, the following page will show up.



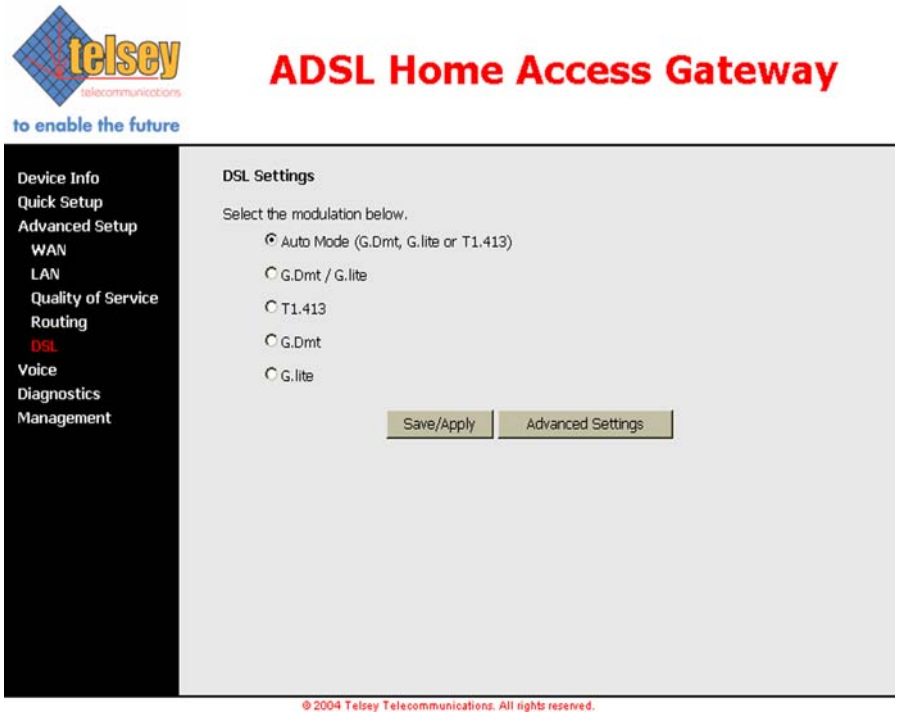
Web Interface

To activate RIP for the device, select "Enabled" radio button for global RIP mode. To configure an individual interface, select the desired RIP version (*1*, *2* or *both*) and operation (*Active*, *Passive*), followed by placing a check in the "Enabled" checkbox for the interface. Click the "Save/Apply" button to save the configuration, and to start or stop RIP based on the global RIP mode selected.

DSL

The DSL Settings dialog box allows you to select an appropriate modulation mode.

By clicking on **DSL** in the Advanced Setup menu, the following page will show up.



Tab. 11: DSL modulation settings

Option	Description
Auto Mode (G.Dmt, G.lite or T1.413)	Sets the system auto-sense between G.Dmt, G.lite, or T1.413.
G.Dmt/G.lite	Sets G.Dmt/G.lite if you want the system to use either G.Dmt or G.lite mode.
T1.413	Sets the T1.413 if you want the system to use only T1.413 mode.
G.Dmt	Sets the system to use only G.Dmt mode.
G.lite	Sets the system to use only G.lite mode.

Web Interface

By clicking on Advanced Settings, it is possible to select an appropriate test mode.

Tab. 12: DSL Advanced Settings - Test mode choice

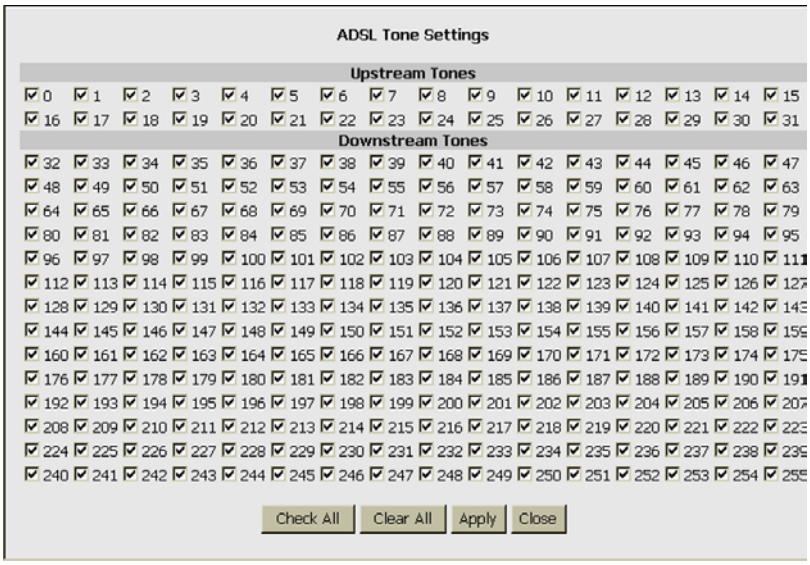
Option	Description
Normal	Normal mode of operation.
Reverb	Send Reverb signal only.
Medley	Send Medley signal only.
No retrain	Stay in showtime even after the modem is disconnected.

The following page shows the DSL Advanced Settings page.

All three of these modes enable PSD measurements for each phase of training and showtime.

Web Interface

The **Tone Selection** button prompts the ADSL Tone Settings dialog box. This allows you to select an appropriate number of upstream and downstream tones.



Click Apply after you have made your selections.

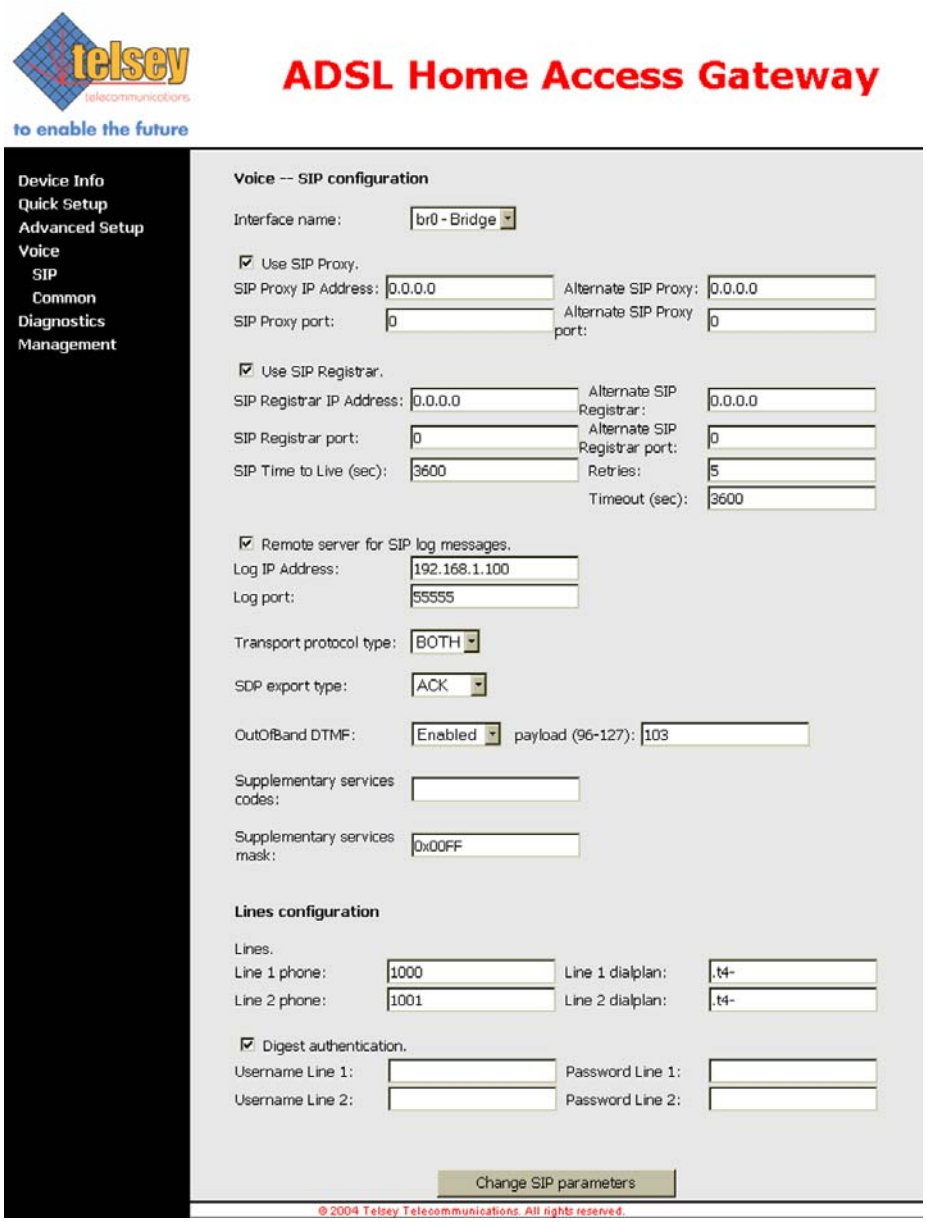
Web Interface

VOICE

The **Voice** menu enables VoIP SIP settings.

SIP

By clicking on **SIP** (Voice sub-menu), the following configuration page shows up.



Web Interface

- Select a WAN interface from the drop-down menu (*Interface name*).
- SIP Proxy Server's IP Address and port can be typed in after selecting *Use SIP Proxy* checkbox. It is also possible to use an alternate SIP Proxy Server is case the main one is down or unreachable.
- If a SIP Registrar is required in the network, then it is possible to set its IP Address, port and SIP Time to Live after selecting *Use SIP Registrar* checkbox. It is also possible to use an alternate SIP Registrar in case the first one is down or unreachable. *TimeOut* parameter determines when the CPE sends the request to Alternative Proxy. When the TimeOut is expired the CPE will try to go back to Proxy (Registrar).

Note: The number of requests (*Retries*) to send to Proxy (or Registrar), before the CPE switches to Alternative Proxy (Alternative Registrar) MUST be specified (1 request by default).

- If a SIP log messages server is required in the network, then it is possible to set its IP address and port, after selecting *Remote Server for SIP log messages* checkbox.
- The SIP protocol can be configured to use the UDP/TCP or BOTH protocol as *Transport protocol type*.
- *SDP Export Type*. When the application is initiating a session, it can choose to be the offerer or the answered. If it acts as the *offerer*, the application must include an SDP packet in the *INVITE*. The remote UA must then include the answer SDP packet into its 200 OK response. If the application wants to act as the *answerer*, then it must not include any SDP packet into the INVITE: it will be up to the remote UA the inclusion of an offer in its 200 OK response. After receiving an offer into a 200 OK response, the application must include its answer into the following *ACK* request.
- It is possible to enable *OutOfBand DTMF* and assign a suitable payload of the RTP packets, according to RFC2833. Valid payload range is from 96 to 127.
- ***Supplementary Services***

CLIR:

- To set the caller ID restriction, dial *31# (default) then the number.
- CLIR permanent: enable *32# (default).
- CLIR permanent: disable #32# (default).

Call Hold:

- To put a call on hold, press flash than hang up (optional).
- To return to the original call, press flash or pick up the phone.
- The phone will issue a short ring burst every 20 seconds or so while on-hook to remind you that a call is on hold.

Call transfer:

- To transfer a call, press flash then dial the new number.
- To transfer immediately, hang up (blind transfer)
- To transfer with consultation, wait for the party to answer, consult, and then hang up.

Web Interface

- To abort the transfer (if the third party does not answer), press flash to return to the original call.

Conference calling:

- To turn a two-party call into a three-party conference call, press flash and dial the third party.
- To place the old (current) call on hold and take the new call press flash+2 (R2).
- To switch between the old and the new call press flash+2 (R2).
- To connect to both the old and the new call press flash+3 (R3). Starts a 3-party conference call.
- To return in the state before the conference, press flash+2 (R2).
- To drop yourself out of the conference, hang up. The call will be transferred (so that the other two parties remain connected to each other).

Note: In conference mode, the conference initiator performs the audio bridge/mixing function. There are only 2 voice streams established.

Call Waiting:

- If call waiting is enabled on a line, you will hear the call waiting tone during a call.
- To press flash+2 to answer the second call. The first call is automatically placed on hold.
- To switch between calls, press flash+2 (R2).
- To connect both the old and the new call flash+3 (R3). Starts a 3-party conference call.
- To reject the new call without answering it, press flash+0 (R0).
- To release the old call and take the new call, press flash+1 (R1).
- To enable the call waiting feature, dial *43# (default).
- To disable the call waiting feature, dial #43# (default).
- Call forward feature settings (Busy or All) takes priority over the call waiting feature.
- Call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

Call forward:

- To set the call forward on no answer, dial *61* (default), then the number and the termination character "#". Incoming calls will be forward if unanswered for 18 seconds (default).
- To set the call forward if busy, dial *67* (default), then the number and the termination character "#". Incoming calls will be immediately forwarded if the phone id off-hook.
- To set the call forward unconditional, dial *21* (default), then the number and the termination character "#".
- To disable all the forward, dial #21# (default).

Call return:

Web Interface

- To place a call to the last know incoming caller (unanswered or not), dial *69# (default).

Redial:

- To redial the last outgoing number, dial *68# (default).

SS Configuration

Use the CLI (command `suppServs`) or Web page to set the special codes.

See the following table for code configuration:

Tab. 13: Supplementary services codes

Supplementary service	Code
Call Waiting ON	WO
Call Waiting OFF	WF
Call forwarding Unconditional (All)	FU
Call forwarding if Busy	FB
Call forwarding on No answer	FA
Call forwarding OFF	FF
Call Return	CR
Call Redial	CD
CLIR for call	RT
CLIR permanent ON	RO
CLIR permanent OFF	RF

The suppServer command string has the following structure:

```
CodeCommand, CodeCommand
```

Example WO*43#,WF#43#,FU*21*

Enable Call Waiting --> *43#
Disable Call Waiting --> #43#
Enable Call Forwarding Unconditional --> *21*

SS Enable/Disable services

Use the CLI or Web page to enable or disable the service. The following table provide information on the services and call features parameters. The services parameter is in bitmap format. The default is 0xffff.

Tab. 14: SS bitmap codes

Bit	Mask	Explanation
Bit 0	0x1	Call Waiting
Bit 1	0x2	Call Forwarding
Bit 2	0x4	Call Transfer

Web Interface

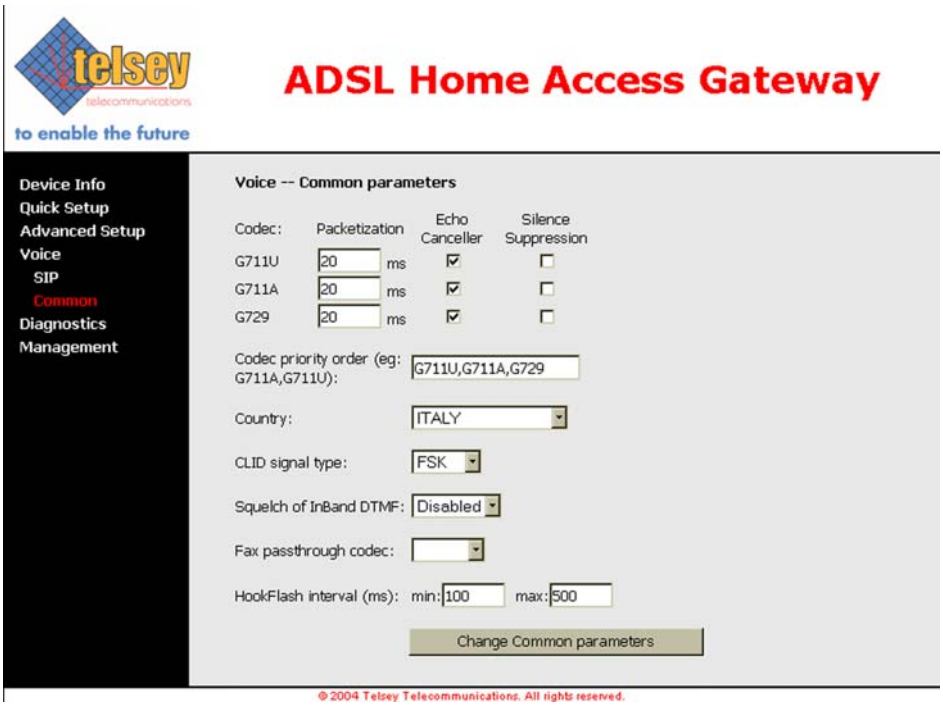
Tab. 14: SS bitmap codes

Bit	Mask	Explanation
Bit 3	0x8	Call Hold
Bit 4	0x10	3-Way Conference
Bit 5	0x20	Call Return
Bit 6	0x40	Call Redial
Bit 7	0x80	CLIR

- It is possible to set a *Digest Authentication,* by choosing an username and password for each telephone line, if the SIP Registrar supports this feature.
- Type the phone numbers for Line 1 and Line 2 and select an appropriate Dial Plan (see Appendix A for more details).

Click on *Change SIP Parameters* and reboot to apply new settings.

By clicking on **Common** (Voice sub-menu), the following page shows up.



For each available Codec (G711μ-law, G711A-law, G729), it is possible to choose:

- *Packetization time*
- *Echo Canceller*
- *Silence Suppression*
- *Codec Priority order:* select the preferred order for the available codecs.

Web Interface

- *Country tone* (North America, Italy, UK, France, Sweden, Netherlands, Belgium and Germany)[1]
- *Caller ID Signal Type* (FSK, DTMF)
- It is possible to activate *Squelch for InBand DTMF.*
- *Fax passthrough codec*: select the preferred codec among G711A-law, G711μ-law. Echo canceller will be disabled when fax/modem tone has been detected.
- *HookFlash interval*: type the time range, in milliseconds, for the HookFlash.

Click on *Change Common parameters* to apply the new settings.

1. See Appendix A for more specifications regarding Country tones.

Web Interface

DIAGNOSTICS

The Diagnostics menu provides feedback on the connection status of the CPVA500 and the ADSL link. A description of each test can be obtained by clicking on the help button associated with the test.

Without an active ADSL connection, many of the tests will not be activated, and when the current network operating mode is in bridge, the default gateway and DNS server tests will not be activated.

There are two buttons at the bottom of the screen:

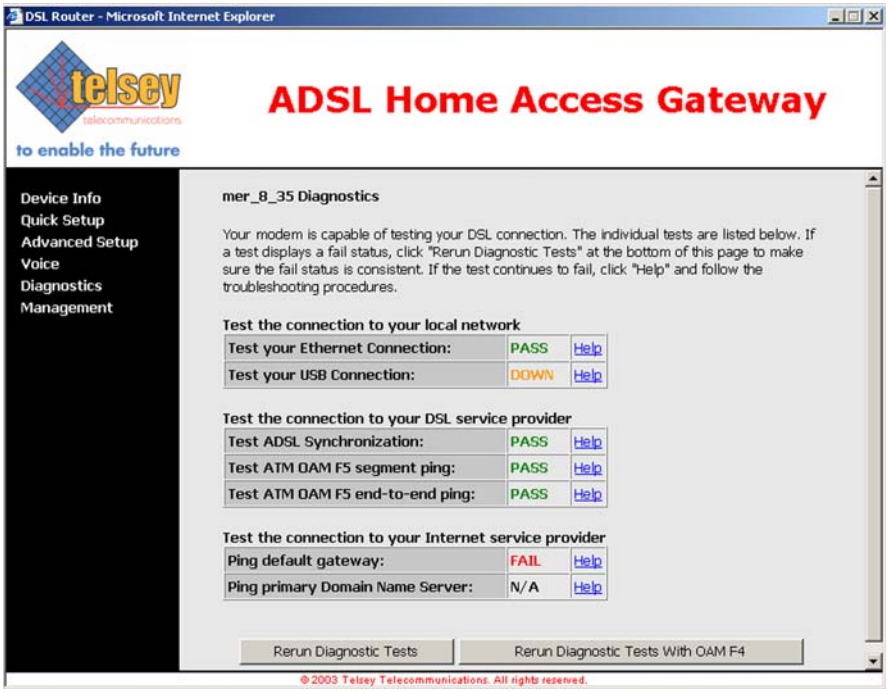
- Rerun Diagnostic Tests
- Rerun Diagnostic Tests With OAM F4

When either of the Rerun Diagnostic Tests buttons are pressed, all the diagnostic tests are repeated. Normally, if one or more tests return a failure status, the user should rerun all the tests again to more thoroughly diagnose the problems encountered.

When Rerun Diagnostic Tests With OAM F4 is pressed, ATM OAM F4 loopback cells are also transmitted, in addition to OAM F5 cells. It is possible that the ATM OAM F4 loopback or segment tests may not be supported by the ATM devices in the DSL service provider's network. For this reason, the OAM F4 test is separated from the general diagnostics tests. When an OAM F4 failure is encountered, the output screen will appear as an F4 Fail.

Web Interface

The following figure shows an example of diagnostics page, when the PVC is configured in MER mode.



The following table provides a brief description of each diagnostics test.

Tab. 15: Diagnostics test description

Test	Description
Ethernet Connection	• **Pass**: Indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful. • **Fail**: Indicates that the DSL Router does not detect the Ethernet interface on your computer.
USB Connection	• **Pass**: Indicates that the USB interface from your computer is connected to the LAN port of your DSL Router. • **Down**: Indicates that the DSL Router does not detect the USB interface on your computer.
ADSL Synchronization	• **Pass**: Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid DSL LED on the modem also indicates the detection of a DSL signal from the telephone company. • **Fail**: Indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The DSL LED will continue to flash green.

Web Interface

Tab. 15: Diagnostics test description

Test	Description
ATM OAM Segment Ping	The modem transmits OAM F4/F5 (if you rerun the test with OAM F4, both F4 and F5 are sent, otherwise only F5 is sent) segment loopback requests and expects a reply within 5 seconds. This test verifies that ATM continuity exists between the virtual channel link segment from the modem to the DSL provider network (typically this is a DSLAM at the DSL provider site). • Pass: Indicates that the DSL modem can communicate with the DSL provider network. • Fail: Indicates that the DSL modem may not be able to communicate with the DSL provider network. This test may have an effect on your Internet connection. Occasionally the DSL provider network may intentionally block this traffic. Therefore if this test fails, but you are still able to access the Internet, there is no need to troubleshoot this issue.
ATM OAM end-to-end Ping	The modem transmits OAM F4/F5 (if you rerun the test with OAM F4, both F4 and F5 are sent, otherwise only F5 is sent) end to end loopback requests and expects a reply within 5 seconds. This test verifies ATM connectivity of the virtual channel link with the ATM PVC endpoint, such as a remote broadband access router located at the DSL provider or ISP site. • **Pass**: Indicates that the DSL modem can communicate with the DSL provider network. • **Fail**: Indicates that the DSL modem may not be able to communicate with the DSL provider network. Occasionally the DSL network provider may intentionally block this traffic. Therefore if this test fails, but you are still able to access the Internet, there is no need to troubleshoot this issue.
PPP Server	For PPPoA operating mode, the modem checks if PPP (LCP and IPCP) are connected to the remote PPP server. For PPPoE operating mode, this test verifies that the modem can detect a PPPoE server by checking if it can receive a PADO (PPPoE Active Discovery Offer) packet from a PPPoE server after sending a PADI (PPPoE Active Discovery Initiation) broadcast packet. • **Pass**: Indicates that the DSL modem has discovered a PPPoE server or can connect to a PPPoA server. • **Fail**: Indicates that the DSL modem failed to discover a PPPoE server or connect to a PPPoA server. • A **flashing green** PPP LED on the modem signifies an attempt to establish a PPP connection.

Web Interface

Tab. 15: Diagnostics test description

Test	Description
Authentication with ISP	Verifies that the provided PPP username and password stored in the DSL modem have been authenticated by the PPP server within the ISP network. • **Pass**: Indicates that your username and password stored in the DSL modem has authenticated with the ISP's network. • **Fail**: Indicates that the PPP username and password were rejected by the PPP server at the ISP site. Either the PPP user name or password were configured incorrectly, or the user account has not been properly established at the ISP. The user should re-enter the PPP user name and password and retry. If a failure condition persists, contact the ISP support.
Assigned IP Address	Verifies that the DSL modem has a valid IP address (here, a PPP WAN IP address) from the PPP server. • **Pass**: Indicates that the DSL modem has a valid IP address from the PPP server. • **Fail**: Indicates that the DSL modem does not have a valid IP address from the PPP server.
Ping Default Gateway	• **Pass**: Indicates that the DSL modem can communicate with the initial network entry point. This is usually the IP address of the ISP router. • **Fail**: Indicates that the DSL modem was unable to communicate with the initial network entry point.
Ping Primary Domain Name Server	Verifies that the DSL modem can communicate with the primary domain name server (DNS). • **Pass**: Indicates that the DSL modem can communicate with the primary DNS. • **Fail**: Indicates that the DSL modem was unable to communicate with the primary DNS.

Web Interface

MANAGEMENT

In this menu it is possible to configure:

- Settings (Provisioning, Backup, Update, Restore Default)
- System Log
- Access Control
- Update Software
- Save/Reboot

Provisioning

For large-scale networks, you can use a TFTP server to download a configuration for each CPVA500. The TFTP server's URL and file name can be provided (provisioned) from the DHCP server or can be configured via Web page or Telnet/CLI. At the moment it is possible to configure the equipments through TFTP about the VoIP functionalities.

In this mode of provisioning, at power-up, CPVA500 contacts the TFTP server for a specific profile to download. If CPVA500 does not reach the TFTP server after 30 attempts, it continues normal operation by using its locally cached profile.

It is possible to configure a cfginterval (time in second). At cfginterval CPVA500 attempts to refresh its profile from the TFTP server.

CPVA500 updates the configuration file with frequency defined by cfginterval. If any relevant parameter has changed, CPVA500 will be rebooted.

The default filename will have the following format: tlsxxxxxxxxxxxx, where xxxxxxxxxxxx represents MAC address. The default cfginterval is 3600. The default TFTP server's is 192.168.1.100.

If auto provisioning is configure in dynamic mode, TFTP server is mandatory (default is not applicable).

In the filename is possible to configure the voice parameters.

The automatic configuration can be configured via Web page or via Telnet/CLI.

Example of configuration file via TFTP

For futher information regarding CLI command, please refer to CLI Chapter.

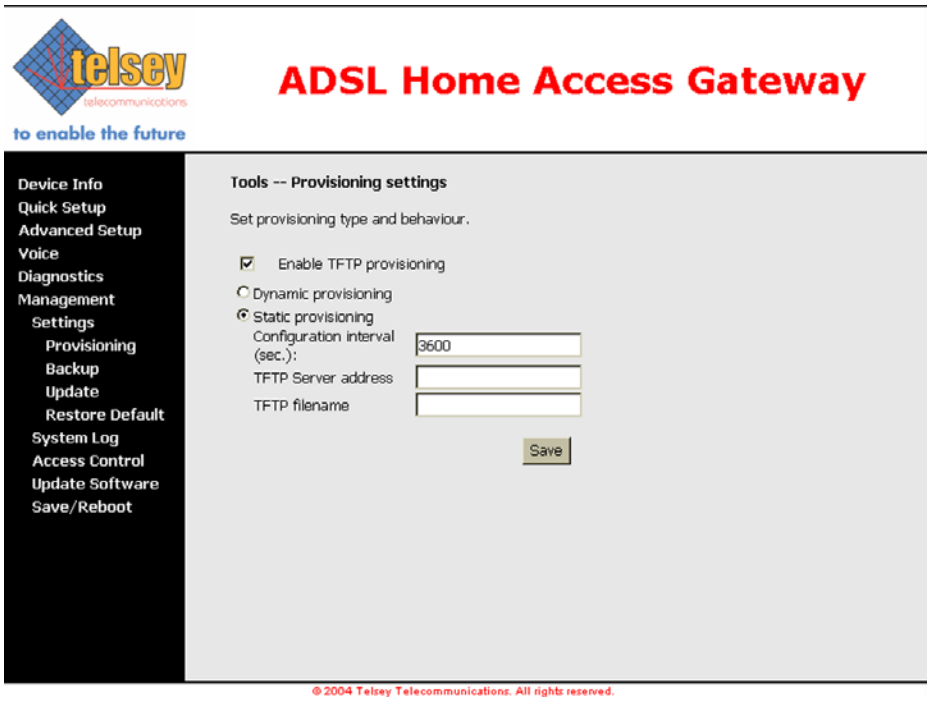
```
;
; CPVA500 SIP
; Voice Configuration
;
voice set proxy 192.168.0.29:5060
voice set ttl 3600
voice set registrar 192.168.0.29:5060
voice set altRegistrar 0.0.0.0:5060
voice set altTimeout 10
```

Web Interface

```
voice set altRetries 5
voice set logserver 192.168.1.144:5444
voice set phone1 1351
voice set phone2 1352
voice set dialplan1 .>*>#t4-
voice set dialplan2 .>*>#t4-
voice set auth Off
voice set user1 1351
voice set user2 1352
voice set passw1 1351
voice set passw2 1352
voice set oobEnable On
voice set dtmf 100
voice set sdpExport ACK
voice set transport UDP
voice set sdpExport
voice set suppServs
voice set interface ppp41
;
; commmon variable
;
voice set clid DTMF
voice set country GERMANY
voice set hookflash_min 40
voice set hookflash_max 500
voice set squelch On
voice set passthru G711A
voice set codec_G711A_packet 20
voice set codec_G711A_ec On
voice set codec_G711A_ss On
voice set codec_G711U_packet 30
voice set codec_G711U_ec On
voice set codec_G711U_ss On
voice set codec_G729_packet 30
voice set codec_G729_ec On
voice set codec_G729_ss On
voice set codec_priority G711A,G711U,G729
voice save
```

Web Interface

By clicking on Management-Settings-Provisioning, the following page will be displayed.



Click on "Enable TFTP provisioning".

- Set "*Dynamic provisioning*" if the configuration file is uploaded by means of DHCP. TFTP Server's IP Address and configuration file name are passed by using DHCP options 66 and 67.
- Set "*Static provisioning*" if the configuration file (TFTP filename) is downloaded from a TFTP Server (TFTP Server address). The value set in the "Configuration interval (sec.)" field shows the provisioning frequency.

  E.g.: if 3600 seconds is set, then the CPE looks for the configuration file in the TFTP server every hour.

Backup Settings

By clicking on "Backup Settings" it is possible to save CPVA500 settings file on your PC.

Update Settings

Browse and find the settings file on your PC and click on "Update Settings" to update CPVA500 using your saved files.

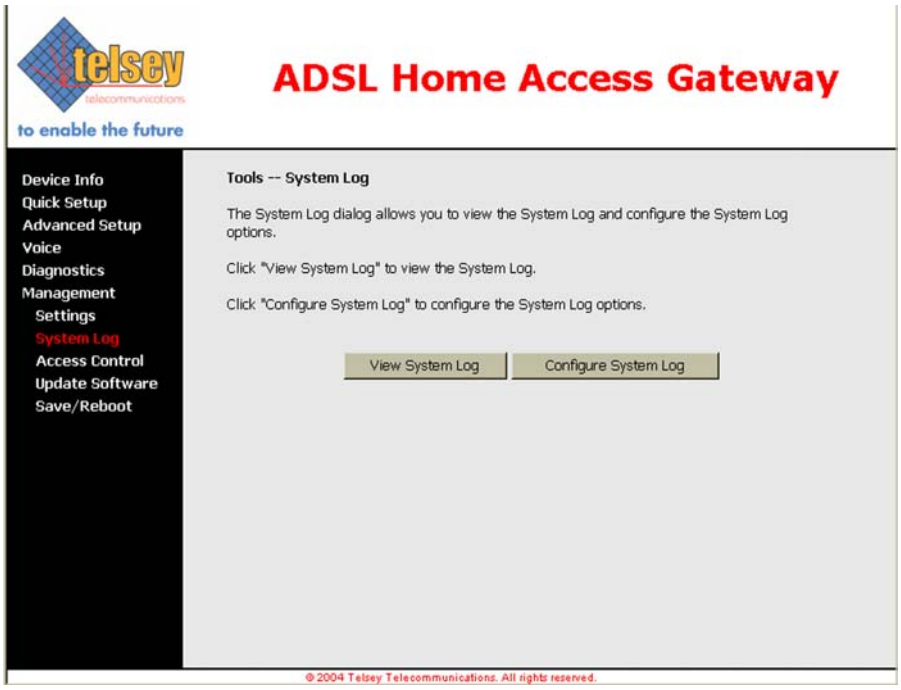
Restore Default

Click on "Restore Default Settings" to go back to factory defaults.

System Log

Web Interface

The **System Log** screen allows you to view the system events log, or to configure the System Log options.



Click "Configure System Log" to display the following screen.

Web Interface

Select from the desired System Log options described below, enter an option, then click Apply.

Tab. 16: System Log - Configuration options

Option	Description
Log Status	Log Status indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is enabled. To disable it, click on Disable and then Apply button.
Log Level	Log Level allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the BCM96345 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = error conditions • Warning = warning conditions • Notice = normal but significant condition • Informational = information events • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Display Level allows the user to select the logged events and display on the "View System Log" page for events of this level and above to the highest Emergency level.
Mode	Mode allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If "remote" mode is selected, view system log will not be able to display events saved in the remote syslog server. When either “Remote” mode or “Both” mode is configured, the WEBUI will prompt the user to enter the Server IP address and Server UDP port.
Server IP Address	Field that appears when Remote or Both is selected in the Mode field.
Server UDP Port	Field that appears when Remote or Both is selected in the Mode field. Prompts the user to enter UDP port number of the SysLog server. A well known UDP port number, 514, is normally assigned to syslog. However, the user can overwrite with other UDP port number if different UDP port is used by that particular syslog server.

Access Control

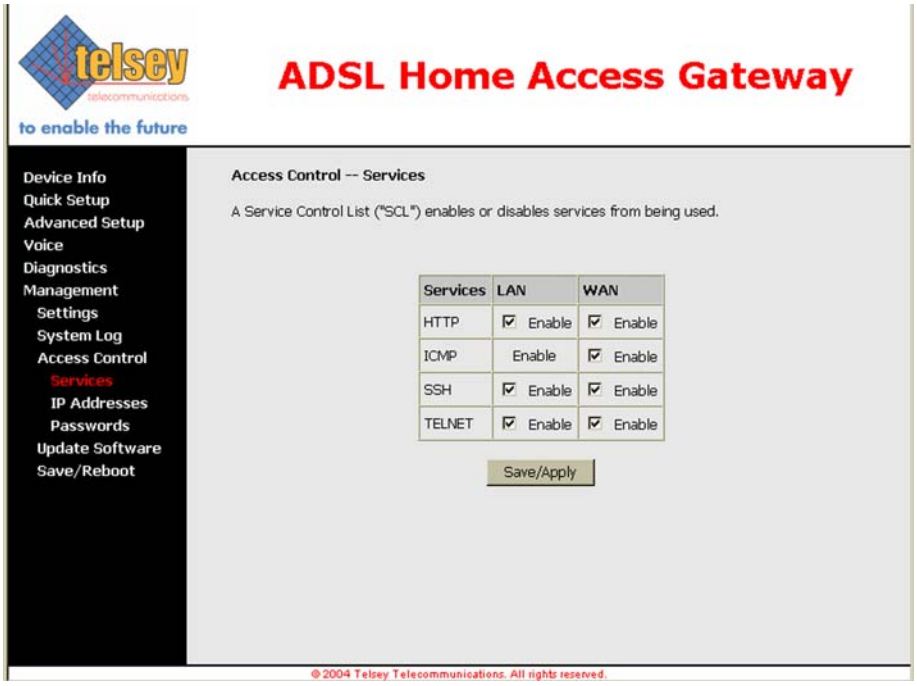
Web Interface

In the **Access Control** menu it is possible to choose among:

- **Services**
- **IP Addresses**
- **Passwords**

Services

By clicking on **Services** the following page shows up.



It is possible to enable or disable WAN and/or LAN access for the following services within the router:

- HTTP Server
- SSH Server
- Telnet Server
- ICMP Response

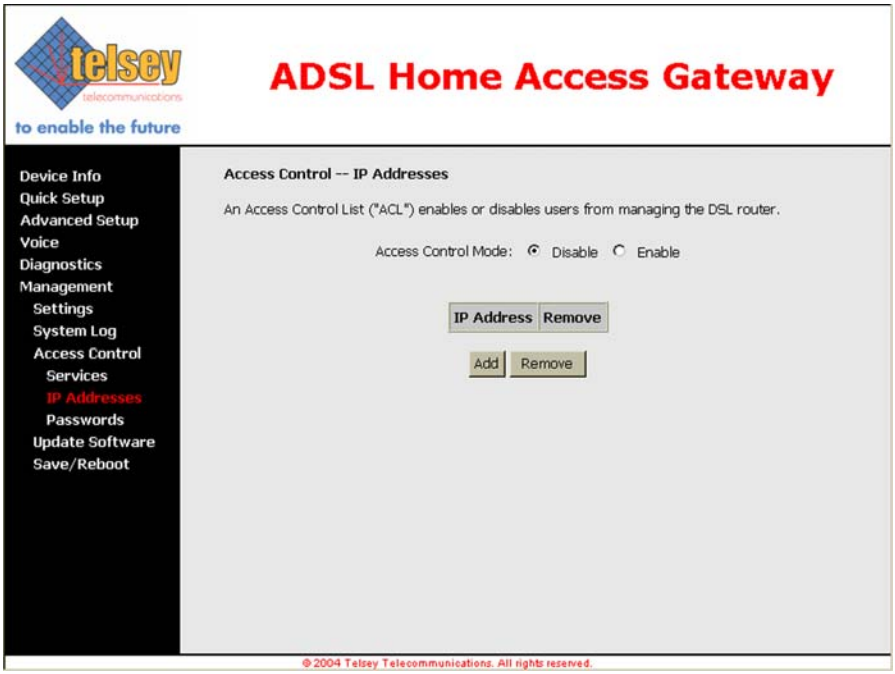
IP Addresses

By clicking on **IP Addresses** it is possible to configure up to 16 IP addresses to be included in the Access Control list (ACL). If ACL is enabled, then the following local applications will verify the source IP address of the packets received from the LAN or WAN:

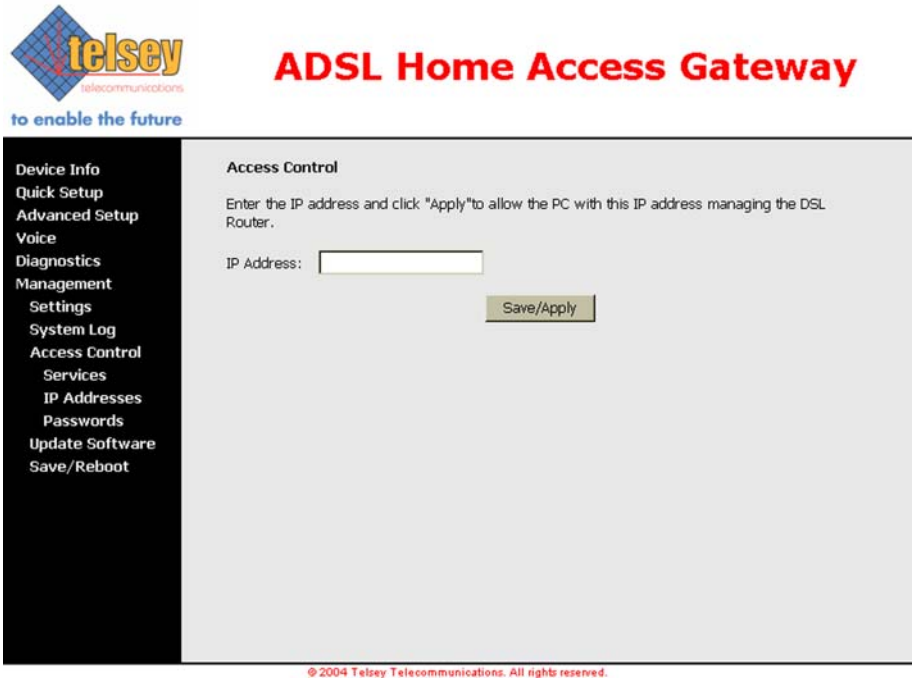
- HTTP Server
- SSH Server
- Telnet Server

Web Interface

Click on "Enable" in the *Access Control Mode* to enable Access Control list. Then click on "Add" to add a new IP address.



After clicking on Add, the following page shows up.

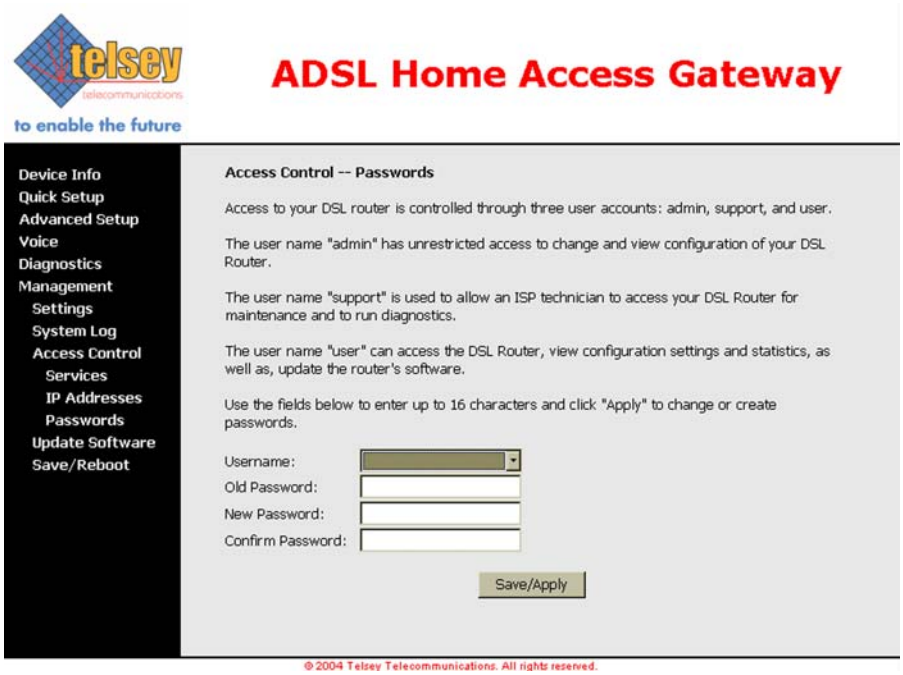


Web Interface

Warning **Be careful when adding a new IP address in the Access Control list. The device will be unreachable in case it is contacted by an IP address not included in the ACL.**

Passwords

By clicking on **Passwords** the following page shows up.



It is possible to set a password for the following profiles:

- **admin** - gives unrestricted access to change the configuration of the router. Max password length is 16 characters.
- **support -** gives access for router maintenance and diagnostics. Max password length is 16 characters.
- **user -** gives access to view the configuration, statistics, and to update the router software. Max password length is 16 characters.

Click on "Save/Apply" to store the new passwords.

Update Software

The **Update Software** screen allows you to obtain an updated software image file from your ISP. Manual software upgrades from a locally stored file can be performed using the following screen.

Select the new image file after clicking the Browse button. Click the Update Software button. Completion of this step takes about two minutes to complete. The CPVA500 will reboot in the process.

Web Interface

Note **Updating the software requires a system reboot. During this time, the current WEB UI screen will be temporarily unavailable, but will come back to the Device Info page after the system is up again. Configuration data stored in the ADSL router flash memory is retained after the software upgrade.**

Save/Reboot

This page allows you to easily reboot CPVA500 router by clicking on "Save/ Reboot" button.

Web Interface

RESTORE FACTORY DEFAULT SETTINGS

In case of a misconfiguration, CPVA500 could become unreachable. For this reason, a crash recovery procedure has been introduced starting from SIP software version 1.0.2.

Initial conditions

- CPVA500 not reacheable
- Phone line unregistered

Procedure

Default factory settings (as reported on page 17) can be restored by using a telephone connected to **Line2** and by dialling the following string:

###*1973*5*2846*147896325*###

Web Interface

Chapter 6

Command Line Interface

INTRODUCTION

The following commands are available from TELSEY ADSL router command line interfaces.

From Linux busybox:

- Cat
- Df
- Echo
- Ifconfig
- Kill
- Ping
- Ps
- Pwd
- Reboot
- Traceroute
- Sysinfo

From Linux public domain:

- Brctl

From Telsey:

- adsl
- arp
- atm
- defaultgateway
- dhcpserver
- dltftp
- dnsrelay
- help
- lan
- logout
- passwd
- ppp

- remoteaccess
- restoredefault
- route
- save
- swversion
- voice
- wan

Control Key Support

- Command history scrolling (maximum 15 commands in history)
    - UP: UP arrow key, or CTRL+p
    - DOWN: DOWN arrow key, or CTRL+n
- Move cursor
    - LEFT: LEFT arrow key, or CTRL-b
    - RIGHT: RIGHT arrow key, or CTRL-f
    - Beginning of line: CTRL+a
    - End of line: CTRL+e
- Clear screen: CTRL+l (lowercase letter of L)
- Clear to the beginning of line: CTRL+u
- Clear to the end of line: CTRL+k
- Delete: DEL key, or CTRL+h
- Terminate CTRL-c (can not terminate certain running application such as ping and traceroute)

Command Line Interface

ADSL

NAME: **adsl** - allows an user to control Telsey ADSL driver

SYNOPSIS:

```
adsl start [options]
adsl stop
adsl connection [options]
adsl configure [options]
adsl bert [options]
adsl info [options]
```

DESCRIPTION: Adsl is used to control the Telsey ADSL driver. This utility can:

- start and stop the driver
- activate, deactivate and control ADSL connection
- configure ADSL driver and connection parameters
- start, stop and monitor Bit Error Rate Test (BERT)
- display status and information of ADSL driver and connection
- display statistics for ADSL driver and connection

All information are displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output.

COMMANDS:

start

Starts the Telsey driver. This command initialize the driver and start ADSL PHY connection if [--up] is specified. This command takes parameters that can specify various connection modes. These parameters are the same as in "configure" command.

stop

Stops ADSL connection and Telsey ADSL driver.

configure

Configures ADSL connection parameters. These command takes the same parameters as "start" command except for [--up] . This command will cause ADSL PHY to retrain.

connection

Controls ADSL connection modes, such as up and down and several special test modes. This command can also be used to specify tone selection for upstream and downstream.

bert

Controls ADSL bit error rate test (BERT). This command can start/stop the BERT test and monitor its results.

Command Line Interface

info

Display information about ADSL driver and PHY status.

OPTIONS: *Options for the* **start** *and* **configure** *commands:*

```
adsl start [--up] [--mod <a|d|l|t>] [--lpair <(i)nner|(o)uter>] [--bm <(D)BM|(F)BM>] [-- ccw]

adsl configure [--mod <a|d|l|t>] [--lpair <(i)nner|(o)uter>][--bm <(D)BM|(F)BM>] [--ccw]
```

`--up:`

Start ADSL PHY connection.

`--mod <a|d|l|t>`

`a` : all modulations allowed.
`d` : G.DMT only
`l` : G.Lite only
`t` : T1.413 only
More than one mode letter can be given to specify several modes.

`--lpair <(i)nner|(o)uter>`

`(i)nner` : inner loop pair is used
`(o)uter` : outer loop pair is used

The following options apply to AnnexC only

`--bm <(D)BM|(F)BM>`

`(D)BM` : DBM mode
`(F)BM` : FBM mode

`--ccw`

Enables special CRC workaround for Centillium modems

Options for the **stop** *command:*

```
adsl stop
```

Options for the **connection** *command:*

```
adsl connection [--up] [--down] [--loopback] [--reverb] [--medley] [--noretrain] [--tones <xmtStart xmtNum xmtMap rcvStart rcvNum rcvMap>]
```

`--up`

Starts ADSL connection in normal mode

`--down`

Puts ADSL PHY in idle mode

`--loopback`

Command Line Interface

Puts ADSL PHY in ATM cell loopback mode. In this modem ADSL PHY will not try to establish connection

`--reverb`

Puts ADSL PHY in test mode in which it only sends REVERB signal

`--medley`

Puts ADSL PHY in test mode in which it only sends MEDLEY signal

`--noretrain`

In this mode ADSL PHY will be trying to establish connection as in normal mode, but once the connection is up it will not retrain even if the signal is lost.

`--tones <xmtStart xmtNum xmtMap rcvStart rcvNum rcvMap>`

Specifies tones which can be used by ADSL PHY.
`xmtStart` : first tone used in upstream direction (usually 0)
`xmtNum` : number of tones in upstream direction (usually 32)
`xmtMap` : bitmap for tones used in upstream direction. Specified as a hexadecimal string. Bit value zero means the corresponding tone is not used, bit value one means it is used.
`rcvStart` : first tone used in downstream direction (usually 32)
`rcvNum` : number of tones in downstream direction (usually 224)
`rcvMap` : bitmap for tones used in downstream direction. Specified as a hexadecimal string. Bit value zero means the corresponding tone is not used, bit value one means it is used.

Tone configuration command does not cause ADSL PHY retrain automatically. To experience the effect of this command ADSL connection must be restarted using for example adsl connection -down followed by adsl connection -up command. Tone selection is not affected by adsl configure commands and has to be changed explicitly. Default tone configuration (all tones enabled) will be set by adsl tones 0 32 0xFFFFFFFF 32 224 0xFF… (repeated 28 times)

Options for the **`bert`** *command:*

`adsl bert [--start <seconds>] [--stop] [--show]`

`--start`

Starts Bit Error Rate Test (BERT) seconds - duration of BERT test in seconds

`--stop`

Stops the BERT test.

`--show`

Display BERT results to stdout in the following format:

```
BERT Status = [NOT] RUNNING
BERT Total Time = 10 sec
BERT Elapsed Time = 10 sec
```

Command Line Interface

```
BERT Bits Tested = 0x00000000045A6380 bits
BERT Err Bits = 0x0000000000000002 bits
```

BERT Status indicates whether or not the BERT test is currently running.

It can be used to monitor when the BERT test is complete after it is started. The numbers of total bit tested and errorred bits are displayed as 64 bit hexadecimal numbers.

Options for the **`info`** *command:*

```
adsl info [--state] [--show] [--stats] [--reset]
```

`--state`

Displays the shortest message about ADSL PHY connection state, e.g.

```
adsl: ADSL driver and PHY status
Status: Showtime Channel: FAST, Upstream rate = 8064 Kbps,
Downstream
rate = 1024 Kbps
```

`--show`

Displays more statistics about ADSL connection.

`--stats`

Displays all available statistics about ADSL connection.

`--reset`

Clears all statistic counters in ADSL driver

EXAMPLES: *A simple initialization.*

```
adsl start [--up] or adsl start
adsl connection -up
```

A more complex initialization.

```
adsl start --up --mod dl --lpair I or adsl start
adsl connection --up --mod dl --lpair I
```

Getting in and out of the test modes

```
adsl connection --reverb
...
adsl connection --up
```

Selecting tones

```
adsl connection --tones 0 32 0xFEFFFF7F 32 224
0xFEFFFFFFFFFFFF7F
```

selects tones from 1 to 31 for upstream and from 33 to 95 for downstream

Starting and monitoring BERT

Command Line Interface

```
adsl bert -start 60
```

to run BERT test for 60 seconds. After about 20 seconds of BERT running the results will look like:

```
adsl bert -show
```

```
adsl: BERT results:
BERT Status = RUNNING
BERT Total Time = 60 sec
BERT Elapsed Time = 20 sec
BERT Bits Tested = 0x0000000008B4C700 bits
BERT Err Bits = 0x0000000000000067 bits
```

After 60 seconds when the BERT has completed the results of -show command will be:

```
adsl bert -show
```

```
adsl: BERT results:
BERT Status = NOT RUNNING
BERT Total Time = 60 sec
BERT Elapsed Time = 60 sec
BERT Bits Tested = 0x000000001A1E5500 bits
BERT Err Bits = 0x0000000000000067 bits
```

Display minimal ADSL state.

```
adsl info --state
```

```
adsl: ADSL driver and PHY status
Status: Showtime Channel: FAST, Upstream rate = 8064
Kbps, Downstream rate1 = 1024 Kbps
```

Display complete ADSL driver and PHY status.

```
adsl info --show
```

```
adsl: ADSL driver and PHY status
Status: Showtime Channel: FAST, Upstream rate = 8064
Kbps, Downstream rate = 1024 Kbps
Mode: G.DMT
Channel: Fast
Trellis: ON
Line Status: No Defect
Training Status: Showtime
Down Up
SNR (dB): 16.1 7.0
Attn(dB): 0.0 5.5
Pwr(dBm): 6.5 7.8
Max(Kbps): 11040 1088
Rate (Kbps): 0 0
K: 0(0) 0
R: 0 0
S: 1 1
D: 1 1
SF: 25288 25286
SFErr: 1 0
```

Command Line Interface

```
RS: 0 0
RSCorr: 0 0
RSUnCorr: 0 0
HEC: 1 0
OCD: 0 0
LCD: 0 0
ES: 1 0
```

Command Line Interface

ARP

NAME: **arp** - manipulate modem's ARP (Address Resolution Protocol) table

SYNOPSIS:

```
arp add <IP address> <MAC address>
arp delete <IP address>
arp show
arp --help
```

DESCRIPTION: **arp** is used to manipulate modem's ARP table. Note that ARP entries added by this command are not saved in the flash memory by the save command. After system reboot, ARP entries need to be re-added.

COMMANDS: None

EXAMPLES: *Add a static ARP entry for IP address 192.168.1.2 with MAC address 00:11:22:33:44:55.*

```
arp add 192.168.1.2 00:11:22:33:44:55
```

Show ARP table.

```
arp show
```

IP address	HW type	Flags	HW address	Mask	Device
192.168.1.3	0x1	0x2	00:01:03:E3:4F:F9	*	br0
192.168.1.2	0x1	0x6	00:11:22:33:44:55	*	br0

Delete ARP entry for IP address 192.168.1.2.

```
arp delete 192.168.1.2
```

Command Line Interface

ATM

NAME: **atm** - allows an user to control the Telsey ATM driver

SYNOPSIS:

```
atm start [options]
atm stop
atm operate tdte|intf|vcc [options]
```

DESCRIPTION: Atm is used to control the Telsey ATM driver. This utility can:

- start and stop the driver
- activate and deactivate an ATM interface (port) or a Virtual Channel Connection (VCC)
- add and remove traffic descriptor table entries
- add and remove VCCs
- display the configuration for traffic descriptor table entries, ATM interfaces and VCCs
- display statistics for ATM interfaces and VCCs

All information are displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output.

COMMANDS:

start

Starts the Telsey ATM driver. This command to initialize the driver and add one UBR traffic descriptor table entry.

stop

Stops the Telsey ATM driver.

operate

Operates on traffic descriptor table entries, ATM interfaces and VCCs.

OPTIONS: *Options for the* **start** *command:*

```
atm start [--cqs <size>] [--pqs <size>] [--bs <size>] [--bo
<offset>] [--intf <port> <type> <address>]
```

```
--cqs <size>
```

`size` : Size used to create the Free and Receive cell queues. Default value is 10.

```
--pqs <size>
```

`size` : Size used to create the Free and Receive packet queues. Default value is 200.

```
--bs <size>
```

`size` : Size of a buffer used in the Free and Receive packet queues.

Command Line Interface

Default value is 1600.

`--bo <offset>`

`offset` : Offset into a receive buffer where data is to be received. Default value is 32.

`--intf <port> <type> <address>`

`port` : Port number starting at 0 to be configured.
`type` : adsl|loopback|utopia|tc
`address` : UTOPIA address. Only used if type is utopia.
More than one intf option can be specified to configure multiple ports. If no intf option is specified, the default value is "0, adsl, 0".

Options for the **`stop`** *command:*

`atm stop`

Options for the **`operate tdte`** *command:*

`atm operate tdte [--add <type> [<pcr>] [<scr>] [<mbs>]] [--delete <index>] [--show [<index>]]`

`--add <type> [<pcr>] [<scr>] [<mbs>]`

`type` : ubr|ubr_pcr|cbr|rtvbr|nrtvbr
`pcr` : Peak Cell Rate (PCR) if type requires it
`scr` : Sustainable Cell Rate (SCR) if type requires it
`mbs` : Maximum Burst Size (MBS) if type requires it

`--delete <index>`

`index` : Traffic descriptor table entry index to delete. The show option displays the current index values.

`--show [<index>]`

`index` : Traffic descriptor table entry index to display information about. If index is omitted, all traffic descriptor table entries are displayed.

Options for the **`operate intf`** *command:*

`atm operate intf [--state <port> <type>] [--show [<port>]] [--stats [<port>][reset]]`

`--state <port> <type>`

`port` : Port number starting at 0 to enable or disable.
`type` : enable|disable

`--show [<port>]`

`port` : Port number starting at 0 to display configuration information about. If port is omitted, configuration information is displayed for all configured ports.

`--stats [<port>] [reset]`

Command Line Interface

`port` : Port number starting at 0 to display statistics for.
`reset` : Resets statistics fields.
If port is omitted, statistics are displayed for all configured ports.

Options for the **`operate vcc`** *command:*

```
atm operate vcc [--add <port.vpi.vci> <aal_type> <tdte_index>
<encapsulation_type>]    [--delete    <port.vpi.vci>]    [--addq
<port.vpi.vci> <size> <priority> ] [--deleteq <port.vpi.vci> <size>
<priority>]    [--state    <port.vpi.vci>    <type>]    [--show
[<port.vpi.vci>]] [--stats [<port.vpi.vci>] [reset]]
```

```
--add <port.vpi.vci> <type> <tdte_index> <encapsulation_type>
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to add.
`type` : aal5|aal2|aal0pkt|aal0cell|aaltransparent
`tdte_index` : Traffic descriptor table entry index to use for this VCC. The command, atm operate tdte --show, displays the current index values.
`encapsulation_type` : vcmux_routed|vcmux_bridged8023|llcencaps|other|unknown

```
--delete <port.vpi.vci>
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to delete.

```
--addq <port.vpi.vci> <size> <priority>
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to add a new queue for.
`Size` : Size of the queue.
`Priority` : Priority of the queue.

```
--deleteq <port.vpi.vci> <size> <priority>
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to delete a queue for.
`size` : Size of the queue.
`priority` : Priority of the queue.

```
--state <port.vpi.vci> <type>
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to enable or disable.
`type` : enable|disable

```
--show [<port.vpi.vci>]
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to display configuration information about.
If port.vpi.vci is omitted, configuration information is displayed for all configured VCCs.

```
--stats [<port.vpi.vci>] [reset]
```

`port.vpi.vci` : Port number, VPI and VCI that identifies the VCC to display statistics for.
`reset` : Resets statistics fields.

If port.vpi.vci is omitted, statistics are displayed for all configured VCCs.

EXAMPLES: *A simple initialization.*

```
atm start
atm operate vcc --add 0.0.35 aal5 1 vcmux_bridged8023
```

A more complex initialization.

```
atm start --pqs 400 --bo 0
atm operate tdte --add ubr_pcr 15000
atm operate tdte --show
```

index	type	pcr	scr	mbs
1	ubr	0	0	0
2	ubr_pcr	15000	0	0

```
atm operate vcc --add 0.0.35 aal5 2 vcmux_bridged8023
```

Display interface configuration (assumes that the ATM driver is started).

```
atm operate intf --show
```

port	status	type
0	enabled	adsl

Create and display a VCC configuration (assumes that the ATM driver is started).

```
atm operate vcc --add 0.0.35 aal5 1 vcmux_bridged8023 --addq
0.0.35 64 2 --addq 0.0.35 80 1
atm operate vcc --add 0.0.36 aal5 1 vcmux_routed --addq 0.0.36
128 1
atm operate vcc --show
```

vcc	status	type	tdte_index	q_size	q_priority	encapsulation
0.0.35	enabled	aal5	1	64	2	vcmux_bridged8023
				80	1	
0.0.36	enabled	aal5	1	128	1	llcencaps

Display interface statistics (assumes that the ATM driver is started).

```
atm operate intf --stats
```

```
interface statistics for port 0
in octets 8130336
out octets 46512
in errors 0
in unknown 0
in hec errors 0
in invalid vpi vci errors 0
in port not enable errors 0
in pti errors 0
in circuit type errors 0
in oam rm crc errors 0
in gfc errors 0
aal5 interface statistics for port 0
in octets 8130336
```

Command Line Interface

```
        out octets 46512
        in ucast pkts 5426
        out ucast pkts 189
        in errors 0
        out errors 0
        in discards 0
        out discards 0
```

Display VCC statistics (assumes that the ATM driver is started and two VCCs are configured).

```
atm operate vcc --stats
        aal5 vcc statistics for 0.0.35
        crc errors 0
        oversized sdus 0
        short packet errors 0
        length errors 0
        aal5 vcc statistics for 0.0.36
        crc errors 0
        oversized sdus 0
        short packet errors 0
        length errors 0
```

Command Line Interface

BRCTL

NAME: **brctl** - bridge administration utility

SYNOPSIS: **brctl [command]**

DESCRIPTION: **brctl** is used to set up, maintain, and inspect the bridge configuration. A bridge is a device commonly used to connect different networks (Ethernet, USB, 802.11x wireless network or ATM) together, so that these networks will appear as one network to the participants. Each of the networks being connected corresponds to one physical interface (port) in the bridge. These individual networks are bundled into one bigger ('logical') network, this bigger network corresponds to the bridge network interface such as "br0".

COMMANDS:

addbr <bridge>

Creates a new instance of the bridge. The network interface corresponding to the bridge will be called <bridge>.

delbr <bridge>

Deletes the instance <bridge> of the bridge. The network interface corresponding to the bridge must be down before it can be deleted.

show <bridge>

Shows the instance <bridge> of the bridge.

show

Shows all current instances of the bridge.

addif <bridge> <device>

Makes the interface <device> a port of the bridge <bridge>. This means that all frames received on <device> will be processed as if destined for the bridge. Also, when sending frames on <bridge>, <device> will be considered as a potential output interface.

delif <bridge> <device>

Detaches the interface <device> from the bridge <bridge>.
showmacs <bridge>
Shows a list of learned MAC addresses for this bridge.

showstp <bridge>

Shows the STP (Spanning Tree Protocol) status of this bridge.

setageing <bridge> <time>

Sets the MAC address ageing time, in seconds. After <time> seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from the Forwarding DataBase (fdb).

Command Line Interface

`setbridgeprio <bridge> <priority>`

Sets the bridge's priority to <priority>. The priority value is an unsigned 16-bit quantity (a number between 0 and 65535), and has no dimension. Lower priority values are 'better'. The bridge with the lowest priority will be elected 'root bridge'.

`setfd <bridge> <time>`

Sets the bridge's 'bridge forward delay' to <time> seconds.

`setgcint <bridge> <time>`

Sets the garbage collection interval for the bridge <bridge> to <time> seconds. This means that the bridge will check the forwarding database for timed out entries every <time> seconds.

`sethello <bridge> <time>`

Sets the bridge's 'bridge hello time' to <time> seconds.

`setmaxage <bridge> <time>`

Sets the bridge's 'maximum message age' to <time> seconds.

`setpathcost <bridge> <port> <cost>`

Sets the port cost of the port <port> to <cost>. This is a dimensionless metric.

`setportprio <bridge> <port> <prio>`

Sets the port <port>'s priority to <priority>. The priority value is an unsigned 8-bit quantity (a number between 0 and 255), and has no dimension. This metric is used in the designated port and root port selection algorithms.

`stp <bridge> <state>`

Controls this bridge instance's participation in the spanning tree protocol. If <state> is "on" or "yes" the STP will be turned on, otherwise it will be turned off. When turned off, the bridge will not send or receive BPDUs, and will thus not participate in the spanning tree protocol. If your bridge isn't the only bridge on the LAN, or if there are loops in the LAN's topology, DO NOT turn this option off. If you turn this option off, please know what you are doing.

OPTIONS: None.

EXAMPLES: *Display all the learned MAC addresses on br0*

```
brctl showmacs br0
```

Set the ageing timer value to be 400 seconds on br0

```
brctl setageing br0 400
```

Command Line Interface

Turn off STP

```
brctl stp br0 off
```

Command Line Interface

CAT

NAME: **cat** - concatenates FILE(s) and prints them to standard output

SYNOPSIS: **cat [FILE] ...**

DESCRIPTION: Concatenates FILE(s) and prints them to standard output

COMMANDS: None.

OPTIONS: None.

EXAMPLES: *Display system memory information.*

```
cat /proc/meminfo
```

Command Line Interface

DEFAULTGATEWAY

NAME: **defaultgateway** - configure or show the default gateway or default route

SYNOPSIS:

```
defaultgateway config auto
defaultgateway config static [<ipaddress>] [<interface>]
defaultgateway show
defaultgateway -help
```

DESCRIPTION: The primary use of defaultgateway command is to set up a static default gateway or default route, or to retrieve the default gateway information automatically from remote ISPs through DHCP protocol for a MER interface or through PPP protocol for a PPPoA or PPPoE interface. A PPPoA or PPPoE interface will always retrieve remote gateway information automatically. This command will save configuration to the Permanent Storage. If the default gateway is configured with static data, it will override any remote gateway address received automatically from some WAN interface and become effective immediately in the runtime system. Ipaddress is optional if the default route is en route a PPPoE, PPPoA or IpoA interface. If the default gateway is en route a MER interface, ipaddress must be configured and the interface parameter is optional. If there is only one IPoA WAN interface, you must configure static default gateway or default route since IPoA does not support DHCP.If the default gateway is configured with the "auto" option, the system needs to be rebooted before it can take effect. If there are multiple WAN interfaces with DHCP or PPP enabled, multiple remote gateway addresses may be received and the first received will be chosen to be the default gateway.

COMMANDS: None

OPTIONS:

`ipaddress`

the IP address of the default gateway in dotted decimal.

`interface`

forces the default gateway to be associated with the specified device, as the kernel will otherwise try to determine the device on its own by checking already existing routes and devices.

EXAMPLES: *Enable the system to retrieve the default gateway information automatically from the remote dhcp server when system starts. The system needs to be rebooted for modified configuration to take effect.*

```
defaultgateway config auto
```

Set up a static default gateway to 10.6.33.125. It should be effective right away and is saved to Permanent Storage on the flash memory.

```
defaultgateway config 10.6.33.125
```

Command Line Interface

DF

NAME: **df** - print the filesystem used space and available space

SYNOPSIS: **df [OPTION]... [FILESYSTEM]...**

DESCRIPTION: df displays the amount of disk space available on the file system of each filesystem name argument. If no file system name is given, the space available on all currently mounted filesystems is shown. Disk space is shown in 1 kb blocks by default.

COMMANDS: None.

OPTIONS: `-h`

print sizes in human readable format (e.g., 1K 243M 2G)

`-m`

print sizes in megabytes

`-k`

print sizes in kilobytes (default)

EXAMPLES: *Display the space available on all the mounted file systems*

```
Df
```

Display the space available on the flash root file system

```
df /dev/mtdblock0
```

Command Line Interface

DHCPSERVER

NAME: **dhcpserver** - allows an user to configure, or show the DHCP Server data

SYNOPSIS: **dhcpserver config <start IP address> <end IP address> <leased time (hour)>**

dhcpserver show
dhcpserver -help

DESCRIPTION: **dhcpserver** is used to configure, or show the DHCP server data. This utility can:

- configure the DHCP server on the primary LAN interface.
- show the DHCP server configuration data.
- display usage.

All information is displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output.

COMMANDS: **config**

configure the DHCP server with the given data.

Notice: the command saves the configuration data to the flash but does not take effect until the system is rebooted.

show

show the DHCP server configuration data.

--help

display usage.

OPTIONS: *Options for the* **config** *command:*

`dhcpserver config <start IP address> <end IP address> <leased time (hour)>.`

`<start IP address>` : The IP address of the first address in the range. The value of range start must be less than or equal to the value of range end.
Valid values: any valid IP address. Default value: 192.168.1.2.

`<end IP address>` : The IP address of the last address in the range. The value of range end must be greter than or equal to the value of range start. Valid values: any valid IP address. Default value: 192.168.1.254.

`<leased time (hour)>` : The lease period for which the server assigsn an IP address to the client in case the client does not request for the specific lease period itself.
Valid values: 0 - 8760. Default value: 24 hours (this equals a day).

Command Line Interface

Options for the **show** *command*

```
dhcpserver show
```

Options for the **--help** *command:*

```
dhcpserver -help
```

EXAMPLES: *Configure DHCP server.*

```
dhcpserver config 192.168.1.2 192.168.1.254 24
```

Display DHCP server configuration data.

```
dhcpserver show
```

```
start 192.168.1.2
end 192.168.1.254
interface br0
option lease 86400
option min_lease 30
option subnet 255.255.255.0
option router 192.168.1.1
option dns 192.168.1.1
```

Display usage.

```
Dhcpserver -help
```

```
Usage: dhcpserver config <start IP address> <end IP
address> <leased time (hour)>
dhcpserver show
dhcpserver -help
```

Command Line Interface

DLTFTP

NAME: **dltftp** - allows an user to download a binary image from a TFTP server to the DSL router using TFTP protocol

SYNOPSIS: **dltftp <tftp_server_ip_address> <file_name>**

DESCRIPTION: Download a binary image from a TFTP server to the DSL router using TFTP protocol.

COMMANDS: None

OPTIONS: `dltftp <tftp_server_ip_address> <file_name>`

`<tftp_server_ip_address>` : The IP address of the TFTP server from which the file is to be downloaded.
Valid values: any valid IP address.
`<file_name>` : The name of the binary file to be downloaed. The filename contains the complete path in the TFPT server. The file must be a valid image file for the DSL router.
Valid values: String of up to 128 characters.

EXAMPLES: *A simple TFTP download setup.*

```
dltftp 192.168.1.2 bcm96345R_fs_kernel
```

Command Line Interface

DNSRELAY

NAME: **dnsrelay** - allows an user to configure or show the DNS relay data

SYNOPSIS:

```
dnsrelay config auto
dnsrelay config static <primary DNS> [<secondary DNS>]
dnsrelay show
dnsrelay -help
```

DESCRIPTION: dnsrelay is used to configure, or show the DNS relay data. This utility can:

- configure the DNS relay with the given data.
- show the DNS relay configuration data.
- display usage.

All information is displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output.

COMMANDS: **config**

configure the DNS relay with the given data. Notice: the command only saves the configuration data to the flash, and does not take effect until the system is rebooted.

show

show the DNS relay configuration data.

--help

display usage.

OPTIONS: *Options for the* **config auto** *command:*

```
dnsrelay config auto
```

Options for the **config static** *command:*

```
dnsrelay config static <primary DNS> [<secondary DNS>]
```

`<primary DNS>` : The IP address of the primary DNS server. Valid values: any valid IP address.

`[<secondary DNS>]` : The IP address of the secondary DNS server. It's optional and can be omitted. Valid values: any valid IP address.

Options for the **show** *command:*

```
dnsrelay show
```

Options for the **--help** *command:*

```
dnsrelay -help
```

Command Line Interface

EXAMPLES: *A auto DNS configuration.*

```
dnsrelay config auto
```

A static DNS configuration without secondary DNS.

```
dnsrelay config static 10.6.33.1
```

A static DNS configuration with secondary DNS.

```
dnsrelay config static 10.6.33.1 10.6.33.2
```

Display DNS relay configuration data.

```
dnsrelay show
```

```
Primary 10.6.33.1
Secondary 10.6.33.2
```

Display usage.

```
dnsrelay -help
```

```
Usage: dnsrelay config auto
Usage: dnsrelay config static <primary DNS> [<secondary
DNS>]
dnsrelay show
dnsrelay --help
```

Command Line Interface

ECHO

NAME: **echo** - display a line of text or an environment variable's value

SYNOPSIS: **`echo [OPTION]... [STRING]...`**

DESCRIPTION: echo displays a line of text, or an environment variable's value. Notice that "ls" command is not supported in the CLI. Echo can be used to display files and subdirectories using wildcard '*'.

COMMANDS: None.

OPTIONS: `-n`

suppress trailing newline

`-e`

interpret backslash-escaped characters (i.e., \t=tab)

`-E`

disable interpretation of backslash-escaped characters

EXAMPLES: *Display a string*

```
echo "Hello, world"
```

Display the vaule of the environment variable $TERM

```
echo $TERM
```

Display all files or subdirectories

```
echo /etc/*
echo *
echo /var/*
```

Command Line Interface

HELP

NAME: **help** - list all of available CLI commands that the DSL router supports

SYNOPSIS: **Help | ?**

DESCRIPTION: list all of available CLI commands that the DSL router supports.

COMMANDS: None

OPTIONS: None

EXAMPLES: *An example is shown.*

```
?
help
logout
reboot
adsl
atm
brctl
cat
df
dltftp
echo
ifconfig
kill
arp
defaultgateway
dhcpserver
dnsrelay
lan
passwd
ppp
remoteaccess
restoredefault
route
save
swversion
wan
ping
ps
pwd
sysinfo
traceroute
voice
```

Command Line Interface

IFCONFIG

NAME: **ifconfig** - configure a network interface

SYNOPSIS:
ifconfig [interface]
ifconfig interface [aftype] options | address ...

DESCRIPTION: Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed. I f no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

COMMANDS: None.

OPTIONS:

`interface`

The name of the interface. This is usually a driver name followed by a unit number, for example eth0 for the first Ethernet interface.

`address`

The IP address to be assigned to this interface.

`Up`

This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.

`down`

This flag causes the driver for this interface to be shut down.

`[-]arp`

Enable or disable the use of the ARP protocol on this interface.

`[-]promisc`

Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.

`[-]allmulti`

Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.

`metric N`

This parameter sets the interface metric.

`mtu N`

This parameter sets the Maximum Transfer Unit (MTU) of an interface.

Command Line Interface

`dstaddr addr`

Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the pointopoint keyword instead.

`netmask addr`

Set the IP network mask for this interface. This value defaults to the usual class A, B or C network mask (as derived from the interface IP address), but it can be set to any value.

`irq addr`

Set the interrupt line used by this device. Not all devices can dynamically change their IRQ setting.

`io_addr addr`

Set the start address in I/O space for this device.

`mem_start addr`

Set the start address for shared memory used by this device. Only a few devices need this.

`[-]broadcast [addr]`

If the address argument is given, set the protocol broadcast address for this interface. Otherwise, set (or clear) the IFF_BROADCAST flag for the interface.

`[-]pointopoint [addr]`

This keyword enables the point-to-point mode of an interface, meaning that it is a direct link between two machines with nobody else listening on it. If the address argument is also given, set the protocol address of the other side of the link, just like the obsolete dstaddr keyword does. Otherwise, set or clear the IFF_POINTOPOINT flag for the interface.

`[-]trailers`

Set or clear the IFF_NOTRAILERS flag for the interface.

`[-]dynamic`

Set or clear the IFF_DYNAMIC flag for the interface.

`hw class address`

Set the hardware address of this interface, if the device driver supports this operation. The keyword must be followed by the name of the hardware class and the printable ASCII equivalent of the hardware address. Hardware classes currently supported include ether (Ethernet) only.

`multicast`

Set the multicast flag on the interface. This should not normally be needed as the drivers set the flag correctly themselves.

Command Line Interface

`outfill N`

This parameter sets the interface outfill timeout.

`keepalive N`

This parameter sets the interface keepalive timeout.

`txqueuelen length`

Set the length of the transmit queue of the device. It is useful to set this to small values for slower devices with a high latency (modem links, ISDN) to prevent fast bulk transfers from disturbing interactive traffic like telnet too much.

EXAMPLES: *Display all the active interfaces*

```
ifconfig
```

Set interface eth0's IP address to be 192.168.1.1, netmask to be 255.255.255.0

```
ifconfig eth0 192.168.1.1 netmask 255.255.255.0
```

Command Line Interface

KILL

NAME: **kill** - send a signal to the specified process(es)

SYNOPSIS:
```
kill [ -signal ] pid ...
kill -l [ signal ]
```

DESCRIPTION: kill sends the specified signal to the specified process or process group. If no signal is specified, the TERM signal is sent. The TERM signal will kill processes which do not catch this signal. For other processes, it may be necessary to use the KILL (9) signal, since this signal cannot be caught.

COMMANDS: None.

OPTIONS:

`pid...`

Specify the list of processes that kill should sigal.

`-signal`

given as a signal name or number.

`-l`

List all signal names and numbers.

EXAMPLES:

Terminate the process with pid 120

```
kill 120
```

Send KILL signal to the process with pid 120

```
kill -SIGKILL 120
```

List all signal names and numbers

```
kill -l
```

Command Line Interface

LAN

NAME: **lan** - allow a user to configure the IP layer for the LAN interfaces

SYNOPSIS: **lan config [--ipaddr <primary|secondary> <IP address> <subnet mask>][--dhcpserver <enable|disable>]**

lan delete -ipaddr <primary|secondary>
lan show [<primary|secondary>]
lan -help

DESCRIPTION: Lan is used to configure the IP layer data for the primary and secondary LAN interfaces. A LAN interface is a logic interface toward IP stack from the Bridge module. Both primary and secondary LAN interfaces share the same MAC address from the physical Ethernet port. This utility can:

- Configure the IP address and subnet mask for the primary LAN interface. It can be either a private or a public IP address.
- Configure the IP address and subnet mask for the secondary LAN interface. NAT is not supported on the secondary LAN interface. Only public IP address is allowed.
- Enable or disable the DHCP server on the primary LAN interface. DHCP server is not supported on the secondary LAN interface.
- Display configuration data for the primary and secondary LAN interfaces.
- Display usage.

All information is displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output.

COMMANDS: **config**

configure IP layer for the primary or secondary LAN interface.

delete

delete the primary or secondary LAN interface configuration.

show

show configuration data for the primary and secondary LAN interfaces.

--help

display usage.

OPTIONS: *Options for the* **config** *command:*

`lan config [--ipaddr <primary|secondary> <IP address> <subnet mask>] [--dhcpserver <enable|disable>] --ipaddr <primary|secondary><IP address> <subnet mask>`

Command Line Interface

`primary|secondary` : specify which LAN interface will be configured. Valid values: primary or secondary.

`IP address` : The IP address of the LAN interface. Valid values: any valid IP address. Default value: 192.168.1.1.

`Subnet mask` : The subnet mask of the LAN interface. Valid values: 0.0.0.1-255.255.255.255. Default value: 255.255.255.0

`--dhcpserver <enable|disable> enable|disable` : specify DHCP server should be enabled or disabled. This option is only valid for the primary LAN interface.
Valid values: enable or disable. Default value is enable for the primary LAN interface.

Options for the **`delete`** *command:*

```
lan delete --ipaddr <primary|secondary> --ipaddr <primary|secondary>
```

`primary|secondary` : specify which LAN interface will be deleted. Valid values: primary or secondary.

Options for the **show** *command:*

```
lan show [<primary|secondary>]
```

`primary|secondary` : specify which LAN interface will be shown. Valid values: primary or secondary.
If it is omitted, all LAN interfaces are displayed.

Options for the --help command:

```
lan -help
```

EXAMPLES: *Configure a primary LAN interface.*

```
lan config -ipaddr primary 192.168.1.1 255.255.255.0
```

Remove a secondary LAN interface.

```
lan delete -ipaddr secondary
```

Display all LAN interfaces.

```
lan show
```

```
br0 Link encap:Ethernet HWaddr 02:10:18:01:00:01
inet addr:192.168.1.1 Bcast:192.168.1.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:42083 errors:0 dropped:0 overruns:0 frame:0
TX packets:107786 errors:0 dropped:0 overruns:0
carrier:0
collisions:0 txqueuelen:0
RX bytes:7412118 (7.0 MiB) TX bytes:34445874 (32.8 MiB)
br0:0 Link encap:Ethernet HWaddr 02:10:18:01:00:01
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Command Line Interface

Display usage.

```
lan -help
```

```
Usage: lan config [--ipaddr <primary|secondary> <IP
address> <subnet mask>]
[--dhcpserver <enable|disable>]
lan delete --ipaddr <primary|secondary>
lan show [<primary|secondary>]
lan -help
```

Command Line Interface

LOGOUT

NAME: **logout** - log out current user console

SYNOPSIS: **logout**

DESCRIPTION: logout is used to log out current user console. After logout command is executed, a bye bye message appears. Hit return to see a new Login prompt.

COMMANDS: None

OPTIONS: None

EXAMPLES:

```
logout

     Bye bye. Have a nice day!!!
     Login:
```

Command Line Interface

PASSWD

NAME: **passwd** - allow a user to change password

SYNOPSIS: **passwd <admin|support|user> <password>**

DESCRIPTION: **passwd** is a CLI command used to change password for user account admin, support or user.

COMMANDS: None

OPTIONS: None

EXAMPLES: *Change password for user admin to broadcom.*

```
passwd admin Broadcom
```

Command Line Interface

PING

NAME: **ping** - send ICMP echo requests to target host

SYNOPSIS: **Ping [-c <count>] [-s <size>] host**

DESCRIPTION: Ping sends out ICMP echo requests over the ICMP protocol to a host on the network. The default number of the ICMP echo request packets ping sends out is four. To continually send out packets without stop, use "-c 0" option.

COMMANDS: None

OPTIONS: `count`

The number of ICMP echo request packets ping command will send out.

`size`

force the ping to send out ICMP echo request packets with this number of data bytes.

`host`

The name or ip address of the target host.

EXAMPLES: *Send eight ICMP echo requests to 192.168.0.5*

```
Ping -c 8 192.168.0.5
```

Command Line Interface

PPP

NAME: **ppp** - allow a user to bring up or bring down a ppp connection

SYNOPSIS: **ppp config <port.vpi.vci> up|down**

DESCRIPTION: ppp is used to control the ppp interfaces.

COMMANDS: None

OPTIONS: `up|down`

Ppp command brings up the ppp connection with "up" option, and brings down the connection with "down" option. For ppp connection in on-demand mode, in addition to the "up" option, traffic to the ppp interface needs to be initiated to bring the connection up.

`<port.vpi.vci>`

Port number, VPI and VCI that identifies the VCC where the ppp connection is established.

EXAMPLES: *Bring down the ppp connection on the 0.0.35 VCC.*

```
ppp config 0.0.35 down
```

Command Line Interface

PS

NAME: **ps** - report process status

SYNOPSIS: **ps**

DESCRIPTION: ps gives a snapshot of the current processes. The output consists of six columns:

PID	The process ID
TTY	The terminal device the process attaches to, such as /dev/ttyp0
Uid	The user ID of the process owner
Size	The amount of virtual memory taken by the process (kilobytes)
State	The state of the process. (S-Sleeping, R-Running, W-Waiting)
Command	The command that launches the process

COMMANDS: None.

OPTIONS: None.

EXAMPLES: *Report process status*

```
ps
```

Command Line Interface

PWD

NAME: **pwd** - print name of current working directory

SYNOPSIS: **pwd**

DESCRIPTION: pwd is a CLI command used to display name of current working directory.

COMMANDS: None

OPTIONS: None

EXAMPLES: *To see current working directory.*

pwd

Command Line Interface

REBOOT

NAME: **reboot** - reboot the system

SYNOPSIS: **reboot**

DESCRIPTION: Reboot the system.

COMMANDS: None.

OPTIONS: None.

EXAMPLES: *Reboot the system*

```
reboot
```

Command Line Interface

RECVERSION

NAME **recversion** - display current running recovery software version

SYNOPSIS **recversion show**

DESCRIPTION **recversion** is a CLI command used to view the recovery software version.

EXAMPLES *Display current recovery software version.*

```
> recversion show

     Telsey Tlc
     Firmware version 1.0
```

Command Line Interface

REMOTEACCESS

NAME: **remoteaccess** - allows certain protocols to access the modem from the WAN side

SYNOPSIS:
remoteaccess <enable|disable>
remoteaccess show
remoteaccess -help

DESCRIPTION: **remoteaccess** sets security level to allow or disallow remote access into the route using telnet, http, snmp or ping from the WAN side. The options are enable, disable and show.

COMMANDS: None

OPTIONS: None

EXAMPLES: *Show current remote access mode.*

```
remoteaccess show
     remote access is disabled
```

Enable remote access.

```
remoteaccess enable
```

Disable remote access.

```
remoteaccess disabile
```

Command Line Interface

RESTOREDEFAULT

NAME: **`restoredefault`** - restores modem configuration to factory defaults

SYNOPSIS: **`restoredefault`**

DESCRIPTION: **`restoredefault`** is a CLI command used to erase all configurations made by user, and restore the modem back to factory default configuration. Once this command is executed, modem reboots automatically with default configuration.

COMMANDS: None

OPTIONS: None

EXAMPLES: *Restore configuration to factory defaults.*

```
restoredefault
```

Command Line Interface

ROUTE

NAME: **route** - show / manipulate the IP routing table

SYNOPSIS: **route add <ipaddress> <subnetmask> <[<gateway>] [<interface>]>**

route delete <ipaddress> <subnetmask>
route show
route -help

DESCRIPTION: **route** manipulates the IP routing table. Its primary use is to set up static routes to specific hosts or networks via an interface. When the add or delete options are used, route modifies the routing tables. Show option displays the current contents of the routing tables. Note default gateway route should use another "defaultgateway" command. If 0.0.0.0 is entered using route add command, it is treated the same as a static default gateway where a subnetmask must be entered.

COMMANDS: **add**

add a new route entry

delete

delete a route entry

show

show current content of routing table including static and dynamic route entries

OPTIONS: `ipaddress`

the destination network or host IP address in dotted decimal notation.

`subnetmask`

when adding a network route, the netmask must be specified. Target address must have zero matching with the zero portion in NM. Otherwise, command will fail and display message "netmask doesn't match route address" gateway route packets via a gateway.

NOTE: The specified gateway must be reachable first. This usually means that you have to set up a static route to the gateway beforehand. If you specify the address of one of your local interfaces, it will be used to decide about the interface to which the packets should be routed to.

`interface`

force the route to be associated with the specified device, as the kernel will otherwise try to determine the device on its own by checking already existing routes and devices.

EXAMPLES: *Add a route to the network 192.56.76.x via "br0" interface.*

Command Line Interface

```
route add 192.56.76.0 255.255.255.0 br0
```

Add route to to gateway 10.6.33.129 for network 192.57.66.x.

```
route add 192.57.66.0 255.255.255.0 10.6.33.129
```

OUTPUT: The output of the kernel routing table is organized in the following columns

Destination

The destination network or destination host.

Gateway

The gateway address or * if none set.

Genmask

The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
Flags Possible flags include
U (route is up)
H (target is a host)
G (use gateway)
R (reinstate route for dynamic routing)
D (dynamically installed by daemon or redirect)
M (modified from routing daemon or redirect)

FILES: `/proc/net/route`
`/proc/net/rt_cache`

Command Line Interface

SAVE

NAME: **save** - save current configuration to Permanent Storage on the flash memory

SYNOPSIS: **save**

DESCRIPTION: **save** is a CLI command used to save current configuration to flash.

COMMANDS: None

OPTIONS: None

EXAMPLES: *Save all current configuration to flash.*

```
save
```

Command Line Interface

SWVERSION

NAME: **swversion** - display current running software version

SYNOPSIS: **swversion show**

DESCRIPTION: swversion is a CLI command used to view the current running software version.

COMMANDS: None

OPTIONS: None

EXAMPLES: *Display current software version.*

```
swversion show
     1.00.00.a0_23a
```

Command Line Interface

SYSINFO

NAME: **sysinfo** - display the general system information

SYNOPSIS: **sysinfo**

DESCRIPTION: sysinfo displays the number of processes in the system, system time, system uptime, the average system load in the past 1, 5 and 15 minutes, and the system memory consumption. The figures in the memory consumption table are in 1kb unit.

COMMANDS: None.

OPTIONS: None.

EXAMPLES: *Display the system information*

```
sysinfo
```

Command Line Interface

TFTPPROV

NAME: **tftpprov** - automatic provisioning via tftp command

SYNOPSIS: **tftpprov enable [--static [-s <address>] [-f <filename>] [-c <cfginterval>]] [--dynamic [-c <cfginterval>]]**

DESCRIPTION: **tftpprov** enables the configuration via TFTP. It can be either static or dynamic (via DHCP options).

COMMANDS: Static configuration:

```
tftpprov enable --static [-s <address>]  [-f <filename>] [-c <cfginterval>]
```

Dynamic mode (via DHCP). The option 66 and 67 contains the information about TFTP Server and Filename that will be used to configure CPVA500. This parameter will not be saved in flash:

```
tftpprov enable --static  --dynamic [-c <cfginterval>]]
```

Save the parameters and configuration:

```
tftpprov save
```

Show the parameters:

```
tftpprov show
```

Disable the provisioning:

```
tftpprov disable
```

OPTIONS: See above.

EXAMPLE: See configuration file example in the Web Interface chapter.

Command Line Interface

TRACEROUTE

NAME: **traceroute** - print the route packets take to network host

SYNOPSIS: **traceroute [-dnrv] [-m max_ttl] [-p port#] [-q nqueries] [-s src_addr] [-t tos] [-w wait] host [data size]**

DESCRIPTION: **traceroute** utilizes the IP protocol `time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

COMMANDS: None.

OPTIONS:

`-d`

set SO_DEBUG options to socket

`-n`

Print hop addresses numerically rather than symbolically

`-r`

Bypass the normal routing tables and send directly to a host

`-v`

Verbose output

`-m max_ttl`

Set the max time-to-live (max number of hops)

`-p port#`

Set the base UDP port number used in probes (default is 33434)

`-q nqueries`

Set the number of probes per ‘’ttl’’ to nqueries (default is 3)

`-s src_addr`

Use the following IP address as the source address

`-t tos`

Set the type-of-service in probe packets to the following value (default 0)

`-w wait`

Set the time (in seconds) to wait for a response to a probe (default 3 sec.).

EXAMPLES: *Trace the route to www.yahoo.com*

```
traceroute www.yahoo.com
```

Command Line Interface

VOICE

NAME: **voice** - manipulate voice-related parameters or start voice application

SYNOPSIS:

```
voice help
voice show
voice start
voice save
voice set <parameter> <value>
```

DESCRIPTION: Voice command enables manipulation of the voice-related parameters or starting the voice application.

COMMANDS:

help

Displays command syntax.

show

Shows voice-related parameters.

start

Starts voice application.

save

Save voice parameters.

set

Configures the voice related parameters. These parameters are specific to type of voice protocol used in the voice application.

For SIP, the following parameters can be set:

proxy: Proxy IP address or domain-name and port
registrar: Registrar IP address or domain-name and port
ttl: Time to Live
altProxy: Alternative Proxy IP address or domain-name and port.
altRegistrar: Alternative Registrar IP address or domain-name and port.
altTimeout: Timeout for alternate server use.
altRetries: Numbers of retries to swap to alternate Sever.
logserver: IP address and port for log server
phone1: Telephone number Line1
phone2: Telephone number Line2
auth: Enable (On) or Disable (Off) Digest Authenticaion
user1: Username for Digest Authenticaion Line1
user2: Username for Digest Authenticaion Line2
passw1: Password for Digest Authenticaion Line1

Command Line Interface

passw2: Password for Digest Authenticaion Line2
dialplan1: Dial Plan Line1
dialplan2: Dial Plan Line2
oobEnable: Enable (On) or Disable (Off) OOB DTMF
dtmf: DTMF rtp payload code (96 - 127)
sdpExport: SDP information are export in INVITE/200OK or 200OK/ACK
suppServs: Defined supplementary service codes
serviceMask: Mask to allow supplementary service
transport: Transport protocol type (UDP, TCP, BOTH).
interface: Interface name over which the SIP and voice packets are sent (e.g. br0, nas25, etc.)
codec_G711A_packet: Codec G711A, packetization (ms) Min=10, Max=30
codec_G711A_ec: Codec G711A, Enable or Disable echo canceller
codec_G711A_ss: Codec G711A, Enable or Disable silence suppression
codec_G711U_packet: Codec G711U, packetization (ms) Min=10, Max=30
codec_G711U_ec: Codec G711U, Enable or Disable echo canceller
codec_G711U_ss: Codec G711U, Enable or Disable silence suppression
codec_G729_packet: Codec G729, packetization (ms) Min=10, Max=30
codec_G729_ec: Codec G729, Enable or Disable echo canceller
codec_G729_ss: Codec G729, Enable or Disable silence suppression
codec_priority: Codec priority order (ex: G729,G711A,G711U)
country: Country (ex: ITALY, NORTH_AMERICA, UK, FRANCE, SWEDEN, NETHERLANDS, BELGIUM, GERMANY)
clid: trasmission caller ID (FSK or DTMF)
hookflash_min: Minimum time for hookflash detection.
hookflash_max: Minimum time for hookflash detection.
squelch: Enable (On) or Disable (Off) squelch of inband DTMF.
passthru: Codec to use with Fax Passthrough swichover (G711A, G711U, Off).

Command Line Interface

WAN

NAME: **wan** - allow a user to configure the WAN interfaces for the DSL router

SYNOPSIS:

wan config <port.vpi.vci> [--protocol <bridge|pppoe|pppoa|mer|ipoa>] [--encap <llc|vcmux>][--state <enable|disable>] [--service <servicename>] [--firewall <enable|disable>] [--nat <enable|disable>] [--username <username> --password <password>] [--pppidletimeout <timeout>] [--pppipextension <disable|enable>] [--ipaddr <wanipaddress> <wansubnetmask] [--dhcpclient <enable|disable>]

wan delete <port.vpi.vci>
wan show [<port.vpi.vci>]
wan --help <bridge|pppoe|pppoa|mer|ipoa>

DESCRIPTION: **wan** is used to configure the networking protocols for each WAN interface. Currently each WAN interface occupies one ATM PVC. It does not support multiple PPPoE sessions on one ATM PVC. Before using this command, the ATM PVC of which the WAN interface is based on, must be configured first by using the atm command. This command can:

- configure the protocol, encapsulation mode over ATM PVC, state, service name for each WAN interface.
- configure the username, password, idle timeout, and PPP IP extension for a PPPoE or a PPPoA interface.
- configure the IP address and subnet mask for a MER or a IPoA interface.
- enabling NAT or firewall for a MER or IPoA interface.
- enable or disable the DHCP client for a MER interface.
- delete the existed WAN interface (it will not delete the ATM PVC).
- show ATM PVC and WAN interface summary data and status.
- display usage for WAN interface.

All information are displayed to stdout. A program or shell script that calls this utility can redirect stdout to a file and then parse the file in order to interpret the displayed output. Note that special characters are supported in all options of character string type.

COMMANDS: **config**

configure the WAN interface for the DSL router.

Notice: the command only saves the configuration data to the flash, and does not take effect until the system is rebooted.

delete

remove the existed WAN interface.

Command Line Interface

Notice: the command only saves the configuration data to the flash, and does not take effect until the system is rebooted.

show

show ATM PVC VPI/VCI, service category, WAN interface service name, WAN interface name, WAN protocol, WAN interface service state, WAN interface up/down status, and WAN IP address.

--help

display usage for WAN interface.

OPTIONS: *Options for the* **config** *command:*

```
wan config <port.vpi.vci> [--protocol <bridge|pppoe|pppoa|mer|ipoa>] [--encap <llc|vcmux>] [--state <enable|disable>] [--service <servicename>] [--firewall <enable|disable>] [--nat <enable|disable>] [--username <username> --password <password>] [--pppidletimeout <timeout>] [--pppipextension <disable|enable>] [--ipaddr <wanipaddress> <wansubnetmask>] [--dhcpclient <enable|disable>]
```

`<port.vpi.vci>`

`port` : port number of the ATM VCC to add.
Valid values: 0.
`vpi` : VPI of the VCC to add.
Valid values: 0 - 255.
Default value: 0
`Vci` : VCI of the VCC to add.
Valid values: 32 - 65535.
Default value: 35.

`--protocol <bridge|pppoe|pppoa|mer|ipoa>` : The protocol of the WAN interface. Valid values: bridge, pppoe, pppoa, mer, or ipoa. Default value: bridge.

`--encap <llc|vcmux>` : the encapsulation type over the ATM PVC. Valid values: llc or vcmux.

`llc` - For mer, pppoe or bridge, it's RFC2684 bridged encapsulation For pppoa, it's RFC2364 LLC/NLPID encapsulation
`Vcmux` - RFC2684 VC-MUX (null encapsulation).

Default value: `llc` for bridge, pppoe, mer, or ipoa. `Vcmux` for pppoa.

`--state <enable|disable>` : the service state of the WAN interface.
Valid values: enable or disable.
Default value: enable.

`--service <servicename>` : the service name of the WAN interface.
Valid values: strings of 32 characters.
Default value: <protocol>_<vpi>_<vci>.

`--firewall <enable|disable>` : the firewall state of the MER or IPoA interface. Notice that firewall is always enabled on a PPPoE or a PPPoA interface.

Command Line Interface

Valid values: enable or disable. Default value: enable.

`--nat <enable|disable>` : the NAT state of the MER or IPoA interface. Notice that NAT is always enabled on a PPPoE or a PPPoA interface. Valid values: enable or disable.
Default value: enable.

`--username <username>` : the login name of the PPPoE or PPPoA interface. This option is only applied to a PPPoE or PPPoA interface. The --password option is also needed when this option is used.
Valid values: string of 32 characters.

`--password <password>` : the password of the PPPoE or PPPoA interface. This option is only applied to a PPPoE or PPPoA interface. The --username option is also needed when this option is used.
Valid values: string of 256 characters.

`--pppidletimeout <timeout>` : the PPP timeout of a PPPoE or PPPoA interface. This option is only applied to a PPPoE or PPPoA interface. Valid values: 0 - 1090 (minutes). 0: PPP connection is always-on. Greater than 0: WAN traffic will be monitored and PPP connection will be torn down when there is no user data activity over the WAN interface for more than this idle time period.
Default value: 30 minutes.

`--pppipextension <disable|enable>` : the PPP IP extension mode of a PPPoE or PPPoA interface. This option is only applied to a PPPoE or PPPoA interface. Valid values: disable or enable.
Default value: disable.

`--ipaddr <wanipaddress> <wansubnetmask>` : the WAN IP address and WAN subnet mask of a MER or IPoA interface.
This option should only be used for a MER or IPoA interface. PPPoE and PPPoA interface always receives the IP address, submask and DNS addresses automatically from the ISP through the PPP protocol. If this option is used and the dhcpclient value is "enable", DHCP client will be disabled on this interface. In general principle, static configuration overwrites dynamically assigned data.
`<wanipaddress>` : the WAN IP address. Valid values: any valid IP address.
`<wansubnetmask>` : the WAN subnet mask. Valid values: 0.0.0.1 - 255.255.255.255.

`--dhcpclient <enable|disable>` : the DHCP client state of the MER interface. This option is only valid to a MER interface. DHCP client is not supported over any other type of WAN interface.
Valid values: enable or disable.
Default value: enable.

Options for the **`delete`** *command:*

`wan delete <port.vpi.vci>`

`port` : port number of the VCC to add. Valid values: 0.
`vpi` : VPI of the VCC to add. Valid values: 0 - 255. Default value: 0
`vci` : VCI of the VCC to add. Valid values: 32 - 65535. Default value: 35.

Command Line Interface

Options for the **show** *command:*

```
wan show [<port.vpi.vci>]
```

`port` : port number of the VCC to add. Valid values: 0.
`vpi` : VPI of the VCC to add. Valid values: 0 - 255. Default value: 0
`vci` : VCI of the VCC to add. Valid values: 32 - 65535. Default value: 35

If <port.vpi.vci> is obmitted then it will display summary state of all existing WAN interfaces. Notice, configuration needs to be saved to the Permanent Storage first and then become effective after reboot. The wan show command shows the WAN interfaces after reboot, the second stage.

Options for the **`--help`** *command:*

```
wan --help [ < bridge | pppoe | pppoa | mer | ipoa > ]  < bridge | pppoe | pppoa | mer | ipoa>
```

Display only valid options for the specified protocol.
If it is obmitted then the help for all protocols is diplayed.

EXAMPLES:

Configure a PPPoE interface

```
wan config 0.0.35 --protocol pppoe --username username --password password --encap llc
```

Configure a PPPoA interface

```
wan config 0.0.36 --protocol pppoa --username username --password password --encap vcmux
```

Configure a MER configuration using DHCP client

```
wan config 0.0.37 --protocol mer --encap llc
```

Configure a MER configuration using static WAN address

```
wan config 0.0.37 --protocol mer --encap llc --ipaddr 10.6.33.163 255.255.255.0
```

Configure a IPoA configuration without fireware, without NAT

```
wan config 0.0.40 --protocol ipoa --encap llc --firewall disable --nat disable --ipaddr 10.6.33.227 255.255.255.0
```

Configure a bridge configuration

```
wan config 0.2.35
```

Remove a WAN interface

```
wan delete 0.2.35
```

Display all WAN interfaces

```
wan show
```

Command Line Interface

```
=========================================================================
=========
VCC Catego. Service Intf. Proto. State Status IP
Name Name address
=========================================================================
=========
0.0.35 UBR pppoe_0_35 ppp33 PPPoE Enable Up 10.6.33.143
0.0.36 UBR pppoa_0_36 ppp42 PPPoA Enable Up 10.6.33.152
0.0.37 UBR mer_0_37 nas27 MER Enable Up 10.6.33.193
0.0.40 UBR ipoa_0_40 atm52 IPoA Enable Up 10.6.33.227
=========================================================================
```

Display usage for all protocols

```
wan --help
```

```
Usage: wan config <port.vpi.vci>
[--protocol   <bridge|pppoe|pppoa|mer|ipoa>]   [--encap
<llc|vcmux>]
[--state <enable|disable>] [--service <servicename>]
[--firewall <enable|disable>] [--nat <enable|disable>]
[--username <username> --password <password>]
[--pppidletimeout     <timeout>]     [--pppipextension
<disable|enable>]
[--ipaddr <wanipaddress> <wansubnetmask]
[--dhcpclient <enable|disable>]
wan delete <port.vpi.vci>
wan show [<port.vpi.vci>]
wan --help <bridge|pppoe|pppoa|mer|ipoa>
```

Display usage for bridge

```
wan --help bridge
```

```
Usage: wan config <port.vpi.vci>
[--protocol   <bridge|pppoe|pppoa|mer|ipoa>]   [--encap
<llc|vcmux>]
[--state <enable|disable>] [--service <servicename>]
wan delete <port.vpi.vci>
wan show [<port.vpi.vci>]
wan --help <bridge|pppoe|pppoa|mer|ipoa>
```

Chapter 7

Technical Features

Broadband Interface		
	ADSL compliant with: • ANSI T1.413 I2 • ITU Automode • G.992.2G.Lite • G.992.1 Annex A - G.dmt • Up to 840 Kbps upstream (CPE to CO) • Up to 8 Mbps downstream (CO to CPE): conforming TR048 • Up to 8 PVC in UBR, CBR, VBRrt, VBRnrt mode	
Voice		
Simultaneous voice calls	2	
Analogue Interfaces	• 2xFXS RJ11 connectors • Dial tone supported: DTMF • Tones: customizable • Ringing voltage: 35 Vrms, Sine wave • Ringing frequency: 25Hz default (frequency and cadence programmable for each FXS interface)	• REN: 5 per FXS port • On-hook voltage: 48V nominal • Off-hook current: 22mA nominal (other values programmable) • Terminating impendance: 600 Ohm default (other impendances programmable) • Loop signalling: Loop Start • Loop length: 200m max
VoIP Protocols	H.323 v4	
Properties	• Echo cancellation G.168 • Silence suppression/comfort noise generation	• Modem/fax passthrough
Voice Codecs	G.711 Alaw/MiLaw, G.729A	
Others	Autodetection of cut-over	
Class 5 Services		
Caller ID	V.23 Modem and DTMF transmitter on board	
Data		
Domestic LAN Interfaces	• 1 Ethernet 10/100 BaseT half/full duplex autonegotiating • 1 USB port • RJ 45 connectors	
Layer 3	• NAT (RFC 1631) • RIP v1/RIP v2 • Static Route • LLC/SNAP, VCMUX for bridged/ routed PDU's (RFC 2684/1483) • PPPoE (RFC 2516) max.5 PVC • PPPoA (RFC 2364)	• IPoA • MER (a.k.a. IP over Ethernet over AAL5) • ARP • DNS Relay • DNS server fallback in DNS relay • User authentication PAP (RFC 1334) and CHAP (RFC 1994)
Others	• DHCP Client/Server • TFTP Client	
Management		
	• Integrated Web Server • Upgradeable via Telnet, TFTP and Web Server	
Power Supply		
	12Vdc ±15%, 10W Input Voltage 230Vac, 50Hz	

Technical Features

Physical Dimensions	
	Width 150mm, Depth 140mm, Heigth 38mm. Wall mountable
Environmental Conditions	
	Operation temperature: 5°C to 45°C Storage temperature: -5°C to 55°C Operating humidity: 5% to 85% (not condensing)
Certifications	
	• European Community Directive for Low Voltage Electrical Equipment 73/23/ EEC according to EN 60950 • European Community Directive for Electromagnetic Compatibility EMC 89/336/ EEC according to EN55022 and EN55024

Appendix A

DIAL PLAN

It is possible to specify a dialplan, by following the rules indicated in the table.

Tab. 17: Dial Plan Rules

Symbol	Rule
.	Match any digit entered.
-	Additional digits can be entered. This command can be used only at the end of a dial plan rule.
tn	Defines timeout as n seconds. Valid values are 0-9 and a-z, where a-z indicates a range of 10 to 35.
rn	Repeat the last pattern n times, where n is 0-9 or a-z. The values a-z indicate a range of 10-35.
^	Logical not. Match any character except the character immediately following the ^ command.
>#	Defined the # character as a termination character. When the termination character is entered, the dial string will automatically be sent.
|	Used to separate multiple dial plan rules.
S	Seize rule matching. If a dial plan rule matches the sequence of digits entered by the users to this point, and the modifier S is the next command in the dial plan rule, all other are negated for the remainder of the call.
I	Change the default timeout of 36 seconds by adding the following rule to your dial plan string: In, where n is 1-9 or a-z(for 10-35) seconds. Specifying your own inter digit timeout also changes the behavior of the dial plan so that, rather than the entire dial string being sent at timeout, it is sent only as a result of a matching rule or time intended by a matching rule.
H	Rule to support hot/warm line: Hdnnnn, where d is a delay in seconds parameter 0-9,a-z (for 0 to 35 seconds delay), and nnnn is the variable length phone number to call when no digits are entered for d seconds after off hook. *Example 1: H05551212 (off hook and call 5551212 immediately)* *Example 2: H5923123456 (off hook, if digits entered for 5 seconds, call 923123456)* **Note: H rule is set only once**
X	Rule that allow suppress a digit string so that dialing cannot be completed (Blocking call): *Example 1: |071SX|0900SX|* (no match when is dialing one whichever digit after 071 and no match when is dialing one whichever digit after 0900)

Appendix A

Tab. 17: Dial Plan Rules

Symbol	Rule
P	Rule to support dial prefix: Ptnnnn, where t is a single leading trigger digit if occurs as the FIRST entered digit when making a new call will trigger the prepending of a variable length prefix (as specified in "nnnn") in the dial string. 't' can take one of the following values: 0-9, 'n' (= any of 1-9), 'N' (any of 'n' and 0). *Example: Pn12345, will prepend 12345 to the dial string when the first entered digit is any of 1-9.* **Note: the trigger digit is not removed from the dial string.** **Note: P rule is set only once.**

Appendix A

COUNTRY TONES

The countries supported in this release are NORTH_AMERICA, ITALY, UK, FRANCE, SWEDEN, NETHERLANDS and the tones are the following:

DIAL TONE: Dial tone is sent to the calling party to indicate that the network is ready to receive call information and inviting the user to start sending call or service related information.

BUSY TONE: Busy tone is sent to the calling party to indicate that a connection has been made but that the called party is busy.

RINGBACK TONE: Ringing tone is sent to the calling party to indicate that a connection has been made and that an alerting signal is being applied to the called terminal or service. The ringing tone is not intended to coincide with the ringing signal that is sent to the called terminal.

CONFIRMATION TONE: Confirmation tone is sent to the calling party to indicate the understanding of the combination of keys: for example to enable or disable some particular service.

CONGESTION TONE: Congestion tone is sent to the calling party to indicate that some part of the network required for setting up of the requested call or for the use of a specific service is temporarily engaged.

SPECIAL DIAL TONE (STUTTERING): The special dial tone is sent to the calling party to indicate that the network is ready to receive call information and inviting the user to start sending call or service related information, at the same time reminding the user that special conditions apply to the terminal from which the call is being made.

CALL WAITING TONE: Call waiting tone is sent to a user during a call to indicate that a new call is arriving. The indication is presented when the Call Waiting supplementary service is active and a new call invokes the service. The network sends the call waiting tone to the party that the new call addresses.

NETWORK BUSY TONE: Network Busy tone is sent to the calling party to indicate that a transfer of call hasn't been made.

ONHOOK WARNING TONE: OnHook warning tone is sent to the calling party in the following cases:

a) after 36 seconds from the called party onHook;

b) after 36 seconds of during the calling party dialing if no digit are pressed.

Tab. 18: North America Tones

NORTH_AMERICA	Cadence	Freq.	Power
Dial Tone	Continuous	350,440 Hz	-13 dB
Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	480,620 Hz	-24 dB

Appendix A

Tab. 18: North America Tones

NORTH_AMERICA	Cadence	Freq.	Power
Ringback Tone	[2000 (ms) On, 4000 (ms) Off], Repeat	440,480 Hz	-19 dB
Confirmation Tone	[100 (ms) On, 100 (ms) Off], Repeat 3 times	350,440 Hz	-13 dB
Congestion Tone	[240 (ms) On, 260 (ms) Off], Repeat	480,620 Hz	-24 dB
Special Dial Tone (stuttering)	[100 (ms) On, 100 (ms) Off], Repeat 3 times and then Continuos	350,440 Hz	-13 dB
Call waiting Tone	[300 (ms) On, 10000 (ms) Off], Repeat	440 Hz	-16 dB
Network Busy Tone	500 (ms) On [freq 950], 500 (ms) On [freq 1400], 500 (ms) On [freq 1750]	950,1400, 1750 Hz	-16 dB
OnHook warning Tone	[100 (ms) On, 100 (ms) Off], Repeat	1400,2060, 2450,2600 Hz	-6 dB
RING phone	Cadence: [2000 (ms) On, 4000(ms) Off] Voltage: 45 Vrms Frequency: 20 Hz		

Tab. 19: Italy tones

ITALY	Cadence	Freq.	Power
Dial Tone	[200 (ms) On, 200 (ms) Off, 600 (ms) On, 1000 (ms) Off], Repeat	425 Hz	-15 dB
Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	425 Hz	-25 dB
Ringback Tone	[1000 (ms) On, 4000 (ms) Off], Repeat	425 Hz	-25 dB
Confirmation Tone	[100 (ms) On, 100 (ms) Off], Repeat 3 times	425 Hz	-13 dB
Congestion Tone	[200 (ms) On, 200 (ms) Off], Repeat	425 Hz	-25 dB
Special Dial Tone (stuttering)	[200 (ms) On, 200 (ms) Off, 600 (ms) On, 1000 (ms) Off], Repeat	425 Hz	-15 dB
Call waiting Tone	[300 (ms) On, 10000 (ms) Off], Repeat	440 Hz	-16 dB
Network Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	425 Hz	-16 dB

Appendix A

Tab. 19: Italy tones

ITALY	Cadence	Freq.	Power
OnHook warning Tone	[100 (ms) On, 100 (ms) Off], Repeat	425 Hz	-6 dB
RING phone	Cadence: [1000 (ms) On, 4000(ms) Off] Voltage: 45 Vrms Frequency: 20 Hz		

Tab. 20: UK tones

UK	Cadence	Freq.	Power
Dial Tone	Continuous	350,440 Hz	-13 dB
Busy Tone	[375 (ms) On, 375 (ms) Off], Repeat	400 Hz	-18 dB
Ringback Tone	[400 (ms) On, 200 (ms) Off, 400 (ms) On, 2000 (ms) Off], Repeat	400,450 Hz	-18 dB
Confirmation Tone	[100 (ms) On, 100 (ms) Off], Repeat 3 times	400 Hz	-13 dB
Congestion Tone	[400 (ms) On, 350 (ms) Off, 225 (ms) On, 525 (ms) Off], Repeat	400 Hz	-22 dB
Special Dial Tone (stuttering)	[100 (ms) On, 100 (ms) Off], Repeat 3 times and then Continuos	400 Hz	-13 dB
Call waiting Tone	[300 (ms) On, 10000 (ms) Off], Repeat	440 Hz	-16 dB
Network Busy Tone	1000 (ms) On	400 Hz	-16 dB
OnHook warning Tone	[100 (ms) On, 100 (ms) Off], Repeat	400 Hz	-6 dB
RING phone	Cadence: [400 (ms) On, 200(ms) Off, 400 (ms) On, 2000(ms) Off] Voltage: 45 Vrms Frequency: 16.66 Hz		

Tab. 21: SWEDEN Tones

SWEDEN	Cadence	Freq. (Hz)	Power (dBm)
Dial Tone	Continuos	425	-15
Busy Tone	[250 (ms) On, 250 (ms) Off], Repeat	425	-20
Ringback Tone	[1000 (ms) On, 5000 (ms) Off], Repeat	425	-20
Confirmation Tone	[100 (ms) On, 100 (ms) Off], Repeat 3 times	425	-20

Appendix A

Tab. 21: SWEDEN Tones

SWEDEN	Cadence	Freq. (Hz)	Power (dBm)
Congestion Tone	[250 (ms) On, 750 (ms) Off], Repeat	425	-20
Special Dial Tone (stuttering)	[320 (ms) On, 20 (ms) Off], Repeat	425	-15
Call waiting Tone	[200 (ms) On, 500 (ms) Off, 200 (ms) On, 10000(ms) Off], Repeat	425	-20
Network Busy Tone	[250 (ms) On, 250 (ms) Off], Repeat	425	-20
OnHook warning Tone	[100 (ms) On, 100 (ms) Off], Repeat	425	-20
RING phone	Cadence: [1000 (ms) On, 5000(ms) Off] Voltage: 45 Vrms Frequency: 25 Hz		

Tab. 22: FRANCE Tones

FRANCE	Cadence	Freq. (Hz)	Power (dBm)
Dial Tone	Continuos	440	-4
Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	440	-8
Ringback Tone	[1500 (ms) On, 3500 (ms) Off], Repeat	440	-8
Confirmation Tone	[300 (ms) On][330 (ms) Off, 300(ms) On][660 (ms) Off, 300(ms) On]	950 1400 1800	-8
Congestion Tone	[500 (ms) On, 500 (ms) Off], Repeat	440	-8
Special Dial Tone (stuttering)	Continuos	330 440	-5
Call waiting Tone	[300 (ms) On, 10000(ms) Off], Repeat	440	-8
Network Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	440	-8
OnHook warning Tone	[100 (ms) On, 100 (ms) Off], Repeat	440	-8
RING phone	Cadence: [1500 (ms) On, 3500(ms) Off] Voltage: 45 Vrms Frequency: 50 Hz		

Tab. 23: NETHERLANDS Tones

NETHERLANDS	Cadence	Freq. (Hz)	Power (dBm)
Dial Tone	Continuos	425	-15
Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	425	-15

Appendix A

Tab. 23: NETHERLANDS Tones

NETHERLANDS	Cadence	Freq. (Hz)	Power (dBm)
Ringback Tone	[1000 (ms) On, 4000 (ms) Off], Repeat	425	-15
Confirmation Tone	[300 (ms) On][300 (ms) Off, 300(ms) On][600 (ms) Off, 300(ms) On]	950 1400 1800	-20
Congestion Tone	[250 (ms) On, 250 (ms) Off], Repeat	425	-15
Special Dial Tone (stuttering)	[500 (ms) On, 55 (ms) Off], Repeat	425	-15
Call waiting Tone	[500 (ms) On, 9500(ms) Off], Repeat	425	-20
Network Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	425	-15
OnHook warning Tone	[250 (ms) On, 250 (ms) Off], Repeat	425	-15
RING phone	Cadence: [1000 (ms) On, 4000(ms) Off] Voltage: 45 Vrms Frequency: 25 Hz		

Tab. 24: BELGIUM Tones

BELGIUM	Cadence	Freq. (Hz)	Power (dBm)
Dial Tone	Continuos	435	-12
Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	435	-20
Ringback Tone	[1000 (ms) On, 3000 (ms) Off], Repeat	435	-20
Confirmation Tone	[300 (ms) On][330 (ms) Off, 300(ms) On][660 (ms) Off, 300(ms) On]	900 1380 1860	-20
Congestion Tone	[167 (ms) On, 167 (ms) Off], Repeat	435	-20
Special Dial Tone (stuttering)	Continuos	330 440	-12
Call waiting Tone	[300 (ms) On, 10000(ms) Off], Repeat	440	-20
Network Busy Tone	[500 (ms) On, 500 (ms) Off], Repeat	435	-20
OnHook warning Tone	[500 (ms) On, 500 (ms) Off], Repeat	440	-20

Appendix A

Tab. 24: BELGIUM Tones

BELGIUM	Cadence	Freq. (Hz)	Power (dBm)
Call Waiting Tone Indication	[200 (ms) On, 200 (ms) Off, 1000 (ms) On, 4000 (ms) Off, 1000 (ms) On, 4000 (ms) Off, 1000 (ms) On, 4000 (ms) Off], Repeat	425	-6
Call Hold Tone Indication	[4700 (ms) Off, 50 (ms) On, 200 (ms) Off, 50 (ms) On], Repeat	425	-6
RING phone	Cadence: [1000 (ms) On, 3000(ms) Off] Voltage: 45 VrmsFrequency: 25 Hz		

Tab. 25: GERMANY tones

GERMANY	Cadence	Freq. (Hz)	Power (dBm)
Dial Tone	Continuos	425	-15
Busy Tone	[480 (ms) On, 480 (ms) Off], Repeat	425	-15
Ringback Tone	[1000 (ms) On, 4000 (ms) Off], Repeat	425	-15
Confirmation Tone	[300 (ms) On][300 (ms) Off, 300(ms) On][600 (ms) Off, 300(ms) On]	950 1400 1800	-20
Congestion Tone	[240 (ms) On, 240 (ms) Off], Repeat	425	-15
Special Dial Tone (stuttering)	[500 (ms) On, 55 (ms) Off], Repeat	425	-15
Call waiting Tone	[200 (ms) On, 200 (ms) Off, 200 (ms) On, 5000(ms) Off], Repeat	425	-20
Network Busy Tone	[480 (ms) On, 480 (ms) Off], Repeat	425	-15
OnHook warning Tone	[480 (ms) On, 480 (ms) Off], Repeat	425	-15
Call Waiting Tone Indication	[200 (ms) On, 200 (ms) Off, 1000 (ms) On, 4000 (ms) Off, 1000 (ms) On, 4000 (ms) Off, 1000 (ms) On, 4000 (ms) Off], Repeat	425	-6
Call Hold Tone Indication	[4700 (ms) Off, 50 (ms) On, 200 (ms) Off, 50 (ms) On], Repeat	425	-6
RING phone	Cadence: [1000 (ms) On, 4000(ms) Off] Voltage: 45 VrmsFrequency: 25 Hz		

Appendix B

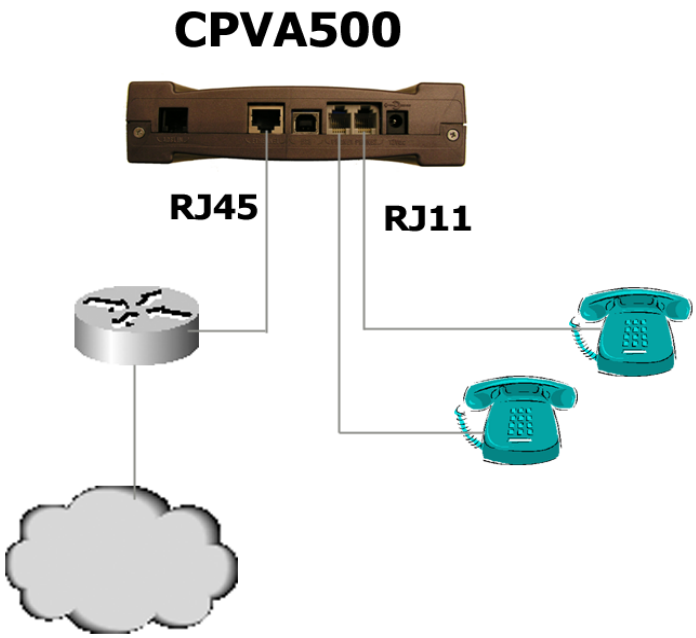
TELEPHONE ADAPTER FUNCTIONALITIES

The equipment can act as a telephone adapter between the two FXS ports and the RJ45 Ethernet interface. In this case, ADSL and Routing functionalities are not used.

In order to configure CPVA500 to work in this way, the following settings have do be performed:

- ADSL WAN interface has to be disabled.
- LAN configuration and VoIP configuration have to be completed.

The following figure illustrates the situation.



Appendix B

Glossary

Numbers

802.1p/q - Parts of the 802 protocol, that define the QoS on Layer 2.

802.3 - The IEEE standard for the definition of the CSMA/CD [Ethernet] medium access method for LANs.

A

Address-of-Record - An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

ADSL - Asymmetric Digital Subscriber Line: Modems attached to twisted pair copper wiring that transmit from 1.5 Mbps to 9 Mbps downstream (to the subscriber) and from 16 kbps upstream, depending on line distance.

ANSI - American National Standards Institute. An organisation responsible for coordinating and approving U.S. standards. Standards approved by ANSI are often called ANSI standards. ANSI is the U.S. representative to ISO.

ASCII - American Standard Code for Information Interchange. A standard character-to-number encoding widely used in the computer industry.

ATM - Asynchronous Transfer Mode: an ultra high speed cell-based data transmission protocol which may be run over ADSL.

Auto Crossing Port - When a port is auto crossing, it is not necessary to make a distinction between straight or cross CAT5 Ethernet Cable.

Autosensing Port - Network adapters that support both traditional and Fast Ethernet -- so-called 10/100 adapters -- choose the speed at which they run through a procedure called autosensing. Autosensing involves probing the capability of the network using low-level signalling techniques to select compatible Ethernet speeds. Autosensing was developed to make the migration from traditional Ethernet to Fast Ethernet products easier.

B

Glossary

Back-to-Back User Agent - A back-to-back user agent (B2BUA) is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior.

Bandwidth - Technically, the difference, in Hertz [Hz], between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, Ethernet has a bandwidth of 10Mbps.

bps - bits per second. A measure of the rate of data transmission.

BRI - ISDN Basic Rate Interface. The common form of ISDN with 2 Bearer Channels and one D Channel. All three channels are on a single copper pair and encoded with type 2B1Q coding.

Bridge - A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street. A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

Broadcast - A packet delivery system that delivers a copy of a given packet to all hosts attached to the network. For example, Ethernet.

C

Call Agent - a.k.a. Media Gateway Controller. Master device in MGCP architecture.

Central Office (CO) - is the office of your local carrier (LEC) closest to your location. Your circuit will be terminated to the CO closest to you and then connected to the closest Point of Presence (POP) of your chosen ISP.

Codec - Compression/decompression. Pertaining to adapters that compress and decompress video files. The letters "CODEC" represent "compression/ decompression"; in the past, they represented "coder/decoder".

Conference - A multimedia session that constrains multiple partecipants.

CPE - Customer Premises Equipment [i.e. CPV/CPL]. Equipment that is installed at customer sites to connect them to the provider's network.

D

Glossary

Dialog - A dialog is a peer-to-peer SIP relationship between two UAs that persists for some time. A dialog is established by SIP messages, such as a 2xx response to an INVITE request. A dialog is identified by a call identifier, local tag, and a remote tag. A dialog was formerly known as a call leg in RFC 2543.

Dialup - A temporary, as opposed to dedicated, connection between machines established over a standard phone line.

DHCP - Dynamic Host Configuration Protocol. TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses [out of a pool] from centrally-administered servers.

DMZ - Demilitarized Zone. It is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

DNS - (Domain Name System) is a protocol used to translate Internet domain and host names (such as www.speedguide.net) to IP addresses. DNS implements a distributed database to store name and address information for all public hosts on the Net, assuming IP addresses are statically assigned.

Domain - A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names [labels] separated by periods [dots], e.g., "machine.company.com".

DSLAM - Digital Subscriber Line Access Multiplexer: specifically, a device which takes a number of ADSL subscriber lines and concentrates these to a single ATM line.

DTMF - Dual-Tone Multi-Frequency. In telephone systems, multi-frequency signaling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol "#" or "*", the "*" being reserved for special purposes.

E

Ethernet - A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thinwire coaxial cable [10BASE2], thickwire coaxial cable [10BASE5], twisted pair cable [10BASET], or fibre optic cable.

F

Firewall - A firewall is a set of related programs that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall

Glossary

to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination.

FXS - Foreign Exchange Service. A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., "foreign", exchange, rather than the local exchange area's central office. A FXS line is normally connected to a standard telephone, fax or modem.

FTP - File Transfer Protocol. The TCP/IP standard, high-level protocol for transferring files from one computer to another over a network. FTP is also usually the name of the program that the user invokes to execute the protocol.

G

Gateway - A device linking two different types of networks that use different protocols [for example, between the packet network and the Public Switched Telephone Network].

Gatekeeper - A gatekeeper identifies, controls, counts, and supervises the traffic or flow through the network. It also provides functions such as terminal and gateway registration, address resolution, band-width control, and admission control.

H

H.323 - An umbrella standard for audio/video conferencing over unreliable networks; architecture and procedures are covered by this standard; H.323 relies on H.225 and H.245.

Header - A header is a component of a SIP message that conveys information about the message. It is structured as a sequence of header fields.

Home Domain - The domain providing service to a SIP user. Typically, this is the domain present in the URI in the address-of-record of a registration.

I

ICMP - Internet Control Message Protocol. The TCP/IP protocol used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram.

IGMP - Internet Group Management Protocol. Protocol used to dynamically register individual hosts in a multicast group on a particular LAN.

IEEE - Institute of Electrical and Electronics Engineers. A standard-making body in the U.S. responsible for the 802 standards for local area networks.

Glossary

Invitation - An INVITE request.

IP -Internet Protocol. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address - A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself.

IPsec - IP security. It is the Internet standard protocol for tunneling, encryption and authentication.

ISDN -Integrated Services Digital Network. A technology which combines voice and digital network services in a single medium, making it possible for telecommunications providers to offer customers digital data services as well as voice connections through a single "wire". The standards that define ISDN are specified by CCITT.

ISO - International Organisation for Standardisation. An international body that develops standards in many areas, including network protocols. It is best known for the seven-layer OSI [Open Systems Interconnection] suite of network protocols.

L

LAN - Local Area Network. Any physical network technology [such as Ethernet] that operates at high speed [typically 10 Mbits per second or more] over short distances [up to a few kilometres].

LED - Light Emitting Diode. A luminous indicator.

Location Service - A location service is used by a SIP redirect or proxy server to obtain information about a callee's possible location(s). It contains a list of bindings of address-of-record keys to zero or more contact addresses. The bindings can be created and removed in many ways; this specification defines a REGISTER method that updates the bindings.

Loop - A request that arrives at a proxy, is forwarded, and later arrives back at the same proxy. When it arrives the second time, its Request-URI is identical to the first time, and other header fields that affect proxy operation are unchanged, so that the proxy would make the same processing decision on the request it made the first time. Looped requests are errors, and the procedures for detecting them and handling them are described by the protocol.

M

MAC - Media Access Control. The lower portion of the data link layer. The MAC differs for various physical media.

MAC address -The hardware address of a device connected to a shared media. For example, the MAC address of a PC on an Ethernet is its Ethernet address.

Media Gateway Controller - See Call Agent.

Glossary

MGCP - Media Gateway Control Protocol. Protocol that specifies a Master/Slave architecture for decomposed gateways.

MIB - Management Information Base. The set of parameters an SNMP management station can query or set in the SNMP agent of a network device [e.g., router]. Standard MIBs have been defined, and vendors can develop private MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB.

Modem - Modulator/demodulator. A device that takes digital data from a computer and encodes it in analogue form for transmission over a phone line.

Multicast - A special form of broadcast where copies of the packet are delivered to only a subset of all possible destinations.

N

NAT - Network Address Translation - also called IP masquerade, is a process of translating the source header of IP packets so they will be routable across wide area networks.

Network - A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs, MANs or WANs.

Network address - The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique.

O

OSI - Open Systems Interconnection. A suite of protocols, specifically ISO standards, to be the international standard computer network architecture.

P

Packet - The unit of data sent across a network. "Packet" is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units.

Packet switching - Communications paradigm in which packets [messages] are individually routed between hosts, with no previously established communication path.

PAT - Port Address Translation. It is the process where packets arriving to a particular IP address/port can be translated and thus redirected to a different IP/port. This functionality is a way to create a persistent passage through NAT.

Glossary

PPPoA - (point-to-point protocol over ATM) A standard very similar to PPPoE (point-to-point protocol over Ethernet), with some minor differences, for example a DSL modem pumping ATM is internal to the computer, rather than being an ethernet cable away. PPPoA allows for MTUs (maximum transmission units) of 1500, as opposed to PPPoE.

PPPoE - (Point-to-Point Protocol over Ethernet) is a method for building PPP sessions and encapsulating packets, as described in RFC2516. Although it is not a standard, PPPoE is already being used by a number of DSL providers. It requires either routers that have built-in PPPoE support, or PPPoE software to "dial up" and establish the session.

Protocol - A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces [e.g., the order in which bits and bytes are sent across a wire] or high-level exchanges between allocation programs [e.g., the way in which two programs transfer a file across the Internet].

Proxy - A proxy server is an intermediate gateway that sits between a client PC and the Internet and provices forwarding/caching service, as well as security, logging and administrative control. A caching web proxy server saves content (such as Web pages) in its local cache the first time a request is made, and then serves the pages to other local clients from cache, without the need to forward the request to the Internet. Pages are only requested from the Internet if they are not found in cache. The proxy server forwards requests acting as a client, with its own IP address, and then in turn serves the pages to local clients. Caching proxy servers offer transparent service to clients, they can save bandwidth and improve performance, however they can also cause slowdowns when congested, as well as some problems delivering dynamic and secure content.

R

RAS - Reliability, availability, and serviceability. Rated throughput for data links, the rate at which all of the offered frames are forwarded by the device.

RFC - Request for comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

RIP - (Routing Information Protocol) A protocol in which routers periodically exchange information with one another so that they can decide minimum distance paths between sources and destinations.

Router - A system responsible for making decisions about which of several paths network [or Internet] traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics".

RTCP - Real-time transport control protocol. Is the counterpart of RTP that provides control services.

Glossary

RTP - Real-time transport protocol. Provides end-to-end delivery services of real-time audio and video.

S

Serial - A method of transmission in which each bit of information is sent sequentially on a single channel rather than simultaneously as in parallel transmission.

SNMP - Simple Network Management Protocol. The Internet standard protocol developed to manage nodes on an IP network.

T

TCP - Transmission Control Protocol. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

TFTP - Trivial File Transfer Protocol. The TCP/IP standard protocol for file transfer with minimal capability and minimum overhead, based on UDP. It is often used by diskless workstations that keep software in ROM and use it to bootstrap themselves. It is used in the router for downloading patches.

Throughput - (or transfer rate) in data transmission is the amount of data moved successfully from one place to another in a given time period. For data networks, throughput is usually measured in number of bits per second (bps) that are transmitted, also quoted as Kiobits per second (Kbps) or Megabits per second (Mbps).

Tunneling - refers to the ability to encapsulate packets of data formatted for one network protocol (or a private secure network) in packets used by another protocol (or a public network). Tunneling allows the use of the (public) Internet to transfer data on behalf of a private network. See also: VPN, PPTP. Note that tunneling and VPN is not intended as a substitute for data encryption by itself. For a higher security level strong encryption should be used within the VPN.

U

Unicast - A packet broadcast to a single host attached to the network.

User Agent Client - A user agent client (UAC) is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction.

User Agent Server - A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other

Glossary

words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction.

V

VLAN - Virtual Local Area Network. Secure connection of TCP/IP based networks, intranets and extranets across the Internet.

VoIP - Voice Over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

VPN - Virtual Private Network. A private network of computers that's at least partially connected by public phone lines. A good example would be a private office LAN that allows users to log in remotely over the Internet (an open, public system). VPNs use encryption and secure protocols like PPTP to ensure that data transmissions are not intercepted by unauthorized parties.

W

WAN -Wide Area Network. Any physical network technology that spans large geographic distances. WANs usually operate a slower speeds than LANs or MANs.

WWW - World Wide Web. A hypertext-based, distributed information system based on a client-server architecture. Web browsers [client applications] request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs [Uniform Resource Locators].

Glossary

Index

NUMERICS

A

B

C

D

E

F

G

Index

Index

S

T

U

V

W

Index

Offices

Treviso Headquarters and Training Site
Viale dell'Indutria, 1
31055 Quinto di Treviso (TV)
Italy

ph. (+39) 0422 470840
fax. (+39) 0422 470920

telsey
telecommunications

to enable the future

http://www.telsey.com - e-mail: support@telsey.it