INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# FS-VDSL
# FGTS

# Full-Service VDSL

## Focus Group
## Technical Specification

---

## Part 3: Customer Premises Equipment

Version 1.0.0
5 June 2002

**ITU-T STUDY GROUP 16 "MULTIMEDIA SERVICES, SYSTEMS AND TERMINALS"**

**FULL-SERVICE VDSL FOCUS GROUP**

FOCUS GROUP TECHNICAL SPECIFICATIONS SERIES

| FOCUS GROUP TECHNICAL SPECIFICATIONS | | |
|---|---|---|
| FULL-SERVICE VERY HIGH-SPEED DIGITAL SUBSCRIBER LINE | | **Version control:** |
| Part 1: | Operator Requirements | Version 1.00 / 5 June 2002 |
| Part 2: | System Architecture | Version 1.00 / 5 June 2002 |
| Part 3: | Customer Premises Equipment | Version 1.00 / 5 June 2002 |
| Part 4: | Physical Layer Specification for Interoperable VDSL Systems | Version 1.00 / 5 June 2002 |
| Part 5: | Operations, Administration and Maintenance & Provision aspects for FS-VDSL Services | Version 1.00 / 5 June 2002 |

## FOREWORD

The procedures for establishment of a Focus Group are defined in Rec.A.7. After assessment of the requirements in A.7 the TSB Director decided in consultation with the SG 16 management to follow provisions under clause 2.1.1/A.7 for the establishment of Focus Groups between study group meetings. The FGRC for the Full-Service Very-high-speed Digital Subscriber Line (FS-VDSL) Focus Group met on 3 May 2002 and agreed to proceed with the steps for the establishment of the FS-VDSL Focus Group, having ITU-T Study Group 16 as parent stuffy group. The formalities laid down in ITU-T Rec. A.7 were completed on 10 May 2002 and the formal approval of the Focus Group by ITU-T SG 16 took place on [24 October 2002].

Even though Focus Groups have an ITU-T Study Group as a parent organization, Focus Groups are organized independently from the usual operating procedures of the ITU, including financial independence. Texts approved by Focus Groups (including its Technical Specifications) do not have the same status of ITU-T Recommendations.

## INTELLECTUAL PROPERTY RIGHTS

The Focus Group draws attention to the possibility that the practice or implementation of this Technical Specification may involve the use of a claimed Intellectual Property Right. The Focus Group takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by Focus Group members or others outside of the Technical Specification development process.

As of the date of approval of this Technical Specification, the had Focus Group received notice of intellectual property, protected by patents, which may be required to implement this Technical Specification. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the FS-VDSL patent database.

# ITU-T FS-VDSL Focus Group Technical Specification 1

## Part 3: Customer Premises Equipment specification

**Summary**

This text provides a framework for the VDSL Customer Premises Equipment Specification (CPE) within the ITU-T FS-VDSL Focus Group established under ITU-T Study Group 16 "Multimedia services, systems and terminals.". It is meant to facilitate the standardization of VDSL CPE for mass deployment. It covers Service Requirements, Reference Model, System Functionalities, and Interface Specifications.

This document references other standards that currently exist or are in development.

**Source**

This Technical Specification was produced by the **CPE-SA** Working Group of the ITU-T FS-VDSL Focus Group. Comments on this document are welcome comments. Please refer to the FS-VDSL web site at http://www.fs-vdsl.net for contact details and to download comment form.

**CONTENTS**

**Page**

# ITU-T FS-VDSL Focus Group Technical Specification 2

# Part 2: CUSTOMER PREMISES EQUIPMENT SPECIFICATIONS

## 1. Scope

The CPE working group of the FS-VDSL Committee has produced this specification to address the distribution of video, data and voice services in an in-home environment having a high bit rate DSL broadband access connectivity. The present document aims at defining an architecture that enables the provision of a bundle of these services in a reliable way, with minimal user intervention, respecting the key requirements of security and conditional access to the contents and at a cost compatible with mass market deployment. It is based on published industry wide standards, profiled for the specific purposes of high bit rate DSL connectivity.

Note that this document is intended to specify the CPE architecture at a high level, independent of the underlying broadband physical layer transport mechanism. VDSL is referenced throughout the document as the physical layer technology; however, the architectural specifications contained herein should be equally applicable to CPEs employing other broadband physical layer technologies.

## 2. Abbreviations

This specification uses the following abbreviations:

| | |
|---|---|
| **AAL** | ATM Adaptation Layer |
| **ANSI** | American National Standard Institute |
| **API** | Application Programming Interface |
| **ATM** | Asynchronous Transfer Mode |
| **BAS** | Broadband Access Server |
| **BLES** | Broadband Loop Emulated Services |
| **CBR** | Constant Bit Rate |
| **CHAP** | Challenge Handshake Authentication Protocol |
| **CO** | Central Office |
| **CPE** | Customer Premises Equipment |
| **DAVIC** | Digital Audio-VIsual Council |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DSL** | Digital Subscriber Line |
| **DSM-CC** | Digital Storage Media – Command and Control |
| **DVB** | Digital Video Broadcasting |
| **DVD** | Digital Versatile Disc |
| **EAS** | Emergency Alert System |
| **ETSI** | European Telecommunication Standards Institute |
| **EMS** | Element Management System |
| **ER** | Edge Router |
| **FCC** | Federal Communications Commission |
| **FPD** | Functional processing and Decoding |
| **FSAN** | Full Service Access Network |
| **FTP** | File Transfer Protocol |
| **HPNA** | Home Phone Networking Alliance |

| | |
|---|---|
| **HTTP** | Hyper Text Transfer Protocol |
| **HW** | Hardware |
| **ICMP** | Internet Control Message Protocol |
| **IGMP** | Internet Group Management Protocol |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **ILMI** | Integrated Local Management Interface |
| **IP** | Internet Protocol |
| **IPCP** | PPP Internet Protocol Control Protocol |
| **LCP** | Link Control Protocol |
| **LT** | Line Termination |
| **MAC** | Medium Access Control |
| **MCM** | Multi-Carrier Modulation |
| **MIB** | Management Information Base |
| **MPOA** | Multi-Protocol Over ATM |
| **NAPT** | Network Address and Port Translation |
| **NAT** | Network Address Translation |
| **NSP** | Network Service Provider |
| **NT** | Network Termination |
| **ODN** | Optical Distribution Network |
| **OSI** | Open System Interconnection |
| **OTU – C** | Optical Terminal Unit – Central Office side |
| **OTU-R** | Optical Terminal Unit – Remote side |
| **PAP** | Password Authentication Protocol |
| **PAT** | Port Address Translation |
| **PPP** | Point-to-Point Protocol |
| **PPTP** | Point-to-Point Tunnelling Protocol |
| **PS** | Service Splitter (POTS or ISDN Splitter) |
| **PVC** | Permanent Virtual Circuit |
| **QoS** | Quality of Service |
| **RFC** | Request for Comment (IETF standard) |
| **RIP** | Routing Information Protocol |
| **RTP** | Real Time Protocol |
| **RTSP** | Real Time Streaming Protocol |
| **SAR** | Segmentation And Reassembly |
| **SCM** | Single Carrier Modulation |
| **SCSI** | Small Computer System Interface |
| **SIP** | Session Initiation Protocol |
| **SNMP** | Simple Network Management Protocol |
| **SVC** | Switched Virtual Circuit |
| **SW** | Software |

| | |
|---|---|
| **TE** | Terminal Equipment |
| **TFTP** | Trivial File Transfer Protocol |
| **TM** | Transmission and Multiplexing (ETSI Technical Committee) |
| **UBR** | Unspecified Bit Rate |
| **USB** | Universal Serial Bus |
| **UTOPIA** | Universal Test and Operational PHY Interface for ATM |
| **VBR** | Variable Bit Rate |
| **VDSL** | Very high bit rate Digital Subscriber Line |
| **VoD** | Video on Demand |
| **VoIP** | Voice over IP |
| **VPN** | Virtual Private Network |
| **VTU-C** | VDSL Terminal Unit – Central Office |
| **VTU-R** | VDSL Terminal Unit – Remote |
| **VTP** | VDSL Termination Processing |
| **VTPD** | VTP and Decoding |
| **VTP/D** | VTP or VTPD |

## 3. Definitions

This specification defines the following term:

### 3.1. Access Network (AN) Domain

The AN Domain encompasses the domain between the U-R and V interface of the system reference model.

### 3.2. Core Network Domain

The Core Network Domain takes place beyond the V interface and the OLT physical interface.

### 3.3. Service Domain

The Service Domain includes the physical equipment of multiple or single service nodes that interface the Core/AN and provide users access to various services including data connection, broadcast video, VoD, and voice.

### 3.4. FP

Functional Processing. A point of signal transformation or processing.

### 3.5. FPD

Functional Processing and Decoding. Typically terminals performing the application layer processing of video, audio and data, e.g. set top boxes (STB).

### 3.6. VTP

VDSL Termination Processing. Refers to the unit that operates the VDSL modem termination and protocol processing functions. A device that implements the VTP functions includes Ethernet based layer-2 interface to the in-home Network.

### 3.7. VTPD

VTP and Decoding. Refers to a unit that operates the video decoding function as well as the VTP functions and interfaces.

### 3.8. VTP/D

When mentioned in this document, refers to both the VTP and the VTPD

### 3.9. Residential Centralized Model

When mentioned in this document, refers the use of the VTPD as the decoding unit.

### 3.10. Residential Distributed Model

When mentioned in this document, refers to the use of multiple STBs that are connected to the VTP through the in-home LAN.

## 4. References


[1] DSL FORUM: TR-001 ADSL ForumSystem Reference Model, *DSL Forum*, May 1996

[2] T1.424-trial use: Very-high-bit-rate Digital Subscriber Line (VDSL) Metallic Interface, Part 1: Functional Requirements and Common Specification", *T1E1*, August 2000

[3] T1.424-trial use:Very-high-bit-rate Digital Subscriver Line (VDSL) Metallic Interface, Part 2: Technical Specification for a Single-Carrier Modulation (SCM) Transceiver", *T1E1*, August 2000

[4] T1.424-trial use:Very-high bit-rate Digital Subscriber Line (VDSL) Metallic Interface, Part 3: Technical Specification of a Multi-Carrier Modulation Transceiver", *T1E1*, August 2000

[5] ETSI: TS 101 270-1 V1.2.1 "Transmission and Multiplexing (TM); Access transmission systems on metallic access cables; Very high speed Digital Subscriber Line (VDSL); Part 1: Functional requirements", *ETSI*, October 1999

[6] ETSI: draft TS 101 270-2 V1.1.1 "Transmission and Multiplexing (TM); Access transmission systems on metallic access cables; Very high speed Digital Subscriber Line (VDSL); Part 2: Transceiver requirements", *ETSI*, December 1999

[7] FSAN: "Full Services Access Network Requirements Specification", Issue 3, *FSAN*, August 1998

[8] FS-VDSL Operators WG: FS-VDSL Part 1: Operator Requirements, FS-VDSL, May 2002

[9] FS-VDSL System Architecture WG: FS-VDSL Specification Part 2: System Architecture, *FS-VDSL*, May 2002

[10] FS-VDSL VDSL WG: FS-VDSL Specification Part 4: Interoperable VDSL Systems, *FS-VDSL*, May 2002

[11] FS-VDSL OAM WG: FS-VDSL Specification Part 5: OAM Specification, *FS-VDSL*, May 2002

[12] ITU-T: Recommendation I.363.2, B-ISDN ATM Adaptation Layer specification: Type 2 AAL, *ITU*, 2000

[13] ITU-T: Recommendation I.363-5, B-ISDN ATM Adaptation Layer specification: Type 5 AAL, *ITU*, 1996

[14] ATM Forum: Specification AF-ILMI-0065.000: Integrated Local Management Interface (ILMI) specification, *ATM Forum*, September 1996

[15] ATM Forum: Specification AF-NM-0122.000: Auto-configuration of PVC, *ATM Forum*, May 1999

[16] DSL Forum: Technical Report TR-037: Auto-configuration for the connection between the DSL broadband network termination (B-NT) and the network using ATM, *DSL Forum*, March 2001

[17] ATM Forum: Specification AF-tm-0121.000: Traffic Management V4.1, *ATM Forum*, March 1999

[18] ATM Forum: Specification AF-UNI-0010.002: ATM User-Network Interface Specification v3.1, *ATM Forum*, 1994

[19] ATM Forum: Specification AF-SIG-0061.002: ATM User Network Interface (UNI) Signalling Specification, *ATM Forum*, April 2002

[20] ITU-T: Recommendation Q.2931: Digital Subscriber Signalling System No. 2 – User-Network Interface (UNI) layer 3 specification for basic call/connection control, *ITU*, 1995

[21] IETF: RFC 792: Internet Control Message Protocol, *IETF*, September 1981

[22] IETF: RFC 2131: Dynamic Host Configuration Protocol, *IETF*, March 1997

[23] IETF: RFC 2132: DHCP Options and BOOTP Vendor Extensions, *IETF*, March 1997

[24] IETF: RFC 2364: PPP Over AAL5, *IETF*, July 1998

[25] IETF: RFC 2684: Multiprotocol Encapsulation over ATM Adaptation Layer 5 , *IETF*, September 1999

[26] IETF: RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE), *IETF*, February 1999

[27] IETF: RFC 3022: Traditional IP Network Address Translator (Traditional NAT), *IETF*, January 2001

[28] IETF: RFC 1058: Routing Information Protocol, *IETF*, June 1988

[29] IETF: RFC 2453: Routing Information Protocol version 2, *IETF*, November 1998

[30] IETF: RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, *IETF*, December 1998

[31] IETF: RFC 2475: An Architecture for Differentiated Services, *IETF*, December 1998

[32] IETF: RFC 1112: Host Extensions for IP Multicasting, *IETF*, August 1989

[33] IETF: RFC 2236: Internet Group Management Protocol, Version 2, *IETF*, November 1997

[34] DSL Forum: Technical Report TR-018: References and Requirements for CPE Architectures for Data Access, *DSL Forum*, May 1999

[35] DSL Forum: Technical Report TR-032: CPE Architecture Recommendations for Access to Legacy Data Networks, *DSL Forum*, May 2000

[36] DSL Forum: Technical Report TR-43: Architecture and Transport: Protocols at the U Interface for Accessing Data Networks using ATM/DSL, *DSL Forum*, August 2001

[37] IETF: RFC 2637: Point-to-Point Tunneling Protocol (PPTP), *IETF*, July 1999

[38] IETF: RFC 1889: RTP: A Transport Protocol for Real-Time Applications, *IETF*, January 1996

[39] ETSI: TS 101 224 V1.1.1: Digital Video Broadcasting (DVB); Home Access Network (HAN) with an active Network Termination (NT), *ETSI*, 1998

[40] DAVIC: Specification V1.3, Part 7: High and Mid Layer Protocols, *DAVIC*, September 1997

[41] IETF: RFC 1112: Internet Group Management Protocol V1, *IETF*, August 1989

[42] ISO/IEC 13818-6: International Standard, ISO/IEC JTC1/SC29/WG11 MPEG96/N1300p1, : "Information Technology - Generic Coding of Moving Pictures and Associated Audio: Digital Storage Media Command and Control", *ISO-IEC*, 1996

[43] IETF: RFC 2326:Real Time Streaming Protocol (RTSP), *IETF*, April 1998

[44] DSL Forum: Technical Report TR-039: Requirements for Voice over DSL V1.1, *DSL Forum*, March 2001

[45] ITU-T: Recommendation I.610: B-ISDN operation and maintenance principles and functions, , 1999

[46] ATM Forum: Specification af-vmoa-0145.0000: Voice and Multimedia over ATM: Loop Emulation Service using AAL2, *ATM Forum*, July 2000

[47] ITU-T: Recommendation I.366.1: Segmentation and Reassembly Service Specific Convergence Sub-layer for the AAL type 2, *ITU*, 1998

[48] ITU-T: Recommendation I.366.2: AAL type 2 service specific convergence sublayer for narrow-band services, *ITU*, 2000

[49] ITU-T: Recommendation H.323:Packet-Based Multimedia Communications Systems, *ITU*, 2000

[50] ITU-T: Recommendation H.248: Gateway control protocol, *ITU*, 2000

[51] IETF: RFC 2543: Session Initiation Protocol, *IETF*, March 1999

[52] IETF: RFC 1157: A Simple Network Management Protocol (SNMP), *IETF*, May 1990

[53] IETF: RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II, *IETF*, March 1991

[54] IETF: RFC 1350: THE TFTP PROTOCOL (REVISION 2), *IETF*, July 1992

[55] IETF: RFC 951: BOOTSTRAP PROTOCOL (BOOTP), *IETF*, September 1985

[56] IETF: RFC 1542: Clarifications and Extensions for the Bootstrap Protocol, *IETF*, October 1993

[57] IETF: RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1, *IETF*, June 1999

[58] IEEE: 802.3: Part 3: Carrier Sense Multiple Access with collision detection (CSMA/CD) access method and physical layer specification, *IEEE*, 2002

[59] IEEE: 802.1D: Media Access Control (MAC) Bridges, *IEEE*, 1998

[60] IETF: RFC 1332: The PPP Internet Protocol Control Protocol (IPCP), *IETF*, May 1992

[61] IETF: RFC 1877: PPP Internet Protocol Control Protocol Extensions for Name Server Addresses, *IETF*, December 1995

[62] IETF: RFC 2233: The Interfaces Group MIB using SMIv2, *IETF*, November 1997

[63] ATM Forum: AF-VMOA-0175.000, Loop Emulation Service using AAL2 File Transfer, ATM Forum, October 2001

[64] DSL Forum: TR-027: SNMP-based ADSL LINE MIB, *DSL Forum*, November 1999

[65] IETF: RFC 1901: Introduction to Community-based SNMPv2, *IETF*, January 1996

## 5. Terminology Used

In this document several words (often capitalized) are used to signify requirements.

MUST — This word, or the adjective "required," means that the definition is an absolute requirement of the specification.

MUST NOT — This phrase means that the definition is an absolute prohibition of the specification.

SHOULD — This word, or the adjective "recommended," means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.

MAY — This word, or the adjective "optional," means that this item is one of an allowed set of alternatives. An implementation, that does not include this option, MUST be prepared to interoperate with another implementation, that does include the option.

## 6. CPE System Reference Model

### 6.1. Reference Model

Several views of the reference model for FS-VDSL CPE are presented in this section. The Reference model in the following Figures shows the provision of the three basic service (video, data and voice) application (App) types at multiple locations within the premises.

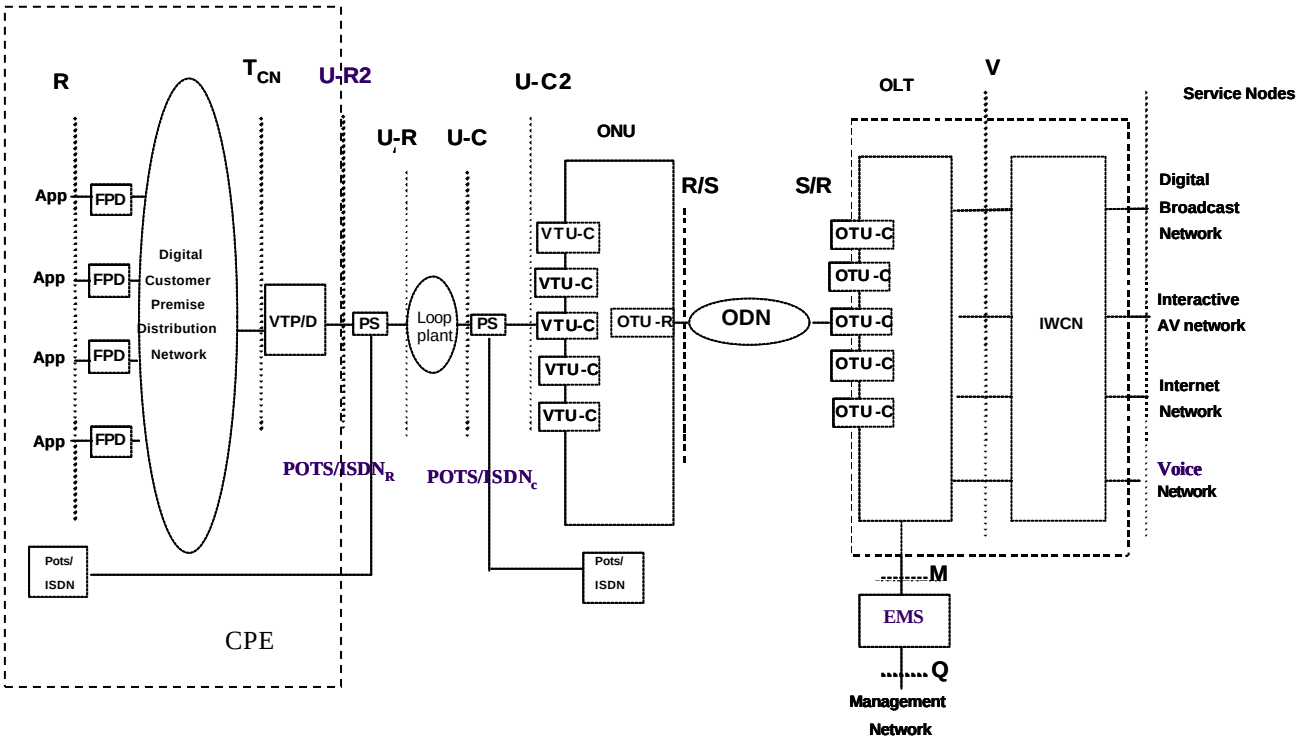



**Figure 1: FS-VDSL reference model with the CPE domain highlighted**

The functional reference model depicted in Figure 1 details the FS-VDSL architectural components. The following functional components fall within the domain of this document, the customer premises equipment. A complete set of definitions is given in the FS-VDSL Part 2 [9].

- **FP** (Functional Processing) is a point of signal transformation or processing
- **FPD** (Functional Processing and Decoding) is function of video, audio, or data decoding.

- **VTP** (VDSL Termination Processing) refers to the function of VDSL modem termination, and protocol processing. A device that implements the VTP function includes interfaces to the in-home network.
- **VTPD** (VTP and Decoding) refers to both the functions of VTP and of video decoding.
- **VTP/D** – Either a VTP or a VTPD.
- **AN (Access Network)** – is the part of the reference model included between U-R2 and the V interface.

Note that from the point of view of the access network, the functionality and interfaces of the VTPD are identical to a VTP.

The relevant architecture reference points are described in Table 1.

**Table 1: Architecture reference points**

| Reference Point | Location |
|---|---|
| U-R | The network side input of the POTS or ISDN splitter |
| U-R2 | The network side input of the VDSL Modem |
| $T_{CN}$ | The output (input) of the digital port(s) of the VTP/D towards (from) the digital network at the customer premises |
| R | The output (input) of the FPD towards (from) the Home appliance |

In an FS-VDSL customer premises environment, one may find the following types of equipment:

- A service splitter **PS**, which electrically separates the VDSL signals from other low frequency services (such as POTS or ISDN). This is the PS box in Figure 1 between the UR and U-R2 interfaces.
- A VDSL modem, a.k.a. VTU-R, which functionalities are described in [10]. This is covered by the VTP or VTPD functions.
- Protocol processing and in-home distribution interfaces. This is covered by the VTP function
- MPEG Decoding units for the viewing of broadcast video and VOD. This is covered by the VTPD and FPD functions.
- PCs, customer premise devices, and other home appliances that connect to IP data services. These are covered by the FPD functions.
- Analogue or digital voice devices that connect to VoATM or VoIP services. These are also covered by the FPD functions.

Physical implementations of FS-VDSL CPE may perform all processing and decoding in a single customer premise device or distribute functional processing and decoding into two or more customer premise devices. The FP, FPD, VTP, or VTPD elements may be combined to describe the following alternative architectures:

- Distributed refers to an architecture in which several FPD elements are interconnected together as shown in Figure 2. These elements contain functional processors and possibly the home appliance itself. The VTP element contains the VDSL modem, together with a protocol and functional processor as well.
- Centralized refers to an architecture in which most if not all processing and decoding is performed within the same physical box termed VTPD as shown in Figure 3. Internal to this box, functional processing and digital signal distribution through busses is also taking place.

When the CPE is a combination of centralized and distributed architectures, the $T_{CN}$ interface must be provided to the VTPD for connecting to the distributed components.

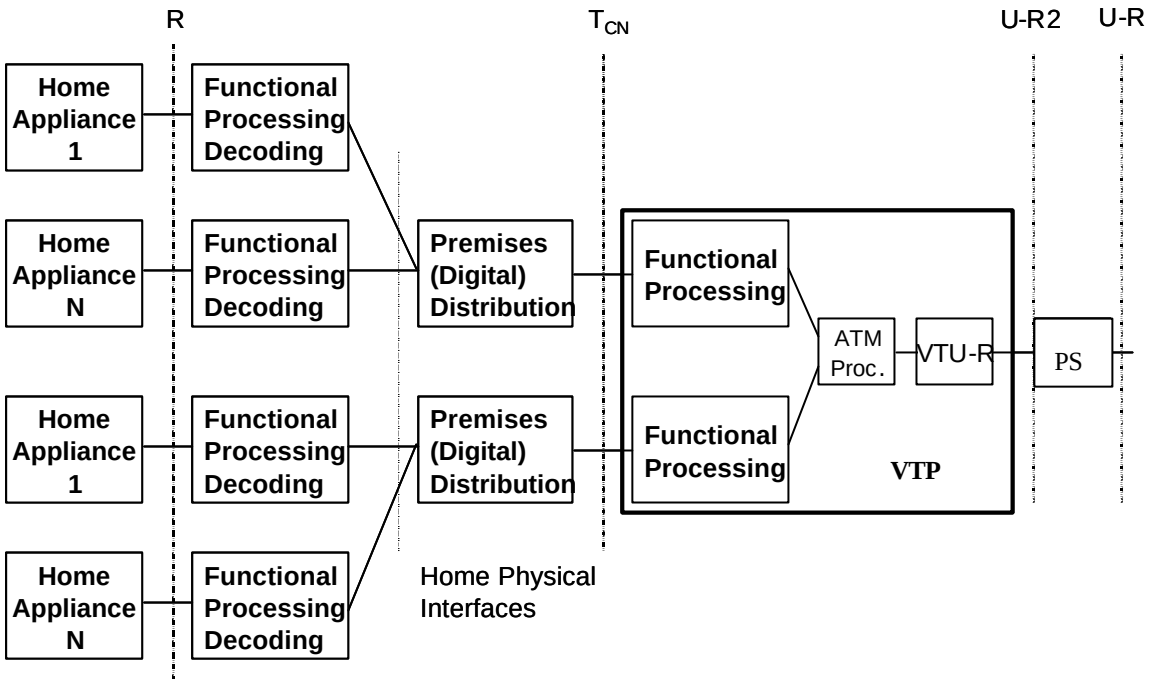



**Figure 2: VTP grouping which implements a fully distributed CPE approach**

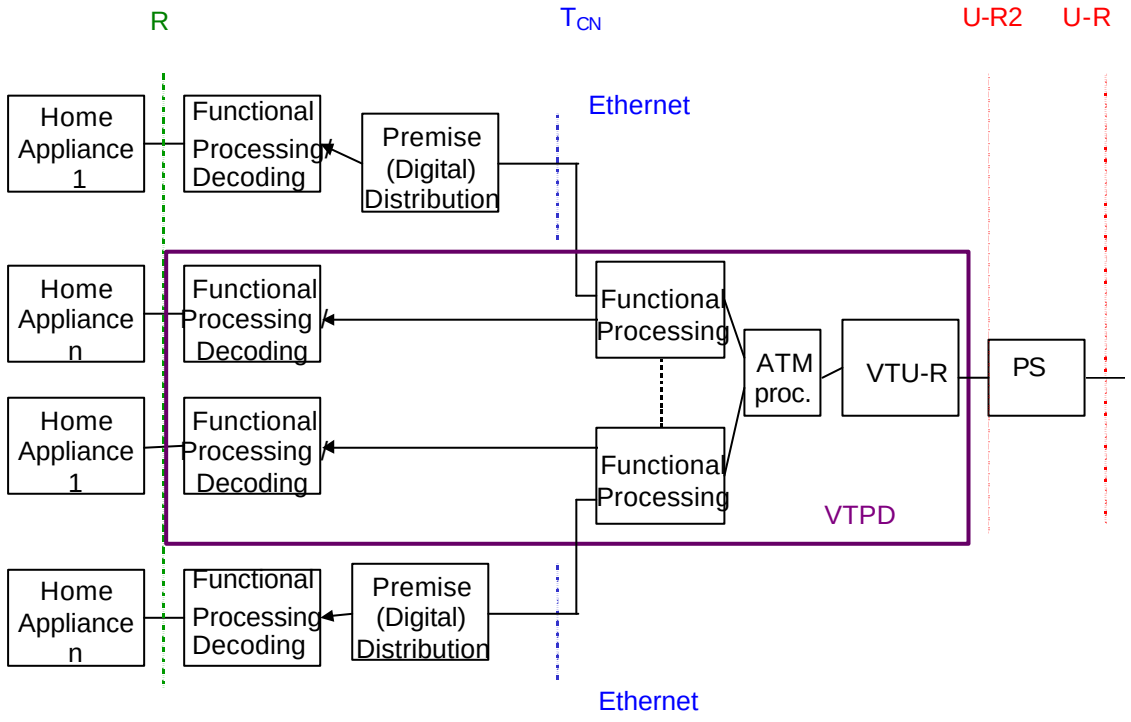



**Figure 3: VTPD grouping which implements a centralized CPE approach with optional distributed FPs.**

### 6.2. Interfaces and Reference Model Elements Description

In this section, the interfaces will be defined according to the assumption that the CPE elements are interconnected following a VTP (distributed) architecture. This does not preclude the implementation of an integrated VTPD (centralized) CPE architecture, as options for interfaces will allow it.

#### 6.2.1 VTP Interface(s)

The VTP contains the VDSL modem (VTU-R) and also some protocol processing functions. The VTP interfaces are defined in section 8.2 of the FS-VDSL Part 2 [9].

#### 6.2.2 FPD to Home Appliances Interfaces

The FPD to Home Appliance interfaces (point (R) in Figure 2) may include technologies shown in Table 2. Further details can be found in [10].

**Table 2: Example Interface(s) at the Home Appliance (towards the final deliver means)**

| |
|---|
| Coaxial Cable (RF modulated composite video) |
| S-Video |
| Composite Video |
| Component Video |
| SCART |
| Dolby Digital/AC-3 |
| L/R Stereo |
| Telephone line |
| Ethernet |
| USB |
| IEEE 1394 |
| 5-channel analogue audio |
| SCSI |
| LPDT parallel |
| RS-232 serial |
| Bluetooth |
| IR Emitter (for control of IR controlled devices) |
| HomeRF |

### 6.2.3 Example Functional Processing/Decoding (FPD) connected to the home appliance

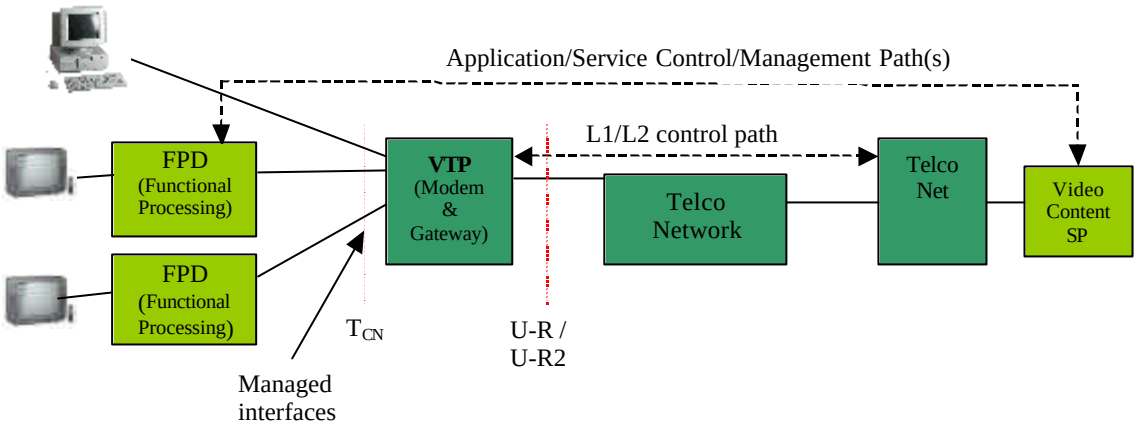
Table 3 shows some example types of decoding that may be performed in a FPD.

**Table 3: Example Functional Processing**

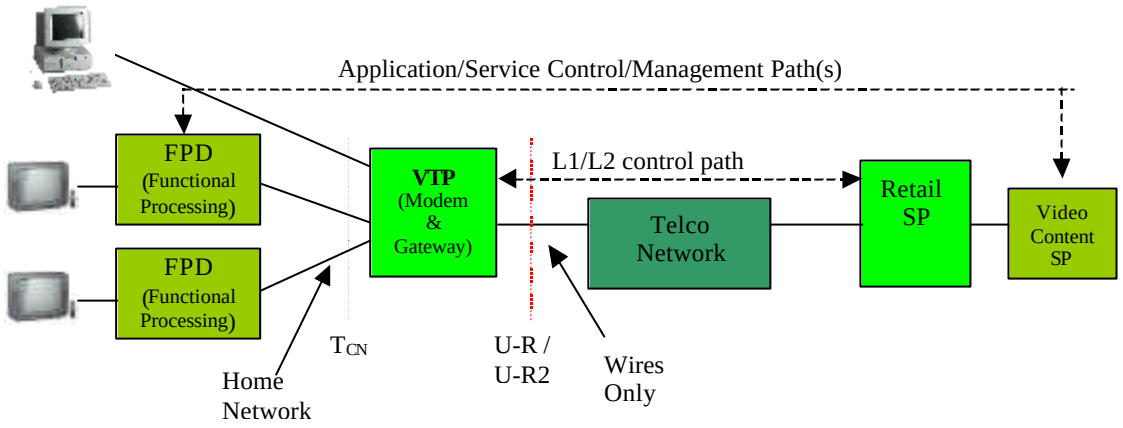
| **Digital Decoding** |
|---|
| • MPEG-1 or 2 video decoding<br>• MPEG-4 video decoding<br>• H.323 Video<br>• MPEG audio / MP3decoding<br>• Dolby Digital (AC-3/AAC)<br>• Decryption and De-scrambling<br>• Conditional Access processing<br>• Rights Management processing<br>• Application processing<br>• Middleware<br>• IP Data processing<br>• Remote Control and Management<br>• RF<br>• IR<br>64 kbps PCM for derived voice services |
| **Encoding Analogue information** |
| • NTSC/PAL/SECAM video encoding<br>• Analogue A/V output<br>• Copy Protection processing |
| **Coaxial Delivery** |
| • Frequency modulation |
| **Derived voice decoding** |

### 6.3. CPE Interface points

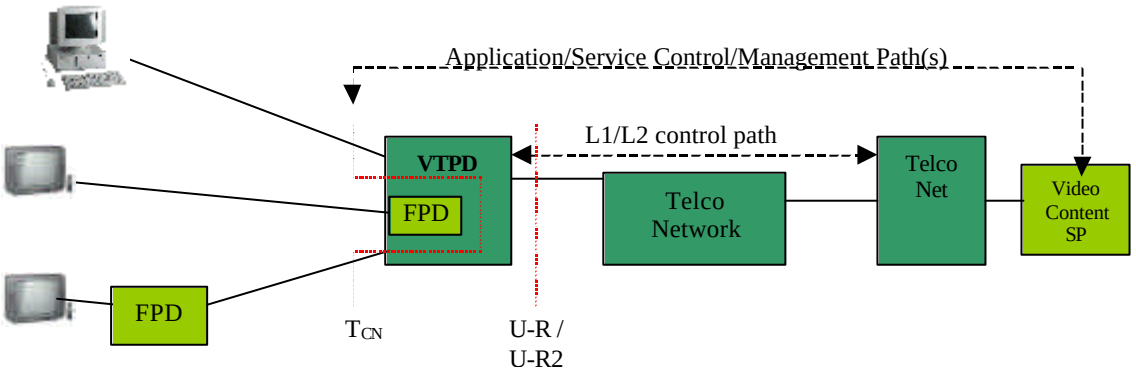
Some providers may include the equipment providing the VTP or VTPD functions as part of their service offering. This is illustrated in parts (a) and (c) in Figure 4. Alternatively, network providers may provide a service at the U-R or U-R2 differentiation point, and therefore the VTP or VTPD functions are provided by the service providers. The VTP case is shown in parts (b) in Figure 4. Interface U-R2 includes the cabling from the splitter U-R interface up to the VTP connector. Control by the provider for QoS and Management may extend to the $T_{CN}$ interface or even to the R interface, depending on the implementation. The home service delivery control extends through the FPD. The demarcation points may vary based on network operator and regulatory requirements.




(a)




(b)




(c)

**Figure 4: Reference Model showing business solutions**

(a) The VTP is controlled by the network domain and the service offerings are managed interfaces.
(b) The VTP is controlled by the service provider
(c) Instead of the VTP in (a) a VTPD is shown.

## 7. Architecture Overview and Packet Flows

The VTP contains a hybrid architecture with layer-3 data forwarding and layer-2 bridging to some protocols in the home network digital distribution. Examples of this layer-2 bridging include PPPoE (as per RFC 2516 [26]) and 802.1 bridging [59]. The integration of a layer-3 router function in the VTP allows sharing an Internet access. The hybrid architecture simultaneously allows terminals with shared (layer-3) and terminals with direct (layer-2) Internet connections to service providers.

An example of a layer-2 and layer-3 concurrent stack is shown in Figure 5. Each functionality is described in more detail in the following subsections. If functional processing or decoding is included in the unit, the centralized VTPD stack to the home appliances is shown in Figure 6.

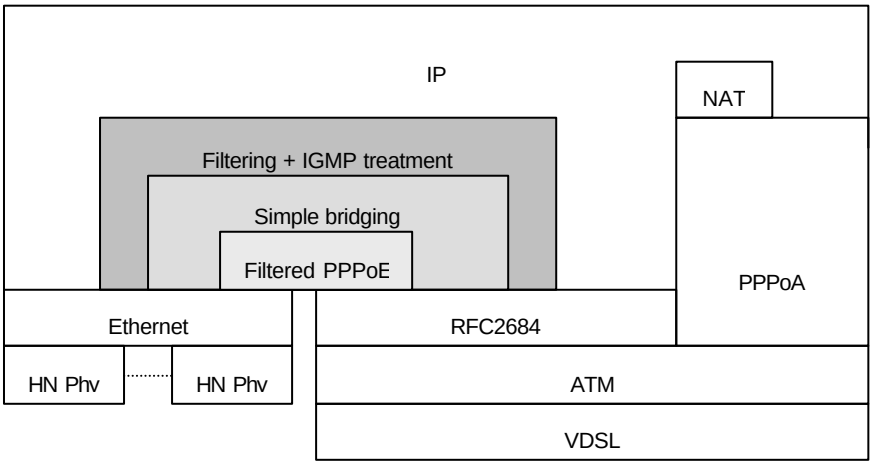



**Figure 5: An example of a hybrid VTP protocol stack**

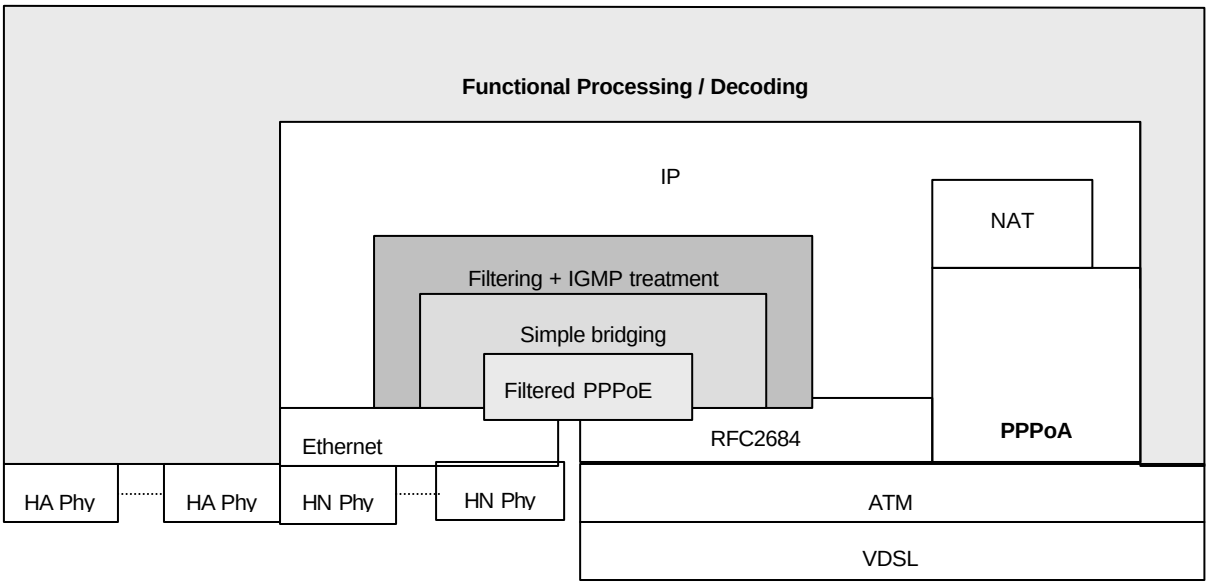



**Figure 6: An example of a hybrid VTPD protocol stack**

The VTP/D MUST be:

1. Hardware ready to support all the connections described in section 7.1
2. Software upgradable through the network to enhance and support additional flow/connection capabilities.

Section 7.1 describes the set of packet flows required within the VTP architecture to provide layer-2 and layer-3 data forwarding. End-to-end protocol outside the home is described in the System Architecture document [9].

### 7.1. Packet flows across the U-R2 reference point

This section defines six required basic packet flows and 1 optional (BLES) packet flow of an FS-VDSL VTP/D across the U-R2 Reference point. The VTP/D's networking function should enable data, video (broadcast and on demand) and voice services. Since there are multiple possible end-to-end service implementations, different deployments may use different flows to realize a given service (See [9]). All of the described basic packet flows MUST be supported by a VTP/D in order to realize specific end-to-end services. Each packet flow is mapped to a specific VC using the indicated encapsulation. For some flows, multiple instantiations may exist if indicated in the text. At the $T_{CN}$ reference point, flows do not necessarily map to a specific interface.

Figure 7 depicts the six required basic packet flows and the optional BLES packet flow within a VTP/D. Note that all packets at the $T_{CN}$ Reference point are Ethernet based and at the U-R2 Reference Point are ATM cells. In Figure 7, "Processing" and "Encapsulation" are examples of Functional Processing shown in Figure 2.

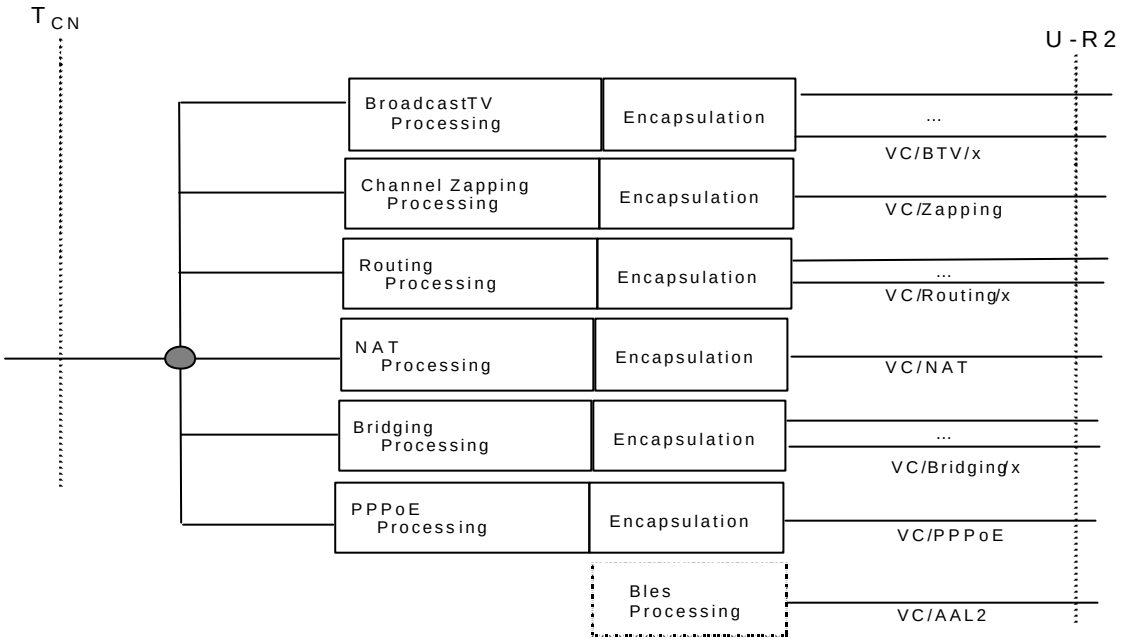



**Figure 7: Packet Flows**

The following terms will be used throughout the document.

- Upstream - refers to the data flowing from the $T_{CN}$ to U-R2 interface
- Downstream – refers to the data flowing from the U-R2 to $T_{CN}$ interface.
- Routed flow – includes the 'NAT' and 'Routing without NAT' flow
- Bridged flow - includes the 'Bridging' and 'PPPoE' flows
- Routed VCs – ATM VCs carrying routed flows
- Bridged VCs – ATM VCs carrying bridged flows
- Routed frames – Ethernet frames arriving at the $T_{CN}$ interface which are carrying a routed flow in the home network and therefore, in the upstream, these are PDUs with Ethernet MAC header containing the VTP/D $T_{CN}$ MAC address as the destination address and a unicast IP destination address.
- Bridged frames – Ethernet frames arriving at the $T_{CN}$ interface, which are carrying a bridged flow in the home network.

Configuration of the flows and associated ATM connections are discussed in Section 8.2.1 (ATM and AAL parameters) and 8.3 (IP layer parameters).

An example implementation of all the flows is given in informative Appendix I.

### 7.1.1 NAT Flow

This flow carries packets that require network address translation (NAT) and port address translation (PAT) within the VTP/D. The translation is performed from IP address domains on the $T_{CN}$ interface to one IP address on the U-R2 interface.

Note: Video services should not use the NAT Flow because of jitter and implementation implications.

- Encapsulation: PPPoA (RFC 2364 [24]) using VC multiplexing encapsulation option.
- Number of VCs: 1 connection, identified as VC/NAT.
- Upstream Input: Ethernet Frames.
- Upstream functional processing: Packets going to VC/NAT MUST pass a routing function as well as Network Address Translation (NAT) and Port Address Translation (PAT) functions as per RFC 3022 [27].
- Upstream Output:
  - Routed packets whose IP destination met the routing criteria of VC/NAT.
  - In case that an IGMP relay function is supported as per [41] (e.g. for enabling joining Internet multicast streams) by the VTP/D and bounded to VC/NAT, the output may include IGMP messages with a class D address that does not belong to the broadcast media (TV) service domain.
  - In case that upstream forwarding of IP multicast PDUs, whose source is in the customer premises, is supported and bounded to VC/NAT, the output may contain IP multicast PDUs with a destination class D address that does not belong to the broadcast media (TV) service domain.
- Downstream Input: VC/NAT carrying IP packets whose source and destination addresses are public IP addresses and whose IP destination address matches the VTP's public IP address assigned for the NAT function.
- Downstream functional processing: Packets within VC/NAT must be routed to the home network after passing the NAT and PAT functions. For routing only address lookup is mandatory.
- Downstream Output: Ethernet frames containing a destination MAC address that was resolved by the routing function after the incoming IP header was translated to a 'local' IP header by the NAT function.

### 7.1.2 Routing without NAT Flow

This flow carries packets that require IPv4 routing without NAT within the VTP/D. This flow contains the following two sub-flows.

#### 7.1.2.1 IP over AAL5

- Encapsulation: IP over AAL5 (IPoA) (RFC 2684 [25], section 5.1, payload format for routed IPv4 PDUs).
- Number of VCs: at least 4 identified with VC/Routing/x, where x is the VC/Routing sequential index number.
- Upstream Input: Ethernet Frames.
- Upstream functional processing: Incoming packets must pass a routing function. . Each VC/Routing/x defines a separate routing interface.
- Upstream Output:
  - Routed packets whose IP destination met the routing criteria of VC/NAT.
  - In case that an IGMP relay function is supported as per [41] (e.g. for enabling joining Internet multicast streams) by the VTP/D and bounded to one of VC/Routing/x, the output may include IGMP messages with a class D address that does not belong to the broadcast media (TV) service domain.
  - In case that upstream forwarding of IP multicast PDUs, whose source is in the customer premises, is supported and bounded to one of VC/Routing/x: the output may contain IP multicast PDUs with a destination class D address that does not belong to the broadcast media (TV) service domain.
- Downstream Input: VC/Routing/x carrying IP packets.
- Downstream functional processing: Packets within VC/Routing/x must pass a routing function.
- Downstream Output: Ethernet frames containing the MAC address that is determined by the routing function.

#### 7.1.2.2 PPP over AAL5

- Encapsulation: PPPoA (RFC 2364 [24]) using VC multiplexing encapsulation option.

- Number of VCs: at least 4 identified with VC/Routing/x, where x is the VC/Routing sequential index number.

  Note: These VCs are not supplemental to the ones identified in 7.1.2.1

- Upstream Input: Ethernet Frames.
- Upstream functional processing: Incoming packets must pass a routing function. Each VC/Routing/x defines a separate routing interface.
- Upstream Output:
  - Routed packets whose IP destination met the routing criteria of VC/NAT.
  - In case that an IGMP relay function is supported (e.g. for enabling joining Internet multicast streams) by the VTP/D and bounded to one of VC/Routing/x, the output may include IGMP messages with a class D address that does not belong to the broadcast media (TV) service domain.
  - In case that upstream forwarding of IP multicast PDUs, whose source is in the customer premises, is supported and bounded to one of VC/Routing/x, the output may contain IP multicast PDUs with a destination class D address that does not belong to the broadcast media (TV) service domain.
- Downstream Input: VC/Routing/x carrying IP packets.
- Downstream functional processing: Packets within VC/Routing/x must pass a routing function.
- Downstream Output: Ethernet frames containing the MAC address that is determined by the routing function.

### 7.1.3 Bridging Flow

This flow carries frames that require IEEE 802.1D bridging [59] within the VTP/D. Upstream and downstream frames are forwarded according to a learning bridge MAC address table. In case of multiple flows, each flow defines a different bridge interface.

- Encapsulation: Ethernet over AAL5 according to RFC 2684 [25] (section 5.2 Payload Format for Bridged Ethernet PDUs) using LLC/SNAP without FCS.
- Number of VCs: at least 4 identified with VC/Bridging/x, where x is the VC/Bridging sequential index number.
- Upstream Input: Ethernet frames
- Upstream functional processing: frames within VC/Bridging/x must pass a bridging function as defined in IEEE 802.1D [59]. Only self learning bridging functionality of [IEEE 802.1D sections 7.7 – 7.9] is mandatory.
- Upstream Output: Frames with destination MAC address meeting the bridging criteria for the output VC and frames with a destination MAC address not matching the VTP MAC address (on the $T_{CN}$ interface) and not containing an IGMP message with a class D address assigned to the broadcast media (TV) service and not carrying a PPPoE Ethertype (as long as the PPPoE filter is on).
- Downstream Input: VC/Bridging/x carrying Ethernet frames.
- Downstream functional processing: valid Ethernet frames are bridged to the home network (no VC to VC bridging is allowed).
- Downstream Output: Ethernet frames.

### 7.1.4 PPPoE Flow

This flow carries only PPPoE (RFC 2516 [26]) frames received from the home network. Upstream frames received via. the $T_{CN}$ reference point are filtered to a dedicated VC if and only if they have one of the PPPoE Ethertypes (0x8863 or 0x8864).

- Encapsulation: Ethernet over AAL5 according to RFC 2684 [25] (section 5.2 Payload Format for Bridged Ethernet PDUs) using LLC/SNAP without FCS
- Number of VCs: 1 identified as VC/PPPoE.
- Configuration aspects: the PPPoE filter MUST be either remotely turned on/off or pre-settable (i.e. set by the manufacturer). In case that ILMI is supported, the PPPoE filter can be remotely activated (deactivated) by simply binding (unbinding) the PPPoE flow to a VC (see Section 5.2.1).
- Upstream Input: Ethernet frames.
- Upstream functional processing: Filtering of PPPoE frames.

- Upstream Output: Frames carrying PPPoE Ethertype (0x8863 or 0x8864) and that the destination MAC address is not the same as the VTP MAC address.
- Downstream Input: VC/PPPoE carrying Ethernet frames.
- Downstream functional processing: none
- Downstream Output: Ethernet frames.

### 7.1.5 Broadcast TV and Entertainment Packet Flow

This flow is unidirectional and carries all broadcast content related packets (e.g. audio, video) in downstream direction.

- Encapsulation: The following options are viable and can co-exist (precise protocol stack specification is described in FS-VDSL Part 2 [9]):
  - Ethernet over AAL5 according to RFC 2684 [25] (section 5.2 Payload Format for Bridged Ethernet PDUs) using LLC/SNAP without FCS. In this case the MPEG-2 TS PDUs are encapsulated with UDP, IP and Ethernet headers, as described in FS-VDSL Part 2 [9], section 9.3.3.5.5.
  - MPEG-2 TS over AAL5.
- Number of VCs: multiple identified as VC/BTV/x, where x is the VC/BTV sequential index number.
- Configuration aspects: In a case where both encapsulation methods are used for the same platform, either two sets of PVCs are used, one for each encapsulation, or an automatic detection procedure is used. Automatic detection of the MPEG encapsulation is for further study.
- Upstream Input: Ethernet Frames
- Upstream functional processing: Block all packets
- Upstream Output: None
- Downstream Input: VC/BTV/x carrying multicast IP packets in Ethernet frames or VC/BTV/x carrying MPEG2 over AAL5.
- Downstream functional processing: in case of MPEG2 over AAL5, the payload of one or several AAL5 frames is encapsulated as one IP multicast packet, including a UDP header over Ethernet. In case of MPEG2 over IP encapsulation, the LLC/SNAP header is chopped off and no further processing is required.
- Downstream Output: Ethernet frames carrying IP multicast packets.

### 7.1.6 Channel Change Flow

The VTP/D Channel Change Flow processing acts as a 'channel change proxy'. It functions as an IGMP server towards the TCN interface and as an IGMP or DSM-CC client towards the UR interface. The corresponding packet flow is carried within the Channel change Flow

- Encapsulation: Two options are possible:
  - When IGMP based channel change is used, the encapsulation is IGMP over IP over AAL5 (IPoA) per RFC 2684 [5], section 5.1, payload format for routed IPv4 PDUs]
  - DSM-CC.
- Number of VCs: 1 identified as VC/Channel Change
- Upstream Input: Ethernet Frames.
- Upstream functional processing: Channel change proxy. The Channel change proxy function accepts frames that contain an IGMP message with a class D address assigned to the broadcast media (TV) service. The channel change proxy function generates corresponding channel change messages towards the access network and makes the IGMP to DSM-CC protocol conversion, if needed.
- Upstream Output: Channel change packets (IGMP or DSM-CC) generated by the channel change proxy function.
- Downstream Input: VC/Channel Change.
- Downstream functional processing: The Channel change protocol on the VC/Channel change interface is processed and IGMP messages (Query messages) towards the Home Network are generated.
- Downstream Output: Ethernet frames containing IGMP messages.

### 7.1.7 BLES flow (optional)

This flow carries Voice over ATM related packets (i.e. AAl2 cells). (see FS-VDSL Part 2 [9]). This flow is optional and MUST be implemented if VoATM services are required.

- Encapsulation: AAL2 according to ITU-T I.366 [47] [48].
- Number of VCs: 1 identified as VC/AAL2.
- Configuration aspects: BLES functionality is configured by the voice gateway using a dedicated AAL2 channel.
- Upstream functional processing: Generating BLES Flow
- Upstream Input: Analogue voice signal
- Upstream Output: AAL2 cells carrying telephony signals
- Downstream Input: AAL2 cells carrying telephony signals.
- Downstream functional processing: Terminating BLES Flow
- Downstream Output: Analogue voice signal

## 8. VTP/D Functional Processing Specifications

This section defines in detail the VTP/D functional specification necessary to handle the previously described flows. The architecture defined in this clause addresses a distributed CPE architecture (VTP & FPD), according to the terms of the reference model defined in Section 5, because , the definition of a distributed approach will also satisfy the requirements for a centralized approach. Both implementation are possible.

The main aim of this clause is to define the layer 2 and layer 3 protocols processing in the VTP/D. There will be corresponding functional processing blocks in the FPD, to ensure that the VTP/D can provide support for services which are consumed by the home appliances. The data, video, and voice interfaces shown in the reference model figures are defined as logical interfaces. It does not reflect any particular implementation.

Forwarding in the VTP/D domain is provided with the following approaches:

- Ethernet Bridging or Switching – An OSI layer 2 device, which connects 2 or more physical networks, that may or may not use different physical layer technologies. Frame forwarding is based on a label field e.g. MAC address, which can be used to direct traffic to an appropriate port or device. An example is a VTU-R with an integrated Ethernet switch connecting the residential devices.
- IP Routing – An OSI layer 3 device, which contains routing functionality for IP-packets. The router has to take a decision based on the destination of the IP packets about whether or not to forward them to a neighbor network or not.
- A combination of the two.

A VTP MUST provide one or more physical interfaces with in-home distribution networks, and MUST ensure adequate signal transport to home appliances. Possible physical interfaces are described in clause 3.2.1.

### 8.1. ATM Processing

The following requirements are mandatory for the U-R2 Reference point.

The VTP/D MUST support ATM adaptation layer 5 (as per ITU I.363.5 [13]) and ATM segmentation and reassembly (SAR) function.

A VTP/D that supports voice over ATM (VoATM) service MUST support ATM adaptation layer 2 (as per ITU I.363.2 [12]) for that purpose.

A VTP/D MUST support the termination of permanent virtual path connections (PVPs).

A VTP/D MUST support the termination of permanent virtual channel connections (PVCs).

A VTP/D MAY support switched virtual channel connections (SVCs).

A VTP/D supporting SVCs MUST comply to the UNI4.0 (SIG4.0, [62]) signaling scheme.

A VTP/D MUST support at least the CBR, VBR-nRT and UBR traffic types as per ATM Forum TM4.1 [17]. The VTP/D MUST be able to shape these traffic types in the upstream (i.e. network) direction. The VTP/D MUST support a UBR service with a specified PCR.

A VTP/D MUST support priority based queuing and scheduling of ATM cells in the upstream direction.

A VTP/D MUST support packet-based discard of AAL5 PDUs, namely it must not transmit to the network incomplete AAL5 frames.

A VTP/D MUST support ATM OAM flows of the F4 and F5 levels [45] (Section 7.2).

A VTP/D MUST support end-to-end ATM OAM flows [45] (Section 7.2).

A VTP/D MUST support ATM OAM loopback function as per [45].

A VTP/D MUST support ATM OAM defect indications, AIS and RDI as per [45].

A VTP/D SHOULD support ATM OAM continuity check (CC) sink function as per [45]. Activation and deactivation may be performed by sending a activation/deactivation cell or by remote management (i.e. TMN).

A VTP/D MAY support ATM OAM performance monitoring (PM) backward reporting (BR) function as per [45].

### 8.1.1 ATM Layer Configuration

The ATM layer parameters (i.e. virtual connections, traffic descriptors, etc.) of a VTP/D can be either statically configured to a default scheme or dynamically configured to support a deployment specific scheme.

#### 8.1.1.1 Default Static Configuration

A VTP/D MUST support the default PVC scheme given in Table 4 if dynamic configuration is not supported or fails.

**Table 4: Default PVC scheme**

| Connection identifier | ATM traffic descriptor | Details |
|---|---|---|
| VC/BTV/1 | VPI / VCI = 1/33<br>Traffic Type: CBR uni-d | Default values are required only for IGMP based channel change |
| VC/BTV/2 | VPI / VCI = 1/34<br>Traffic Type: CBR uni-d | Default values are required only for IGMP based channel change |
| VC/BTV/3 | VPI / VCI = 1/35<br>Traffic Type: CBR uni-d | Default values are required only for IGMP based channel change. See section 7.4 |
| VC/BTV/4 | VPI / VCI = 1/36<br>Traffic Type: CBR uni-d | Reserved for non MPEG2 traffic. |
| VC/Channel Change | VPI / VCI = 1/32<br>Traffic Type : CBR bi-d sym<br>PCR = 42 cells /s | See section 7.5 |
| VC/Bridged/1 | VPI / VCI = 0/32<br>Traffic Type : UBR bi-d | See section 7.8 |
| VC/Bridged/2 | VPI / VCI = 0/33<br>Traffic Type : UBR bi-d | See section 7.8 |
| VC/Bridged/3 | VPI / VCI = 0/34<br>Traffic Type : UBR bi-d | See section 7.8 |
| VC/Bridged/4 | VPI / VCI = 0/35<br>Traffic Type : UBR bi-d | See section 7.8 |
| VC/PPPoE | VPI / VCI = 0/62<br>Traffic Type : UBR bi-d | See section 7.8 |
| VC/Routing/1 | VPI / VCI = 0/42<br>Traffic Type : UBR bi-d | See section 7.6 |
| VC/Routing/2 | VPI / VCI = 0/43<br>Traffic Type : UBR bi-d | See section 7.6 |
| VC/Routing/3 | VPI / VCI = 0/44<br>Traffic Type : UBR bi-d | See section 7.6 |
| VC/Routing/4 | VPI / VCI = 0/45<br>Traffic Type : UBR bi-d | See section 7.6 |
| VC/NAT | VPI / VCI = 0/63<br>Traffic Type : UBR bi-d | See section 7.7 |
| VC/AAL2 | VPI / VCI = 0/40<br>Traffic Type: CBR bi-d sym<br>PCR no default value is specified. | See section 7.9<br>Note: this VC is optional. |
| ILMI channel | ATM Forum defaults for ILMI channel<br>(VPI/VCI = 0/16 bi-d sym) | |
| Remote management channel | VPI/VCI = 0/50<br>VBRnrt bi-d sym<br>PCR = 100 cells/s<br>SCR = 50 cells/s<br>MBS = 50 cells | |

Note : Bi-d = bi-directional connection, Uni-d = unidirectional connection, sym = symmetric bandwidth parameters.

#### 8.1.1.2 Dynamic Configuration

A VTP/D SHOULD support ATM configuration according to the ATM-Forum defined Integrated Local Management Interface (ILMI), which is documented in ATMF ILMI v4.0 [14]. If the connection is based on permanent VC (PVC), the VTP/D SHOULD support the "Auto-configuration of PVCs" as specified in [15] and [16].

ILMI and its relevant extensions provide configuration of the following parameters per ATM connection:

1. Service related parameters that are associated with the connection, such as service provider and service type identifiers, which imply the layer 3 protocol and the encapsulation over the ATM VC.
2. Traffic management parameters, such as service category (e.g. CBR, UBR etc.) and conformance definition (e.g. CBR.1, UBR.1, UBR.2 etc.) and parameters (e.g. PCR, SCR CDVT, etc.)
3. ATM layer parameters, such as AAL type, port, VPI and VCI.

The association between the ATM connections and flows is provided using the service name field (i.e. atmfAtmServiceName), which is a part of a service type object. The following are the FS-VDSL service names representing the 7 flows described in section 7 and an 8$^{th}$ one representing the remote management flow.

1. FS-VDSL-NAT
2. FS-VDSL-ROUTE
3. FS-VDSL-BRIDGE
4. FS-VDSL-PPPOEFILTER
5. FS-VDSL-BROADCAST
6. FS-VDSL-CHANNELCHANGE
7. FS-VDSL-BLES
8. FS-VDSL-MANAGEMENT

A few service sub-names values (i.e. atmfAtmServiceSubName) are defined in order to enhance the service definition.

1. DSMCC – relevant only for the FS-VDSL-CHANNELCHANGE service.
2. IGMPv2 – relevant only for the FS-VDSL-CHANNELCHANGE service.
3. MPEG2 - indicates that MPEG2 over AAL5 encapsulation is used. Relevant for FS-VDSL-BROADCAST service only.
4. MPEG2UDP - indicates that MPEG2 over UDP encapsulation is used. Relevant for FS-VDSL-BROADCAST service only.

A VTP/D connecting to the network on the first time or reconnecting to the network after hard re-initialization process MUST be configured to the default ATM configuration. Upon discovering a network capable of dynamic configuration, the VTP/D will receive its new configuration using the previously mentioned protocols.

### 8.1.2 ATM Processing Defect Indicators

Each point to point ATM VP connection which terminates on the VTP/D MUST originate and terminate an F4 flow as defined in ITU-T recommendation I.610 and generate the associated defect indicators.

Each point to point ATM VC connection which terminates on the VTP/D MUST originate and terminate an F5 flow as defined in ITU-T recommendation I.610 and generate the associated defect indicators.

If a ATM VC AIS is received on a BTV VC (which are point to multi-point connections and are not covered by the current scope of I.610), VTP MUST generate a local defect indicator as if it was a bi-directional point to point connection. This means that no remote defect indication is generated but the local defect indicator is available through the VTP/D MIB.

## 8.2. IP Processing

It is expected that a majority of deployments require a single IP subnetwork for the home network and a single external route (on either a NAT ATM VC or a routed ATM VC). These scenarios are described as standard scenarios.

However, this specification of the IP processing functionality is also designed to allow a wide variety of additional IP networking scenarios. Scenarios with more than one IP subnetwork in the home network and/or more than one outgoing route are described as advanced scenarios.

Complete automatic configuration for both the standard scenarios and the advanced scenarios is possible by using default values and/or using standard configuration protocols, eg DHCP and PPP, and do not require any management configuration. However, further configuration is possible using the remote management and/or local management interfaces to explicitly configure the IP networking parameters.

### 8.2.1 Standard IP Processing Scenarios

The IP processing in the VTP/D allows the home network to operate as an IP subnetwork. Within this subnetwork, the VTP/D acts as the default gateway for the IP subnetwork and also provides the DHCP server which allocating an IP address and other IP client configuration information to the IP configuration client in the FPDs.

The VTP/D automatically supports a number of different addressing arrangements for the IP subnetwork which will be one of the following scenarios.

- An exclusive private address space for the home network, eg 192.168.0.0.
- A subnetwork of an externally routable address space. The subnetwork in the home may be a subnetwork of:
  - the public internet using a subnetwork of public (globally registered) address space.
  - a wider private network using private address space, eg 10.0.0.0 private address space.

IP networking within the IP subnetwork of home network is achieved using the Ethernet MAC layer capabilities with the IP address to MAC address mapping maintained using ARP in a standard way.

Networking beyond this IP subnetwork is achieved using the IP forwarding function in the VTP/D which maintains forwarding routes. These are the rules by which the IP forwarding function decides where to pass IP packets. In the standard scenarios, ie with a single IP subnetwork and a single outgoing route, the forwarding function is trivial based on a single default route. If the IP subnetworking is using exclusive private address space, then the packets are passed through a NAT/PAT function within the IP forwarding function.

The IP subnetwork in the home network is defined as being one of two types, depending on the address space used. The first type is where exclusive private address space is used. The second is where the IP subnetwork is a subnetwork of wider address space, be it private or public address space.

### 8.2.2 Default Configuration of Exclusive Private Address Space Standard Scenario

The configuration of this standard scenario is illustrated in Figure 8 below. The home network uses exclusive private address space (default is 192.168.0.0/24) and since this address range is known independent of the connection to the wider network, the IP subnetwork parameters and the DHCP server parameters can be configured before the network connection is created and configured.

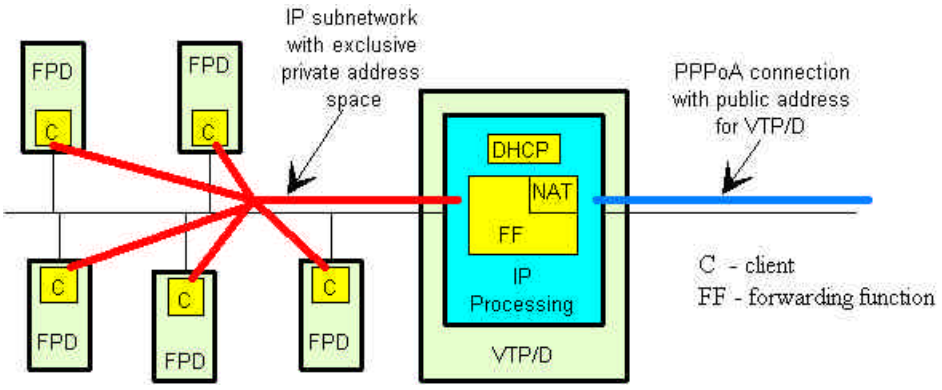



**Figure 8: Standard IP processing scenario with exclusive private address space**

#### 8.2.2.1 Default Configuration Action Sequence

This default configuration action sequence will normally be triggered automatically by powering up the VTP/D. Given this trigger, the following takes place.

- The VTP/D home network interface, the DCHP server, and other IP processing parameters are configured with the parameters of the default IP subnetwork with exclusive private addressing described below.
- Assuming the NAT ATM VC is operational, a PPPoA session is initiated on this ATM VC with PPP parameters using the defaults described below.
- The address allocated by the PPP is used as address of the VTP/D behind which the IP subnetwork masquerades. The PPPoA connection is configured as the layer 2 interface of the default route of the forwarding function. A NAT/PAT function is created within IP forwarding function as part of this default route and is configured with the default parameters described below.

#### 8.2.2.2 Default IP Subnetwork and DHCP Server Configuration

The default is that IP subnetwork in the home network uses the 192.168.0.0/24 private address range.

The parameters defining the home private address subnetwork are give in Table 5 together with their default and/or derived values. The third column specifies what alternative methods of configuration are available for this parameter. Table 6 defines the DHCP server parameters for configuring hosts within the subnetwork.

**Table 5: Default Subnetwork Parameters for an IP Subnetwork with Exclusive Private Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Subnetwork mask (m.m.m.m) | Static – 255.255.255.0 | Static value through management interface |
| Subnetwork address (x.x.x.x) | Static – 192.168.0.0 | Static value through management interface |
| Default gateway | Derived – 192.168.0.1 | No – calculated as x.x.x.x and m.m.m.m + 0.0.0.1 |
| Broadcast address | Derived – 192.168.0.255 | No – calculated as x.x.x.x and m.m.m.m + not m.m.m.m |
| Primary DNS server address | Derived – IPCP (extension per RFC 1877 [61]) from ER (see PPP parameter below) | Static value through management interface or the VTP may implement a DNS relay and/or caching function |
| Secondary DNS server address | Derived – IPCP (extension per RFC 1877 [61]) from ER (see PPP parameter below) | Static value through management interface |
| Intra subnetwork address resolution | ARP | |
| Address of VTP/D within the Subnetwork | 192.168.0.1 | No – calculated as x.x.x.x and m.m.m.m + 0.0.0.1 |

**Table 6: Default DHCP Server Parameters for an IP Subnetwork with Exclusive Private Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Subnetwork mask | Copied from subnetwork parameters | No |
| Address allocation range | Static – 192.168.0.16 to 192.168.0.239 | Static values through management interface |
| Default gateway | Copied from subnetwork parameters | No |
| Broadcast address | Copied from subnetwork parameters | No |
| DNS primary server address | Copied from subnetwork parameters | No |
| DNS secondary server address | Copied from subnetwork parameters | No |

#### 8.2.2.3 Default External Connection Configuration

The following default parameters, given in Table 7 below, as used to configure the external connection to the IP subnetwork as well as negotiate parameters with the edge router in the network.

**Table 7: Default Parameters for External Connection to IP Subnetwork with Exclusive Private Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Encapsulation | PPPoA | No |
| LCP keep alive rate | Static – 1 minute | Static value through management interface |
| Authentication | PAP | CHAP |
| IPCP VTP address offered by VTP | 0.0.0.0 | Static provision using the management interface |
| IPCP VTP address offered by ER | Accept address x.x.x.x offered | Ignore address |
| IPCP ER address offered by ER | Ignore address (PPP link is default route) | No |
| IPCP ER address offered by VTP | No not offer address | No |
| IPCP primary DNS server address offered by ER | Accept address x.x.x.x offered | Ignore address |
| IPCP secondary DNS server address offered by ER | Accept address x.x.x.x offered | Ignore address |

#### 8.2.2.4 Default IP Forwarding Function Configuration

The routes in the IP forwarding function are those of a trivial forwarding function. The main outgoing routes are to the home network and the external connection which is the default route. This default route also includes the NAT/PAT function. In addition to these routes, the VTP/D should implement a loopback route. The default routes are shown in Table 8. The default parameters for the NAT/PAT function are given in Table 9.

**Table 8: Default IP Forwarding Function Parameters for an IP Subnetwork with Exclusive Private Address Space**

| Destination Address Range | | Masquerading | Outgoing Layer 2 interface |
|---|---|---|---|
| **Destination Address** | **Subnet Mask** | | |
| x.x.x.x (derived from subnetwork parameters) | s.s.s.s (derived from subnetwork parameters) | No | Home network interface, eg eth0 |
| 127.0.0.0 | 255.0.0.0 | No | VTP/D - loopback route |
| Default route | | Yes | External connection, eg ppp0 |

**Table 9: Default NAT/PAT Parameters for an IP Subnetwork with Exclusive Private Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Upstream open port values | All ports open | All port closed except those opened by a static configuration through either the local or the remote management interface, by a dynamic protocol, e.g. UPnP, or by a vendor specific solution. |
| Downstream port to local address mapping | No mapping of any port value | Mapping of a port value to a home network private IP address either by static mapping configured through either the local or the remote management interface, by a dynamic protocol, e.g. UPnP, or by a vendor specific solution. |
| NAT application protocol relay | FTP | Additions may be added by the vendor and/or dynamically by UpnP |

### 8.2.3 Default Configuration of the Standard Scenario with Externally Routable Address Space

The configuration of this standard scenario is illustrated in Figure 9 below. In this standard scenario, the default address range is assigned using by the network through the edge router, either using PPP or DHCP. (Note this DHCP transaction is between the VTP/D as DHCP client and the edge router as DHCP server, and completely independent of the DHCP transactions with the IP subnetwork).

Since the address range is not known until the external connection has been established, the creation and configuration of the IP subnetwork must follow the establishment of the external connection.

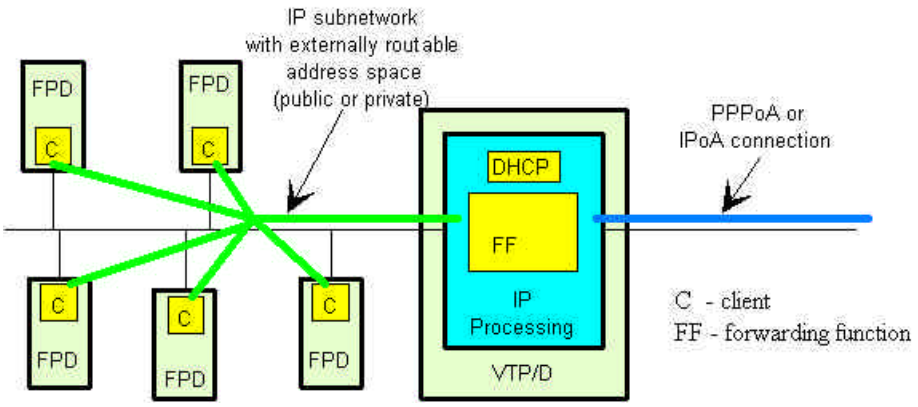



**Figure 9: Standard IP processing scenarios with external routable address space**

#### 8.2.3.1 Default Configuration Action Sequence

The default configuration is initiated by the VTP/D following the establishment of the external Routing ATM VC.

This triggers the following actions if the Routing ATM VC is configured as PPPoA.

- A PPPoA session is initiated on this Routing ATM VC with PPP parameters using the defaults described below.
- The VTP/D home network interface, the DCHP server, and other IP processing parameters are configured with the parameters of the default IP subnetwork with described below (derived from the IPCP negotiation).
- The PPPoA connection is configured as the layer 2 interface of the default route of the forwarding function.

If the routing ATM VC is configured as IPoA, then the following actions are triggered.

- A DHCP discover is issued across the IPoA connection.
- The VTP/D home network interface, the DCHP server, and other IP processing parameters are configured with the parameters of the default IP subnetwork with described below (derived from the above DHCP negotiation).
- The IPoA connection is configured as the layer 2 interface of the default route of the forwarding function.

#### 8.2.3.2 Default External Connection Configuration

If the external connection to the IP subnetwork uses PPPoA, the default parameters are given in Table 10 while if the external connection uses IPoA the default parameters are as given in Table 11. These are used to configure the external connection as well as to negotiate with the edge router.

**Table 10: Default Parameters for External PPPoA Connection to IP Subnetwork with Externally Routable Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Encapsulation | PPPoA | No |
| LCP keep alive rate | Static – 1 minute | Static value through management interface |
| Authentication | PAP | CHAP |
| IPCP VTP address offered by VTP | 0.0.0.0 | Static provision using the management interface |
| IPCP VTP address offered by ER | Accept address x.x.x.x offered | Ignore address |
| IPCP ER address offered by ER | Ignore address (PPP link is default route) | No |
| IPCP ER address offered by VTP | No not offer address | No |
| IPCP primary DNS server address offered by ER | Accept address x.x.x.x offered | Ignore address |
| IPCP secondary DNS server address offered by ER | Accept address x.x.x.x offered | Ignore address |

**Table 11: Default Parameters for External IPoA Connection to IP Subnetwork with Externally Routable Address Space**

| *Parameter* | *Default* | *Reconfigurability* |
|---|---|---|
| Encapsulation | IPoA (RFC 2684 routed mode) | No |
| Configuration protocol | DHCP | None - ie configuration protocol |
| Routing Protocol | None | Enabling of optional RIP or RIPv2 |

#### 8.2.3.3 Default IP Subnetwork and DHCP Server Configuration

The default for this address range is that it is derived from the parameters negotiated with the edge router over the external connection.

This default derivation of the address range uses the following rules when the external connection uses PPPoA.

- Where the IPCP component of PPP can allocate subnetwork mask, this should is used for the subnetwork.
- If no subnetwork mask is allocated by IPCP, the subnetwork should assume subnetwork mask of 255.255.255.248 (Note this requires that the edge router and RADIUS servers are also aware of this default and configured accordingly).

The default derivation of the address range uses the following rule when the external connection uses IPoA.

- The IP subnetwork should use the IP address and subnetwork mask allocated by DHCP;

The parameters defining the IP subnetwork are give in Table 12 together with their default and/or derived values. The third column specifies what alternative methods of configuration are available for this parameter. Table 13 defines the parameters for the DHCP server in the VTP/D associated with the IP subnetwork.

**Table 12: Default Parameters for IP Subnetwork with Externally Routable Address Space**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Subnetwork mask (m.m.m.m) | Derived from configuration parameters of external connection or Static default (255.255.255.248) – see above | Static value through management interface |
| Subnetwork address (x.x.x.x) | Derived from configuration parameters of external connection – x.x.x.x and m.m.m.m | Static value through management interface |
| Default gateway | Derived – x.x.x.x and m.m.m.m + 0.0.0.1 | No |
| Broadcast address | Derived – x.x.x.x and m.m.m.m + not m.m.m.m | No |
| Primary DNS server address | Derived from configuration parameters of external connection | Static value through management interface<br>or<br>the VTP may implement a DNS relay and/or caching function |
| Secondary DNS server address | Derived from configuration parameters of external connection | Static value through management interface |
| Intra subnetwork address resolution | ARP | |
| VTP Address | Derived – x.x.x.x and m.m.m.m + 0.0.0.1 | No |

**Table 13: Default Parameters for DHCP Server for IP Subnetwork with Externally Routable Address Space**

| Parameter | Default | Reconfigurability |
|---|---|---|
| Subnetwork mask (m.m.m.m) | Copied from subnetwork parameters | No |
| Address allocation range | Derived – a maximum range would be x.x.x.x and m.m.m.m + 0.0.0.2 to x.x.x.x and m.m.m.m + not m.m.m.m – 0.0.0.1 | Static values through management interface |
| Default gateway | Copied from subnetwork parameters | No |
| Broadcast address | Copied from subnetwork parameters | No |
| DNS primary server address | Copied from subnetwork parameters | No |
| DNS secondary server address | Copied from subnetwork parameters | No |

#### 8.2.3.4 Default IP Forwarding Function Configuration

The routes in the IP forwarding function are those of a trivial forwarding function. The main outgoing routes are to the home network and the external connection which is the default route. In addition to these routes, the VTP/D should implement a loopback route. The default routes are shown in Table 14.

**Table 14: Default IP Forwarding Function Parameters for an IP Subnetwork with Externally Routable Address Space**

| Destination Address Range | | Masquerading | Outgoing Layer 2 interface |
|---|---|---|---|
| **Destination Address** | **Subnet Mask** | | |
| x.x.x.x (derived from subnetwork parameters) | s.s.s.s (derived from subnetwork parameters) | No | Home network interface, eg eth0 |
| 127.0.0.0 | 255.0.0.0 | No | VTP/D - loopback route |
| Default route | | No | External connection, eg ppp0 or ipoa0 |

### 8.2.4 Advanced IP Processing Scenarios

If the VTP/D has more than one external connection (NAT ATM VC or Routing ATM VC) and/or there more than one IP subnetwork in the home network, the IP processing scenario can no longer be configured as one of the standard scenarios. This section describes the default configuration of advanced scenarios which can include a wide variety of IP networking situations.

The general principle behind the advanced scenarios is that the default configurations of any additional external connections and any additional IP subnetwork follow the same basic rules as the standard scenarios. Most of the specific configuration for the advanced scenarios is established in the parameters negotiated across the external connections and the routes that are added to the IP forwarding function.

- For the IP forwarding function, these default configurations basically work as follows If there is only one IP subnetwork, each additional external connection will result in at least one additional route in the forwarding table.
- If there is more than one IP subnetwork, the IP forwarding function uses the concept of virtual routers to separate the routes in the forwarding table so that each route is only associated with one IP subnetwork. (Note, this requires that each external connection is uniquely associated with an IP subnetwork.)

For the clarity of explanation, the default configuration associated with adding an IP subnetwork is described first as this introduces the procedures associated with virtual routers. In the description of the default configuration associated with adding external connections, the case where there is only one IP subnetwork can then be treated as a special case where virtual routers are not required.

#### 8.2.4.1 Adding of an Additional IP Subnetwork

The configuration of this advanced scenario is illustrated in Figure 10 below.

In this advanced scenario, the operation of any existing IP subnetworks will be completely unchanged by the creation of the new IP subnetwork. Each IP subnetwork is effectively, fully independent of any other IP subnetwork.

Each IP subnetwork is therefore treated as if it were a standard scenario from the default configuration point of view with the exception that the trigger to create any additional IP subnetwork cannot be wholly automated and will require some external stimulus. While some intelligent intepretation could be made from parameters negotiated over an external connection using PPP or DHCP, the expectation is that this trigger will ultimately come from the management interface.

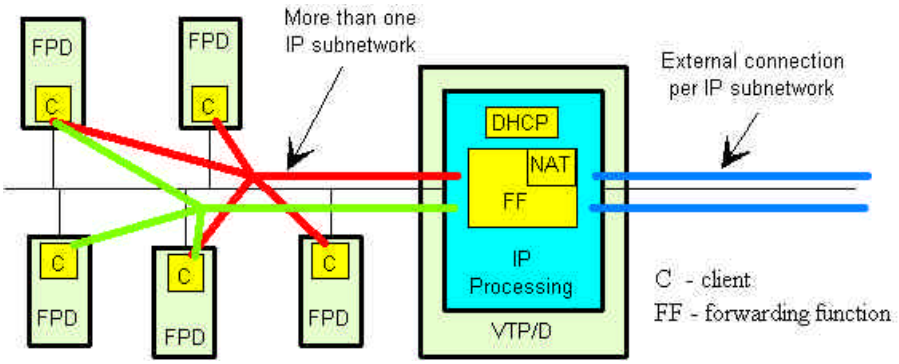



**Figure 10: Advanced Scenario – Adding an IP Subnetwork**

The IP forwarding function consists of an orthogonal set of forwarding rules based on the IP destination address ranges. Each rule is called a route and the complete set of routes is called the forwarding table.

With virtual routing each route belongs to a virtual router. Packets entering the forwarding function are identified as belonging to a virtual router based on one or more parameters however this specification is based only on incoming layer 2 interface and/or IP source address range.

The virtual router id references a set of access control lists where an access control list is either a source address range defined as a source address s.s.s.s and subnetwork mask m.m.m.m or an incoming layer 2 interface eg ppp0, ppp1, ipoa0, eth0, eth1, etc.

The default access control list creation is that the IP subnetwork is identified to a virtual router by its source address range (derived from the IP subnetwork parameters) while the external connection is identified by its incoming layer 2 interface.

With virtual routing, the logical operation of the IP forwarding function is as follows.

- The incoming packet is checked against the access control list to determine virtual router;
- The routes belonging to the virtual router are checked in order and when a match is found, is passed to the outgoing port specified in the forwarding table;
- If no match in found in the routes belonging to the virtual router, the packet is passed to the port defined by the default route of the virtual router.

Table 15 shows the example of the forwarding table resulting from the addition of an external routable IP subnetwork to a standard scenario with an IP subnetwork with exclusive private address space and Table 16 shows the associated access control lists for each virtual router.

**Table 15: Example Forwarding Table with IP Subnetwork added to a Standard Exclusive Private Address Space Scenario**

| Virtual Router ID | Destination Address Range | | Masquerading | Outgoing Layer 2 Interface |
|---|---|---|---|---|
| | Destination Address | Subnet Mask | | |
| 0 | 192.168.0.0 | 255.255.255.0 | No | Home network interface, eg eth0 |
| 0 | 127.0.0.0 | 255.0.0.0 | No | VTP/D - loopback route |
| 0 | Default route | | Yes | External NAT connection, eg ppp0 |
| 1 | x.x.x.x (derived from IPCP or DHCP) | s.s.s.s (derived from default, IPCP or DHCP) | No | Home network interface, eg eth1 |
| 1 | 127.0.0.0 | 255.0.0.0 | No | VTP/D - loopback route |
| 1 | Default route | | No | External routed connection, eg ppp1 or ipoa0 |

**Table 16: Example Access Control Lists with IP Subnetwork added to a Standard Exclusive Private Address Space Scenario**

| Source Address Range | | Incoming Layer 2 Interface | Virtual Router ID |
|---|---|---|---|
| Source Address | Subnet Mask | | |
| 192.168.0.0 | 255.255.255.0 | | 0 |
| | | External NAT connection, eg ppp0 | 0 |
| x.x.x.x (derived from IPCP or DHCP) | s.s.s.s (derived from default, IPCP or DHCP) | | 1 |
| | | External routed connection, eg ppp1 or ipoa0 | 1 |

#### 8.2.4.2 Adding of an Additional External Connection to an IP Subnetwork

The first scenario to consider is the case of adding additional connections to a standard scenario IP subnetwork. This is illustrated in Figure 11 below.

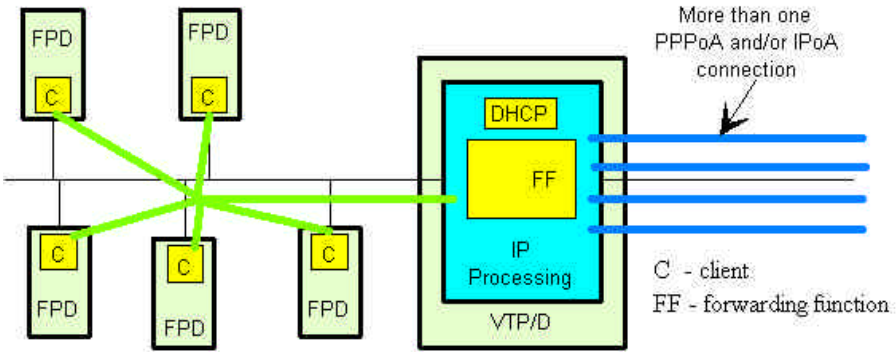



**Figure 11: Adding additional connections to an IP subnetwork**

Where the IP subnetwork is using externally routable address space, when an additional external connection is added, a new route needs to be added to the forwarding table. This will enable packets to be passed across this connection when appropriate to the addresses reachable from the far end. When the connection uses PPPoA, the default is that this route is calculated from the far end address passed from the far end. If the IPCP does not support the passing of a subnetwork mask, then the mask should be derived from the class of the far end address passed (ie 255.0.0.0 for a class A address, 255.255.0.0 for class B address, and 255.255.255.0 for a class C address)

Note, unless the IPCP supports an extension to pass a subnet mask along with an address, this automatic default configuration should be used with caution. The far end will probably calculate an incorrect mask for the IP subnetwork home network, potentially leading the VTP/D to receive packets not destined for the IP subnetwork. On the basis of these defaults, these packets would be passed out through the first connection, the default route, and so the packets will arrive successfully, however, the VTP/D is liable to be loaded with unwanted traffic.

Special consideration is needed for the addition of additional connections to a subnetwork with exclusive private address space. The way in which these connections are treated depends on the address space at the other end of the connection.

- If the address space at the other end of the connection is another subnetwork of the same exclusive address space (eg 192.168.1.0/24), then associated route can be added to the forwarding table as described above (without the need for additional masquerading with NAT/PAT).
- If the address space at the other end of the connection a different address space to either the IP subnetwork or the address at the end on the standard connection (eg 10.0.0.0 when the standard connection connects to public internet), then the forwarding function can set up a route (eg 10.0.0.0 subnet mask 255.0.0.0) to this address space with masquerading with NAT/PAT (separate to the NAT/PAT used to the public internet address space)
- If the address space at the end of the connection is the same at that at the end of the standard connection, then the forwarding function needs to define a suitable route for this connection. When the connection uses PPPoA, this route is calculated from the address passed from the other end. If the IPCP does not support the passing of a subnetwork mask, then the mask should be derived from the class of the address passed. The route needs use masquerading with NAT/PAT.

The consequence of the above rules for adding addition external PPPoA connections for the PPPoA parameters and negotiation with the far end is captured in Table 17.

**Table 17: Default Configuration Parameters for a Subsequent Connection to an IP Subnetwork if it is Using PPPoA**

| Parameter | Default | Alternative Configurability |
|---|---|---|
| Encapsulation | PPPoA | No |
| LCP keep alive rate | Static – 1 minute | Static value through management interface |
| Authentication | PAP | CHAP |
| IPCP VTP address offered by VTP | Derived - x.x.x.x (ie the subnetwork address) | Static provision using the management interface |
| IPCP VTP address offered by ER | Ignore address | Accept address x.x.x.x offered |
| IPCP ER address offered by ER | Use address to populate forwarding table | Ignore address |
| IPCP ER address offered by VTP | No not offer address | No |
| IPCP primary DNS server address offered by ER | Ignore address | Accept address x.x.x.x offered |
| IPCP secondary DNS server address offered by ER | Ignore address | Accept address x.x.x.x offered |

An example forwarding table is shown in Table 18. This example is where the IP subnetwork has externally routable address space, the external connection uses PPPoA and its IPCP does pass a subnetwork mask.

**Table 18: Default IP Forwarding Function Parameters after the Addition of a PPPoA External Connection to an IP Subnetwork with Externally Routable Address Space**

| Destination Address Range | | Masquerading | Outgoing Layer 2 interface |
|---|---|---|---|
| Destination Address | Subnet Mask | | |
| x.x.x.x (derived from subnetwork parameters) | s.s.s.s (derived from subnetwork parameters) | No | Home network interface, eg eth0 |
| y.y.y.y (derived from address passed by IPCP on additional connection) | y.y.y.y (parameter passed by IPCP on additional connection) | No | Additional external connection, eg ppp1 |
| 127.0.0.0 | 255.0.0.0 | No | VTP/D - loopback route |
| Default route | | No | External connection, eg ppp0 or ipoa0 |

If IPoA is used for an additional connection to an IP subnetwork, then the default is that no new entries are automatically added to the forwarding table and all additions are added using static provisioning through the management interface. The default parameters for the additional connection using IPoA are given in Table 19.

**Table 19: Parameters for Subsequent Connection to a Subnetwork if it is Using IPoA**

| Parameter | Default | Reconfigurability |
|---|---|---|
| Encapsulation | IPoA (RFC 2684 routed mode) | No |
| Configuration protocol | None | No |
| Routing Protocol | Static routing | Enabling of optional RIP or RIPv2 |

Further scenarios are created when there is more than one IP subnetwork as illustrated in Figure 12 below.

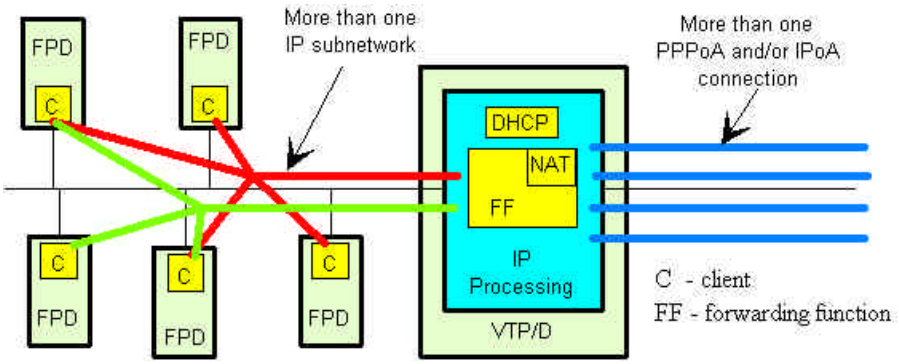



**Figure 12: Adding additional connections to an IP subnetwork when there is more than one IP subnetwork**

Using the rules for creating additional subnetworks, these scenarios can be described as multiple instances of the first scenario shown in Figure 11, as the IP subnetworks are kept entirely separate using virtual routers.

### 8.2.5 IP QoS

In some cases, the nature of IP traffic and any associated quality of service requirements can be clearly handled as a separate subnetwork and ATM VC has been dedicated to a traffic type. In these cases, standard IP forwarding rules can be used to select a routing flow of appropriate quality. An example of this case may be Voice over IP.

However, the VTP/D may implement IP diff-serv buffer management. If this is implemented, an end device can support mixed traffic types routing to the same IP address. In this case the ATM VC traffic type must be CBR.

## 8.3. Broadcast IP processing and encapsulation

A detailed description of Broadcast IP processing is given in sections 8.4.3.5 and 10 of Part 2 [9].

## 8.4. Channel change processing and encapsulation

A detailed description of end-to-end channel change message processing including required protocol parameter tuning is given in sections 10.3 and 10.4 of Part 2 [9]. In addition, a VTP/D MUST assume default class D address subnet of 239.192.0.0/14 for the broadcast TV and entertainment channels. An implementation example of interworking between IGMPv2, that is used on the residential network, and DSM-CC, that may be used in the access network, is given in FS-VDSL Part 2 [9], Appendix IV.

## 8.5. Bridge processing

The VTP/D must implement bridging functionality according to IEEE 802.1D [59]. Where more than one Bridging flow exists, The bridge processing MUST NOT allow bridging between the bridged ATM VCs. (Note this restriction allows the VTP/D to function correctly without the need to a spanning tree protocol). The bridge processing also needs to implement frame filtering needed to extract out the frames for the PPPoE flow and the channel change flow in the upstream direction and insert frames from these flows in the downstream direction.

### 8.6. BLES processing (optional)

The requirements shall be according to DSL Forum Requirements for Voice over DSL Version 1.1: [44].

ATM architecture elements shall be found in ATMF Loop Emulation Service using AAL2 [46]. Specific elements for the use of AAL2 shall be compliant to ITU I.366.1 [47] for the Segmentation and reassembly (SAR) and I.366.2 [48] for AAL2 Convergence sub-layer.

### 8.7. Management

The VTP/D MUST be capable of being remotely and locally managed. It MUST also support remote file transfer capability so that the VTP/D software may be remotely upgraded.

#### 8.7.1 Remote Management

The VTP/D can be remotely managed using the mechanisms listed below:

- VDSL Embedded Operations Channel (EOC) – The VDSL EOC is associated with the VDSL physical link and is used to manage the VDSL line parameters such as the VDSL rates, signal to noise margins and line coding. The VDSL EOC exists between the VTP/D and the ONU.
- Integrated Local Management Interface (ILMI) – ILMI is used to manage and configure the ATM layer parameters of the VTP/D as defined in af-nm-0165.000. ILMI utilises a predefined VPI/VCI value and this channel exists between the VTP/D and the Access Network. The configuration parameters include the identification of the pre-established ATM PVCs. The traffic descriptor, AAL parameter and the flow associated with the PVC.
- VTP/D remote management – A dedicated ATM PVC is used for remote management of the VTP/D MIB and this has been termed as the "Remote Management Flow". The Remote Management flow exists between the VTP/D and the VTP/D Management System that resides within the core network. The management protocol can be SNMPv2c (RFC1901 [65]), HTTP or a Command Line Interface. The remote management protocol MUST use either PPPoE, PPPoA or IPoA encapsulation.

This remote management flow is used for managing and configuring the layers not covered by the previous two mechanisms. These are essentially the IP and ethernet layers of the VTP/D. In the situation where ILMI is not used, then the ATM layer parameters may be configured using the remote management flow. In this case the remote management flow shall use the default VPI/VCI of "0/50" with a PPPoE encapsulation. Where ILMI and remote management flow mechanisms are supported by the VTP/D, then the ILMI MIB shall be deemed the master.

#### 8.7.2 Management Information Model

In order to enable management of the VTP/D, there needs to exist a management information model at the VTP/D as shown in Figure 13. The aim of this model is to encourage standard use of various functions within the VTP/D, thus allowing off-the-shelf components to be used in the production of such a VTP/D. The aim is also to make as much use of existing information models as possible. Thus later on a description is given on how the VTP/D model fits into an overall architecture consisting of other models.

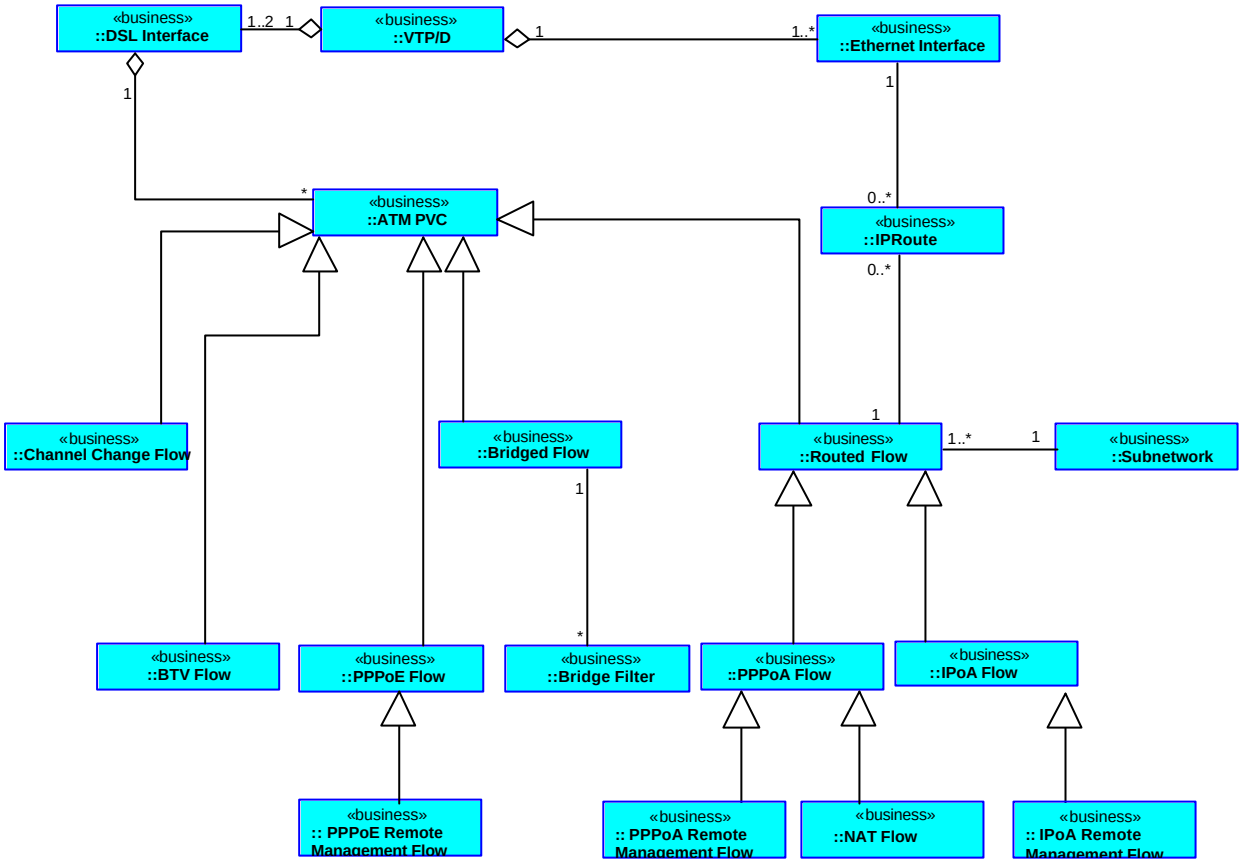



**Figure 13: VTP/D Management Information Model**

The VTP/D management model reads as below.

A VTP/D contains up to two DSL interfaces (i.e. fast and/or interleaved path) for interconnecting to an Access Network and one or more Ethernet interfaces for interconnecting to the home network.

The DSL interface contains 1 or more ATM Permanent Virtual Circuit (PVC) connections. Each of these PVCs is nominated to transport a particular type of packet and this is termed a flow. The following flows can exist within the VTP/D:

- Channel Change – A single flow per VTP/D that is used for transporting IGMPv2 or DSM-CC packets to and from the AN.
- Broadcast TV – This flow is used for transporting broadcast TV packets that are encapsulated using MPEG2/AAL5 or MPEG2/UDP/IP. The number of Broadcast TV flows that are established is dependent upon the number of simultaneous broadcast TV flows that are required to be delivred to the home network.
- PPPoE – used for transporting any IP packets from and towards the home network that use PPPoE encapsulation
- Bridged Flow – Bridged flows carry any 802.3 Ethernet II frames that are subject to 802.1d bridging via the bridging function within the VTP/D. Bridged flows may also be subject to special configurable filtering requirements that can determine if the frame is to be sent over the bridged flow.
- Routed Flow - Routed flows are used to carry IP packets that are subject to IP routing by the VTP/D. There are two different types of routed flows:
    - PPPoA flows carry routed IP packets that use PPPoA encapsulation. Packets that have a source IP address that is not routeable by the network must therefore have their IP address substituted with a routeable address which was allocated via PPPoA. These packets are carried via a NAT flow. This function is performed by the NAT function within the VTP/D and enables many FPDs to share the same IP address when communicating with the network. The NAT flow is a specialisation of the PPPoA flow.

- IPoA flows carry routed IP packets that use IPoA encapsulation.

- Remote Management Flow - A dedicated flow is allocated for remote management of the VTP/D. Depending upon the encapsulation method used for the remote management flow, in the information model it is represented as either a PPPoE Remote Management Flow, PPPoA Remote Management flow or an IPoA Remote Management flow. This enables the remote management flow to inherit the attributes from the super classes. It should be noted that PPPoA and IPoA encapsulated remote management flows are not subject to IP forwarding within the VTP/D. Remote management packets are sent directly over the route flow. This simplifies configuration within the VTP/D, since an IP Route entry is not required to be created etc.

Each Routed flow carries IP packets to and from with a single IP subnetwork. Packets from a single IP subnetwork can be carried by multiple Routed flows. For example packets from a home subnetwork that identifies IP VPN addresses are carried on a VPN routed flow. While packets that identify Public IP addresses are carried on the Public Internet routed flow.

The IP Route is a forwarding entry used for IP routing. Each IP route is either associated with a Routed Flow for onward routing of the packet towards the AN or an Ethernet interface for onward routing towards the home network. A routed flow may be referenced from one or more IP routes and an Ethernet interface may also be referenced from one or more IP routes.

### 8.7.3 Description of Classes and Attributes

This section provides a textual description of all the classes contained in the Management Information model and the attributes associated with each of the classes

| **VTP/D – This class represents the VTP/D entity.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| *Vendorname* | Text String | The name of the vendor that supplied the VTP/D device |
| *DeviceType* | Text String | Vendors model number for the VTP/D device |
| *HardwareVersion* | Text String | The hardware revision for the VTP/D device |
| *SoftwareVersion* | Text String | The software revision for the VTP/D device |
| *SerialNumber* | Text String | The serial number for the VTP/D device. |
| *InstallationDate* | Date | The date the VTP/D was installed. In the form day/month/year. |
| *AdminStatus* | Unlocked,locked,,shuttingdown, testing | Indicates the desired state of the VTP/D device |
| *OperStatus* | enabled, disabled, testing | Provides the current operation status of the VTP/D device. |
| *BTVEncapDetection* | MPEG2/UDP/IP, MPEG2/AAL5, Auto | Broadcast TV flows may be sent using MPEG2/AAL5 or MPEG2/UDP/IP. This attribute describes what detection capabilities are provided within the VTP/D. “Auto” means that the VTP/D has the capability to detect the type of flow. |
| *SVCCapability* | No, UNI4.0 | Indicates whether or not the VTP/D has the capability to establish VC connections using ATM-F UNI 4.0 Signalling. If the attribute specifies “No”, then the VC connections are established as PVCs. |
| *VoATMSupport* | No, Yes | If the attribute indicates “Yes”, then the VTP/D must support the Voice over ATM MIB defined in AF-VMOA-0175.000 [63] and this is outside the scope of the main stream VTP/D MIB. |

| DSL Interface – **This class represents the DSL interface that is used for attaching the VTP/D device to the AN.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| | | For details refer to the ADSL Forum TR-027 [64] which integrates the DSL interface type into the IETF MIB II<br>Typical attributes supported are:<br>• DSL type (e.g. ADSL, VDSL, RADSL)<br>• Latency Path (i.e. fast or interleaved). |

| ATM PVC – **This class represents an ATM PVC.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| VPI | 0-255 | The VPI value of the PVC |
| VCI | 32-65535 | The VCI value of the PVC |
| Traffic Descriptor | Sequence | The set describes the following:<br>ATM service class supported (i.e. CBR, UBR, VBR-nrt, VBR-rt, UBR, UBR+).<br>Cell Rates (e.g. PCR, SCR, MBS, MCR) |
| AAL5 Descriptor | Sequence | The set describes the following:<br>Maximum size of the AAL5 PDU |
| AAL5pdusreceived | 0-65535 | The number of AAL5 PDUs received on the ATM PVC |
| AAL5pdussent | 0-65535 | The number of AAL5 PDUs sent on the ATM PVC |
| AAL5crcerrors | 0-65535 | The number of received AAL5 PDUs discarded due to a CRC error in the AAL5 frame. |
| ATMcellhecerrors | 0-65535 | The number of ATM cells discarded due to a header error check. |
| F4ccsink | off, on | The value “On” means that if F4 OAM end-to-end and segment continuity check cells are not received on this VPI within a specified duration, then Loss Of Cell state will be declared. If “off”, then the F4 OAM end-to-end and segment continuity check cells are ignored. |
| F5ccsink | off, on | The value “On” means that if F5 OAM end-to-end and segment continuity check cells are not received on this VPI within a specified duration, then Loss Of Cell state will be declared. If “off”, then the F5 end-to-end and segment OAM continuity check cells are ignored. |

| Channel Change Flow – **This class is a specialisation of the ATM PVC class that is used for transporting IGMP and DSM-CC channel change packets towards and from the AN.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| ChannelChangeProtocol | IGMPv2, DSM-CC | Indicates whether IGMP or DSM-CC is used as the channel change protocol between the VTP/D and OLT/ONU. |
| Lastmemberqueryinterval | 1-100 (multiples of 100ms) | The interval within which an FPD must respond to a Group Specific Query from the VTP/D. The value corresponds to a multiple of 100ms. For example value 2 means 200ms. |
| Lastmemberquerycount | 1-10 | Defines the number of group specific queries sent before the VTP/D assumes there are no members of the multicast group. |
| Multicastaddressrange | Any contiguous IP class D address range | The Class D address range used by the broadcast TV flows. This information is needed by the VTP/D so that if the IGMP request contains a IP class D address in the range specified by this attribute, then it will be sent on the channel change flow. Otherwise it will be bridged and or routed. |

| Broadcast TV Flow – **This class is a specialisation of the ATM PVC class that is used for transporting Broadcast TV packets from the AN.** | | |
|---|---|---|
| Attribute | Values | **Description** |
| Non currently defined. | | |

| PPPoE Remote Management Flow – **This class is a specialisation of the ATM PVC class that is used for transporting Management flows that are used to remotely manage the VTP/D and use PPPoE encapsulation.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently identified. | | |

| Bridged Flow – **This class is a specialisation of the ATM PVC class that is used for transporting Bridged flows which are packets that have are subject to 802.1d bridging.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non defined currently. | | |

| Bridged Filter – **This class identifies the type of Ethernet packets that may be sent on the bridged flow that references this filter.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Filter | Any, PPPoE, IPoE, ARP, RARP, Source MAC Address Match Pattern, Destination MAC Address Match Pattern. | Identifies the type of packets that may be sent on the associated bridged flow. It shall also possible to perform logical operation such as “AND”, “OR” , “NOT” operations on these filter values and create more complex structures. |

| Routed Flow – **This class is a specialisation of the ATM PVC class that is used for transporting IP Packets that have been subject to routing.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently defined. | | |

| PPPoA Flow – **This class is a specialisation of the Routed Flow that is used for transporting IP Packets that are encapsulated using PPPoA.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| EchoIntervalTimer | -1 to 65535 (In seconds) | Indicates the interval that LCP Echo Request packets must be sent in order to keep the PPP link active. The value –1 indicates echo packets are not sent. |
| LoginId | Text String | Indicates the user identity in the form user@domain that is used by the RADIUS server within the network in order to authenticate the user. |
| Password | Text String | The password of the user that will be used by the RADIUS server within the network in order to authenticate the user. |
| AuthenticationProtocol | PAP, CHAP, none | This attribute identifies the preferred authentication protocol that the VTP/D wishes the Edge Router to use. |

| IPoA Flow – **This class is a specialisation of the Routed Flow that is used for transporting IP Packets that are encapsulated using PPPoA.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently defined. | | |

| NAT Flow – **This class is a specialisation of the PPPoA flow and is used to carry IP packets that cannot be routed by the network. These packets have had the non-routeable IP address substituted with a routeable IP address that was allocated via PPPoA IPCP. This substitution is performed by the NAT function within the VTP/D.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| UpStreamAllowedPorts | List of allowed UDP/TCP ports. | The list of upstream UDP/TCP port numbers that the NAT function will perform address translation for. |
| DownStreamdPortMapping | List of UDP/TCP ports to a Private Home Network Address | Mapping of UDP/TCP ports to a private IP address used within the home network. |
| NATApplicationRelay | List of applications that are subject to relay by the NAT function. | Certain application protocols such as FTP carry IP addresses within the application layer. These addresses must be substituted with a routeable IP address by the NAT function in order for the application protocol to operate correctly. |

| SubNetwork – **Multiple FPDs may be present within the home network and if they have their traffic routed via one or more of the routed flows, then a subnetwork must be configured within the VTP/D. This subnetwork is managed via a DHCP server located within the VTP/D, that then uses the subnetwork parameters to provide configuration details to the FPDs as part of DHCP.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| SubnetworkMask | Octet String (4) | Subnetwork mask to be used by the FPD in order determine the net and sub-network ids. If a PPPoA sub-flow uses the IPCP sub-network mask option, then this value will be dynamically assigned by the Edge Router. |
| SubNetworkAddress | Octet String (4) | The IP sub network address that is to be used for the managed sub-network. If a PPPoA sub-flow uses the IPCP sub-network mask option, then this value will be dynamically assigned by the Edge Router.<br>This value along with the subnetwork mask is used by the DHCP server located within the VTP/D to allocated IP addresses and the default gateway address. |
| PrimaryDNS | Octet String (4) | This IP address of the primary Domain Name Server. If the routed flow uses a NAT or PPPoA sub-flow, then this attribute is not applicable, because the value will be dynamically assigned by the Edge Router as part of IPCP. |
| SecondaryDNS | Octet String (4) | This IP address of the secondary Domain Name Server. If the routed flow uses a NAT or PPPoA sub-flow, then this attribute is not applicable, because the value will be dynamically assigned by the Edge Router as part of IPCP. |

| IP Route – **This class represents a entry in an IP routing table which is used by the VTP/D for routing of IP packets received from the Ethernet Interface and onwards to a Routed Flow and vice versa. IP routes using NAT and PPPoA sub-flows will be automatically configured.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| IPForwardDest | Octet String (4) | The destination IP address of this route. An entry with a value of "0.0.0.0" will be considered as the default route. |
| IPForwardMask | Octet String (4) | Indicates the mask to be logically ANDed with the destination address before being compared with the value in the IPForwardDest field. |
| IPForwardPolicy | -1 to 15 | A value of –1 indicates that the policy attribute is not applicable. Any other valid value indicates that only received IP packets that have the TOS field matching this value will be forwarded on this IP route. |

| PPPoA Remote Management Flow – **This class is a specialisation of the ATM PVC class that is used for transporting Management flows that are used to remotely manage the VTP/D and use PPPoA encapsulation.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently identified. | | |

| PPPoE Flow – **This class is a specialisation of the ATM PVC class that is used for transporting PPPoE flows.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently defined. | | |

| IPoA Remote Management Flow – **This class is a specialisation of the ATM PVC class that is used for transporting Management flows that are used to remotely manage the VTP/D and use IPoA encapsulation.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| Non currently identified. | | |

| Ethernet Interface - **This class represents an 802.3 Ethernet II interface.** | | |
|---|---|---|
| **Attribute** | **Values** | **Description** |
| MAC Address | Octet String (6) | MAC address of the 802.3 Ethernet Interface |
| UnicastEthernetFramesRx | Integer | Unicast Ethernet Frames Received over this interface. |
| UnicastEthernetFramesTx | Integer | Unicast Ethernet Frames Transmitted over this interface. |
| BroadcastEthernetFramesRx | Integer | Broadcast Ethernet Frames Received over this interface. |
| BroadcastEthernetFramesTx | Integer | Broadcast Ethernet Frames Transmitted over this interface. |
| ErroredEthernetFramesRx | Integer | Error Ethernet Frames Received over this interface. |
| AutoNegotiation | Enable, Disable | If set to enable, then the VTP/D will negotiate the speed and the duplex mode. If set to disable, then the speed of the Ethernet interface and the duplex mode is specified by the RateDuplexMode attribute. |
| RateDuplexMode | 10MbpsFullDuplex, 10MbpsHalfDuplex, 100MbpsFullDuplex, 100MbpsHalfDuplex | Defines the speed and duplex mode of the Ethernet Interface of the AutoNegotiation attribute is disabled. |

#### 8.7.4 Relation to other MIBs

It is assumed that the management of the VTP/D will be done using SNMP. As a result the derived SNMP MIB for the VTP/D will have the following relationships with other SNMP MIBs.

- Interfaces MIB [62] – The interfaces MIB defines the physical and logical interfaces of the a system. The VTP/D model has two interfaces that will also exist in the Interfaces MIB. These are the DSL Interface and Ethernet Interface. Hence there will be a link between the VTP/D MIB and the IfTable of the Interfaces MIB.
- ILMI MIB [14] – If ILMI is used for PVC auto-configuration at the VTP/D then the ILMI MIB defines the configuration information associated with the PVCs existing at the VTP/D. This includes the ATM VCCs, associated AAL and Layer2 and 3 protocols. Aspects such as the statistics for the AAL layer and also the configuration of F4/F5 parameters are not provided through ILMI and thus these would have to be modelled within the VTP/D MIB.
- CP-IWF MIB [63] – If Voice over ATM (VoATM) connections are supported then the VTP/D contains a CP-IWF. The management of the CP-IWF and the associated VoATM connections shall be performed through the CP-IWF MIB.
- SNMP DSL Line MIB [64] – The management of the Physical DSL Interface will be as defined by the DSL interface MIB.

#### 8.7.5 File Transfer to the VTP

A file transfer capability MUST be provided within the VTP in order to allow the software that is resident on the VTP to be updated. The use of the file transfer is not limited to software download only, the capability may be used for other applications such as downloading a configuration file.

##### 8.7.5.1 File Transfer Method

The VTP shall support the Trivial File Transfer Protocol (TFTP) for supporting file transfer operations. The TFTP protocol is defined in detail in [54] and it as been chosen because of its simplicity and therefore does not require any complex processing within the VTP.

#### 8.7.5.1.1 Transport of TFTP

TFTP is transported over UDP/IP that means that the same flow designated for remote management can also be used for TFTP.

#### 8.7.5.1.2 TFTP usage

TFTP can be used to transfer a file to the VTP. TFTP shall use the packet format and procedures defined in RFC1350 [54].

The VTP shall function as the TFTP client. A file transfer is triggered, for example upon start up and the VTP will initiate a RRQ (Read Request) packet indicating a request to read a file. The network shall acknowledge a RRQ by sending a data packet. The connection is then deemed to be successfully opened and files can be transferred in fixed blocks of 512 bytes.

Each data packet contains one block of data and must be acknowledged by an ACK packet before the next packet can be sent. A data packet of less than 512 bytes indicates termination of the transfer. ERR packets can also cause termination of the transfer.

The VTP must be capable of supporting at least one transfer session. The TFTP transfer identifiers (TIDs) are used to distinguish between the different sessions.

The naming convention for files and the file types used (e.g. software image, configuration) are outside the scope of this specification.

## 9. Middleware and Application Programming Interfaces

The FS-VDSL specification is addressing network infrastructure based on VDSL. Within this context there are limited requirements for CPE middleware and APIs.

### 9.1. Middleware

The term “middleware” is typically applied to set top boxes or other devices that do functional processing and/or decoding at the customer premise. Unlike set tops used for cable or satellite distribution (a one-to-many environment), set tops in a VDSL network function, in part, as intelligent network termination devices (a one-to-one environment). These set tops will also support a wide variety of applications including digital TV, interactive program guides, personal video recording, video on demand, and other TV-based services.

Consequently, the FS-VDSL Committee does not intend to specify a single operating environment for supporting client-based applications since this would artificially restrict the options available to the service domain. However, any middleware deployed on set top boxes in a VDSL environment must support the requirements specified in the section on Operations, Administration, Management and Provisioning and the technologies for channel change as specified in the section on Systems Architecture.

### 9.2. Application Programming Interfaces

VDSL-based services will use a variety of set top boxes supporting a variety of operating systems and programming tools. Consequently, the FS-VDSL Committee does not intend to specify a specific set of APIs. However, set top boxes and other CPE must provide APIs needed to support the requirements specified in the section on Operations, Administration, Management and Provisioning and an interface to the technologies for channel change as specified in FS VDSL Part 2.

APPENDIX I (INFORMATIVE)

**Implementation Examples**

*This appendix describes example implementations.*

### Upstream Protocol Processing

Consider Figure A-1, which describes the protocol processing performed by a VTP on upstream traffic. The left hand side denotes the residential network, the $T_{CN}$ interface. The VTP is assumed to be connected to the residential network in promiscuous mode, namely every frame that is transmitted over the residential network is received by the VTP. The right hand side of the figure denotes the access network side, the UR interface. A single named arrow denotes a single ATM VC connection. Additional unlabeled arrows denote that more VCs from the same type are possible.

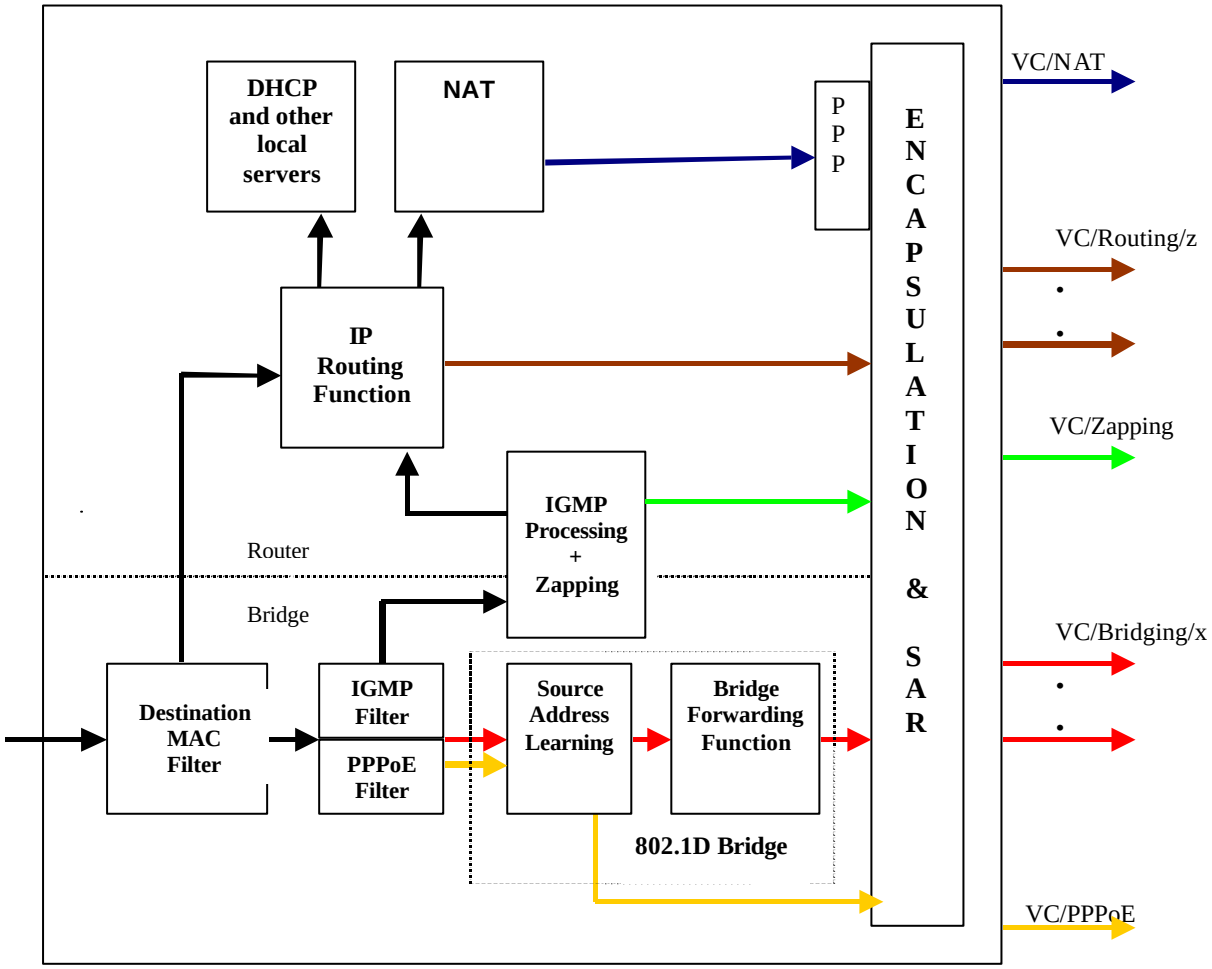



**Figure A-1 VTP Upstream Protocol Processing**

Two blocks are common to all traffic flows. The first is the Encapsulation and SAR block which performs the RFC 2684 [25] encapsulation, the AAL sub-layer processing and the ATM segmentation. The second is the ATM layer, which performs prioritized cell queuing and shaping.

The processing of an incoming frame begins in layer 2. The first stage is to inspect the frame's destination MAC address. If it is identical to the VTP's MAC address, then the frame is transferred directly to layer 3 processing. If not, it is either a broadcast/multicast frame or a unicast frame to be bridged. The aim of the next layer 2 module, the PPPoE filter, is to separate PPPoE and Bridged frames traveling to the same router or BRAS into different ATM VCs. Note that if the PPPoE and Bridged VCs terminate in different routers or BRASes, then almost the same filtering function can be achieved by the Bridging function itself. The PPPoE filtering module inspects the Ethertype field of the received frame. If a PPPoE frame (i.e. Ethertype=0x8863 or 0x8864) is discovered, it is filtered and delivered for transmission on the ATM VC dedicated for PPPoE traffic.

Also at this stage IGMP messages with a destination class D address assigned to the broadcast media (TV) service are passed to the IGMP processing block and corresponding channel change messages (either IGMP or DSM-CC) are transmitted to the access network on a dedicated VC. Any other IGMP multicast and non-PPPoE broadcast frame is forwarded both to the IP (layer 3) and to the Bridge forwarding function. Source MAC address learning is performed on all frames but those that the IGMP filter deviated towards the IGMP processing block. The Bridge forwarding block performs forwarding decisions according to the learning bridge tables (as a standard 802.1D bridge).

Packets forwarded to the IP routing function trigger a lookup into the routing table. It is assumed that the routing table consists of a mapping between each Routed ATM VC and at least one distinct IP subnet (or host). The default gateway is configured to be the NAT PPPoA connection (when active). Therefore, while the NAT PPPoA can be used for Internet communication, the Routed VCs can only be used to communicate with intranets (i.e. specific networks or subnets). Local traffic, for example DHCP requests carrying the VTP's own IP address or a broadcast address, are filtered and sent to local protocol processing. Packets routed to the default gateway are first passed through the NAT block. The public IP address that is used for NAT is received during the IP control protocol (IPCP), which is a standard part of the PPP suite.

Management, BLES and ILMI flows are not shown in the figure nor described in this example.

**Downstream Protocol Processing**

Figure A1-2 describes the protocol processing that is performed in the downstream direction. The first block is the Encapsulation and SAR block, which performs the ATM reassembly, the AAL sub-layer processing and the RFC 2684 [25] de-capsulation. The ATM VCs of the broadcast TV are relevant only to the downstream, since they are uni-directional (i.e. point to multipoint ATM VCs). Frames received on broadcast TV VCs are sent directly to the MAC driver for transmission. Frames coming from the PPPoE VC are forwarded to the Bridge forwarding block (i.e. this is required when multiple physical ports are available towards the residential network). Frames from Bridged VCs are first passed through the Bridging function (i.e. forwarding and learning) and then sent for transmission. Routed packets are handled by the IP routing function (e.g. ARP etc.) and then forwarded to the MAC driver. The same treatment is given to locally generated packets, like DHCP responses. The PPP block handles the PPP sessions running over the VC/NAT and VC/routing connections. I packets at the output of the PPP block are sent to the routing function either directly or through the NAT block, which performs network and port address translations. Management, BLES and ILMI flows are not shown in the figure nor described in this example.

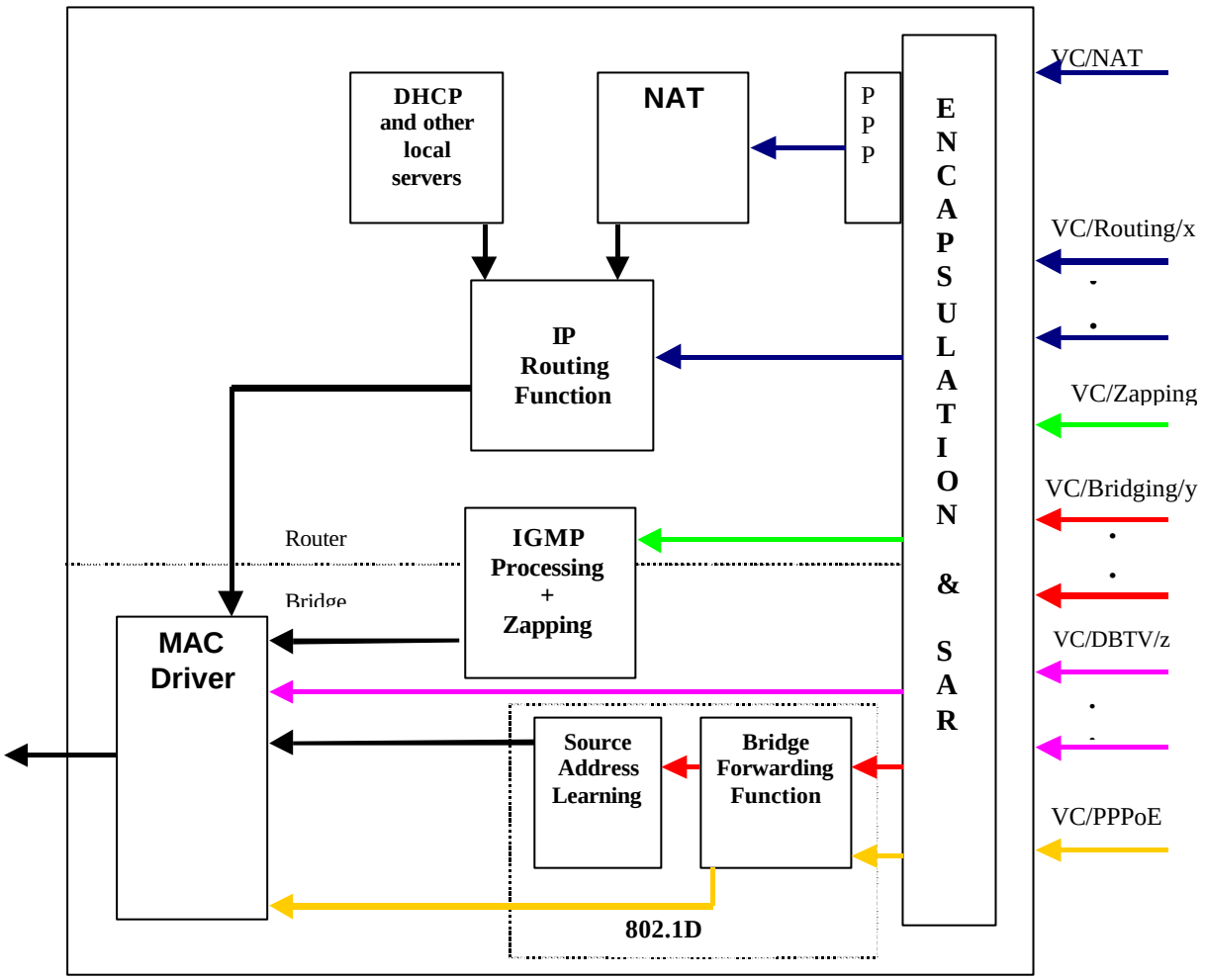



**Figure A1-2. Downstream Protocol Processing**