INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FS-VDSL
FGTS

Full-Service VDSL

Focus Group
Technical Specification

Part 2: System Architecture

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 1.0.0 / 5 June 2002
Part 2:	System Architecture	Version 1.0.0 / 5 June 2002
Part 3:	Customer Premises Equipment	Version 1.0.0 / 5 June 2002
Part 4:	Physical Layer Specification for Interoperable VDSL Systems	Version 1.0.0 / 5 June 2002
Part 5:	Operations, Administration and Maintenance & Provision aspects for FS-VDSL Services	Version 1.0.0 / 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 2: System Architecture specification

Summary

This document specifies the System Architecture requirements in an FS-VDSL system within the ITU-T FS-VDSL Focus Group established under ITU-T Study Group 16 "Multimedia services, systems and terminals.". This specification includes the FS-VDSL System Reference Model, describes all the network elements in an FS-VDSL Network, describes all the Network and transport capabilities required in an FS-VDSL Network, and provides guidelines for the implementation of voice, video and data services.

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

1. SCOPE 1

2. ABBREVIATIONS 1

3. DEFINITIONS 3

3.1. Access Network (AN) Operator 3

3.2. Core Network operator 3

3.3. Service Operator 3

3.4. Service Provider 4

3.5. Content Provider 4

3.6. FP 4

3.7. FPD 4

3.8. VTP 4

3.9. VTPD 4

3.10. VTP/D 4

3.11. Residential Centralized Model 4

3.12. Residential Distributed Model 4

4. REFERENCES 4

5. TERMINOLOGY USED 6

6. SYSTEM ARCHITECTURE REFERENCE MODEL 6

7. NETWORK ELEMENTS 8

7.1. Set Top Box (STB) and Other End User Equipment and the Residential Network 8

7.2. VTP/D 8
7.2.1 Tcn Interface 9
7.2.2 U-R2 Interface 9

7.3. OLT 9
7.3.1 Network Interface Element 9
7.3.2 Telephone Service Network Interfaces 10
7.3.3 ATM Cross Connect 10
7.3.4 Optical Distribution Network Interface (ODN) 10
7.3.5 OAM Block 10
7.3.6 Power Block 10
7.3.7 Clock Block 10

7.4. ONU 10
7.4.1 ODN Interface 11
7.4.2 Voice Adaptation 11

7.4.3 ATM Cross Connect 11
7.4.4 VDSL Interfaces 11
7.4.5 POTS/ISDN Splitter 11
7.4.6 OAM Block 11
7.4.7 Power Block 11
7.4.8 Subtending 11

7.5. Service Node Architecture 12
7.5.1 The ATM to Core Network Device 12
7.5.2 Core Network 12
7.5.3 ATM/IP Edge Service Node 12
7.5.4 Broadcast TV HeadEnd 13
7.5.5 VoD HeadEnd 13
7.5.6 Voice Gateway 13

8. NETWORK AND TRANSPORT CAPABILITIES 13

8.1. ATM Engineering Principles 13
8.1.1 ATM Configuration Requirements 13
8.1.1.1 Access Network 13
8.1.1.1.1 OAM F4 and F5 Support 14
8.1.1.2 OLT 14
8.1.1.2.1 OAM F4 and F5 Support 14

8.2. Protection Switching 14

8.3. IP Engineering 15
8.3.1 VTP/D Private Addressing Scheme 16
8.3.2 VTP/D Initiated Connection to Service Operator Addressing Scheme 16
8.3.3 Session Based Access Initiated by a Terminal for Accessing a Service Operator Addressing Scheme 16
8.3.4 Connectivity to a Service Operator Terminated in a User Terminal Without Session Establishment 16
8.3.5 IP Addressing Policy Using DHCP 17

8.4. Network Connection Capabilities 17
8.4.1 ATM VC Connection 17
8.4.2 ATM VP Connection 18
8.4.3 Functional Connections 18
8.4.3.1 Bridge Connection 18
8.4.3.2 PPPoE Connection 20
8.4.3.3 Channel Change Connection 20
8.4.3.3.1 Use of IGMPv2 21
8.4.3.3.2 Use of DSM-CC 21
8.4.3.4 NAT Connection 21
8.4.3.5 Route Connection 22
8.4.3.5.1 IP over ATM 22
8.4.3.5.2 Routed PPPoA 22
8.4.3.6 Digital Broadcast Connections 23
8.4.3.6.1 Broadcast Services at the V Interface 23
8.4.3.6.2 OLT to ONU 23
8.4.3.6.3 ONU to VTP/D 23
8.4.3.6.4 A/V Content Encoding and Encapsulation 24
8.4.3.6.5 Digital Broadcast Connection Encapsulation 24
8.4.3.7 VTP/D Remote Management Connection 25

9. DATA SERVICE 26

9.1. PPP-based Data Access 26

9.2. Bridged Data Access 26

9.3. Data Connection Sharing 26

10. BROADCAST TV AND ENTERTAINMENT SERVICE 26

10.1. Encoding 26
10.1.1 Broadcast TV IP Addressing Scheme 26
10.1.2 Configuration Options Considerations 27

10.2. Transport 27
10.2.1 Channel Replication and ATM Cross Connect 27
10.2.2 Encryption 27
10.2.3 Administrative Channel 27
10.2.4 DBTV Quality of Service Performance Objectives 27
10.2.4.1 HeadEnd 28
10.2.4.2 OLT-ONU and Copper Loop 28
10.2.4.3 VTP and Home Network 28
10.2.4.4 FPD 28

10.3. Channel Change Signalling 28
10.3.1 IGMPv2 and DSM-CC use for Channel Change control 28
10.3.2 IGMPv2 End-to-End for Broadcast Channel Change Control 29
10.3.2.1 STB Requirements 30
10.3.2.2 VTP Requirements 30
10.3.2.3 AN Requirements 30
10.3.3 IP source addresses used in IGMP messages 30

10.4. Information Model For The Channel Change Function Within The AN 31
10.4.1 Channel Change 31
10.4.2 Connection Admission Control (CAC) 32
10.4.3 Conditional Access at the OLT/ONU 32

11. VOD SERVICE 32

11.1. VOD Back Office Management 34

11.2. VOD Network Engineering 34
11.2.1 VOD Server Farms: Centralized vs. Distributed 34
11.2.2 Two-way Administrative Traffic 35
11.2.3 Downstream Video Traffic 35
11.2.4 QOS Requirements for VOD Traffic 35
11.2.5 Encapsulation 35

11.3. VOD Content Browsing 35

11.4. VOD Session Establishment 36

11.5. VOD Connection Establishment 36
11.5.1 Pre-Established Bandwidth End-to-End 37
11.5.2 Bandwidth Bottleneck in the Transport Network 38
11.5.3 Connection Establishment Protocol Requirements 39
11.5.4 Connection Establishment Protocol Options 39
11.5.5 IP Address Assignment for Downstream VOD Video 39

12. VOICE OVER DSL (VODSL) 40

12.1. BLES 40

12.2. Voice over IP (VoIP) 41

APPENDIX I SNMP MIB FOR THE CHANNEL CHANGE FUNCTION 44

APPENDIX II POSSIBLE ACCESS NETWORK AND CORE NETWORK CONFIGURATIONS (INFORMATIVE) 56

APPENDIX III VDSL DUAL LATENCY CHANNEL SUPPORT (INFORMATIVE)..... 59

APPENDIX IV IGMP V2 TO DSMCC TRANSLATION FUNCTION..... 61

APPENDIX V MESSAGE SEQUENCE CHARTS (INFORMATIVE)..... 63

ITU-T FS-VDSL Focus Group Technical Specification 2

Part 2: System Architecture

1. Scope

This document provides a specification for a Full Service VDSL system architecture within the FSAN FS-VDSL Committee. It is meant to help standardize FS-VDSL system requirements for mass VDSL deployment. This specification includes the FS-VDSL System Reference Model, describes all the Network elements in an FS-VDSL Network, describes all the network and transport capabilities required in an FS-VDSL Network, and provides guidelines for the implementation of voice, video and data services. In addition, the specification points to other standards that currently exist, or are in development by other standards bodies. It is not the intent of this working group to write a VDSL system architecture specification from the ground up, but rather, to create the FS-VDSL specification by leveraging work already done and assist work underway by other standard bodies.

Note that this document is intended to specify the System 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 other broadband systems. employing other broadband physical layer technologies.

2. Abbreviations

This specification uses the following abbreviations:

A/V	Audio/Video
AN	Access Network
AAL	ATM Adaptation Layer
AIS	Alarm Indication signal
ANSI	American National Standard Institute
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BLES	Broadband Loop Emulated Service
CBR	Constant Bit Rate
CC	Continuity Check
CDV	Cell Delay Variation
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CPE	Customer Premises Equipment
DAVIC	Digital Audio-Visual Council
DBTV	Digital Broadcast TV
DHCP	Dynamic Host Configuration Protocol
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSM-CC	Digital Storage Media – Command and Control
EMS	Element Management System
EPD	Early packet Discard
ETSI	European Telecommunication Standards Institute
FPD	Functional processing and Decoding block
FSAN	Full Service Access Network

FS-VDSL	Full Service VDSL
HTML	Hyper Text Mark-up Language
IAD	Integrated Access Device
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IWCN	InterWorking to Core Network
LAN	Local Area Network
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPEG	Moving Pictures Experts Group
NAT	Network Address Translation
OAM	Operation and Management
ODN	Optical Distribution Network
ODN	Optical Distribution Network
OLT	Optical Line Termination
ONU	Optical Network Unit
ONU	Optical Network Unit
OUT-C	Optical Termination Unit - Central Office
OUT-R	Optical Termination Unit - Remote
PBX	Private Branch Exchange
PCR	Program Clock Reference
POTS	Plain Old Telephony Service
PPD	Partial Packet Discard
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPOE	PPP over Ethernet
PS	Pots or ISDN Splitter
PVC	Permanent Virtual Circuit
PVC	Permanent Virtual Connection
PVP	Permanent Virtual Path
QoS	Quality of Service
QoS	Quality of Service
RDI	Remote Defect Indication
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SGCP	Simple Gateway Control Protocol

SIP	Session Initiated Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPTS	Single Program Transport Stream
STB	Set Top Box
SVC	Switched Virtual Circuit
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
UBR	Unspecified Bit Rate
UPC	Usage Parameter Control
VBR	Variable Bit Rate
VBRnrt	Variable Bit Rate non real time
VBR_{rt}	Variable Bit real time
VC	Virtual Connection
VCI	Virtual Channel Identifier
VDSL	Very High Bit Rate Digital Subscriber Line
VLAN	Virtual LAN
VoD	Video on Demand
VoDSL	Voice over DSL
VoIP	Voice over IP
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VTP	VDSL Termination Processing
VTP/D	VTP and/or VTPD
VTPD	VDSL Termination Processing and Decoding
VTU-C	VDSL Terminal Unit – Central Office
VTU-C	VDSL Termination Unit - Central Office
VTU-R	VDSL Terminal Unit – Remote

3. Definitions

This specification defines the following terms:

3.1. Access Network (AN) Operator

The AN Operator operates the physical access system. Encompassing the domain between the U-R and V interface of the system reference model.

3.2. Core Network operator

The Core Network Operator maintains and manages the core network beyond the V interface and the OLT physical interface.

3.3. Service Operator

The Service Operator maintains and manages 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. Service Provider

The Service Provider is the entity that uses the Service Operator's physical platform to provide access to various services, including data services, broadcast video services, VoD services, and voice services.

3.5. Content Provider

The Content Provider generates content such as video copies in various digital or analog formats. The Service Provider is expected to contract the Content Provider in order to have access to its content and to allow access to subscribed users.

3.6. FP

Functional Processing. A point of signal transformation or processing.

3.7. FPD

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

3.8. 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.

3.9. VTPD

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

3.10. VTP/D

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

3.11. Residential Centralized Model

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

3.12. 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] IEEE 802.3, "Telecommunication & Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications" 2002

[2] FS-VDSL Part 4, "Physical Layer Specification for Interoperable VDSL Systems," Oz Micka, June 2002

[3] ITU-T Recommendation I.610, "B-ISDN operation and maintenance principles and functions," February 1999

[4] ATM Forum Specification af-tm-0056.000, "Traffic Management Specification, Version 4.0," April 1996

[5] ATM Forum Specification af-sig-0061.000, "ATM User-Network Interface (UNI), Signalling Specification, Version 4.0," July 1996

[6] ITU-T Recommendation G.783, "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks," October 2000

[7] ITU-T Recommendation I.630, "ATM protection switching," February 1999

[8] RFC 2131, "Dynamic Host Configuration Protocol," R. Droms, March 1997

[9] RFC 2132, "DHCP Options and BOOTP Vendor Extensions," S. Alexander, R. Droms, March 1997

[10] IEEE 802.1D, "Media Access Control (MAC) Bridges" 1998

[11] RFC2684, “Multiprotocol Encapsulation over ATM Adaptation Layer 5,” D. Grossman, J. Heinanen, September 1999

[12] RFC2516, “A Method for Transmitting PPP Over Ethernet (PPPoE) ,” L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, R. Wheeler, February 1999

[13] RFC 2236, “Internet Group Management Protocol, Version 2,” W. Fenner, November 1997

[14] ISO/IEC 13816-6 – Information Technology – “Generic Coding of moving pictures and associated audio information” – Part 6: “Extensions for DSM-CC”. © ISO/IEC. 1998

See Chapter 10, “U-N Switched Digital Broadcast – Channel Change Protocol”, and Annex H (informative), Switched Digital Broadcast Service.

[15] RFC2364, “PPP Over AAL5,” G. Gross, M. Kaycee, A. Lin, A. Malis, J. Stephens, July 1998

[16] ITU-T Recommendation J.82, “Transport of MPEG-2 constant bit rate television signals in B-ISDN,” July 1996

[17] ATM Forum Specification AF-ILMI-0065.000, “Integrated Local Management Interface (ILMI) specification” 1996

[18] ETSI TR 101 290, “Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems”, May 2001

[19] AF-TM-0121.00, "The ATM Forum Technical Committee Traffic Management Specification Version 4.1," March 1999.

[20] RFC2326, “Real Time Streaming Protocol (RTSP),” H. Schulzrinne, A. Rao, R. Lanphier, April 1998

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

[22] FS-VDSL Part 3, “Customer Premises Equipment Specification,” Olivier van de Wiel, Steve Palm, Amit Cohen, Wolfgang Kluge, Andy Reid, June 2002

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. System Architecture Reference Model

The committee acknowledges existing DSL Networks reference models. Some modifications and additions were applied to existing reference models to accommodate them for the FS-VDSL system. The reference model in Figure 1 uses ITU and DSL Forum models as its basis. The intent of the FS-VDSL model is that it should:

- Be representative.
- Clearly identify the interfaces and the reference points.
- Be compatible with other appropriate industry standard reference models.
- Be as simple as possible to facilitate the clear mapping of the protocol stacks.
- Be access oriented. That is, the model should represent the delivery process at the access network.

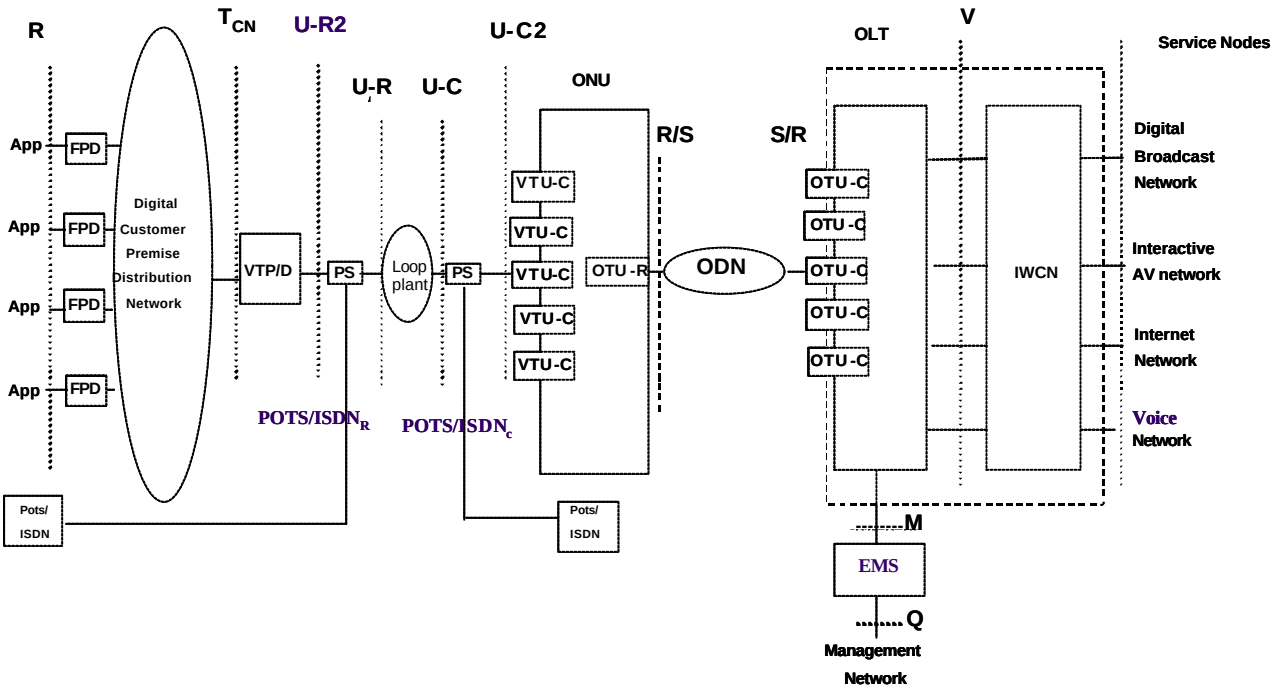


Figure 1: FS-VDSL reference model

The following definitions apply to the reference model:

AN: Access Network. Includes the ONU and the OLT. In the reference model, this is between the U-R2 and the V interface.

Digital Broadcast Network: A multicast Network that is used to efficiently distribute point to multi-point traffic such as digital TV and radio.

EMS: Element Management System.

FPD: See 3.7

Interactive A/V Network: A unicast Network used to deliver point to point video and audio services such as VoD.

Internet Network: Broadband data Network in duplex mode for IP based services, typically Internet services.

ISDN: Integrated Services Digital Network.

IWCN (InterWorking to Core Network): Any function that may be included in the OLT to interwork with non ATM core networks. Due to the variety of core network technologies and configurations (see Appendix II for an overview), this specification only covers the OLT requirements up to the V reference point, which are ATM based.

M: Reference point used between the OLT and the EMS.

ODN (Optical Distribution Network): Provides the optical transmission medium, linking the OLT towards the ONUs, and vice versa, between the S/R and R/S reference points.

OLT (Optical Line Termination): Provides the network interface to several service nodes for multiple ONUs that are connected through the ODN.

ONU (Optical Network Unit): Provides the user side interfaces and is interconnected to a parent OLT via the ODN.

OTU-C (Optical Termination Unit): Optical termination unit at the OLT.

OTU-R (Optical Termination Unit): Optical termination unit at the ONU.

POTS: Plain Old Telephone Service.

PS (POTS or ISDN Splitter): Passive splitter which combines low frequency signal (e.g., POTS or ISDN) and high frequency signal (i.e. VDSL) at the ONU side and at the Customer premises side.

Q: Reference point used to describe the interface to the management network, typically for system configuration, maintenance and provisioning.

R: The output (input) of the FPD towards (from) the home appliance.

R/S: Reference point used between the ODN and ONU.

S/R: Reference point used between the OLT and the ODN. This can be a point to point or a point to multipoint optical interface.

Tcn: The output (input) of the digital port(s) of the VTP/D toward (from) the digital Network at the customer premises.

U-C2: Reference point used between the Pots or ISDN splitter and the VTU-C.

U-C: Reference point used between the splitters, located at the ONU, and the copper network.

V: Reference point used between the OLT and one or more service nodes, either directly or via the Core Network.

VTU-C (VDSL Termination Unit): VDSL transmission unit at the ONU.

U-R: The network side of the PS located at the customer premise.

U-R2: The network side input (output) of the VDSL modem.

POTSc/ISDNc: Interface between the PSTN and the PS splitter at the ONU side.

$POTS_R$/$ISDN_R$: Interface between narrowband terminals and the PS splitter at the customer premises side.

Voice Network: A network that is capable of delivering toll quality voice and switched voice services. The network is typically a TDM network such as PSTN or ISDN, but can also be a packet based voice network.

VTP: See 3.8

VTPD: See 3.9

7. Network Elements

7.1. Set Top Box (STB) and Other End User Equipment and the Residential Network

The STB is an instantiation of an FPD (described in 6)

The STB performs the decoding of the digital video signal, interfaces to the TV and performs interactive communication over the residential network. There are no restrictions imposed on the layer 1 of the residential network. However, the residential network must implement Ethernet [1] for its layer 2 and IP for its layer 3.

The STB MAY implement a vendor specific DRM solution. The DRM mechanism should impose no restriction to any specified FS-VDSL services and operations. Any DRM related connections should be performed through the specified FS-VDSL connections.

The unit that implements the decoding function of the STB as well as the VTP functions, is referred to as VTPD.

7.2. VTP/D

The VTP/D performs the VDSL termination and ATM termination (see appendix II for clarification on access and core network types). The VTP/D initiates the Bridge Connections (see 8.4.3.1), Channel Change Connection (see 8.4.3.3), Route Connections (see 8.4.3.4) and the NAT Connection (see8.4.3.4). The VTP/D MAY support multiple emulated voice connections.

In addition to the VTP functions, the VTPD performs the decoding of a single or multiple video streams. The use of VTP/D in this document refers to both the VTP and the VTPD.

7.2.1 Tcn Interface

The Tcn is an 'Ethernet-like' interface in the sense that it MUST present to the VTP/D's protocol processing modules an 802.3 frame as defined in [1] with the Type/Length field specifying the MAC client protocol type. This, however, does not imply that the residential network must use the 802.3 MAC layer or an Ethernet (e.g. 10baseT) physical layer. Different types of MAC (e.g. HomePNA, 802.11b) and physical layers (e.g. USB) may be used. Where the term 'Ethernet', is used in this or companion specifications, within the context of a layer in a protocol stack, it refers to the 802.3 frame format as defined above.

7.2.2 U-R2 Interface

At the U-R2 interface, the VTP/D interfaces are:

- Layer 1: VDSL as described in FS-VDSL Part 4 [2]
- Layer 2: ATM AAL2, AAL5
- Layer 3 and above: Described in Section 8.4.3

7.3. OLT

The OLT operates as an aggregator for a number of ONUs. In the upstream direction, the OLT serves as an ATM layer multiplexer/concentrator between the V interface and connected ONUs; while in the downstream direction, it performs demultiplexing to the distributed ONUs.

FS-VDSL systems can perform the combined functionality of the ONU and the OLT in a single physical box. In the case of a unified ONU and OLT system, all (described below) functional elements of the OLT and ONU MUST be present in the unified physical box.

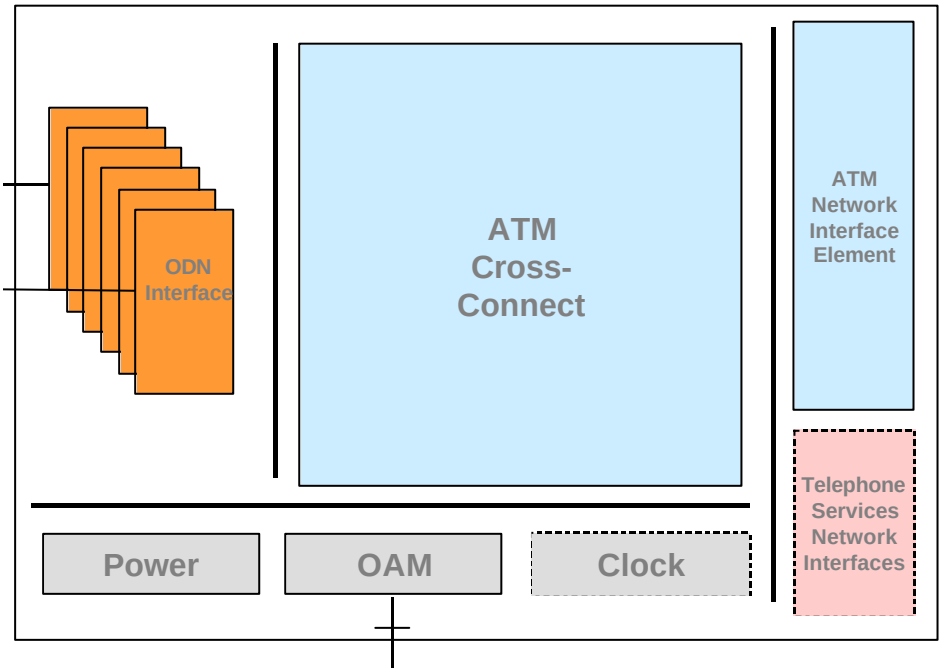


Figure 2: OLT Functional Blocks

7.3.1 Network Interface Element

The Network Interface Element performs the ATM and PHY layer functions to interface the OLT to the ATM network. In the case that other then ATM core networks are implemented, the network interface element performs the protocol

conversion to interface to other core networks. Multiple Network Interface Elements, supporting unidirectional or bi-directional ATM transmission, MAY exist in a single OLT.

7.3.2 Telephone Service Network Interfaces

The OLT MAY contain a Telephone Interface Element that performs the ATM and PHY layer functions to interface the OLT to the core voice network. A Telephone Interface Element MAY support TDM, ATM or IP voice transport and connection control.

7.3.3 ATM Cross Connect

This block performs VPI/VCI cross-connection to and from the appropriate interfaces. This block MUST support ATM point to multipoint connections to replicate a VPI/VCI to multiple downstream VPI/VCI connections. This block SHOULD perform higher layer protocol functions like channel change processing, access control and management.

7.3.4 Optical Distribution Network Interface (ODN)

The Optical Distribution Network Interface performs the ATM and PHY layer functions to interface the OLT ODN interface to the ODN interface of the ONU. The ODN interfaces MAY conform to various optical transmission standards or MAY be vendor specific.

7.3.5 OAM Block

The OAM block enables the operation and management controls of the AN via the M interface. Remote operation and management of the AN MUST be possible through an in-band connection to the OAM block, and MAY be possible through an out-of-band connection. The M interface is permitted to be vendor specific. However, a standard management protocol, (e.g., SNMP, CORBA, CMIP) MUST be supported for operator specific management systems accessing the OAM block directly.

7.3.6 Power Block

The power block supplies the appropriate voltage and current to all the electronic circuits. The OLT, typically located in the Central Office, does not require any dedicated backup battery.

7.3.7 Clock Block

Depending on the implementation of other blocks, a clock interface MAY be implemented.

7.4. ONU

The ONU serves as an ATM cross-connect between the VDSL lines and the ODN.

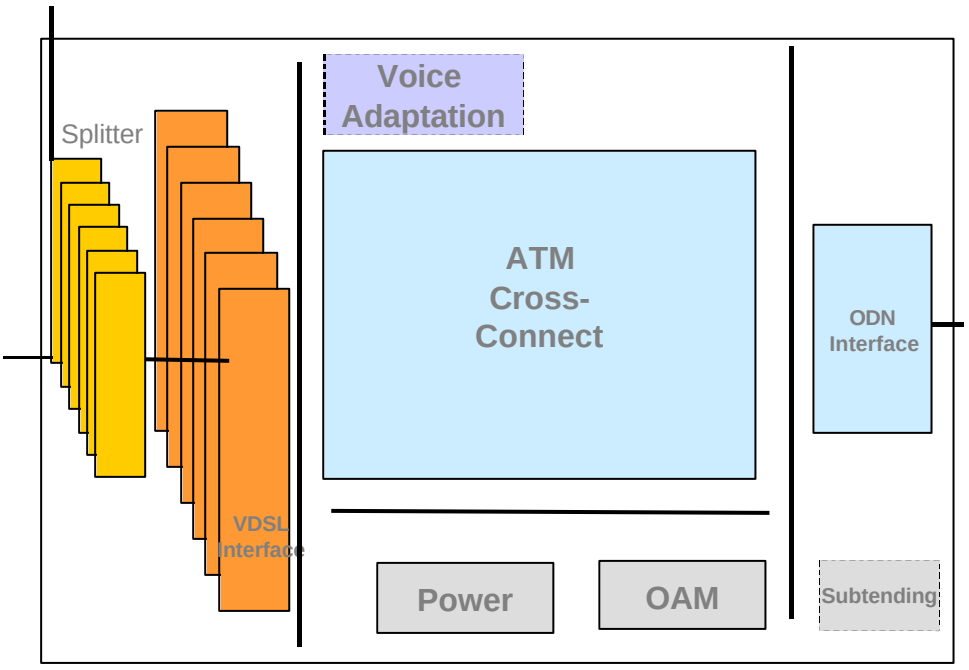


Figure 3: ONU Functional Blocks

7.4.1 ODN Interface

The ONU contains an ODN Interface that performs the ATM and PHY layer functions to interface the ONU to the OLT ODN.

7.4.2 Voice Adaptation

The ONU MAY contain a voice adaptation element that performs mapping of baseband voice signals to Voice over packet, Voice over ATM or voice over IP.

7.4.3 ATM Cross Connect

This block performs VPI/VCI cross-connection to and from the appropriate interfaces. This block MAY support ATM point to multipoint connections to replicate a VPI/VCI to multiple downstream VPI/VCI connections. The decision to implement the channel replication function at the ONU depends on factors such as implementation cost, number of customers served, the fiber capacity between the ONU and OLT, and the number of channels offered. This block MAY perform higher layer protocol functions like channel change processing.

7.4.4 VDSL Interfaces

The VDSL interface performs the VTU-C functionality. It terminates the VDSL PHY layer functions and supports ATM transport over the copper lines.

7.4.5 POTS/ISDN Splitter

In the upstream direction, the POTS splitter performs the PHY layer separation of the POTS/ISDN carrier frequency and the VDSL carrier frequency. In the downstream direction, the POTS/ISDN splitter combines the POTS/ISDN PHY carrier and the VDSL PHY carrier into defined separate carrier frequencies over the same copper drop.

7.4.6 OAM Block

The OAM block enables operation and management control of the ONU including the VDSL drops. Operation MUST be performed through an in-band connection to the OLT OAM block.

7.4.7 Power Block

The power block supplies the appropriate voltage and current to all the electronic circuits of the ONU. If in existence, the power block should supply power to the cooling fans, and to the battery backup circuitry. In addition, if in existence, the ONU Power Block MUST provide power for environmental sensors or external alarm circuits.

Typical ONU powering schemes are composed of local, remote and backup components.

7.4.8 Subtending

The ONU MAY include a subtending block to connect additional secondary ONUs to the OLT.

7.5. Service Node Architecture

Figure 4 proposes a schematic description of the Service Nodes in an FS-VDSL system.

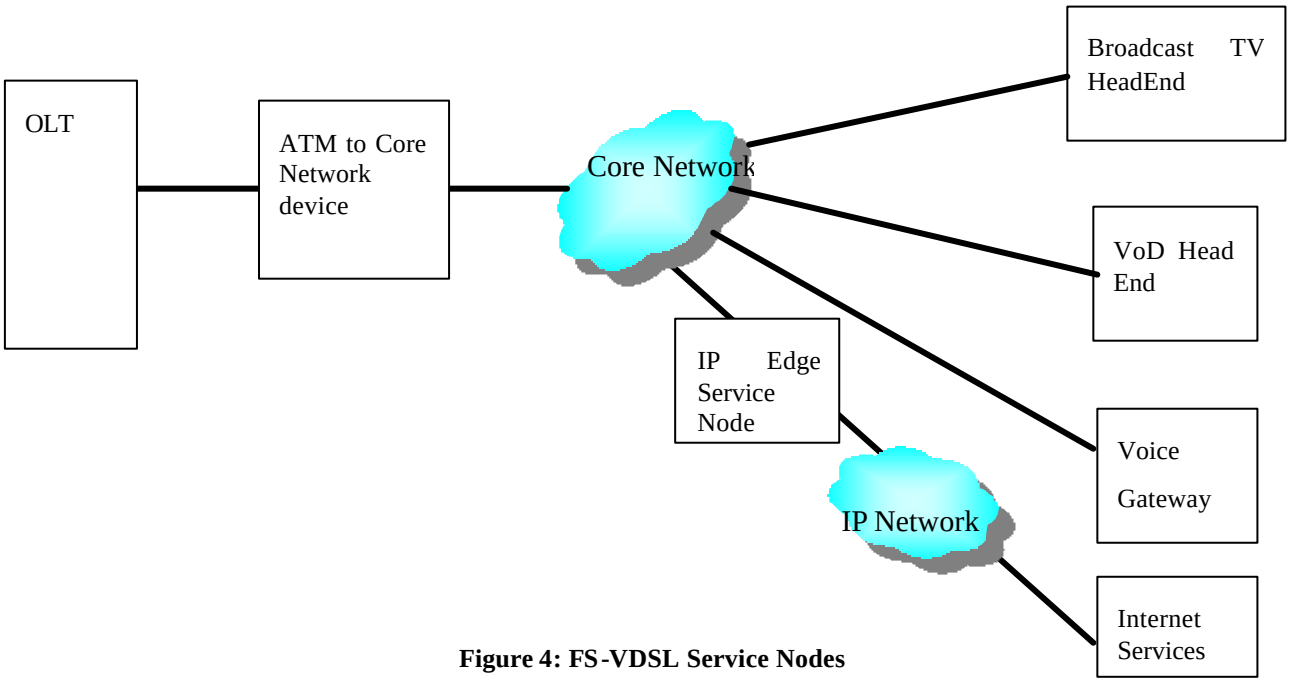


Figure 4: FS-VDSL Service Nodes

7.5.1 The ATM to Core Network Device

Where desired, the ATM to core network device enables the required protocol conversion to interconnect the OLT ATM interface, exclusively or simultaneously, to either an IP based core network or other layer 2 core network. The ATM to core network device could be an embedded element to the OLT or an external one. (See Appendix II for additional details of possible implementation.)

7.5.2 Core Network

The core network is used to flexibly interconnect the AN to various Service Nodes. The Core Network technology used (e.g., ATM, IP, MPLS etc.) is outside the scope of this specification. However, it MUST be able to support the following capabilities:

- Sufficient bandwidth capacity to support the traffic between the AN and the Service Nodes it interconnects.
- Support for the appropriate QoS for the various services.
- Routing/Switching of traffic between the access networks and the service nodes.
- Multicasting of broadcast traffic at the most optimal points within the core network.
- Admission control if concentration of bandwidth occurs within the core network.
- Interworking of hybrid core network technologies (e.g., ATM to IP).
- If interconnection to third party Networks is allowed, then the appropriate peering points must be provided.

7.5.3 ATM/IP Edge Service Node

In the case that the Core Network is an ATM based network, the ATM/IP Edge Service Node operates as the logical termination point between the ATM Network and the IP network. The service node terminates ATM VCs, extracts higher layer PDUs (e.g., PPP, Ethemet, IP) and forwards or tunnels them to the proper destinations. The ATM/IP Edge Service Node SHOULD be able to support multiple PVP and PVC connections as described in 8.4.

7.5.4 Broadcast TV HeadEnd

The HeadEnd system is expected to receive video streams in various formats, reformat and encapsulate the video streams, interface the core network and transmit the video signal over the core network towards the access network. This specification does not aim to specify any restriction on the video acquisition mechanism applied by the HeadEnd system. However, the Network design MUST assure that the appropriate encapsulation of the video signal, as described in 8.4.3.6.5, is performed prior to the video stream appearance at the V interface.

7.5.5 VoD HeadEnd

Due to the interactive nature of VoD services, the VoD Headend is comprised of multiple elements that ensure the on demand video streaming of content. The following are the four elements that comprise the VoD Headend. (see 11 for further details):

- Back office management.
- A "server farm" containing the digital content.
- Transport and AN facilities that can insure QOS.
- Compelling server application software in support of the VoD service.

7.5.6 Voice Gateway

The voice gateway performs the necessary functions to interface the digitally modulated voice traffic to and from the ATM based AN to the legacy PSTN/ISDN. The voice gateway function may be performed by a single device or by multiple devices (such as media gateways, signaling gateways and media gateway controllers).

The main functions of the gateway include:

- Termination of the TDM voice circuits to interface to the PSTN/ISDN.
- Termination of the PSTN/ISDN signaling.
- Call and bearer control.
- AAL2 termination and (de)multiplexing (a single ATM VC carries all voice connections of one VTP/D) in case of BLES.
- VoIP (de)multiplexing (multiple voice connections may be concentrated on a single IP address) in case of VoIP.
- Voice handling functions (e.g., packetization, compression, echo cancellation, echo suppression, silence suppression, comfort noise generation, tones and announcements).
- FPD to Gateway signaling termination.
- Connectivity to the PSTN/ISDN via an open interface.
- V5.2 for ETSI and GR-303 for ANSI.
- Via an NNI (e.g., SS7).

8. Network and Transport Capabilities

8.1. ATM Engineering Principles

8.1.1 ATM Configuration Requirements

The following section describes the OLT and ONU ATM functional requirements. The VTP/D requirements are described in FS-VDSL Part 3. The term *'AN'* is used to describe the overall capabilities of both the OLT and the ONU. For example, if an attribute *x* should be supported by the Access Network, then either the OLT, the ONU or both should implement attribute *x*. Whenever a requirement addresses a specific network component, it is stated so. The above naming convention applies all across this specification.

8.1.1.1 Access Network

The AN MUST support cross-connection of ATM Virtual Path (VP) connections.

The AN MUST support cross-connection of ATM Virtual Channel (VC) connections.

The AN MUST support the termination of VC connections for specific functions like TV channel change, management etc.

The AN MUST be able to act as an ATM OAM endpoint as described in ITU-T I.610 [3], for VC and VP connections (i.e., F5 and F4, respectively) that terminate in it.

The AN MUST be able to act as an OAM segment point for the VC or VP connections that are cross-connected by it.

The AN MUST support ATM point to multipoint connections on which the broadcast TV streams are replicated according to the channel change function.

The AN MUST support traffic policing (i.e., UPC) of user connections as described in the ATM Forum Traffic Management Specification Version 4.0 [4].

The AN MUST support the following ATM Service Categories : CBR, VBRrt, VBRnrt, UBR as defined in [4]

The AN MUST support frame based discard (i.e., EPD/PPD) on a per connection basis designated for AAL5 traffic.

The AN MAY support Switched Virtual Connections (SVCs).

If the AN supports SVCs, it MUST support SIG 4.0 [5] scheme.

8.1.1.1.1 OAM F4 and F5 Support

The following requirements are referring to the OAM implementation as specified in [3]. Note that the access network's behaviour on a specific connection should be according to its configured function on the specific connection (e.g., endpoint, segment point etc.).

The AN MUST respond to OAM loopbacks according to [3]

The AN MUST generate defect indication messages (i.e., AIS, RDI) according to [3]

The AN SHOULD be able to report detected defect indication messages to the OAM blocks.

The AN SHOULD be able to function as a continuity check (CC) sink point according to [3]

8.1.1.2 OLT

The OLT SHOULD support shaping of VP connections towards the Network (i.e. at the V interface).

8.1.1.2.1 OAM F4 and F5 Support

The OLT SHOULD be able to function as a continuity check (CC) source point towards the Access Network.

The OLT SHOULD be able to generate loopback cells (LB) towards the Access Network.

8.2. Protection Switching

In order to provide minimal service disruption for key services (e.g. Broadcast TV and Voice) under interface failure conditions, an FS-VDSL system MAY provide support for "fast" protection switching. The protection switch over

should occur within tens of milliseconds upon detection of the failure, in order to minimise service disruption. There are a number of domains within the system architecture that may be protected. These protected domains and the corresponding protection scheme used are highly dependent upon the network topology and under the control of the network/service operator.

The following list represents an example of fast protection switching schemes that are commonly found and used.

- SDH/SONET Multiplexor Section Protection (MSP) - This scheme utilises two sets of diversely routed feeds, one designated as the working and the other as the protected link. The working link carries traffic under fault free conditions, while the protected link carries all the traffic carried by the working link under fault conditions. Both the protected and working links are terminated at the same end point in the network, so that the bridge (responsible for transmission of traffic) and selector (responsible for reception of traffic) functions can be co-ordinated at both ends of the link (see [6] for further details).
- ATM protection switching – This scheme utilises two sets of diversely routed feeds in a similar fashion to the SDH/SONET MSP scheme. However, since protection occurs at the ATM layer, only Virtual Path Connections (VPC) and Virtual Channel Connections (VCC), that are required to be protected, are designated. This provides savings in bandwidth, since the protected link needs to only have sufficient bandwidth for transporting the protected VPCs and VCCs (see [7] for further details).
- MPLS fast re-route – This scheme requires the establishment of two alternative Label Switch Paths (LSPs) between the source and destination switches, in order to provide a protection domain between the two switches. In case of failure of an interface, it is the responsibility of the source switch to re-direct the traffic using the alternative LSP to the destination switch.

The domains of an FS-VDSL system that may require protection are specified below:

- The ODN interface between the OLT and ONU – Since the ODN interface represents a closed interface, any standardised or proprietary protection scheme is suitable.
- The V interface from the OLT – Either the SDH/SONET MSP, or the ATM protection switching scheme, are appropriate for this interface.
- Core network – The adopted protection scheme is dependent upon the core network technology (e.g. ATM, IP). Therefore, SDH/SONET MSP, ATM protection switching and MPLS fast re-route are all possible.

8.3. IP Engineering

In order to facilitate multiple services through multiple service operators to specific subscribers, several IP addressing schemes need to coexist simultaneously at the subscriber residential Network. Depending on what entity administers the system IP configuration, Network Operators and/or Service Operators must provide guidelines to ensure consistency of all IP addressing schemes. This Includes ensuring that all sub-networks that could be simultaneously accessed by a specific VTP/D do not have conflicting IP address ranges.

The current IP engineering specification is limited to the use of IPv4.

The following constraints dictate the IP engineering scheme applied in an FS-VDSL system.

- Limited IPv4 public address spaces, and the “always on” nature of the service, imply a clear preference toward minimum usage of public addresses.
- In the case of applications sensitive to NAT, like point to point gaming and voice over IP, either public address space or private address space may be implemented.
- The customer is likely to make multiple logical connections to multiple networks within the home Network environment.
- Any entity that provides as part of the service any of the CPE appliances, including the VTP, STB and Internet appliances, will need to be able to communicate with those devices. This may be for upgrade purposes, reconfiguration or initialisation.

The figure below illustrates the addressing schemes considered:

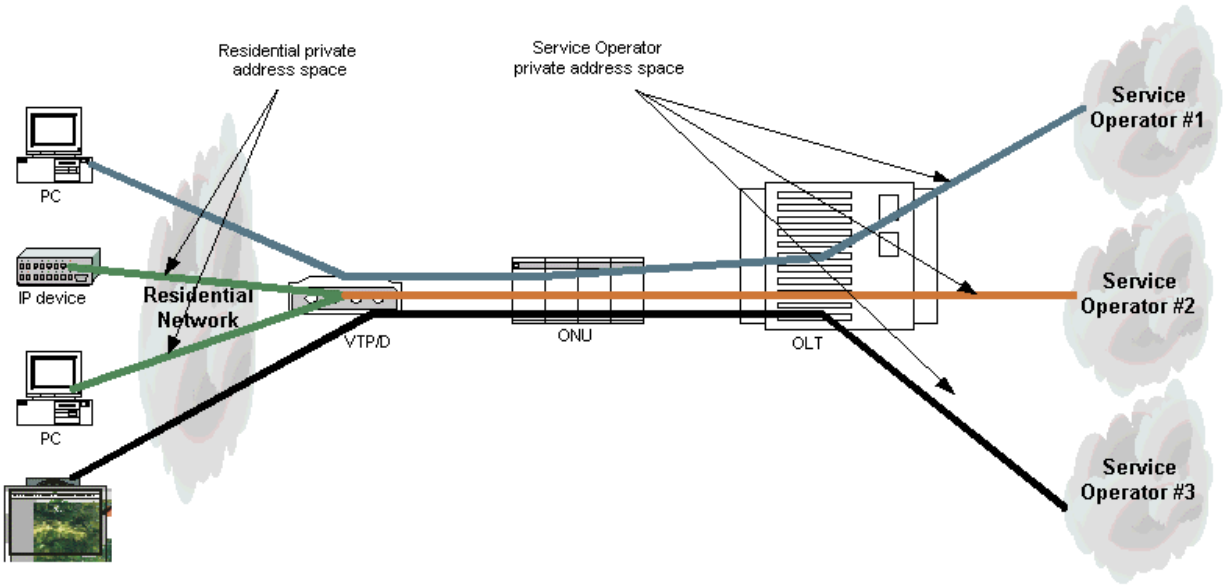


Figure 5: Network addressing schemes

There MAY be up to four simultaneous distinct IP addressing schemes.

- VTP/D private addressing scheme
- VTP/D initiated connection to service operator addressing scheme.
- Terminal session based on service operator addressing scheme.
- Terminal non-session based on service operator addressing scheme.

8.3.1 VTP/D Private Addressing Scheme

In this scheme the VTP/D allocates designated terminals a private IP address through its DHCP server. Optionally, this scheme can be implemented by static IP configuration. However, the use of static IP configuration in this scheme is not recommended.

8.3.2 VTP/D Initiated Connection to Service Operator Addressing Scheme

In this scheme, the service operator implements the below methods to assign the VTP/D with an IP address. Several VTP/D IP address assignments MAY be established simultaneously by different Service Operators. In such case, the routing function of the VTP/D MUST manage the correct forwarding of IP packets to the appropriate connections.

- Session establishment - The VTP/D initiates a PPPoA session with the service operator edge router.
- Non-session based - The VTP/D obtains its IP address from the Service Operator DHCP/BOOTP server.
- Static configuration - Static configuration is possible but is NOT RECOMMENDED.

8.3.3 Session Based Access Initiated by a Terminal for Accessing a Service Operator Addressing Scheme

In this scheme, the terminal initiates a PPPoE session with the service operator data service node. Multiple residential terminals can use this scheme.

8.3.4 Connectivity to a Service Operator Terminated in a User Terminal Without Session Establishment

In this scheme, residential terminals are assigned with an IP address by the service operator using the following methods.

- Dynamic configuration – The terminal IP addresses is assigned by the Service Operator's DHCP server.
- Static configuration – Not recommended.

8.3.5 IP Addressing Policy Using DHCP

Multiple DHCP servers may operate simultaneously in an FS-VDSL system . In order to ensure that the correct DHCP server responds to DHCP messages, an FS-VDSL compliant system must conform to the following:

1. The only DHCP server allowed within the home Network MUST be the one in the VTP/D.
2. DHCP DISCOVERY (see RFC 2131 – sect 4.3.1 [8]) messages initiated by any FS-VDSL FPD MUST include a Vendor Client Identifier specifying the FS-VDSL service (see section 8.4 of [9]) . This identifier MUST be prefixed by the value "FSVDSL" followed by a service name. A service name is defined for Set Top Boxes as "STB." Other service names (e.g., "IPTELEPHONE") are for further study.
3. The VTP/D DHCP server MUST ignore DHCP DISCOVERY messages with a Vendor Class identifier string conforming to the item described above.
4. A Network DHCP server that is intended to pass configuration information exclusively to specific residential FPDs MUST reply to DHCP DISCOVERY messages only if the vendor client identifier prefix, vendor client identifier and service name matches the pre-configured corresponding parameters at that Network DHCP server.

8.4. Network Connection Capabilities

Multiple network connection capabilities are used in a full service network. The following represents the naming conventions and description for the optional network connections. Some connections described are functional utilizations of others (e.g., Routed NAT connection carried over a Routed PPPoA connections).

In order to permit the use non ATM Core Networks, such as IP Network, for the connections between Network elements, some of the below connections are not established exclusively through an ATM Network. However, for the purpose of conventional naming, these connections are represented as ATM Connections between the corresponding two Network elements. The characteristics of the below connections MUST apply to the connection flow at the V interface.

8.4.1 ATM VC Connection

These connections can be established between two elements of the FS-VDSL Network. The naming method of the ATM VC connection indicate the elements between which the connection is established, the “name” of the connection, and, in the case that multiple connections of the same kind are used, the number of the connection. The “name” of a connection is intended to indicate on the functional use of a connection.

Connections between the VTP and the AN – ONU and OLT:

- ATM/VCC/VTP-ONU/<name>/x
- ATM/VCC/VTP-OLT/<name>/x

Connections between the VTP and the Management:

- ATM/VCC/VTP-MNGT/<name>/x

Connections between the VTP and the Service Nodes:

- ATM/VCC/VTP-<Service node name>/<name>/x

Connections between the ONU and the OLT:

- ATM/VCC/ONU-OLT/<name>/x

Connections between the OLT and the Service Nodes:

- ATM/VCC/OLT-<Service node name>/<name>/x

Connections between the OLT and the Management:

- ATM/VCC/OLT-MNGT/<name>/x

8.4.2 ATM VP Connection

These connections can be established between two elements of the FS-VDSL Network. The naming method of the ATM VP connection indicate the elements between which the connection is established, the "name" of the connection, and, in the case that multiple connections of the same kind are used, the number of the connection. The "name" of a connection is intended to indicate on the functional use of a connection.

Connections between the VTP and the AN – ONU and OLT:

- ATM/VPC/VTP-ONU/<name>/x
- ATM/VPC/VTP-OLT/<name>/x

Connections between the VTP and the Service Nodes:

- ATM/VPC/VTP-<Service node name>/<name>x

Connections between the ONU and the OLT:

- ATM/VPC/ONU-OLT/<name>/x

Connections between the OLT and the Service Nodes:

- ATM/VPC/OLT-<Service node name>/<name>/x

Connections between the OLT and the Management:

- ATM/VPC/OLT-MNGT/<name>/x

Every VP can contain VCs as defined above.

8.4.3 Functional Connections

This section describes the required FS-VDSL connections that provide specific functional services. The section provides an indication of the mandatory number of each functional connection an FS-VDSL system must support.

The actual number of connections initiated is dependent upon the operator specific network design topology.

The VTP/D MUST be:

1. Hardware ready to support all the connections described in this section.
2. Software upgradeable through the Network to enhance and support additional flow/connection capabilities.

8.4.3.1 Bridge Connection

This connection is intended for the bridging of Ethernet frames between the VTP/D and a Service Node (SN). Multiple bridge connections MAY be initiated, so that different services MAY simultaneously use different connections. Every instantiation is identified as a **Bridge Connection**. At the V interface a bridge connection MUST use a dedicated ATM VC; it is identified as ATM/VCC/VTP-<service node name>/bridge/x. The Network MUST have the capability to support a minimum of four bridge connections per VDSL line. The bi-directional flow of PDUs received and transmitted on the Bridge connection is identified as the **bridging flow**.

The implementation of the bridging function on the VTP/D MUST be compliant with 802.1D [10]. The forwarding of Ethernet frames is based on self learning and the use of bridge filters. The two bridge points MUST ensure security by explicitly preventing VC-to-VC forwarding. The Ethernet encapsulation at the V and U-R2 interfaces MUST be in accordance with RFC2684 [11] bridge mode using LLC/SNAP without FCS.

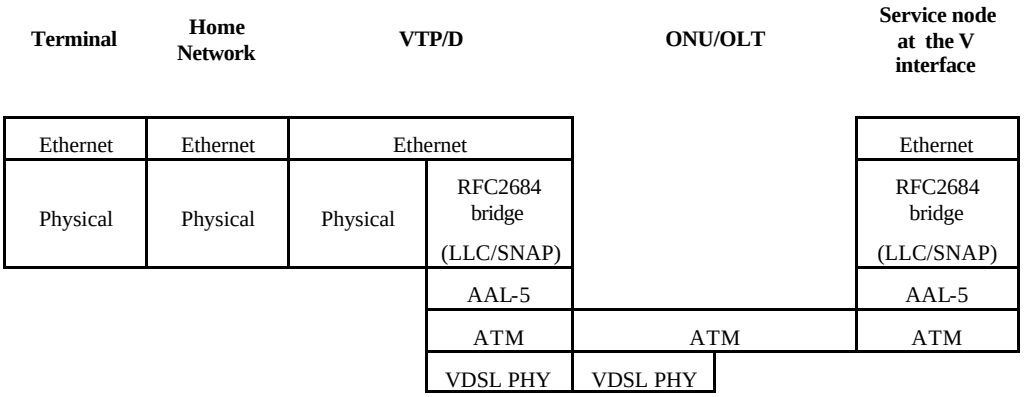


Figure 6: Bridge Connection Protocol Stack

8.4.3.2 PPPoE Connection

This connection is intended to support a PPPoE session between a designated residential terminal and the service node. At the V interface a PPPoE connection MUST use a dedicated ATM VC; it is identified as ATM/VCC/VTP-<service node name>/pppoe/x/. Multiple PPPoE sessions may be established onto the same ATM VC. The network MUST have the capability to support a minimum of one PPPoE connection per VDSL line. The bi-directional flow of PDUs received and transmitted on the PPPoE connection is identified as the **PPPoE flow**.

PPPoE implementation in the terminal and the service node MUST be in accordance with RFC2516 [12].

The encapsulation at the U-R2 and V interface of the PPPoE connection MUST be in accordance with RFC2684 bridge mode using LLC/SNAP without FCS.

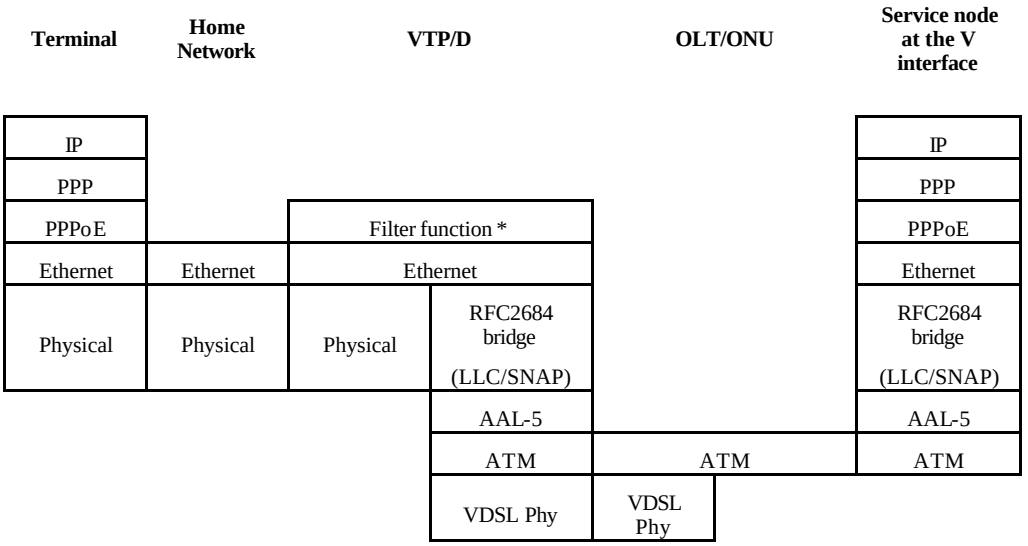


Figure 7: PPPoE Connection Protocol Stack

8.4.3.3 Channel Change Connection

This connection is intended to support the channel change messaging between the VTP/D and the access network. On this connection, channel change messages MUST be IGMPv2 [13] or DSM-CC [14].

A channel change connection MUST use an ATM VC between the VTP/D and the access Network, it is identified as ATM/VCC/VTP-OLT/<channel change>, or ATM/VCC/VTP-ONU/<channel change>.

The Network MUST have the capability to support one channel change connection per VDSL line.

8.4.3.3.1 Use of IGMPv2

In the case that IGMPv2 is used, the encapsulation of the channel change Connection MUST be in accordance with RFC 2684 routed mode using LLC/SNAP.

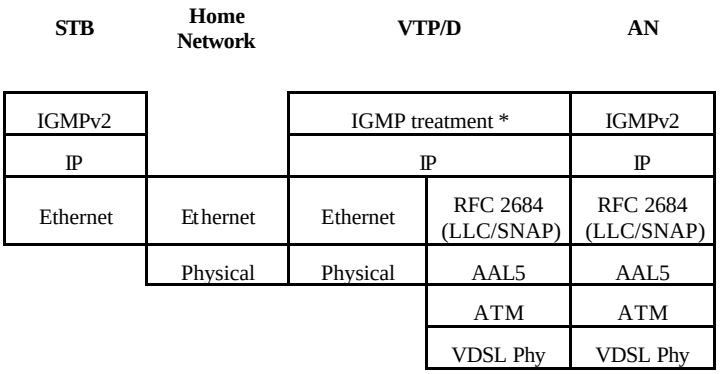


Figure 8: IGMP End-to-End Protocol Stack

* See 8.4 in FS-VDSL Part 3

8.4.3.3.2 Use of DSM-CC

In the case that DSM-CC is used, DSM-C is directly transported over AAL5.

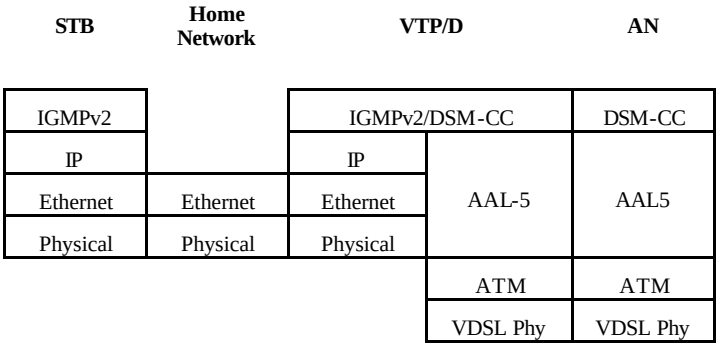


Figure 9: IGMP to DSM-CC Protocol Stack

8.4.3.4 NAT Connection

A NAT connection allows the sharing of a single IP address for Accessing the public Network by multiple end devices. This connection is intended to facilitate a routed connection between the VTP/D and a service node. Whereby, the service operator's VTP assigned IP address is mapped to the residential terminals IP addresses. The associated Port Address Translation (PAT) allows mapping of a single IP address on one interface of a router to multiple (private) IP addresses on the other interfaces. The network MUST have the capability to support one NAT connection per VDSL line.

Both the VTP/D and the service node terminating the ATM VC MUST support PPPoA, in accordance with RFC2364.

The NAT connection is identified as ATM/VCC/VTP/<service node name>/NAT.

The bi-directional flow of PDUs received and transmitted on the NAT connection is identified as the **NAT flow**.

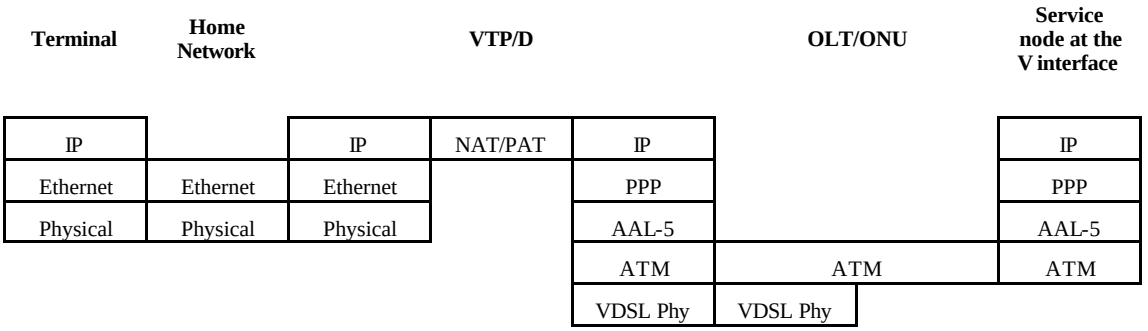


Figure 10: NAT Connection Protocol Stack

8.4.3.5 Route Connection

In the following, the term *'Route'* refers to the function applied to the connection and not to the encapsulation scheme. This connection is intended to facilitate a routed connection between the VTP/D and a service node. Every single connection is identified as a **Route Connection**. The Network MUST have the capability to support a minimum of four route connections per VDSL line. The bi-directional flow of PDUs received and transmitted on the route connection is identified as the **routing flow**.

Several types of route connections are identified based on their IP flow encapsulation. The route connections MAY be an IP over ATM connections (8.4.3.5.1) and/or PPPoA connections (8.4.3.5.2).

8.4.3.5.1 IP over ATM

IP over ATM is performed through RFC 2684 routed mode connections. Both the VTP/D and the service node terminating the ATM layer MUST support RFC2684 routed mode using LLC/SNAP. Unlike the other routed connections, this encapsulation method does not support inherent user authentication. At the V and U-R2 interfaces a route connection using IP over ATM MUST use a dedicated ATM VC, it is identified as ATM/VCC/VTP-<service node name>/ipoa/x.

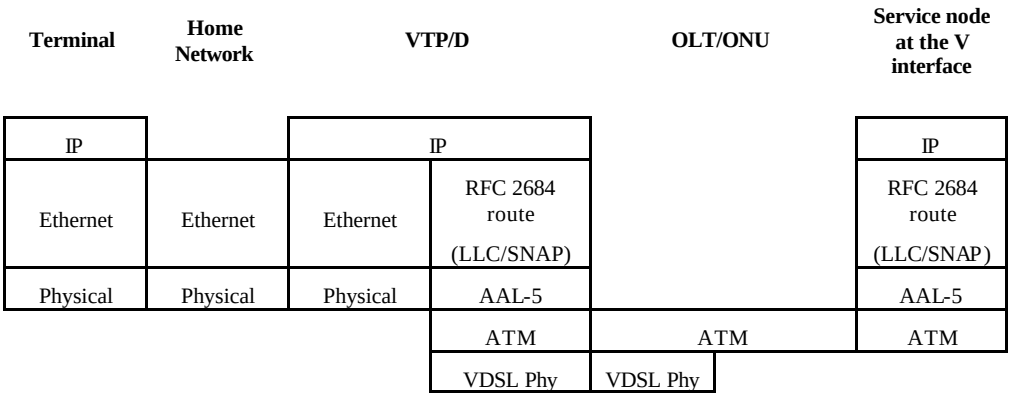


Figure 11: IP over ATM Connection

The IP stack on the VTP can be configured statically or dynamically through DHCP.

8.4.3.5.2 Routed PPPoA

This connection is intended to facilitate the routing of data traffic to and from residential terminals into a PPPoA connection established between the VTP/D and the service node. At the V and U-R2 interfaces a route connection using PPPoA MUST use a dedicated ATM VC, it is identified as ATM/VCC/VTP-<service node name>/pppoa/x.

In order to support a PPPoA connection, both the VTP/D and the service node terminating the ATM VC MUST support PPPoA, in accordance with RFC2364 [15].

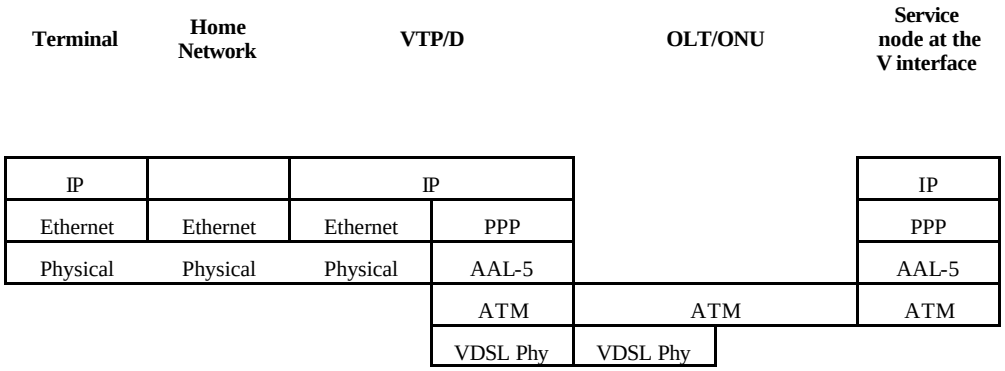


Figure 12: Routed PPPoA Connection Protocol Stack

8.4.3.6 Digital Broadcast Connections

8.4.3.6.1 Broadcast Services at the V Interface

The Service Node tasked with interfacing the video HeadEnd to the Core Network is identified as the TV HeadEnd (TVHE). Every Audio/Video (A/V) content originated at the Broadcast Headend MUST appear at the V interface over a single unique unidirectional ATM VC, identified as ATM/VCC/OLT-TVHE/channel/x. All encapsulated A/V content delivered by the same source MAY appear at the V interface over the same ATM VP, identified as ATM/VPC/OLT-TVHE/channel/x. All A/V content offered to connected subscribers MUST be presented at any time at the V interface.

8.4.3.6.2 OLT to ONU

An A/V content MUST be transported over a single dedicated ATM VC identified as ATM/VCC/OLT-ONU/broadcast/x. All A/V content transported from the OLT to the ONU MAY be transported in the same ATM VP identified as ATM/VPC/OLT-ONU/broadcast.

8.4.3.6.3 ONU to VTP/D

An A/V content MUST be transported over a single ATM VC, identified as ATM/VCC/ ONU-VTP /broadcast/x. All A/V content transported from the ONU to the VTP/D MAY be transported in the same ATM VP identified as ATM/VPC/ONU- VTP /broadcast.

Between the VTP/D and the ONU, there SHOULD be at least four VCs to support the broadcast streams transport.

Figure 13 describes the broadcast connection at all its segments in the case that video decoding STBs are feeding off the VTP.

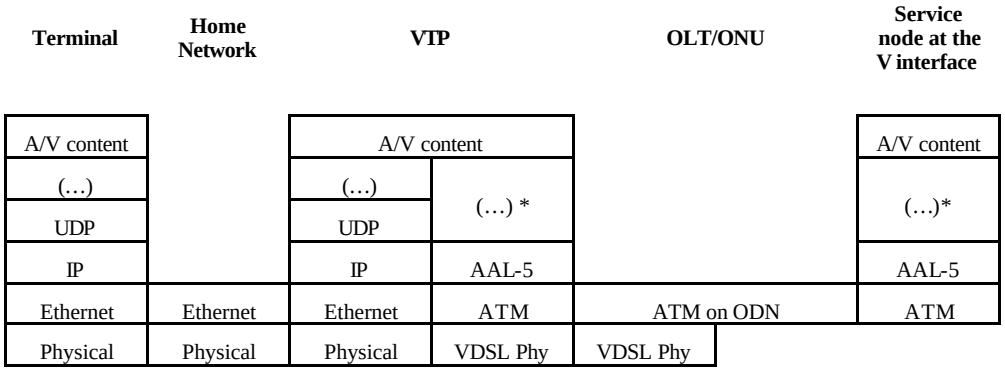


Figure 13: Digital Broadcast Connections Protocol Stack with VTP

Figure 14 describes the broadcast connection at all its segments in the case that the VTD/P is used for the decoding of the video stream.

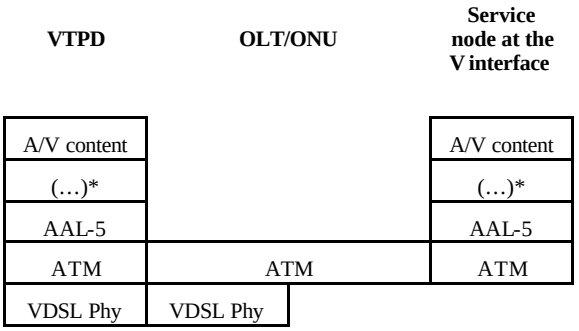


Figure 14: Digital Broadcast Connections Protocol Stack with VTPD

*The A/V content encapsulation is described in 8.4.3.6.4 and 8.4.3.6.5 below.

8.4.3.6.4 A/V Content Encoding and Encapsulation

There are several coding techniques that may be used for audio and video, such as MPEG2 or MPEG-4.

A/V content streams MUST be encapsulated through MPEG-2 SPTS.

8.4.3.6.5 Digital Broadcast Connection Encapsulation

Various A/V content acquisition processes are expected to take place prior to the encapsulation of the MPEG-2 transport streams and their distribution over the core network. FS-VDSL specification puts no constraints on the content acquisition methods.

Prior to transmission of the A/V content over the V interface, appropriate encapsulation must be performed. FS-VDSL proposes two encapsulation options referred to as MPEG2-TS/ATM and MPEG2-TS/IP/ATM, described in detail in 8.4.3.6.5.1 and 8.4.3.6.5.2 Both encapsulations options require that the A/V content be transmitted in a SPTS. Both encapsulation options MAY coexist in a single network. The transport of A/V content in the ONU and OLT MUST be transparent to the existence of any of the two encapsulation options.

In the case where the residential distributed model is implemented, and the encapsulation method is MPEG/ATM, the VTP MUST perform the IP re-encapsulation, to conform to the protocol stack described in 8.4.3.6.3, at the point of streaming the video signal to the residential network. The class D address to be used is retrieved through the BPID indication in the DSM-CC messaging. Since the UDP encapsulation requires a UDP port number, the UDP port to use MUST be 1970.

8.4.3.6.5.1 MPEG2-TS/ATM Encapsulation

MPEG2-TS/ATM encapsulation MUST conform to ITU J.82 section 8 [16], which describes ATM/AAL5 encapsulation of MPEG2-TS.

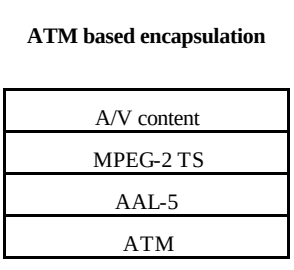


Figure 15: ATM based encapsulation Protocol Stack

8.4.3.6.5.2 MPEG2-TS/IP/ATM Encapsulation

The encapsulation is based on UDP/IP/Ethernet/AAL5/ATM. The encapsulation of the Ethernet frames MUST conform to RFC 2684, bridge mode using LLC/SNAP without FCS.

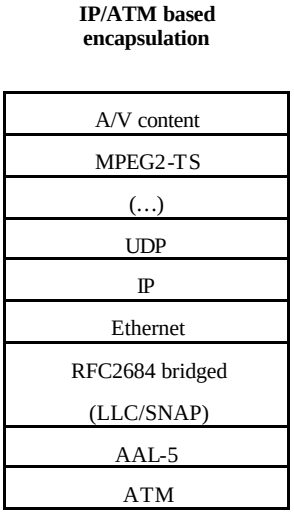


Figure 16: MPEG2-TS/IP/ATM encapsulation Protocol Stack

8.4.3.6.5.3 Additional Encapsulation Methods

The use of an IP based encapsulation of MPEG streamed content is still in its early development in the wider broadcast TV industry. It is not possible, at this stage, to be certain that all other bodies will choose precisely this encapsulation. However, the AN and the VTP provide a transparent pipe to the contents of the IP/UDP packet payload. Any alternative encapsulations above the UDP layer, that may emerge elsewhere, can still be transported across the AN and VTP part of an FS-VDSL based system, for example between a head end system and a STB.

The transport of the A/V content may be done directly over this protocol stack. It is also possible to add a specific encapsulation like RTP. Note that the access network is transparent to such an additional encapsulation.

8.4.3.7 VTP/D Remote Management Connection

Three different mechanisms are used to remotely manage the VTP/D; the VDSL Embedded operations channel, ILMI [17] and the VTP/D MIB Connection. The VTP/D has a default configuration, described in chapter 7.1.1.1 of [2]. In the case that changes to the default configurations are desired, the VTP/D remote management connections, or the local management interface on the VTP/D, may be used.

1. VDSL Embedded Operations Channel

The VDSL physical interface is managed by the VDSL embedded operations channel. The VDSL embedded operations channel exists between the VTP/D and the ONU. The parameters that are configured are described in the VS specification document.

2. ILMI

In the case that ILMI is supported by the VTP/D, the ATM parameters SHOULD be configured using ILMI. The ILMI connection exists between the VTP/D and the access network. The ILMI MIB is configured through the M interface. The AN MUST be able to support the dedicated ILMI VC as described by the ILMI protocol.

3. VTP/D MIB Connection

This connection is intended for the management of the VTP/D MIB for the purpose of configuring the Ethernet bridging, IP routing and filtering functions. A dedicated connection is established between the VTP/D and the VTP/D Management Node. At the V and U-R2 interfaces, the VTP/D MIB Connection, using either PPPoE, PPPoA or IP over ATM, MUST use a dedicated ATM VC; it is identified as ATM/VCC/VTP<VTP management node >/VTP MIB. In the case that ILMI is not supported by the VTP/D, the VTP/D MIB Connection may be used to configure the ATM parameters. The VTP/D MIB is defined in chapter 7.9 of [2]. The Network MUST have the capability to support one remote VTP/D MIB Connection per VDSL line. The bi-directional flow of PDUs received and transmitted on the VTP/D MIB Connection is identified as the **VTP/D MIB flow**.

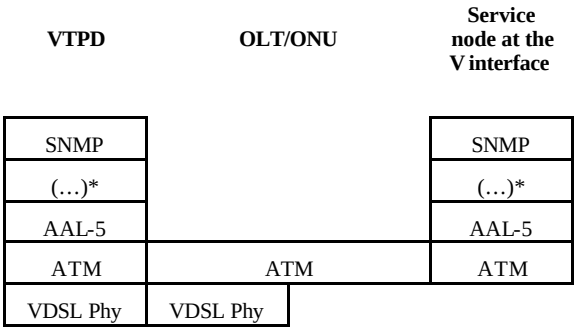


Figure 17: VTP/D MIB Connection

* The SNMP is encapsulated using PPPoA, PPPoE or IP over ATM

The VTP/D software MAY be upgraded using TFTP, described in the 7.9 of [2]. TFTP is transported over the VTP/D MIB connection.

9. Data Service

In order to provide greater flexibility for the deliverance of data services in a Full Service VDSL Network, several options are permitted in this specification. The following describe some of the optional methods for data service. Furthermore, other methods for data service that use the connections described in 8.4.3 are permitted.

For the purpose of simplicity, the data service access node is identified as a Broadband Access Server (BAS)

9.1. PPP-based Data Access

This data access scheme proposes to establish a dial up connection by each residential terminal implementing this scheme. This scheme is provided through terminal initiated PPPoE connections conforming to 8.4.3.2.

9.2. Bridged Data Access

This data access scheme proposes to use the bridge connection described in 8.4.3.1

9.3. Data Connection Sharing

This data access scheme proposes to have a number of residential terminals share a single VTP/D data connection to the BAS. All terminals belonging to the VTP/D private addressing scheme (see 8.3.1) use a connection sharing function in the VTP/D, described in [2]. The NAT connection, as described in 8.4.3.4, MAY be used to support data connection sharing.

10. Broadcast TV and Entertainment Service

This chapter aims to provide the technical specification for the delivery of Broadcast TV and other broadcast services, such as broadcast radio, over the FS-VDSL network. The term broadcast TV refers to the user experience of accessing video streams that conform to a broadcasting schedule. The FS-VDSL broadcast TV user experience is expected to be similar to the one proposed by a satellite or a cable operator.

10.1. Encoding

10.1.1 Broadcast TV IP Addressing Scheme

In the case that the MPEG-2/IP/ATM encapsulation scheme is used for the video streaming (described in 8.4.3.6.5.2), only class D IP addresses MUST be used. In the case where the residential distributed model is implemented, and the encapsulation method is MPEG/ATM, the VTP MUST perform the IP re-encapsulation, as described in 8.4.3.6.3, prior to streaming the video signal over the residential network. The class D address to be used should be retrieved through the BPID indication in the DSM-CC messaging. Since the UDP encapsulation requires the indication of the UDP port number, the UDP port to use MUST be 1970.

10.1.2 Configuration Options Considerations

The optional use of two video stream encapsulation methods at the V interface, i.e. MPEG/ATM and MPEG/IP/ATM, and two channel change protocols (i.e., IGMP and DSM-CC), and the optional implementation of the residential distributed or centralized models, imply that there are eight potential combinations of the above. However, not all combinations are required to be supported by FS-VDSL systems.

The following table describes the eight potential combinations of the video stream encapsulation method, channel change protocol and the residential model implemented. A combination that is marked S indicates that the combination is supported by FS-VDSL. A combination that is marked NS is not supported by FS-VDSL.

Encapsulation	Channel change protocol between VTP/D and the AN	CPE architecture	Viability	Comment
MPEG/IP	IGMP	Distributed	S	There is no need for IP re-encapsulation capability in the VTP
		Centralized	S	
	DSM-CC	Distributed	S	
		Centralized	S	
MPEG/ATM	IGMP	Distributed	NS	The use of MPEG/ATM encapsulation is not viable in the case where IGMP is used between the VTP and the Access Network
		Centralized	NS	
	DSM-CC	Distributed	S	IP re-encapsulation is required to take place in the VTP
		Centralized	S	
Hybrid MPEG/ATM and MPEG/IP	IGMP	Distributed	NS	The use of MPEG/ATM encapsulation is not viable in the case where IGMP is used between the VTP and the Access Network
		Centralized	NS	
	DSM-CC	Distributed	S	IP re-encapsulation is required to take place in the VTP
		Centralized	S	

Figure 18: Broadcast compatibility matrix

10.2. Transport

10.2.1 Channel Replication and ATM Cross Connect

The OLT MUST replicate and the ONU MAY replicate the incoming broadcast streams (channels) to all users accessing simultaneously the same channel, such that each broadcast channel is received by the AN no more than once. Channel replication is performed using a separate ATM point to multipoint connection for every channel (i.e., ATM multicast). A user's channel change request causes a user side VC link to be cross-connected to the appropriate point to multipoint root.

10.2.2 Encryption

The AN and the home Network MUST be transparent to the implementation of encryption based conditional access

10.2.3 Administrative Channel

The administrative channel includes all messaging and data flows between STBs and the broadcast TV management platform. Administrative messaging includes STB boot files, software upgrade, EPG data, etc. The Administrative Channel may take use of one of the bridge connections.

10.2.4 DBTV Quality of Service Performance Objectives

In order to provide the resiliency necessary for reliable delivery of high bit rate MPEG-2 content, the proposed FS-VDSL DBTV architecture relies heavily on the core network and AN engineering for guarantees on packet delivery, correct packet sequencing, and packet delay variation. The network engineering on the core network and AN sides MUST take into account these constraints.

While Cell Delay Variation (CDV) is an appropriate measure of jitter performance for the ATM access network, the jitter of the Program Clock Reference (PCR) is the most critical value to be controlled in the delivery of video services transported within MPEG-2 transport streams. CDV has a contribution to the PCR jitter of the delivered service as indicated below. A detailed definition of PCR jitter and measurement techniques for PCR jitter are contained in Clause 5.3.2 and Annex I of ETSI TR 101 290 [18].

10.2.4.1 HeadEnd

The following conditions apply to the launch of DBTV services at the HeadEnd:

- Encapsulation methods are PCR unaware
- Encapsulation is 2 MPEG Transport Stream (MTS) packets per AAL5 PDU when MPEG2/ATM is used at the V interface
- Encapsulation is 7 MTS packets per IP packet in an AAL5 PDU when MPEG2/IP/ATM is used at the V interface

The HeadEnd (together with the contribution of any intervening core network) MUST not contribute more than 5 ms of PCR jitter to the delivery of the MPEG SPTS packets measured at the V interface**.**

10.2.4.2 OLT-ONU and Copper Loop

For the AN span from the V interface to the U-R2 interface, the peak to peak cell delay variation as defined in the ATM Forum TM 4.1 [19] MUST be less than 2 ms**.** Errors due to cell loss and cell errors MUST be less than 10^{-8}.

10.2.4.3 VTP and Home Network

The home network MUST not contribute more than 5 ms of PCR jitter to the delivery of the MPEG SPTS packets. It is both possible and desirable for the VTP/D to remove the 'positional jitter' of the placement of the PCR within the IP frame or ATM cell by using the average bit rate of the stream and the knowledge of the position of the PCR bearing MTS packet. NOTE: The 'positional jitter' of the PCR is of increasing importance as the bit rate of the stream is reduced (as enabled by MPEG-4 and other proprietary compressions).

10.2.4.4 FPD

The FPD MUST be able to tolerate PCR jitter of at least 12 ms. An error rate of 10^{-8} assumes a somewhat resilient FPD. Results will be dependant on the "sophistication" of the MPEG-2 decoder in the FPD. To facilitate the error concealment that may be present in the FPD, any errored packets should be passed on to the MPEG-2 decoder and marked as such

10.3. Channel Change Signalling

Dual residential video decoding schemes MAY be used. The first scheme, identified as the Residential Centralized Model, uses the VTPD as the decoding unit. The second scheme, identified as the Residential Distributed Model, is of multiple STBs that are connected to the VTP through the in-home LAN. In the distributed scheme, the STBs are connected to the VTP through an Ethernet MAC based Network. Consequently, IGMPv2, being an IP based multicast control protocol, MUST be used for channel change signaling by residential STBs. DSM-CC and/or IGMPv2 MUST be used as the channel change signaling between the VTP or VTPD and the access network. In relation to the specification reference model, the above restriction translates to:

- At the Tcn interface, channel change protocol MUST be IGMPv2.
- At the U-R2 interface, the channel change protocol MUST be DSM-CC and/or IGMPv2. The OLT MUST support at least one of the channel change protocols. In the situation where both IGMPv2 and DSM-CC channel change signaling are used by different VTP/Ds connected to the same physical OLT, the OLT MUST support both channel change protocols.

Channel change messages initiated by the VTPD and the VTP are sent over the channel change connection (see 8.4.3.2) to the access network. The AN is expected to terminate the channel change request and to initiate the streaming of the desired video stream to the appropriate user.

10.3.1 IGMPv2 and DSM-CC use for Channel Change control

The use of DSM-CC in the case of the distributed model for broadcast control, requires an IGMPv2 to DSM-CC translation at the VTP. This translation implies that the VTP implements a multicast state machine, and that class D addresses are converted to BPIDs (Broadcast Program IDs used in the DSM-CC CCP signaling). The use of identical numbering schemes for the class D addresses and the BPIDs eliminates the need for any computed translation. DSM-CC

messages between the VTP and the AN are to be transported over the dedicated channel change VC described in 8.4.3.3. For further details on IGMPv2 to DSM-CC translation see Appendix IV.

10.3.2 IGMPv2 End-to-End for Broadcast Channel Change Control

Due to the inherent characteristics of the IGMPv2 protocol, such as lack of explicit ACK messages, and the need for more then one message exchange to accomplish a channel change command, an appropriate implementation that achieves a good level of service is required. Such implementation should guarantee sufficient computing capacity at peak channel change times in order to limit the channel change time.

In general, channel change times depends on several parameters:

- *Command processing*
  The time interval between the remote control action and the transmission of the join message.
- *Network delay*
  The time interval between the transmission of the join message and the reception of the first multicast packet of the requested channel.
- *STB layer delay*
  The time needed by the STB IP stack to process incoming packets and deliver the content to the MPEG decoder engine.
- *STB jitter buffer delay*
  The time until the STB jitter buffer reaches the fullness set point prior to the forwarding of the video signal to the decoder function.
- *MPEG decoder delay*
  The time interval associated to the decoding process.

In this specification, only the network delay is addressed, and a target below 500ms is pursued. To this aim, some optimizations are required to reduce the network delay by a proper selection of the IGMP timer values.

The reduction of the default timer values implies an acceleration of the processes that regulate the join and the leave operations, resulting in the reduction of the channel change time. The drawbacks of the reduction are that both the STB and the VTP should be able to operate at the required speed (i.e., they may require more processing power than with the default timer values indicated in RFC2236). The following list reports the recommended timer values.

LastMemberQuery interval

The *LastMemberQuery* interval is the maximum time allowed to STBs to reply to the group specific queries that the VTP sends after the reception of a leave message. Since the time required to remove a channel when no STBs are tuned to it is equal to 3 times the *LastMemberQuery* value, the smaller is its value the faster will be the release of unused resources.

RFC2236 default value: 1 second

Recommended value: 100ms

LastMemberQuery Count

The *LastMemberCount* is the number of group-specific queries sent before the VTP assumes there are no local members.

RFC2236 default value: 2

Recommended value: 1

UnsolicitedReport (join) interval

When a STB joins a multicast group, it should immediately transmit an unsolicited membership report for that group. To cover the possibility of the initial membership report being lost or damaged, RFC2236 recommends that it be repeated once or twice after short delays (Unsolicited Report Interval).

RFC2236 default value: 10s

Recommended value: 100ms

The STBs and VTPs SHOULD support recommended values, and MUST interwork with other equipment using these values (e.g., A VTP must interoperate with an STB that uses the default RFC 2236 values for the unsolicited report interval). However, the use of the recommended values is not mandatory. Parameters for which no optimisation is recommended MUST default to the values specified in RFC 2236.

10.3.2.1 STB Requirements

The set-top box MUST implement the RFC2236 host processing including the following additional requirements:

- Every time a channel is left the STB MUST send a leave message.
- The leave message MUST always be sent before the join message, with the exception of multiple channels reception (e.g., for picture-in-picture).
- The STB MUST be able to reply to specific queries with a maximum response time of 100ms.
- The STB SHOULD generate 2 (or 3) unsolicited reports with a 100ms interval.

10.3.2.2 VTP Requirements

The VTP MUST implement the RFC2236 querier process at the home network interface and relay IGMPv2 requests (joins[1] and leaves) to the access network. When a report message is received for a channel that has no members, the VTP MUST relay this message towards the OLT. The VTP MUST send a single leave message each time a received channel is removed from its multicast group membership list. The VTP shall also comply with the following optimizations :

- The VTP SHOULD be able to generate specific queries with a maximum response time of 100ms
- The VTP SHOULD be able to set the *LastMemberQuery* count to 1

10.3.2.3 AN Requirements

In order to reduce complexity, the AN can implement the simplified IGMPv2 processing described in the following. The AN MUST react to a join message by connecting the requested channel to the proper PVC connection and MUST react to a leave message by disconnecting it.

Due to the requirements on the VTP, the AN does not need to implement the "specific query" mechanism specified in clause §3 of RFC2236. the AN MUST, however, implement the "general query" mechanism in order to recover from leave message losses. This last process MAY be started periodically (as per RFC2236) or triggered by a specific event. For example, when the AN receives a join message, but the resources are not sufficient to satisfy the new request. The specification permits flexibility in the choice of IGMPv2 parameters between the AN and the VTP in order to reduce the processing load. The AN processing load can be alleviated by a proper choice of the IGMPv2 protocol parameters (i.e., time intervals).

10.3.3 IP source addresses used in IGMP messages

IGMP messages are encapsulated in IP/Ethernet in the home Network, and, in the case that IGMP is used for channel change signalling between the VTP/D and the AN, in IP/ATM, per RFC2684 (LLC/SNAP routed encapsulation) between the VTP/D and the access network. The IP destination address of the IP packets carrying the IGMP messages is a multicast address, indicating the group to join/leave, or a predefined multicast address (all routers/all systems address).

Since, the STB and VTP/D home network address assignment may be managed by different entities, resulting in IP addresses belonging to different subnets, and considering that:

- The FS-VDSL specified channel change connection does not extend beyond the V interface, but rather it is terminated within the AN.
- All broadcast channels are expected to be transmitted to the OLT. However, for future expansion of this specification, signaling between the AN and the core network for the purpose of retrieving broadcast channels dynamically, will be based on standard protocols, and not on simple forwarding of IGMP messages generated by the VTP/D.

The following apply:

- FPD, VTP/D, and AN are permitted to use any source IP address for IGMP messaging.

[1] This document often refers to the unsolicited report messages as join messages

- FPD, VTP/D, and AN MUST process IGMP messages regardless of their source IP address.

10.4. Information Model For The Channel Change Function Within The AN

The scope of this chapter is intended exclusively to the M interface. The below functions are performed at the delivery of broadcast entertainment services (The term 'broadcast entertainment services' includes broadcast TV/radio, pay-per-view (PPV), and, in the case that IP multicast streams are used, VoD).

- Channel Change
- Connection Admission Control (CAC)
- Conditional Access (CA)

Additional management information is required to be communicated to the AN in order to perform these functions. Figure 19 depicts the management information model that MUST be implemented at the AN. This management information model is referred to as the Channel Change Function Management Information Model (CCF MIM). Figure 19describes the necessary objects, attributes, relationships and operations that need to be maintained. The CCF MIM can be used to derive an appropriate SNMP management information base (MIB) for the AN that can be accessed over the M-interface. The SNMP MIB is defined in Appendix I.

The following describes the parts of the information model used by each function.

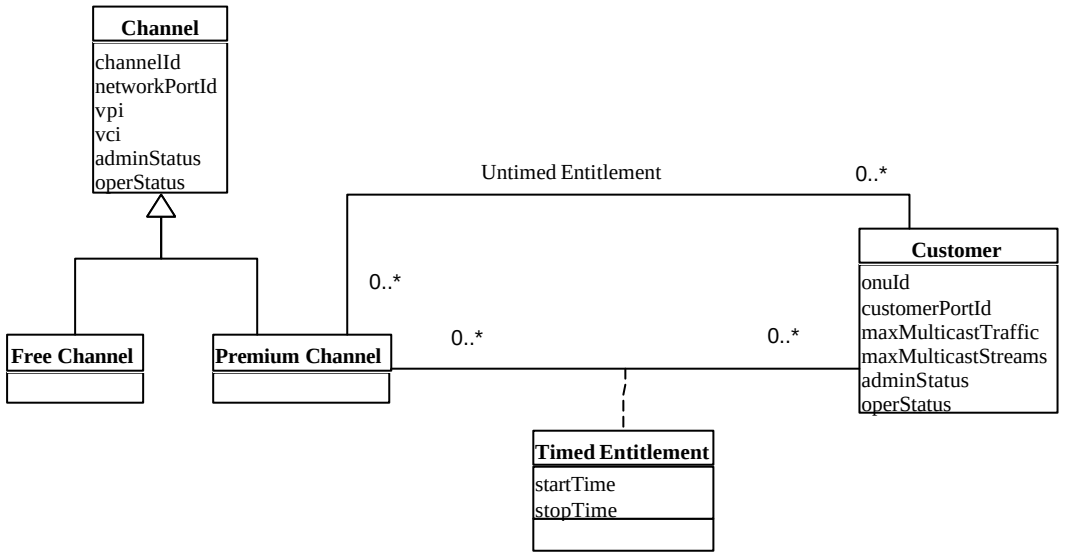


Figure 19: Channel Change Function Management Information Model

10.4.1 Channel Change

The channel function takes use of the information in the 'Channel' and 'Customer' objects.

The **Channel** object defines each broadcast entertainment channel and its associated channelId, which can be an IP multicast address or a DSM-CC programme ID. In addition, it defines at the V interface the networkPortId, VPI and VCI values.

The **Customer** object is used to describe each VDSL UNI at an ONU that is attached to a customer receiving broadcast entertainment services. The identifying attributes being the onuId and the customerPortId. If the ONU is integrated into the OLT or the channel change function is performed at the ONU then the onuId is not applicable.

Both objects have two management state attributes adminStatus and operStatus. The adminStatus defines the desired state of the associated object. The operStatus defines the actual state of the associated object. A management system manipulates the adminStatus attribute and not the operStatus attribute.

Together the Channel and Customer objects provide all the required information to perform the ATM point-to-multipoint cross connect, namely the association between the channelId received in the channel change message and the ATM connection.

10.4.2 Connection Admission Control (CAC)

The Customer object defines the attribute maxMulticastStreams maxMulticastTraffic. maxMulticastStreams specifies the maximum number of separate streams that can be simultaneously active across the Customer's VDSL link. And, maxMulticastTraffic specifies the maximum amount of traffic allocated to broadcast services. The bandwidth of the channel is available by referencing the ATM replication point information stored as part of the ATM VCC information in the OLT/ONU. This information is outside the scope of the CCF MIM but should be accessible by the CCF MIM management entity.

A management system can use maxMulticastStreams to control the number of instances of broadcast entertainment services a customer can receive simultaneously. The CAC function can use maxMulticastTraffic to compare the available bandwidth with the bandwidth of the channel to be joined.

10.4.3 Conditional Access at the OLT/ONU

For conditional access the model need to support the following.

- A distinction between channels that do not require conditional access and those that do.
- The concept of timed and un-timed entitlements
- The maximum number of instances of a broadcast entertainment service that can be active for a customer.

'Free-to-air' channels do not require conditional access to be applied and these are modeled using the Free Channel object. Premium channels do require conditional access to be applied and these are modeled using the Premium Channel object. Both the Free Channel and Premium Channel objects are specialized forms of the Channel object and therefore inherit the attributes and operations of the Channel object.

The entitlements to Premium Channels are modeled through two types of relationships between the Customer and Premium Channel objects. An Untimed Entitlement relationship describes an entitlement to a Premium Channel that a customer is granted which lasts indefinitely or until that entitlement is revoked by removing the relationship to the Premium Channel. There is also a Timed Entitlement relationship, which describes an entitlement to a Premium Channel that a customer is granted for a finite period of time. As the Timed Entitlement relationship has properties which do not belong to either the Premium Channel object or the Customer object an association class is defined to model this and is called the Timed Entitlement object. The Time Entitlement object specifies a window of time (startTime and stopTime) during which an entitlement to a Premium Channel is granted to a customer. After this window of time, the Timed Entitlement object and associated relationship is autonomously destroyed by the OLT/ONU. The Time Entitlement relationship is needed to support the services of PPV and multicast VoD. A customer can have either an Untimed or Timed Entitlement to the same Premium Channel but not both.

In order to satisfy the timing accuracy of Timed Entitlements, the OLT/ONU MUST be synchronised in time with the entity setting the entitlement. The way this synchronisation is achieved is outside the scope of this specification.

Together the Untimed relationship, Timed relationship, and the maxMulticastStreams attribute of the Customer object provides all the required information for performing the CA function at the OLT/ONU. By manipulating these relationships and attributes a management system can grant and revoke timed and untimed entitlements for a particular Premium Channel and limit the number of instances of a broadcast entertainment service the customer can obtain simultaneously.

11. VOD service

This chapter defines requirements for the implementation of Video On Demand (VOD) service in an FS-VDSL system. The specification acknowledges VOD as an emerging technology and aims not to restrict future innovation by over-specifying the VOD service. VOD service is an on-demand service that delivers multimedia assets such as video, audio, and games[2]. VOD service is a "high QOS" and "high bandwidth" service; it delivers broadcast quality MPEG-2 encoded video, and it allows for interactivity, such as "trick mode" control, "pause" and "fast-forward."

---

[2] A « VOD » service can deliver non-video assets, and so the term is a imprecise. However, since the main application, and the most strict bandwidth and QOS requirements, are derived from the transport of video. the term « VOD » is used in this specification without further clarification or explanation.

An implementation of VOD service typically requires:

- Back office management
- A “server farm” containing interesting content
- Transport and AN facilities that can insure QOS
- Compelling client server application software

A VOD service provider maintains a business relationship with the end consumer. More than one service provider can be supported by the architecture; a service provider typically aggregates content from content providers and charges consumers for content. The service provider may also own physical equipment and may manage a portion of the network.

Key resources must be coordinated among VOD service providers, among the network operator, and among the data service provider. As a simplifying assumption, it is assumed that a single “VOD service operator” exists to perform this coordination when needed. In the discussions below, only a single service operator is assumed, and there no explicit distinctions are made between service provider and service operator.

Although VOD service may be implemented in a standalone manner, it is typically offered along with a broadcast video service. The implementation of broadcast and VOD will be integrated, perhaps minimally, but perhaps very highly. The VTP/D software that performs VOD content selection and EPG may be implemented as a single application. The transport Network may share physical facilities. In the back office, functions such as subscriber management and billing may be highly integrated.

In order to accommodate a range of solutions, the requirements in this chapter borrow heavily from the requirements on broadcast video service and data service to allow for maximal commonality between implementation.

11.1. VOD Back Office Management

VOD back office functions include: Asset Management, Subscriber Management, Session Management, and Digital Rights Management.

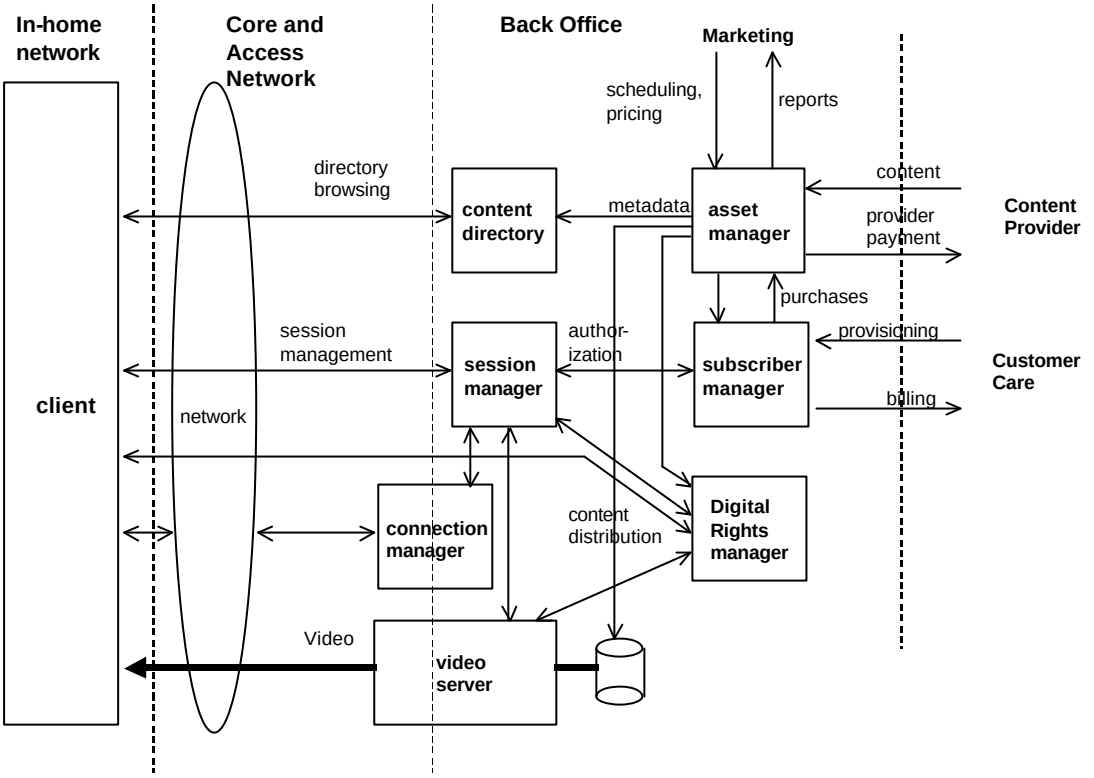


Figure 20: VOD Back Office Management

Back office components are illustrated in Figure 20, above. Content (and possibly, associated metadata) arrives to the Asset Manager, which places it onto the servers ("content distribution"), and, with input from Marketing (e.g.,, scheduling, and pricing), populates the "content directory".

Content may be stored in an encrypted form on the video server; in this case rights information is placed in the Digital Rights Manager from the Asset Manager as part of content loading. When the session is established, the client and Session Manager communicate with the Digital Rights Manager to determine the rights information and communicate them to the client; and the Digital Rights Manager communicates with the video server to apply the proper keys.

The Subscriber Manager creates accounts for users as they sign up and maintains current account status. At the end of a billing cycle, the Subscriber Manager provides billing records to the customer care system (where, presumably, an integrated bill for all services is created). The Asset Manager collects purchase information.

When content is purchased, the consumer selects his content from the Content Directory. Session and Connection Establishment are invoked when a client wishes to view a VOD asset. These are described below.

11.2. VOD Network Engineering

11.2.1 VOD Server Farms: Centralized vs. Distributed

VOD server hardware may be "centralized", where a complex of VOD servers provide content to a large population of users. Alternately, a "distributed" approach may be used, where there are several smaller servers "closer" to users. A centralized architecture may be simpler to manage, but requires more transport bandwidth and may not scale as well as

distributed approaches. In practice, a hybrid implementation may be optimal: popular content, such as first-run movies, could be held in small servers close to the edges of the network and less popular content held in a centralized servers.

Each subscriber can be served by a collection of VOD server output ports. At the time of connection establishment, the resource manager in the VOD server will use the identity of the subscriber and allocate the necessary resources in the VOD server to stream the content to the user.

11.2.2 Two-way Administrative Traffic

The VTP/D must be able to perform directory browsing, interact with the DRM HeadEnd (if applicable), and provide VOD session establishment and stream control. IP protocols are used to communicate with the VOD applications servers.

A bridged, PPPoE, or routed connection MUST be provided for the VOD administrative traffic. The applications servers that support these functions MAY be in a separate physical network than the public Internet and data service in general, and it is a requirement of the VTP/D to be able to segregate and route the VOD applications traffic to the network.

11.2.3 Downstream Video Traffic

One-way transport bandwidth is required between the video server and the VTP/D to carry the VOD content. A wide range of network architectures is possible. The administrative traffic could, in principle, share the same route as the downstream video traffic (e.g., using "in-band" signaling). However, in-band signaling introduces MPEG jitter and complicates VOD server design, and so it is expected that "out of band" signalling would be preferred by most implementations. This approach allows the network operator to optimize for the one-way nature and QOS requirements of the video traffic.

The core network transport facilities may share the capacity of the data network or the broadcast distribution network, or use facilities dedicated to VOD transport. As VOD traffic travels the core network, it may traverse several hops and different transport technologies, such as IP, ATM, or MPLS.

Regarding bandwidth management and the network engineering of the VOD transport network, there are three main approaches that may be taken:

- Pre-established bandwidth end-to-end (e.g., from video server and VTP/D).
- Pre-established bandwidth in the core network, but concentration at the access network.
- Concentration in the core network and in the access network.

Other variations are, of course, possible. The approach taken has an impact upon connection establishment procedures, which are described in more detail below.

11.2.4 QOS Requirements for VOD Traffic

The transport network MUST NOT allow undue packet loss, introduce excessive packet jitter, or allow packet reordering. The VOD flow MUST be provided with a QOS that ensures that it has precedence over non-priority traffic, which would otherwise degrade the video quality.

The detailed QOS requirements for VOD service are identical to those for broadcast service. See section 10.2.4.

11.2.5 Encapsulation

With the exception of IP addressing, the MPEG/IP/ATM and MPEG/ATM encapsulation requirements are identical to those required for broadcast service. See Section, 8.4.3.6.5.2 and 8.4.3.6.5.1.

11.3. VOD Content Browsing

To purchase a movie (or game, or other on-demand asset), the subscriber begins by browsing the Content Directory. No specific requirements are placed on how the Content Directory is managed or how browsing is performed, but it is expected that "web based" techniques, such as HTML and JavaScript (or MHP/Java) be used. Information in the

Content Directory should be automatically populated based on the efficient propagation of content metadata (e.g., title, ratings, descriptions, and so on).

Once a selection has been made by the user, the Content Directory provides the identifier for the VOD asset (possibly in the form of a "url"), and may provide additional information, such as QOS information, encoding rates and formats, and the IP address of the Session Management server that can provide the desired asset. (Providing the Session Manager IP address as part of the Content Directory information simplifies Network configuration and allows more than one Session Manager signaling entity, and thereby facilitates scaling).

11.4. VOD Session Establishment

Session Management signaling is performed between the VTP/D application and the VOD session management entity. RTSP [20] MUST be used as the session management protocol. It is recognized that RTSP is an extensible protocol and that there are several non-interoperable "dialects" of RTSP in use. Although guidelines are given below, it is not the intent of this specification to precisely define a set of FS-VDSL RTSP extensions.

The RTSP SETUP message contains the following fields:

- A unique identifier of the VTP/D MUST be provided. The syntax and semantics of the identifier are not defined, but could be a Serial Number, Mac Id, or Smart Card Id.
- An identifier for the desired content MUST be provided. This information comes from the Content Directory.
- A VOD session manager identifier MAY be included. The VOD session manager may be identified by IP address or host name as information from the Content Directory.
- An OLT identifier or service area identifier MAY be provided, to further identify the VTP/D.
- QOS information such as desired encoding rate, MAY be provided.

Before the session can be admitted, a number of business rules are typically checked by the Session Manager: whether the user has permission, access, credit; whether the asset is available for purchase, whether there are sufficient server resources. If the user can purchase the movie, the connection manager makes the necessary bandwidth calculations and invokes the connection establishment procedures to determine if there are sufficient Network resources.

Digital Rights Management is typically invoked at this time to grant the user the necessary rights, and to provide key and access information back to the VTP/D for decryption.

The RTSP SETUP REPLY contains the following fields:

- Connection and QOS information MAY be provided. This information could include the class D multicast address or DSM-CC BroadcastProgramId.
- DRM rights or key information MAY be provided.

Once the session has been established, the user then performs RTSP stream control within the session to start/pause/play the movie.

When the client has finished viewing the movie, it can release the session by the RTSP TEARDOWN command. This releases both session and connection resources, as necessary. In general, any party to the session or connection should be able to initiate a release of the session and recovery of the associated resources.

11.5. VOD Connection Establishment

This section describes connection establishment procedures. In the first case described below, bandwidth is pre-established between the VOD server and the VTP/D client beforehand and connection establishment procedures are not needed. Alternately, there is a bandwidth bottleneck in the core or access networks and connection establishment procedures must be invoked at the time of session establishment.

Note that although not specifically addressed in the text, multiple VOD sessions per VDSL line are supported by the architecture.

11.5.1 Pre-Established Bandwidth End-to-End

This section describes the case where bandwidth is pre-established between VOD server and VTP/D client.

Having truly dedicated end-to-end bandwidth for VOD service might be used in a lab or small field trial scenario. However, bandwidth is typically "overbooked" in the AN and on the VDSL line; this allows the subscriber bandwidth to be shared among other services such as broadcast video and data. Here, it is the responsibility of the VTP/D software and the back office VOD components to ensure that the total bandwidth for the subscriber is correctly arbitrated among the different services. At the time of session establishment, resource allocation is required in the VOD server, and the core network and AN are unaware of the session.

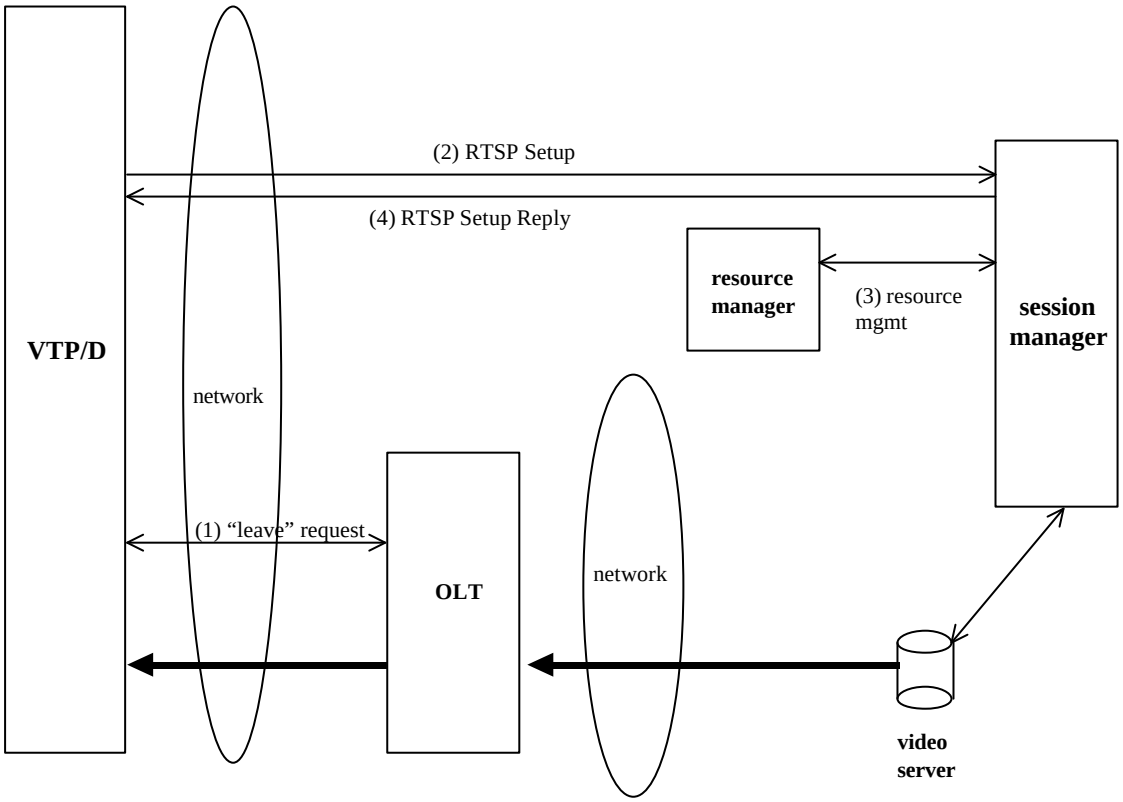


Figure 21: VOD Session Establishment - Pre-Established Bandwidth End-to-End

Figure 21, above, illustrates the message flow to establish a VOD session.

Step 1. The client "leaves" an existing broadcast channel.

Step 2. VOD Session Signaling is performed between the VTP/D and a Session Manager.

Step 3. Allocation of VOD server resources will typically be required: the Session Manager invokes Resource/Bandwidth Manager. Note that the Resource Manager may need to map the identity of the VTP/D (or the OLT) to the appropriate video server resources.

Step 4. Confirmation and connection resource information (e.g., the VOD "channel") is sent back to the VTP/D.

11.5.2 Bandwidth Bottleneck in the Transport Network

This section describes the case where bandwidth is not pre-established between VOD server and VTP/D client. Here, connection establishment procedures are required.

As an example, the AN may be engineered to support 200 simultaneous streams of VOD for a population of 1000 subscribers. (Note that the AN has several possible places of bandwidth contention: at the ingress to the OLT, between the OLT and ONU, and the VDSL line between the ONU and the VTP/D). In this example, the connections in the core network are pre-established: a bundle of connections are created from the VOD server to each AN OLT.

Other possibilities exist: multiple points of concentration are supported with the proviso that the connection management protocol be hierarchical and all points of concentration participate in connection establishment signalling. In the example below, on the simple case of a single point of concentration, the AN OLT is used.

Figure 22**,** below, gives an overview of VOD session and connection establishment procedures in this case:

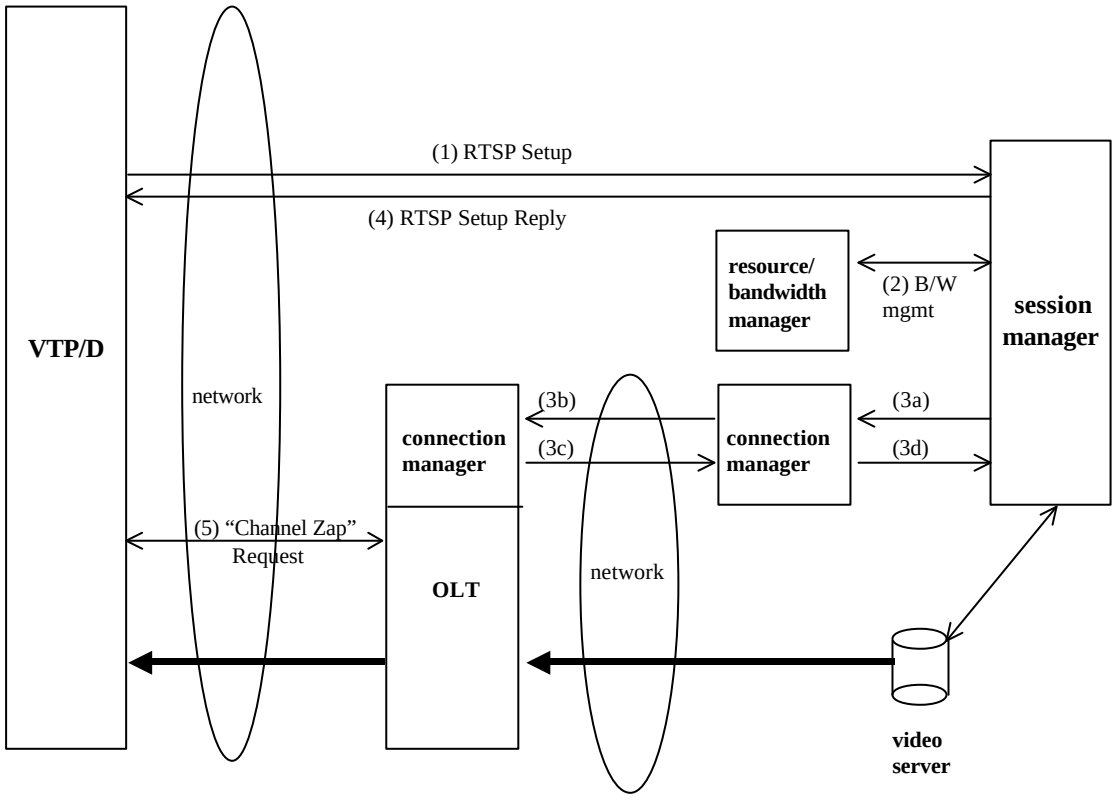


Figure 22: VOD Session Establishment - Concentration in Access Network

Step 1. VOD Session Signaling is performed between the VTP/D and a Session Manager.

Steps 2 and 3a. Allocation of VOD server resources and network bandwidth is required. The Session Manager will invoke Resource/Bandwidth Manager and Connection Manager to establish a connection from video server to VTP/D.

Step 3b. Connection establishment procedures are used to reserve bandwidth for the downstream video connection. The Connection Establishment entity in the Session Manager will be required to map the VTP/D identity to AN OLT to determine the route of the connection. There are different methods of grouping VTP/Ds associated with an OLT:

- Local configuration in the VTP/D
- Implicitly, by the IP address assignment mechanisms (e.g., DHCP server or RADIUS). One possible convention is to assign a range of IP addresses to an OLT.
- Provided by other configuration.

If access control procedures are used in the access network, the connection establishment procedures must create the connection with the necessary permissions for the VTP/D.

Step 3c, 3d, and 4. Once connection establishment procedures have successfully negotiated a connection, confirmation and connection resource information (e.g., the VOD "channel") is sent back to the VTP/D.

Step 5 (recommended). The VTP/D uses channel change procedures to tune to the desired "channel." By using explicit signaling from the VTP/D to the AN OLT, the VTP/D may easily switch from VOD to broadcast services, and it allows the AN OLT to explicitly manage the bandwidth between the two services. (Note that using Class D (e.g., multicast IP addresses) simplifies the signaling).

11.5.3 Connection Es tablishment Protocol Requirements

The connection establishment protocol SHOULD BE performed out of band.

The connection establishment protocol SHOULD BE server initiated, as server initiated signaling is more secure than VTP/D initiated signaling.

The connection establishment protocol SHOULD BE "hard state." This approach creates a well-defined path to insure QoS for the life of the session. Hard State connections also eliminate the per-connection "keepalive" traffic that hurts scaling. Standard RSVP is a "soft state" protocol and is not recommended as a long-term solution.

11.5.4 Connection Establishment Protocol Options

Various protocols satisfy these requirements; the choice of protocol depends upon the transport network.

For IP transport networks, RSVP-TE or CR-LDP appear to be good candidates, but additional research is needed.

For ATM transport networks, SVCs or "soft PVCs" (connections established in the management plane) may be used.

In the case of ATM SVCs, the signalling might be end-to-end, terminating on the VTP/D (in which case the VTP/D requires an ATM signalling stack and the AN is required to act as an ATM switch). Such a connection would be end-to-end, and it may be necessary for the VTP/D to release the bandwidth for a broadcast connection in order for the SVC signalling to succeed (e.g., satisfy the CAC in the Access Network).

An interesting variant to end-to-end ATM SVCs is to terminate the signalling on the access system, which then acts as a signalling "proxy" for the VTP/D. In this second case, channel change signalling might be used to establish the AN to VTP/D leg of the connection.

11.5.5 IP Address Assignment for Downstream VOD Video

If an IP layer is present, either unicast or multicast (e.g., class D) IP addresses MAY be used.

The motivation for using class D addresses for VOD flows is that it allows the VTP/D to switch between a VOD stream and a broadcast video stream in a straightforward way (e.g., using the channel change signaling), and allows the AN OLT to participate in the bandwidth management.

If class D addresses are not used for VOD traffic, then alternative solutions must be found for bandwidth management and connection establishment procedures.

12. Voice over DSL (VoDSL)

VoDSL refers to digitally emulated voice transported over the DSL access architecture simultaneously to the data transport. VoDSL supports end-user access to voice-band telecommunication services via existing terminals (e.g., plain old telephone, fax) while using the newly deployed data Access technology on copper wires (i.e., DSL.) In some cases, VoDSL services are offered through data-centric devices, such as, but not restricted to, multimedia PCs and Ethernet phones or VoIP phones. This chapter aims to provide informative principals for the use of VoDSL in an FS-VDSL network based on previous VoDSL specifications in the ATM forum, DSL forum, IETF, ITU-T SG15/16, IMTC / VoIP Forum and ETSI TIPHON.

VoDSL can be characterized by the follows:

- Voice services digitally emulated by the Voice over Packet gateway functionality in the VTP/D and by the Voice over Packet functionality in the core network, are called “derived voice services.” At the VTP/D, the analog interfaces provided through RJ11 jacks are correspondingly called “derived voice lines”. The derived voice lines do NOT support lifeline services (i.e., are not powered from the central office).
- While VoDSL services are implemented, simultaneous data services (e.g., Internet access, file transfer, is enabled).
- Since usually the VoDSL VTP/D offers multiple service interfaces, the VoDSL VTP/D is referred to as the Integrated Access Devices (IAD).
- VoDSL can support voice quality that is equal to other forms of digital telephony like ISDN. Indeed, impairments of analog lines are not encountered, as a digital transport is foreseen. Pulse code modulation, such as PCM or G.711, can be applied when needed. However, compression schemes that use less bandwidth, such as ADPCM or G.726 can also be applied without any noticeable loss of voice quality. It should also be noted that VoDSL makes use of echo cancellation techniques.

The following chapters describe two different Voice over DSL architectures. The first architecture takes use of AAL-2 [21] as the ATM adaptation layer for the transport of legacy voice service up to the interface point of the public network and is referred to as BLES. The second architecture relies on IP to transport the voice packets and will be referred to as voice over IP.

The below represent some of the criteria in consideration for the choice of either architectures:

- The extent at which the core voice (TDM) network will evolve towards a fully packetized network.
- The capability to introduce the gateways between the voice network and the data network.
- Integration of the current voice services (including feature services).
- The desired extent of enhanced data oriented services within voice terminals.

12.1. BLES

Loop Emulation Service (LES) has been defined by the ATM Forum and has been adopted by the DSL Forum. This specification does not differ from the above specifications. In the context of VoDSL, it is sometimes referred to as Broadband Loop Emulation Service (BLES). BLES uses ATM/AAL2 as the transfer mode. The blend of the data oriented digital signal and the voice oriented digital signal occurs in the VTP/D, while the segregation occurs at the far end of the access network. At that point, data is fed into the edge of the data Network and voice is fed into legacy local switching equipment (i.e., Local exchanges/Class5 switches).

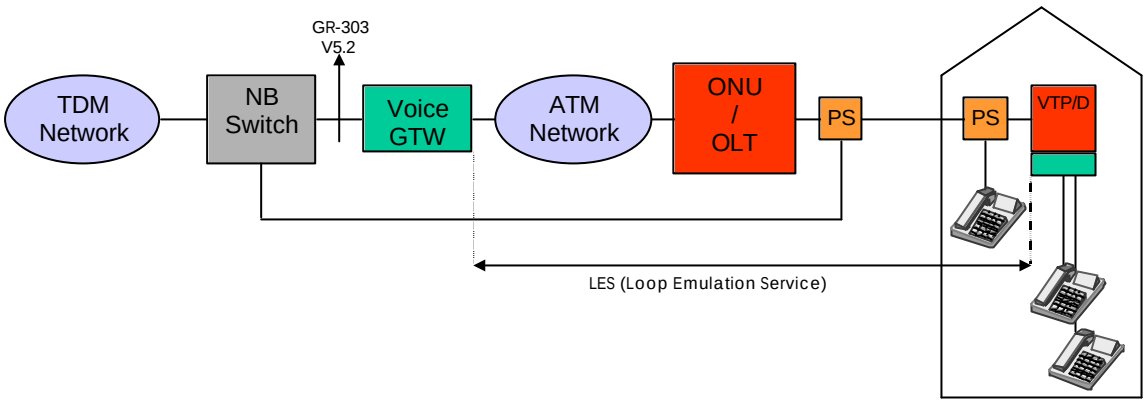


Figure 23: VoDSL Network Elements

The following principles apply:

- VoDSL in enabled by the VoDSL gateway functionality in the ATM access network, and in the VTP/D.
- The VoDSL gateway performs the necessary functions to compatibly interface the POTS network. The VoDSL gateway initiates and terminates the ATM AAL2 voice connection, performs the (de-)coding function and supports the necessary signaling means between the customer premises and the Local exchanges/Class5 switches. In addition, the VoDSL gateway performs the voice handling function such as compression and echo cancellation.
- The ATM AN voice gateway handles the appropriate protocol conversion to interface the Local exchanges/Class5 switches through known interfaces such as V5.2 and GR-303.
- The VTP/D VoDSL Gateway performs the necessary conversion of voice signals from legacy voice band end-user interfaces (e.g., POTS service interface provided over RJ11 connectors), to packetized voice, (i.e., ATM for transport over the access network) and vice versa. Events such as hook-on, hook-off and ringing are notified via the LES signaling.

12.2. Voice over IP (VoIP)

This method suggests that both the voice signal and the voice signaling messages are carried within IP packets. VoIP has been specified in different standardization forms and industry consortia, such as IETF, ITU-T SG15/16, IMTC / VoIP Forum and ETSI TIPHON. This extensive specification activity of VoIP has generated different protocols that may handle similar functionality. Furthermore, different network control elements are proposed for VoIP.

The following represent the VoIP protocols mostly in use.

- RTP / RTCP for the encapsulation of the (compressed or uncompressed) voice frames
- H.323 for call setup (includes H.225 and H.245)
- SIP (Session Initiation Protocol) for call setup
- SDP (Session Description Protocol)
- SGCP (Simple Gateway Control Protocol) and MGCP (Media Gateway Control Protocol) for control of VoIP devices such as VoIP (media) gateways and VoIP terminals
- H.248 and Megaco (providing similar functionality as MGCP)

The following are network elements that are traditionally used for the implementation of VoIP :

Customer Premises:

- Multimedia PC containing and running VoIP software. Similarly, STB could evolve to support VoIP.
- A VTP/D that provides legacy phone interfaces (RJ-11) and includes the VoIP functionality. This device could be referred to as an IAD.
- VoIP voice-only terminal, such as an Ethernet phone, that connects into the home or corporate LAN
- LAN PBX that connects legacy phone terminals and provides packetization as well as PBX services
- Optionally, some local call control functionality, such as gatekeeper or SIP proxy, may be provided as well by a local server or embedded in the VDSL IAD or LAN PBX.

Core Network:

- VoIP gateway that converts Voice over IP interfacing the TDM network.
- VoIP aware NAT routers
- Call controller, that provides call control functionality for the VoIP devices in the network. Depending on the architecture and protocols used, this call controller may be referred to as the SIP proxy, H.323 Gatekeeper or Media Gateway Controller.

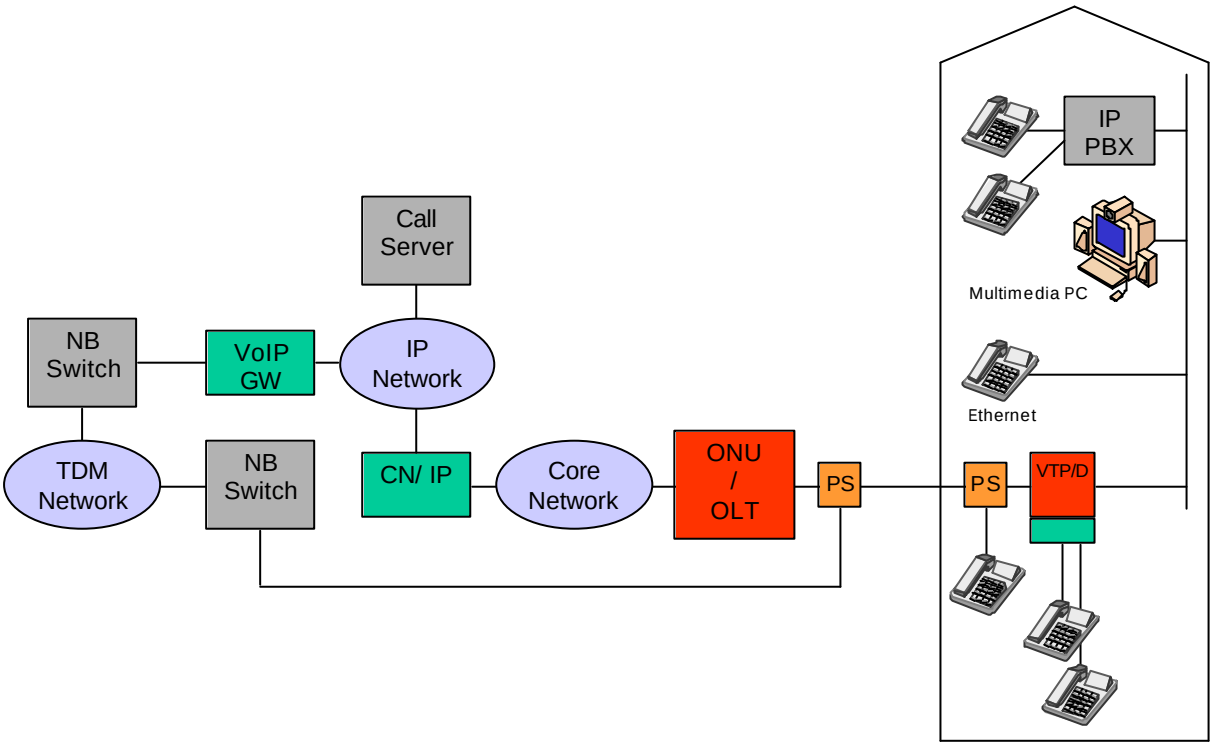


Figure 24: VoIP Network Elements

The blend of voice and data occurs in the customer premises domain. The segregation may occur either in the core network, where the voice signal interfaces the TDM network; or, optionally, no segregation occurs in the case where VoIP is deployed end-to-end.

The following principles apply for VoIP:

- VoIP can be performed by adding the VoIP functionality in the customer premises, and the VoIP call control and VoIP gateway at the interface point to the legacy TDM network .
- At the VTP/D, a VoIP conversion function converts traffic from legacy voice band end-user interfaces (e.g., POTS service interface provided over RJ11 connectors) to VoIP and vice versa. This VoIP conversion includes speech compression, packetization, RTP encapsulation and VoIP signaling, such as H.323, SIP or MGCP flavor. This

functionality may reside in the VTP/D or in a stand-alone device, such as a VoIP adapter or a LAN PBX. In addition, VoIP may be implemented through a software application in a multipurpose data device, such as a multimedia PC or STB.

- At the VTP/D, QoS capabilities should be provided in order to guarantee low packet loss and delay for the VoIP traffic. This may be implemented in different ways such as VLAN tagging (IEEE 802.1Q & Prioritization / IEEE 802.1P), IP diffserv or intserv or ATM QoS.
- If the VoIP traffic is routed through the NAT connection at the VTP/D, the VTP/D is expected to be IP aware and to provide the necessary VoIP handlings.
- Through the DSL access network, IP voice traffic can be directed to either a Voice over IP service provider dedicated IP voice network, that is architect to provide the necessary IP based QoS for voice services, or the public Internet, which currently lacks the appropriate QoS capabilities enabling quality voice services.
- At the core network, packetized IP voice is converted to legacy interfaces (i.e., ISDN / PSTN NNI) via Media Gateways and Signaling Gateways. The main functions of these gateways include the termination of the TDM voice circuits, VoIP (de)multiplexing, voice handling function, such as compression and echo cancellation, interfacing to call control and connectivity to one or more legacy telephone exchange(s) via an NNI interface. Nonetheless, VoIP may be provided end-to-end. Whereby, the conversion of the IP based voice traffic to legacy TDM traffic is not required.
- The Call Control functions include the address translation (e.g., from E.164 numbers to host names, email addresses and / or IP addresses), session establishment through call setup procedures (e.g., setup, alert, connect, disconnect), session management for intermediate VoIP aware devices, such as gateways and NAT routers, Interfacing to backend services, such as the Intelligent Network, billing, etc and control of Network resources

APPENDIX I

SNMP MIB FOR THE CHANNEL CHANGE FUNCTION

This appendix defines the SNMP MIB using SMIv2 for configuration management of the channel change function (CCF) that resides in the OLT/ONU. The MIB realises CCF Management Information Model (MIM) that is defined in Below.

1.0 Relationship to other MIBs

The CCF MIB contains references to the following SNMP MIBs.

- The appropriate interface MIB, such as RFC 2863, used by the OLT to describe the V-interface and S-R interfaces as defined by the FS-VDSL system reference model. The channelTable references the V-interface and the customerTable references the S-R interface.
- An appropriate ATM MIB, such as RFC 2515, used by the OLT to describe the ATM VCC replication points for the broadcast entertainment services at the V-interface. The channelTable makes reference to the ATM VCC in order to enable the CAC function to check the bandwidth requirements of a broadcast channel.

2.0 MIB Definition

```
-- MIB for configuration management of the Channel Change Function
-- residing in the OLT/ONU.

CHANNEL-CHANGE-MIB      DEFINITIONS ::= BEGIN
       IMPORTS
          RowStatus
             FROM SNMPv2-TC
          enterprises, MODULE-IDENTITY, OBJECT-TYPE, IpAddress
             FROM SNMPv2-SMI
          MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
             FROM SNMPv2-CONF
          InterfaceIndex, InterfaceIndexOrZero
             FROM IF-MIB;

       channelChangeMib  MODULE-IDENTITY
          LAST-UPDATED  "200205121638Z"
          ORGANIZATION  "FS VDSL Architecture Experts Group"
          CONTACT-INFO
             "FS-VDSL Secretariat
             -- editor's note: enter correct address in here
             Email: teresa.marsico@fs-vdsl.net"
          DESCRIPTION
             "This module defines a MIB for managing the Channel
             Change Control Function within an OLT/ONU."
          ::=  {  fsVdsl  1  }

       fsan      OBJECT IDENTIFIER ::=  {  enterprises  1  }
       -- editor's note: must replace with valid OID assigned by IANA
       fsVdsl OBJECT IDENTIFIER ::=  {  fsan  1  }

       channelChangeMibObjects OBJECT IDENTIFIER ::=  {  channelChangeMib  1  }
       channelChangeMibNotifications OBJECT IDENTIFIER ::={channelChangeMib  2}

       -- ------------------------------------------------------------- --
       --
       -- The Channel Table

       channelTable      OBJECT-TYPE
          SYNTAX              SEQUENCE  OF  ChannelEntry
          MAX-ACCESS          not-accessible
          STATUS              current
```

```
    DESCRIPTION
        "This defines the channels and associated ATM replication points
        (ATM VCCs) within the OLT/ONU. Note that the channel table supports
        both IP multicast addresses and DSM-CC program IDs as a means of
        channel lookup."
    ::=  { channelChangeMibObjects  1 }

channelEntry     OBJECT-TYPE
    SYNTAX              ChannelEntry
    MAX-ACCESS          not-accessible
    STATUS              current
    DESCRIPTION
       "An entry in the channelTable represents a single channel."
    INDEX   {  channelId  }
    ::=  { channelTable 1 }

ChannelEntry  ::=  SEQUENCE {
    channelId           IpAddress,
    entitlementIndex    Integer32,
    networkPortId       InterfaceIndex,
    vpi                 Integer32,
    vci                 Integer32,
    channelAdminStatus  INTEGER,
    channelRowStatus    RowStatus
    }

channelId OBJECT-TYPE
    SYNTAX              IpAddress
    MAX-ACCESS          not-accessible
    STATUS              current
    DESCRIPTION
       "The channelId must be a Class D IP address allocated to the
       multicast channel regardless of whether the channel is delivering
       video over UDP/IP multicast or AAL5. Where DSM-CC is used as the
       channel change protocol, this is also the DSM-CC Broadcast Program
       ID (BPID). This facilitates transparent mapping between the IGMP and
       DSM-CC channel change protocols."
       ::=  {  channelEntry  1  }


entitlementIndex  OBJECT-TYPE
    SYNTAX              Integer32  ( 0 .. 4095  )
    MAX-ACCESS          read-create
    STATUS              current
    DESCRIPTION
       "The value of this object is the key for performing conditional
       access. The value zero (0) is reserved and is allocated to a channel
       which is free and does not require conditional access to be
       performed. Note that a maximum of 4095 channels can be supported by
       this MIB."
    ::=  {  channelEntry  2  }


networkPortId    OBJECT-TYPE
    SYNTAX              InterfaceIndex
    MAX-ACCESS          read-create
    STATUS              current
    DESCRIPTION
       "The value of this object must be equal to the ifIndex of the
       network interface in the OLT/ONU carrying the multicast channels.
       This is so that this object along with the vpi and vci objects below
       can be used as an index into the OLT's/ONU's ifTable to gather more
       information about the replication point(ATM VCC) such as peak
       bandwidth."
```

```
   ::=  {  channelEntry  3  }


vpi OBJECT-TYPE
   SYNTAX              Integer32  ( 0 .. 255  )
   MAX-ACCESS          read-create
   STATUS              current
   DESCRIPTION
      "The value of this object is equal to the VPI allocated to
      the replication point (ATM VCC) in the OLT/ONU for this channel."
   ::=  {  channelEntry  4  }


vci OBJECT-TYPE
   SYNTAX              Integer32  ( 32 .. 65535  )
   MAX-ACCESS          read-create
   STATUS              current
   DESCRIPTION
      "The value of this object is equal to the VCI allocated to
      the replication point (ATM VCC) in the OLT/ONU for this channel."
   ::=  {  channelEntry  5  }


channelAdminStatus     OBJECT-TYPE
   SYNTAX              INTEGER  {  locked ( 1 ),
                                  unlocked ( 2 ),
                                  shuttingDown ( 3 )
                       }
   MAX-ACCESS          read-create
   STATUS              current
   DESCRIPTION
      "This object is used to control the management state of this
      channel. When this object is set to locked(1) all existing customers
      connected to this channel must be immediately disconnected and
      further join requests to this channel should be rejected. If this
      object is set to shuttingDown(3), no further join requests should be
      accepted for this channel; when all existing customers have
      disconnected from this channel the value of this object moves to
      locked(1)."
   ::=  {  channelEntry  7  }


channelRowStatus  OBJECT-TYPE
   SYNTAX              RowStatus  { active ( 1 ),
                                    notInService ( 2 ),
                                    notReady ( 3 ),
                                    createAndGo ( 4 ),
                                    createAndWait ( 5 ),
                                    destroy ( 6 )
                       }
   MAX-ACCESS          read-create
   STATUS              current
   DESCRIPTION
      "This object is used to manage row creation and deletion. When the
      channelAdminStatus is locked(1) the value of this object should be
      notInService(2). When the channelAdminStatus is unlocked(2) the
      value of this objects should be active(1) or notReady (3). When the
      value of channelAdminStatus is shuttingDown(3), the value of this
      object should be active(1)."
   ::=  {  channelEntry  8  }

-- ------------------------------------------------------------------ --
--
-- The Customer Table
```

```
customerTable    OBJECT-TYPE
   SYNTAX              SEQUENCE  OF  CustomerEntry
   MAX-ACCESS          not-accessible
   STATUS              current
   DESCRIPTION
      "This defines the customers for broadcast entertainment
      services."
   ::=  { channelChangeMibObjects  2 }

customerEntry    OBJECT-TYPE
   SYNTAX              CustomerEntry
   MAX-ACCESS          not-accessible
   STATUS              current
   DESCRIPTION
      "An entry in the customerTable represents a single customer."
   INDEX   {  onuId, customerPortId  }
   ::=  { customerTable 1 }

CustomerEntry  ::=  SEQUENCE {
   onuId                    InterfaceIndexOrZero,
   customerPortId           InterfaceIndex,
   maxMulticastTraffic      Integer32,
   maxMulticastStreams      Integer32,
   untimedEntitlements1     OCTET STRING,
   untimedEntitlements2     OCTET STRING,
   grantEntitlement         IpAddress,
   revokeEntitlement        IpAddress,
   customerAdminStatus      INTEGER,
   customerRowStatus        RowStatus
   }


onuId  OBJECT-TYPE
   SYNTAX              InterfaceIndexOrZero
   MAX-ACCESS          not-accessible
   STATUS              current
   DESCRIPTION
      "Describes uniquely the ONU to which the customer is attached. The
      value of this object must be the ifIndex of the interface in the OLT
      that connects to the associated ONU. If the OLT/ONU are integrated
      then the value of this object must be zero (0)."
   ::=  {  customerEntry  1  }


customerPortId   OBJECT-TYPE
   SYNTAX              InterfaceIndex
   MAX-ACCESS          not-accessible
   STATUS              current
   DESCRIPTION
      "Describes  uniquely  the  port  within  the  ONU/OLT  to  which  the
customer is attached. The value of this object must be the ifIndex of the port to
which the customer is attached."
      ::=  {  customerEntry  2  }


maxMulticastTraffic    OBJECT-TYPE
   SYNTAX              Integer32
   MAX-ACCESS          read-create
   STATUS              current
   DESCRIPTION
```

```
            "This object defines the maximum amount of bandwidth in kilobit/s
allocated to broadcast entertainment services. The value must be an integer
multiple of 10kbps and must not exceed the DSL line rate."
         ::=  {  customerEntry  3  }


      maxMulticastStreams    OBJECT-TYPE
         SYNTAX              Integer32
         MAX-ACCESS          read-create
         STATUS              current
         DESCRIPTION
            "This object defines the maximum number of multicast streams that
            can be active simultaneously across a DSL UNI. A value of zero (0)
            is used to indicate that this object must not be used as part of any
            decision making process for a channel change request."
         ::=  {  customerEntry  4  }



      untimedEntitlements1   OBJECT-TYPE
         SYNTAX              OCTET STRING  ( SIZE ( 0 .. 256  ) )
         MAX-ACCESS          read-create
         STATUS              current
         DESCRIPTION
            "This object is used as a bitmap to store untimed entitlements to
            premium channels. Note that the first bit of the first octet is
            reserved. Bits 1 to 2048 correspond to entitlements for channels
            with entitlementIndex between 1 and 2047, respectively. In order to
            entitlement channel with entitlementIndex x, the value of bit x in
            this bitmap must be 1. In order to revoke entitlement to channel
            with entitlementIndex y, the value of bit y in this bitmap must be
            0."
         ::=  {  customerEntry  5  }


      untimedEntitlements2   OBJECT-TYPE
         SYNTAX              OCTET STRING  ( SIZE ( 0 .. 256  ) )
         MAX-ACCESS          read-create
         STATUS              current
         DESCRIPTION
            "In order to support a greater number of channels this object is
            used in the same way as untimedEntitlements1 but bits 0 to 2048
            correspond to entitlements for channels with entitlementIndex
            between 2048 and 4095, respectively. The index into this bitmap is
            entitlementIndex - 2048."
         ::=  {  customerEntry  6  }

      grantEntitlement  OBJECT-TYPE
         SYNTAX              IpAddress
         MAX-ACCESS          read-create
         STATUS              current
         DESCRIPTION
            "When granting entitlements to a single channel for many customers
            SNMP Setting the untimedEntitlement1/2 object leads to lots of
            management traffic due to the size of the untimedEntitlement1/2
            object. In this situation it is much more bandwidth efficient to use
            this object. To grant an entitlement, the value of this object is
            SET to the channelId of the Channel for which entitlement is being
            granted to this customer. When this object is SET, the OLT/ONU must
            automatically update the associated bit in the untimedEntitlement1/2
            object to 1."
         ::=  {  customerEntry  7  }

      revokeEntitlement OBJECT-TYPE
```

```
      SYNTAX              IpAddress
      MAX-ACCESS          read-create
      STATUS              current
      DESCRIPTION
         "When revoking entitlements to a single channel for many customers
         SNMP Setting the untimedEntitlement1/2 object leads to lots of
         management traffic due to the size of the untimedEntitlement1/2
         object. In this situation it is much more bandwidth efficient to use
         this object. To revoke an entitlement, the value of this object is
         SET to the channelId of the Channel for which entitlement is being
         revoked for this customer. When this object is SET, the OLT/ONU must
         automatically update the associated bit in the untimedEntitlement1/2
         object to zero (0)."
      ::=  {  customerEntry  8  }


   customerAdminStatus    OBJECT-TYPE
      SYNTAX              INTEGER  {  locked ( 1 ),
                                      unlocked ( 2 ),
                                      shuttingDown ( 3 )
                          }
      MAX-ACCESS          read-create
      STATUS              current
      DESCRIPTION
         "This object is used to control the management state of this
         customer. When this object is set to locked(1) all existing channels
         being delivered to this customer must be immediately disconnected
         and further join requests from this customer must be rejected. If
         this object is set to shuttingDown(3), no further join requests
         should be accepted from this customer; when all existing channels
         have been disconnected from this customer the value of this object
         moves to locked(1)."
      ::=  {  customerEntry  9  }


   customerRowStatus OBJECT-TYPE
      SYNTAX              RowStatus  {active ( 1 ),
                                      notInService ( 2 ),
                                      notReady ( 3 ),
                                      createAndGo ( 4 ),
                                      createAndWait ( 5 ),
                                      destroy ( 6 )
                          }
      MAX-ACCESS          read-create
      STATUS              current
      DESCRIPTION
         "This object is used to manage row creation and deletion. When the
         channelAdminStatus is locked(1) the value of this object should be
         notInService(2). When the channelAdminStatus is unlocked(2) the
         value of this objects should be active(1) or notReady (3). When the
         value of channelAdminStatus is shuttingDown(3), the value of this
         object should be active(1)."
      ::=  {  customerEntry  10  }

   -- ------------------------------------------------------------------ --
   --
   -- The Timed Entitlement Table


   timedEntitlementTable  OBJECT-TYPE
      SYNTAX              SEQUENCE  OF  TimedEntitlementEntry
      MAX-ACCESS          not-accessible
      STATUS              current
      DESCRIPTION
```

```
      "This table is used to store entitlements to channels that
      have a relatively short duration, such as PPV channels."
   ::=  { channelChangeMibObjects  3 }

timedEntitlementEntry  OBJECT-TYPE
   SYNTAX              TimedEntitlementEntry
   MAX-ACCESS          not-accessible
   STATUS              current
   DESCRIPTION
      "An entry corresponds to timed entitlement for a single
      channel identified by the channelId. The same entry may
      be applicable to one or more customers as defined by
      the customerTimeEntitlementTable."
   INDEX   {  timedEntitlementId }
   ::=  { timedEntitlementTable 1 }

TimedEntitlementEntry  ::=  SEQUENCE {
   timedEntitlementId        Integer32,
   timedEntitlementChannelId IpAddress,
   startTime                 OCTET STRING,
   stopTime                  OCTET STRING,
   entitlementRowStatus      RowStatus
   }

timedEntitlementId     OBJECT-TYPE
   SYNTAX                  Integer32 (0 .. 65535 )
   MAX-ACCESS              read-create
   STATUS                  current
   DESCRIPTION
      "Describes uniquely a timed entitlement."
   ::=  {  timedEntitlementEntry  1  }

timedEntitlementChannelId    OBJECT-TYPE
   SYNTAX                    IpAddress
   MAX-ACCESS                read-create
   STATUS                    current
   DESCRIPTION
      "This has the value of the channelId of the channelEntry
      for which this timedEntitlementEntry is for."
   ::=  {  timedEntitlementEntry  2  }

startTime OBJECT-TYPE
   SYNTAX                    OCTET STRING ( SIZE ( 0..16 ) )
   MAX-ACCESS                read-create
   STATUS                    current
   DESCRIPTION
      "This is the time, expressed in UTC, from which time
      the channel is allowed to be viewed. When this time is
      greater than or equal to the current time, the bit in the
      untimedEntitlement1/2 object corresponding to the channel
      for which this timedEntitlementEntry relates is set to 1."
   ::=  {  timedEntitlementEntry  3  }


stopTime  OBJECT-TYPE
   SYNTAX                    OCTET STRING ( SIZE ( 0..16 ) )
   MAX-ACCESS                read-create
   STATUS                    current
   DESCRIPTION
      "This is the time, expressed in UTC, after which time
      the channel is not allowed to be viewed. When this time is
      less than the current time, the bit in the
      untimedEntitlement1/2 object corresponding to the channel
      for which this timedEntitlementEntry relates is set to
```

```
      zero (0). Once this is done this timedEntitlementEntry
      must also be removed from this table in order to stop this
      table growing indefinitely. Note that the information may
      be archived by the management system for audit purposes."
   ::=  {  timedEntitlementEntry  4  }


entitlementRowStatus   OBJECT-TYPE
   SYNTAX                  RowStatus  {active ( 1 ),
                                notInService ( 2 ),
                                notReady ( 3 ),
                                createAndGo ( 4 ),
                                createAndWait ( 5 ),
                                destroy ( 6 )
                           }
   MAX-ACCESS              read-create
   STATUS                  current
   DESCRIPTION
      "This object is used to manage row creation and deletion."
   ::=  {  timedEntitlementEntry  5  }


-- ------------------------------------------------------------------ --
--
-- The Customer Timed Entitlement Table

customerTimedEntitlementTable OBJECT-TYPE
   SYNTAX             SEQUENCE  OF  CustomerTimedEntitlementEntry
   MAX-ACCESS         not-accessible
   STATUS             current
   DESCRIPTION
      "This table defines the timed entitlements used by a
      customer as defined by the associated
      timedEntitlementEntry."
   ::=  { channelChangeMibObjects  4 }

customerTimedEntitlementEntry OBJECT-TYPE
   SYNTAX             CustomerTimedEntitlementEntry
   MAX-ACCESS         not-accessible
   STATUS             current
   DESCRIPTION
      "An entry corresponds to a timed entitlement for a customer."
   INDEX   {  onuId, customerPortId, custTimedEntitlementId }
   ::=  { customerTimedEntitlementTable 1 }

CustomerTimedEntitlementEntry  ::=  SEQUENCE {
   onuId                          InterfaceIndexOrZero,
   customerPortId                 InterfaceIndex,
   custTimedEntitlementId         Integer32,
   custTimedEntitlementRowStatus  RowStatus
   }

onuId  OBJECT-TYPE
   SYNTAX                  InterfaceIndexOrZero
   MAX-ACCESS              not-accessible
   STATUS                  current
   DESCRIPTION
      "Describes uniquely the ONU to which the customer is attached.   The
      value of this object must be the ifIndex of the interface in the
      OLT that connects to the associated ONU. If the OLT/ONU are
      integrated then the value of this object must be zero (0)."
   ::=  {  customerTimedEntitlementEntry  1  }
```

```
customerPortId   OBJECT-TYPE
   SYNTAX                  InterfaceIndex
   MAX-ACCESS              not-accessible
   STATUS                  current
   DESCRIPTION
      "Describes uniquely the port within the ONU/OLT to which the
      customer is attached. The value of this object must be the ifIndex
      of the port to which the customer is attached."
   ::=  {  customerTimedEntitlementEntry  2  }


custTimedEntitlementId  OBJECT-TYPE
   SYNTAX                  Integer32 ( 0..65535 )
   MAX-ACCESS              read-create
   STATUS                  current
   DESCRIPTION
      "This has the value of the timedEntitlementId for the
      timedEntitlementEntry that defined the timed entitlement
      to a channel for this customer."
   ::=  {  customerTimedEntitlementEntry  3  }

custTimedEntitlementRowStatus OBJECT-TYPE
   SYNTAX             RowStatus  {active ( 1 ),
                                  notInService ( 2 ),
                                  notReady ( 3 ),
                                  createAndGo ( 4 ),
                                  createAndWait ( 5 ),
                                  destroy ( 6 )
                      }
   MAX-ACCESS         read-create
   STATUS             current
   DESCRIPTION
      "This object is used to manage row creation and deletion."
   ::=  {  customerTimedEntitlementEntry  4  }


-- ------------------------------------------------------------------ --
--
-- Channel Change Function traps

channelChangeMibNotificationPrefix  OBJECT IDENTIFIER
           ::= { channelChangeMibNotifications 0 }

channelChangeCAFailed  NOTIFICATION-TYPE
   OBJECTS { rejectedOnuId, rejectedCustomerPortId }
   STATUS  current
   DESCRIPTION
      "This trap is generated when conditional access fails for a
      requested channel change. The trap identifies the customer
      that issued the request."
   ::=  {  channelChangeMibNotificationPrefix 1 }

rejectedOnuId    OBJECT-TYPE
   SYNTAX             InterfaceIndexOrZero
   MAX-ACCESS         read-write
   STATUS             current
   DESCRIPTION
      "Identifies the ONU from which the rejected channel change
      request originated."
   ::=  {  channelChangeMibObjects  5  }

rejectedCustomerPortId  OBJECT-TYPE
   SYNTAX             InterfaceIndex
   MAX-ACCESS         read-write
   STATUS             current
```

```
   DESCRIPTION
      "Identifies the DSL portfrom which the rejected channel
      change request originated."
   ::=  {  channelChangeMibObjects  6  }

caFailedNotificationStatus   OBJECT-TYPE
   SYNTAX              INTEGER  {  enabled ( 1 ),
                                   disabled ( 2 )
                       }
   MAX-ACCESS          read-write
   STATUS              current
   DESCRIPTION
      "This object is used to enable and disable the sending of
      the channelChangeCAFailed trap."
   ::=  {  channelChangeMibObjects  7  }


-- ------------------------------------------------------------------ --
--
-- Conformance Information

channelChangeMibConformance  OBJECT IDENTIFIER
   ::=  {  channelChangeMib 3  }

channelChangeMibCompliances  OBJECT IDENTIFIER
   ::=  {  channelChangeMibConformance 1  }

channelChangeMibGroups OBJECT IDENTIFIER
   ::=  {  channelChangeMibConformance 2  }


-- compliance statements

channelChangeMibCompliance MODULE-COMPLIANCE
   STATUS              current
   DESCRIPTION
      "The compliance statement for SNMP entities that support
      the channel change function as specified in FS-VDSL SA
      specification.

      For a system to conform to this MIB it must also implement:

      - ifTable from RFC 2863 to define the physical interfaces."

   MODULE -- this module
   MANDATORY-GROUPS {
      channelChangeBasicGroup
   }

   -- conditionally mandatory groups listed below, where the
   -- condition is given in the DESCRIPTION clause of the group.

   GROUP         channelChangeCACGroup
   DESCRIPTION
      "This group is mandatory if a Channel Change Function
      implements Connection Admission Control (CAC) for channel
      change requests."

   GROUP         channelChangeBasicCAGroup
   DESCRIPTION
      "This group is mandatory if a Channel Change Function
      implements conditional access (CA) for up to 2047 channels
      and supports only untimed entitlements."
```

```
    GROUP         channelChangeCA4095ChannelsGroup
    DESCRIPTION
        "This group is mandatory if a Channel Change Function
        implements conditional access (CA) for up to 4095 channels."

    GROUP         channelChangeCATimedEntitlementsGroup
    DESCRIPTION
        "This group is mandatory if a Channel Change Function
        implements CA based on timed entitlements."

    GROUP         channelChangeCANotificationsGroup
    DESCRIPTION
        "This group is optional if CA is implemented by the Channel
        Change Function."

    ::=  {  channelChangeMibCompliances 1  }

-- Units of Conformance

channelChangeBasicGroup OBJECT-GROUP
    OBJECTS {
        channelId,
        networkPortId,
        vpi,
        vci,
        channelAdminStatus,
        channelRowStatus,
        onuId,
        customerPortId
    }
    STATUS  current
    DESCRIPTION
        "A collection of objects required as a minimum to manage
        the Channel Change Control function."
    ::=  {  channelChangeMibGroups 1  }

channelChangeCACGroup        OBJECT-GROUP
    OBJECTS {
        maxMulticastTraffic
    }
    STATUS  current
    DESCRIPTION
        "A collection of objects required to support CAC."
    ::=  { channelChangeMibGroups 2  }


channelChangeBasicCAGroup          OBJECT-GROUP
    OBJECTS {
        maxMulticastStreams,
        entitlementIndex,
        untimedEntitlements1,
        grantEntitlement,
        revokeEntitlement,
        rejectedOnuId,
        rejectedCustomerPortId,
        caFailedNotificationStatus
    }
    STATUS  current
    DESCRIPTION
        "A collection of objects required to support CA with only
        untimed entitlements. This group is sufficient to support
        conditional access for up to 2047 channels."
    ::=  {  channelChangeMibGroups 3  }
```

```
      channelChangeCA4095ChannelsGroup   OBJECT-GROUP
         OBJECTS {
            untimedEntitlements2
         }
         STATUS  current
         DESCRIPTION
            "This group is required in addition to the
            channelChangeBasicCAGroup to support CA for up to 4095
            channels."
         ::=  {  channelChangeMibGroups 4  }

      channelChangeCATimedEntitlementsGroup    OBJECT-GROUP
         OBJECTS {
            timedEntitlementId,
            timedEntitlementChannelId,
            startTime,
            stopTime,
            entitlementRowStatus,
            custTimedEntitlementId,
            custTimedEntitlementRowStatus
         }
         STATUS  current
         DESCRIPTION
            "This group is required in addition to the
channelChangeBasicCAGroup, and if applicable the
channelChangeCA4095ChannelsGroup, to support timed
            entitlements."
         ::=  {  channelChangeMibGroups 5 }

      channelChangeCANotificationsGroup  NOTIFICATION-GROUP
         NOTIFICATIONS {
            channelChangeCAFailed
         }
         STATUS  current
         DESCRIPTION
            "This group contains the notification used to inform
            management that a conditional access request failed. This
            group is optional if CA is implemented by the Channel
            Change Function."
         ::=  {  channelChangeMibGroups 6  }


END
```

APPENDIX II

POSSIBLE ACCESS NETWORK AND CORE NETWORK CONFIGURATIONS (INFORMATIVE)

1. Basic Architecture of the End-to-End Network

There are a wide variety of ways in which the home network, the access network, and the core network can be constructed. This ability to support different networking scenarios is essential to the FS-VDSL architecture as it allows compatible implementations within the different circumstances of Network operators around the world.

The primary focus of the FS-VDSL is on the AN and the home network, with their basic architecture, the interfaces, and the building blocks described in the preceding sections. This section describes how the capabilities of the AN and home network combine with a variety of core networking options in order to deliver end-to-end network and transport capabilities. These Network and transport capabilities support the services described in section 9.

It should be noted that some core networking may be needed to support the service nodes, for example, to upload content to video servers or to connect the Internet Services service node to a common Internet peering point. This form of Networking is not part of the end-to-end Networking and transport capabilities described in this section. The scope of this section is set by the need to connect VTP/D supporting a service to a service node supplying the service.

1.1 No Core Network Scenario

It is possible to host the services in the same location as the OLT. This means that there is no requirement for a Core Network. The service nodes are therefore directly connected to the OLT using ATM interfaces. This is illustrated in the following Figure.

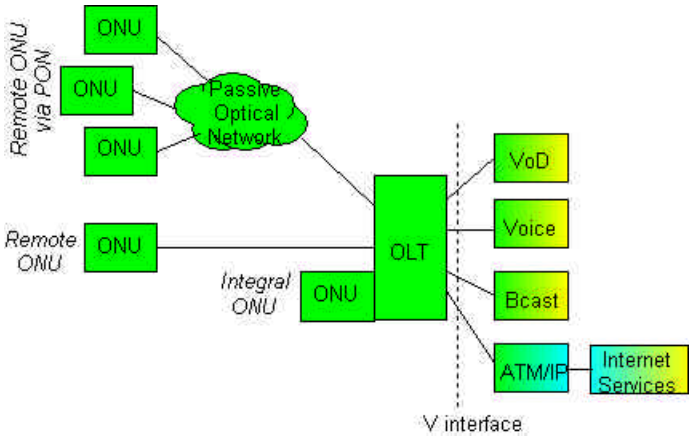


Figure 25: Directly Connected Service Nodes

Figure 25 also illustrates three basic configuration options for the access network. These are a combined OLT and ONU, a ONU subtended from the OLT using a direct fibre, and a set of ONUs subtended from the OLT using a passive optical network.

1.2 ATM Core Network Scenario

Many network operators have a need to centralize their service nodes and therefore a core network is needed to connect the OLT to the service nodes. As the OLT is functionally an ATM cross-connect, it can be connected to an ATM network, offering seamless ATM transport of ATM VCs and ATM VPs. With an ATM core network no protocol interworking is required between the V interface and the core network. The requirement on the ATM core network is that it fully supports all the connection parameters for all flows across the V interfaces across the core network. This scenario is illustrated in the following figure.

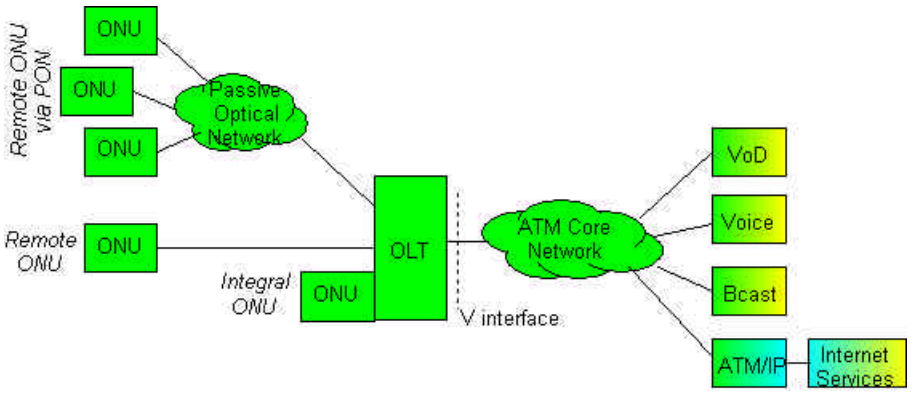


Figure 26: ATM Core Network

1.3 IP Core Network Scenario

IP is the home networking protocol. While this specification does allow services to terminate the IP protocol in the VTP, placing the service protocols directly on the ATM VCs, the IP protocol can be extended transparently across the access network. When this option is chosen in the VTP, the IP protocol layer is always present at the V interface. This allows the ATM VCs to be terminated after the V interface and the core network forward at the IP layer. This is illustrated in the following Figure.

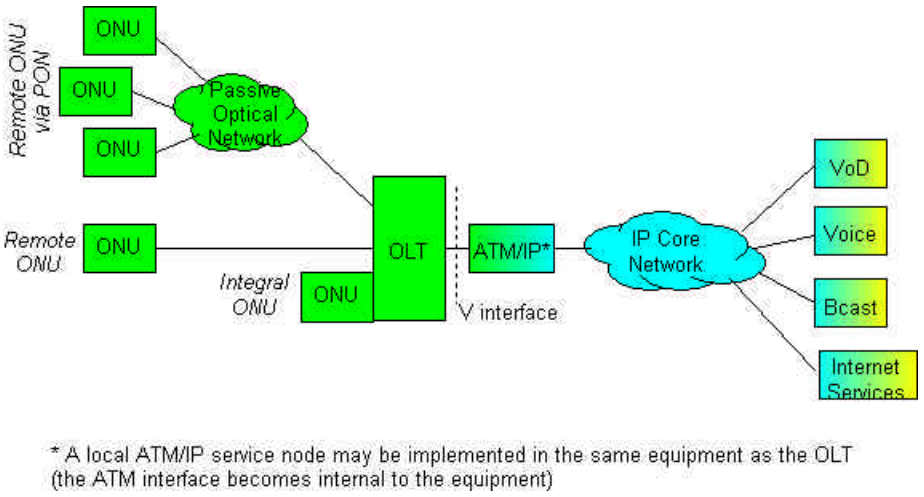


Figure 27: IP Core Network

When the core network is IP, the QoS parameters specified for each flow must be met by the IP network such that the end to end flow at the IP layer performs as if it was supported by an end to end ATM VC with the specified parameters.

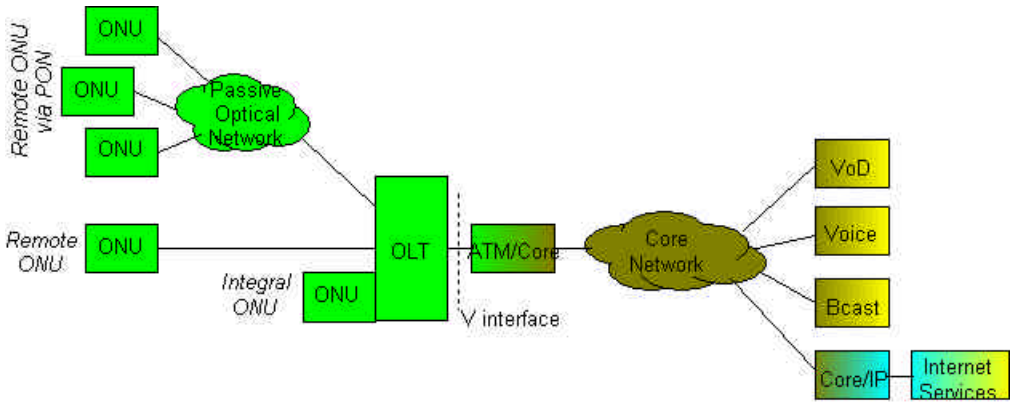
1.4 Other Core Network Scenario

While ATM has been specified by FS-VDSL for the access network, other network protocols/technologies are possible in the core network. Example include SONET/SDH, Ethernet and MPLS. As the OLT is an ATM device, interworking is required between the OLT and this core network. There are three general ways that the interworking function can work.

- Encapsulate and multiplex one or more of the ATM VCs at the V interface into a conformant transport entity of the core network. In this case, the core network is effectively a layer 1 Network. The core network must transport the bundle of VCs in such a way that, when the encapsulation is removed, the ATM VC can be recreated so that all the VC connection parameters described in section 8 are met.
- Emulate the ATM VC with the transport entity of the network. In this case, the core network will a layer 2 network like ATM. This emulation must be done in such a way that all the VC connection parameters described in section 8 are met.

- Terminate the ATM VCs and transport the higher layers transparently. In this case, the core network is effectively a layer 3 network. This should only be considered when IP is the layer 3 protocol and this case then becomes the IP Core Network scenario above.

This scenario is illustrated in the below figure. It is assumed that the service node will contain sufficient functionality to terminate the core network protocol as well as the service protocol stack.

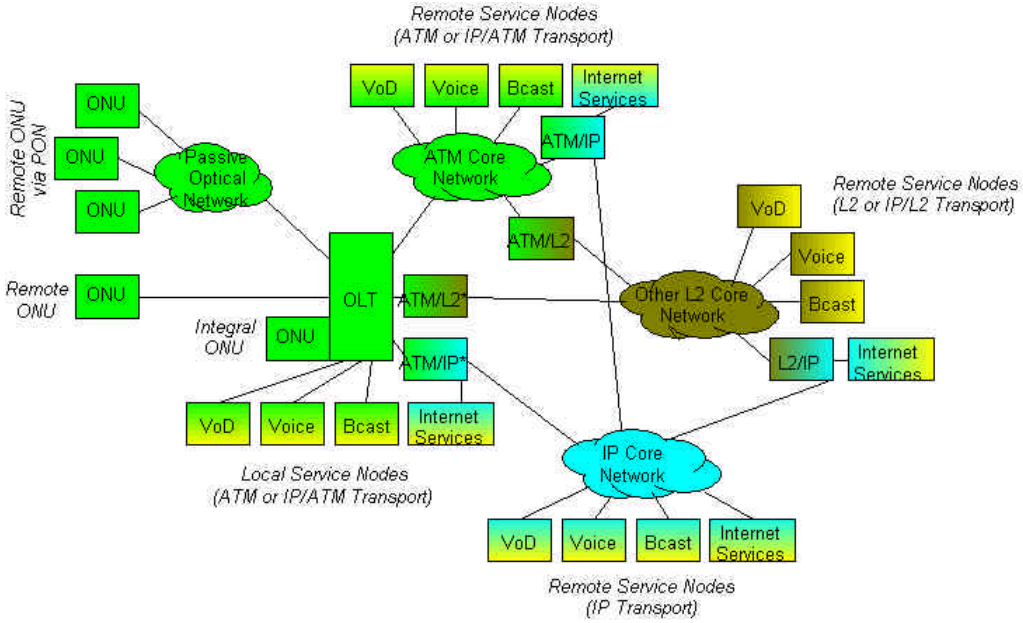


* A local ATM/Core service node may be implemented in the same equipment as the OLT (the ATM interface becomes internal to the equipment)

Figure 28: Optional Core Network

1.5 Hybrid Core Network Scenario

Many network operators do not have a single core network scenario. This is highly likely as networks evolve and older generations of equipment remain in use while newer generations are introduced. The scenarios described above are not exclusive and can be combined in a wide variety of ways, many of which are illustrated in the following Figure.



* A local ATM/IP and/or ATM/L2 service node may be implemented in the same equipment as the OLT (the ATM interface becomes internal to the equipment)

Figure 29: Hybrid Core Network

APPENDIX III

VDSL DUAL LATENCY CHANNEL SUPPORT (INFORMATIVE)

VDSL physical layer provides support for dual latency channels commonly referred to as the fast and interleaved channels. The "fast" channel has a low latency (typically 2ms, but a higher Bit Error Rate (BER) that can be caused by impulse noise in comparison to a "interleaved" channel. In contrast the "interleaved" channel has a higher latency (typically tens of milliseconds) and a lower BER that can be caused by impulse noise. This is due to the fact that the interleaved channel provides support for interleaving across blocks and forward error correction of the payload.

Forr the interleaved channel the interleaver depth can be configured. The interleaving depth is directly proportional to the delay. Thus a larger interleaving depth results in a bigger delay.

The bandwidth assigned to each of the latency channels is normally statically assigned. The VDSL standards do support the concept of "Dynamic Rate Re-partitioning" (DRR), which does enable the bandwidth associated with each of the latency paths to be dynamically assigned between the two latency channels. However, DRR is not commonly used, because of its complexity.

If dual latency channels are supported, then the table below provides a possible mapping of applications to the VDSL dual latency channel. Operators must make a trade-off between delay and bit error sensitivity when selecting the appropriate latency channel.

Application	Delay Sensitive	Bit Error Rate (BER) Sensitive	VDSL dual latency channel
Voice	Yes[1]	No[2]	Fast channel preferred.
Channel Change	Yes	Yes	Fast channel preferred. The fast channel is chosen since latency is more significant compared to the BER.
Video on Demand	No	Yes	Interleaved channel preferred.
Broadcast TV	No	Yes	Interleaved channel preferred.
Data	No	No	Either channel is suitable. If the data uses the UBR service category, then it is advantageous for the data traffic to share the same latency channel as the VoD/Broadcast TV traffic, in order to allow the data service to use any unused VoD/Broadcast TV traffic bandwidth.
Gaming	Yes	Yes	Neither channel is ideally suitable. A trade off must be made as to whether delay or bit error rate is the more significant factor.

1. It is commonly agreed that up to 150 ms mouth to ear delay can be tolerated with virtually no quality degradation if echo cancelling techniques are used. The delay introduced by the interleaver is only one aspect that contributes to the overall ear to mouth delay budget. Other sources of delay include voice encoder, voice decoder, packetisation delay, queuing delay, etc.

2. Depending on chosen voice codec

Figure 30: Typical Mapping of Applications to VDSL Dual Latency Channels

The VDSL modem located in the ONU, or the VTP/D, does not distinguish between applications carried by individual ATM VCCs. The VTP/D and the ONU may use either the ATM VPI or the VPI/VCI ATM cell header values associated with the ATM connection in order to map the payload to either the VDSL fast or interleaved channel.

If the ATM VPI mapping is used, it is recommended that separate interleaved and fast ATM VPs be assigned. Any traffic associated with the interleaved ATM VP is to be transported by the VDSL interleaved channel, while traffic associated with the fast ATM VP is to be transported by the VDSL fast channel. An individual ATM VCC must then be assigned to either the interleaved or fast VP. This assignment should be dependant upon the nature of the application traffic being transported by that VCC (see Table 1) (e.g., the broadcast TV ATM VCCs used to carry individual broadcast TV channels would use the interleaved ATM VP).

If the ATM VPI/VCI mapping is used, then the individual ATM VCCs must be assigned to either the VDSL interleaved or fast channel based on the application traffic carried by that VC (see Table above).

It should be noted that supporting dual latency channels results in additional complexity, since bandwidth across the two latency channels must be managed and additional costs may be incurred in supporting this capability. Operators should objectively assess the benefits of introducing dual latency compared with the additional complexity and costs that can be incurred. The VTP/D and ONU MUST support a single latency channel.

APPENDIX IV

IGMP V2 TO DSMCC TRANSLATION FUNCTION

IGMPv2 is used as the Channel Change protocol within the home network. Either IGMP or DSM-CC may be used as the channel change protocol between the VTP/D and the AN. This Appendix describes how the VTP/D may interwork the two channel change protocols. The interworking would be performed by the IGMPv2-DSM-CC interworking function within the VTP/D as described in the figure below.

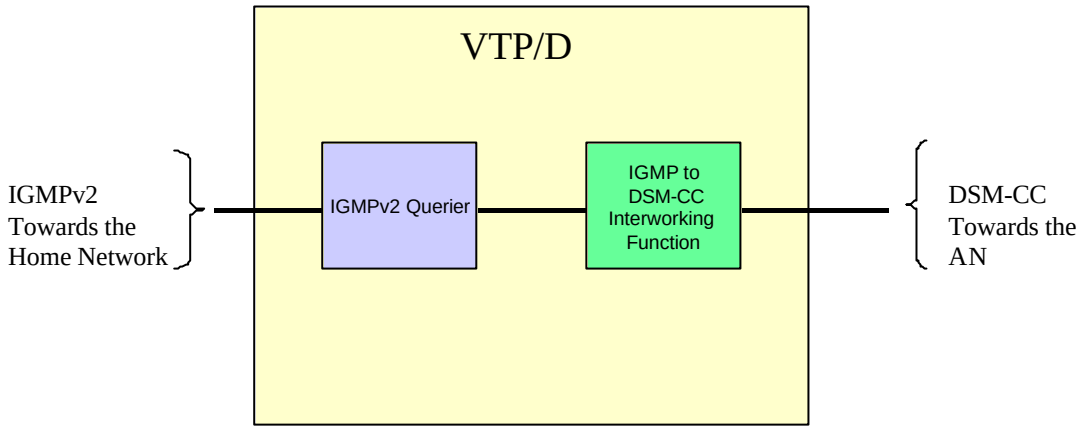


Figure 31: VTP/D DSM-CC Channel Change Functional Architecture

The figure above assumes that only filtered IGMPv2 that are related to the broadcast TV streams are processed by the IGMPv2 Querier.

The IGMPv2 Querier function keeps track of the state of each multicast channel as defined in section 11.4 of the specification. This enables it to determine if a multicast channel has any membership.

With DSM-CC a single message can be used to switch a member from one multicast channel to another. The use of a single message enables the AN to be provide a much faster channel change and thereby improves the overall channel change switch over time. Also it improves the overall channel change throughput and performance of the AN. However IGMPv2 uses two messages when performing a channel change, an IGMP Leave followed by an IGMP Join. Therefore the interworking function will need to perform the following actions in order to exploit the use of a single DSM-CC message:

- When an IGMP Leave message is received, a "Join_Anticipation" timer will be started. This timer will have a default value of a 200ms.

- If a Join message is received while the "Join_Anticipation" timer is running, then timer will be cancelled. This will be followed by the generation of a DSM-CC ProgramSelect message is specifying the session identity associated with the old channel and the new Broadcast Program Id (BPID) that is required.

- If a Join message is received while the timer is not running, then a DSM-CC ProgramSelect is sent specifying a new session id and the BPID of the channel that is required.

- If the “Join_Anticipation” timer expires, then a DSM-CC ProgramSelect message is sent specfying the session identity associated with the channel that is no longer required and a BPID of “0”.

Notes:

The BPID is determined from the IP class D multicast address as defined in section 11.4.3 of the specification.

The optimisation described above enables multiple broadcast TV streams to be received simultaneously.

APPENDIX V

MESSAGE SEQUENCE CHARTS (INFORMATIVE)

This informative appendix proposes a set of message sequence charts describing particular scenarios.

This section provides Message Sequence Charts (MSCs) for some common scenarios that the VTP and the FS-VDSL system are required to support.

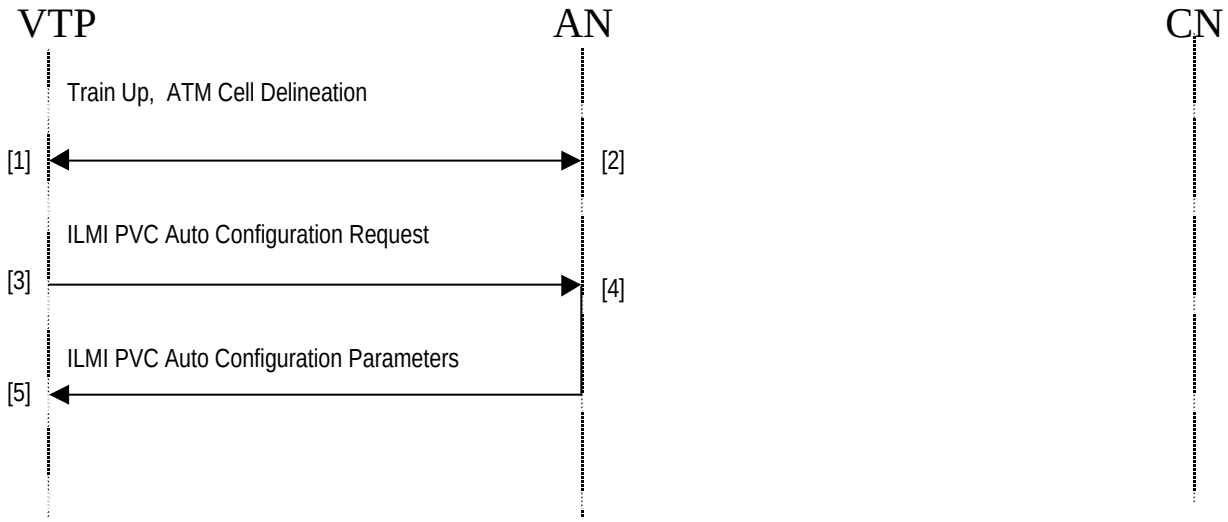
Each of the MSCs is annotated to provide a description of the high level procedures to assist in the understanding of the MSCs.

1. Start Up of the VTP

The scenario describes the flow that occurs when a VTP under goes a cold start, which can for example occur when the VTP is powered up or a malfunction of the VTP occurs resulting in a start up

Pre-conditions:

None.



[1] The VTP is powered up and restarted. The VTP trains up by initially negotiating and agreeing the VDSL physical layer parameters such as the upstream and downstream bandwidth. After train up both the VTP and the AN will check for ATM cell delineation in order to confirm that ATM packets can be exchanged over the VDSL interface.

[2] The AN trains up as described in item [1].

[3] The VTP will issue an ILMI PVC Auto Configuration Request over the well known VCI value of "16". The request enables the VTP to determine the ATM VCs that have been the configured and the traffic descriptor associated with each of these ATM VCs.

[4] The AN responds with the ATM VC configuration parameters. See reference (AF-NM-0122.000 May, 1999 "Auto Configuration of PVCs" for further details of the procedures).

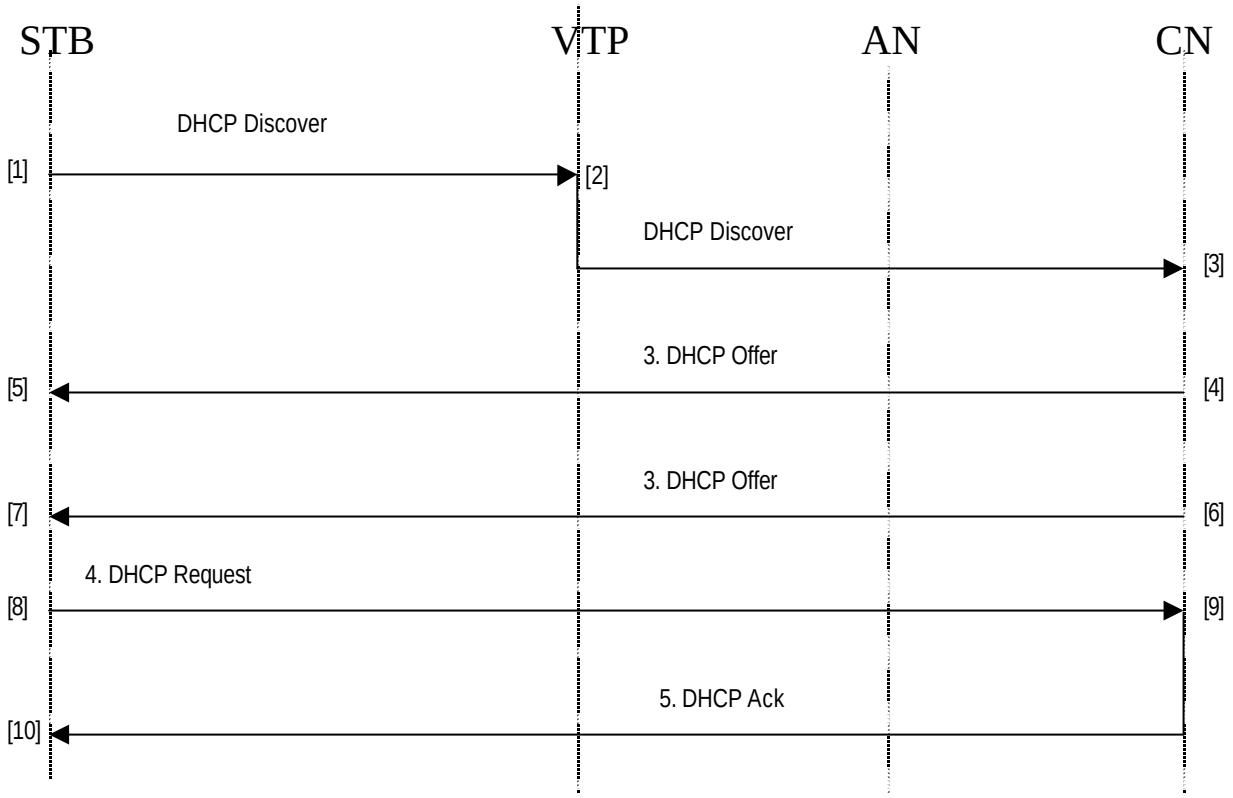
[5] The VTP stores the ATM configuration parameters that identify the ATM VCCs that have been set up and their corresponding traffic descriptors.

2. STB Boot Up

The scenario describes the flow that occurs when a Set Top Box (STB) boots up, which can for example occur when the STB is powered up or a malfunction of the STB occurs resulting in a start up

Pre-conditions:

None.



[1] The STB issues a request to the network in order to request an IP address and other configuration parameters. The DHCP Discover packet contains a destination IP broadcast address (255.255.255.255) and a Vendor Class Identifier service string of "FS-VDSL STB".

[2] The DHCP server located within the VTP will ignore the DHCP Discover packet because it will be configured to ignore DHCP packets containing a Vendor Class Identifier string "FS-VDSL STB.

If the VTP is operating in bridged mode, then the DHCP Discover packet will be sent on all bridged ATM VCs

[3] The DHCP Discover will be processed by one or more DHCP servers.

[4], [6] One or more DHCP servers located within the Core Network will respond with a DHCP Offer that includes an available IP address. The Core Network may include a DHCP relay agent for relaying the broadcast DHCP packets to the required DHCP servers, thus improving scalability and security.

[5], [7] The STB will then choose an appropriate target DHCP Server from the list of those that have responded with a DHCP Offer.

[8] The STB selects a DHCP server from the list of DHCP Offer requests it has received. This is done by sending a DHCP Request packet with a destination IP broadcast address (255.255.255.255) and the address of the target server in the "server IP address" field of the DHCP packet including a Vendor Class Identifier service string of "FS-VDSL STB". The reason for broadcasting the request is so that non selected DHCP servers may be notified.

If the VTP is operating in bridged, then the DHCP Request packet will be sent on all bridged ATM VCs

[9] The target server recognises it's IP address in the "server IP address" field of the DHCP Request packet and responds with a DHCP Ack containing the following configuration parameters; IP address, Subnetwork Mask, Default Gateway, DNS Primary and Secondary Servers.

[10] The STB records the received configuration parameters for the duration of the lease period. The STB can use these parameters to perform some of the following tasks;

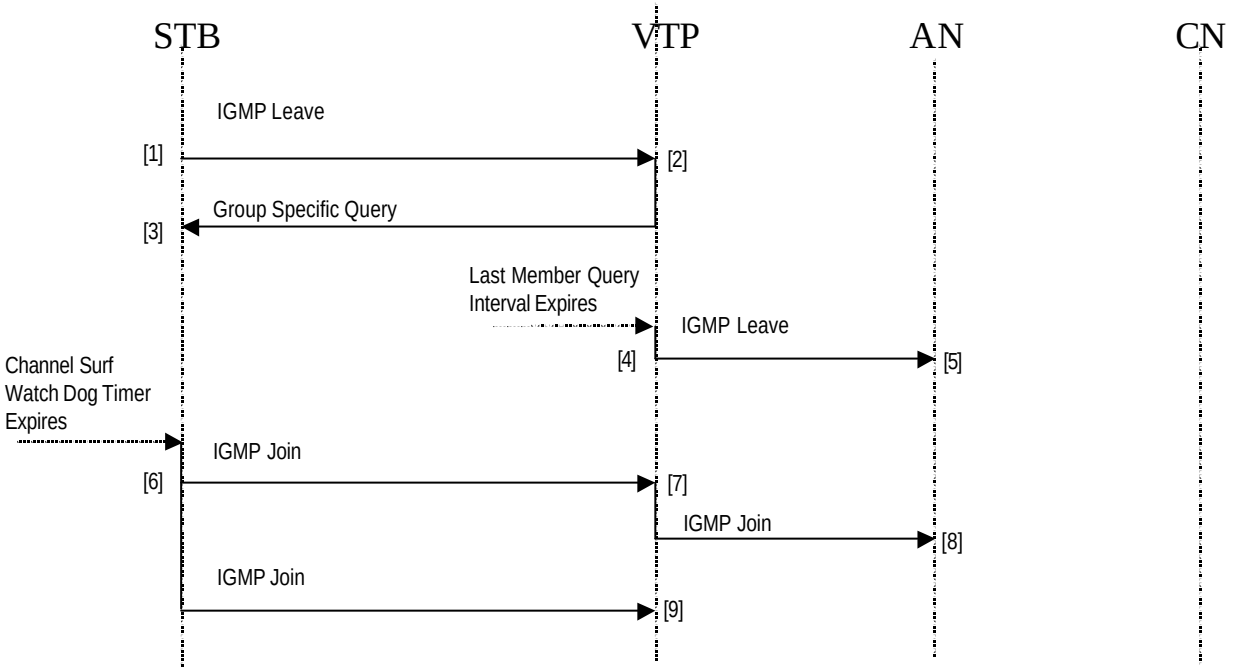
- Download it's software image using mechanisms such as TFTP/FTP.
- Broadcast TV and VoD channel selection as described in the latter MSCs.
- Internet browsing.

3. Broadcast TV Channel Change – IGMP between VTP and AN

The scenario describes the flow when a user switches between two TV channels and IGMP is used as the channel change protocol between the VTP and the AN.

Pre-conditions:

- Successful bootup of the VTP and STB.
- The STB is receiving a broadcast TV channel.



[1] The end user is already watching a broadcast TV channel. He then selects another broadcast TV channel. The STB requests the previously selected broadcast TV stream is disconnected. This is achieved by issuing an IGMP Leave containing the IP multicast address of the channel that is to be disconnected.

In addition the STB starts a "Channel Surf Watch Dog Timer" to guard against unnecessary generation of IGMP Join messages in the case where the end user channel surfing. *Note the running and the value of this timer is implementation dependent and is outside the scope of the specification.*

[2] Upon receipt of the "IGMP Leave" the VTP checks to see if other STBs are still interested in receiving the multicast channel by sending an IGMP Group Specific Query and starting the "lastmemberquery" interval timer.

[3] The Group Specific Query is ignored by all STBs, since none of them are members of the multicast group specified within the message.

[4] The "lastmemberquery" interval timer expires and the VTP generates an IGMP Leave to the AN specifying the multicast group that has no membership.

[5] Upon receipt of the "IGMP Leave" the Access Network stops sending the specified multicast channel stream to the VTP.

[6] Upon expiry of the "Channel Surf Watch Dog" timer the STB generates an IGMP Join which specifies the multicast channel that the end user has selected. The STB allows generates a second IGMP in order to cover the case the first one is lost (as specified by the robustness variable in RFC2236).

[7] Upon receipt of the first IGMP Join the VTP checks to see if there are any members already associated with the multicast group specified in the IGMP Join. Since there are no members, then the IGMP Join is forwarded to the Access Network.

[8] The Access Network upon receipt of the IGMP Join will check if the VDSL drop is entitled to join the requested multicast group, This is optional and only occurs if conditional access is provided by the AN. It will then ensure that there is enough capacity on the VDSL drop for the specified channel.

If there enough capacity, then a free broadcast TV ATM VC will be attached to the multicast source specified in the IGMP Join. This action will result in the broadcast stream being forwarded to the VTP.

[9] The VTP ignores the second IGMP Join message, since there is already an existing member (as a result of the first IGMP Join) of the multicast group specified in the IGMP Join.

Notes;

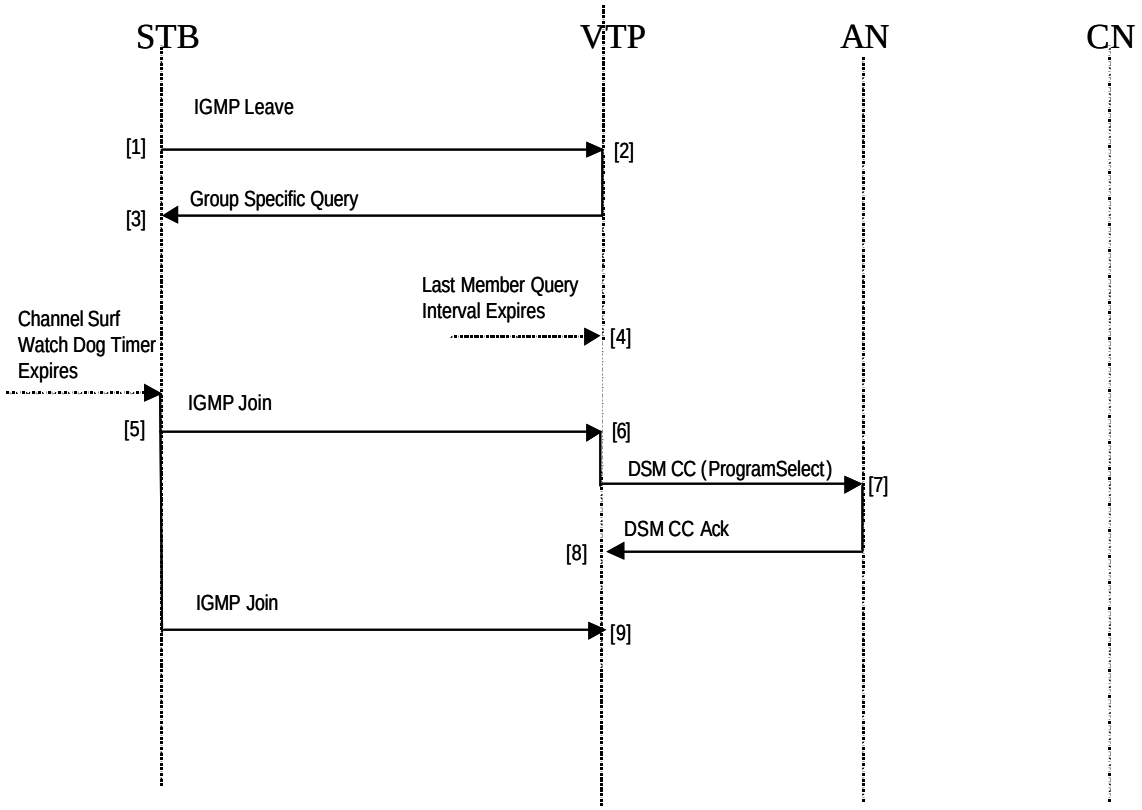
1. The VTP filters any IGMP messages received over the Tcn interface that match any of the multicast addresses associated with the broadcast TV stream
2. IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

4. Broadcast TV Channel Change – DSM-CC between VTP and AN

The scenario describes the flow when an end user switches between two TV channels and DSM CC is used as the channel change protocol between the VTP and the AN.

Pre-conditions:

- Successful bootup of the VTP and STB.
- The STB is receiving a broadcast TV channel.



[1] As per 2.3 [1]

[2] As per 2.3 [2]

[3] As per 2.3 [3]

[4] The "lastmemberquery" interval timer expires and the VTP starts the "JoinAnticipation" timer, so that a single DSM-CC message can be sent to in order to perform a "move" operation. The "move" operation disconnects the Broadcast ATM VC from it is existing multicast group and re-connects the broadcast ATM VC to the new multicast group. This optimises the performance of the AN.
To achieve the optimisation the "JoinAnticipation" timer must be chosen to be greater than the "Channel Surf Watch Dog" timer run by the STB.

[5] As per 2.3 [6]

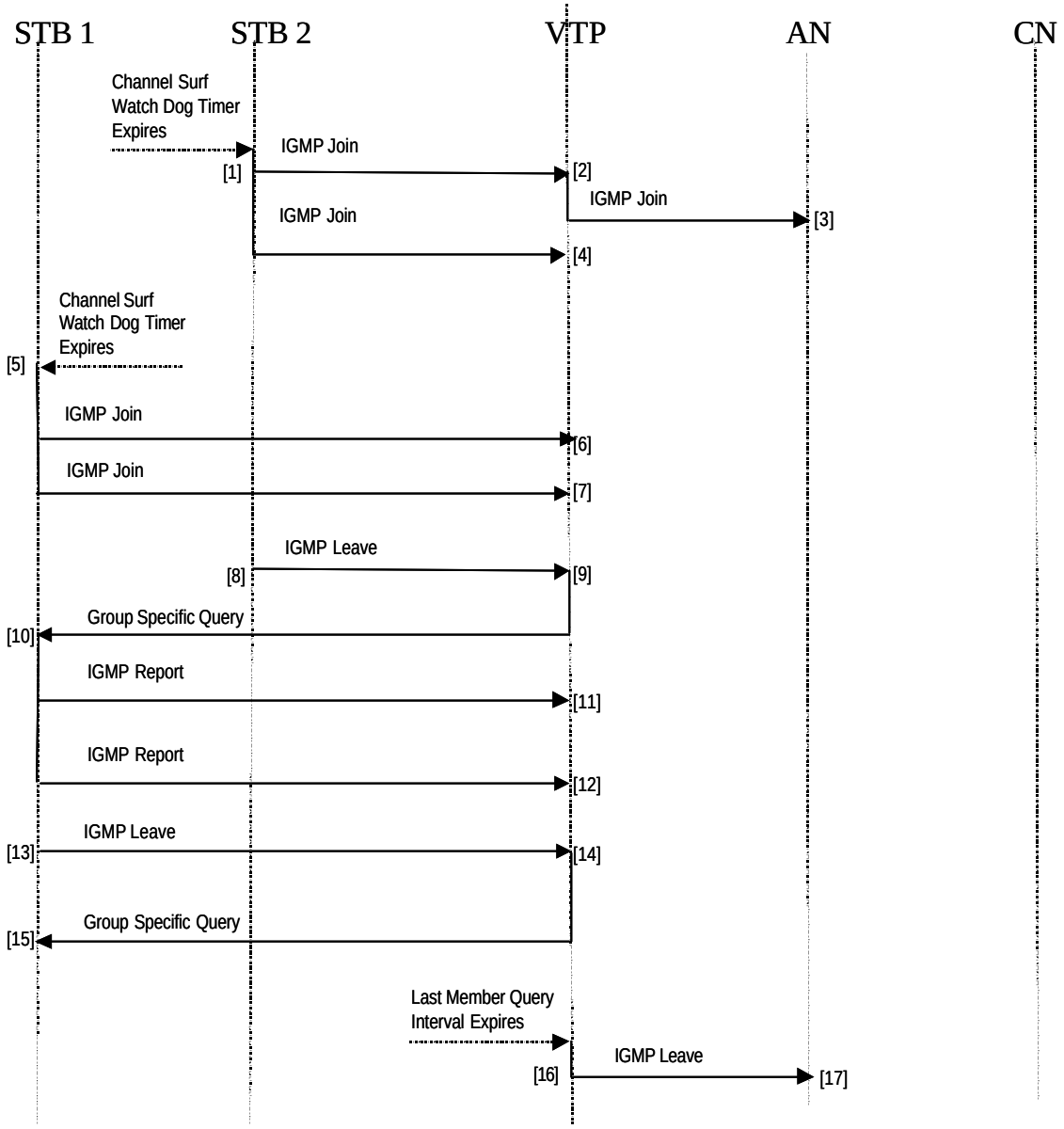
[6]	Upon receipt of the first IGMP Join the VTP checks to see if there are any existing members associated with the multicast group that was specified in the IGMP Join. Since there are no existing members, then the "JoinAnticipation" timer is cancelled and a DSM CC (ProgramSelect) message is sent to the Access Network containing the Broadcast Program Id (BPID) and session identity associated with previous channel that was viewed. The BPID is a copy of the multicast address received in the IGMP Join.
[7]	The Access Network upon receipt of the DSM CC (ProgramSelect) will disconnect the Broadcast TV ATM VC from the previous multicast group. If conditional access is supported, then it will check if the VDSL drop is entitled to view the requested BPID. Finally it will reconnect the Broadcast TV VC will to the new multicast source as specified by the BPID. This action will result in the requested broadcast stream being forwarded to the VTP. In addition the AN will send a DSM CC Ack indicating the ATM VC that will be used for delivering the Broadcast Program Id (BPID).
[8]	The VTP notes that the AN will now start forward the broadcast stream. The VTP also notes the VC that will be used for delivering the BPID. *This information is needed by the VTP in the situation where MPEG2/AAL5 transport is used, so that the VTP can insert the correct IP multicast class address in the stream sent over the Tcn interface.*
[9]	As per 2.3 [9]
Notes;	1. The VTP filters any IGMP messages received over the Tcn interface that match any of the multicast addresses associated with the broadcast TV stream 2. DSCM CC messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

5. Multiple STB Broadcast TV Surfing – IGMP Between VTP and AN

This scenario describes the situation where two STBs in the same home network are watching the same TV channel. This sequence illustrates the IGMP optimisation that is performed by the VTP.

Pre-conditions:

- Successful bootup of the VTP, STB 1 and STB 2.
- STB 1 and STB 2 are not already receiving a broadcast TV channel.



[1] End user 2 selects a broadcast TV channel and the "Channel Surf Watch Dog" timer is started.

Upon expiry of the "Channel Surf Watch Dog", STB 2 generates an IGMP Join specifying the multicast group address that the end user has selected. STB 2 also generates a second IGMP in order to cover the case the first one is lost (as specified by the robustness variable in RFC2236).

[2] As per 2.3 [7]

[3] As per 2.3 [8]

[4] As per 2.3 [9]

[5] End user 1 selects the same broadcast TV channel as end user 2 and the "Channel Surf Watch Dog" timer is started.
Upon expiry of "Channel Surf Watch Dog" timer, STB 1 generates an IGMP Join specifying the multicast group which is the same as that specified by STB 2. STB 1 also generates a second IGMP in order to cover the case the first one is lost (as specified by the robustness variable in RFC2236).

[6] The VTP determines that there is already an existing member (i.e. STB 2) of the same multicast group. Therefore the IGMP Join is not forwarded to the AN.

[7] As per [6].

[8] End User 2/STB2 disconnects from broadcast TV channel. STB2 generates an IGMP Leave message to the VTP indicating that the multicast group is no longer required.

[9] The VTP generates a Group Specific Query and starts the "lastmemberquery" interval timer to check if membership of the multicast group is required by any other STB.

[10] STB 1 determines that it still requires the multicast channel specified the Group Specific Query. It generates an IGMP Report and followed by a second one in case the first one gets lost (as specified by the robustness variable in RFC2236).

[11] The VTP notes that membership of the multicast group is still required.

[12] The IGMP Join is ignored by the VTP, since there is already a member of the multicast group.

[13] End User 1/STB1 disconnects from broadcast TV channel. STB1 generates a IGMP Leave message to the VTP indicating the multicast group that is no longer required to be forwarded.

[14] Upon receipt of the "IGMP Leave" the VTP checks to see if other STBs are still interested in receiving the multicast channel by sending an IGMP Group Specific Query and starting the "lastmemberquery" interval timer.

[15] The Group Specific Query is ignored by all STBs, since none of them are members of the multicast group specified within the message.

[16] The "lastmemberquery" interval timer expires and the VTP generates an IGMP Leave to the AN specifying the multicast group that has no membership.

[17] Upon receipt of the "IGMP Leave" the Access Network stops sending the specified multicast channel stream to the VTP.

Notes;

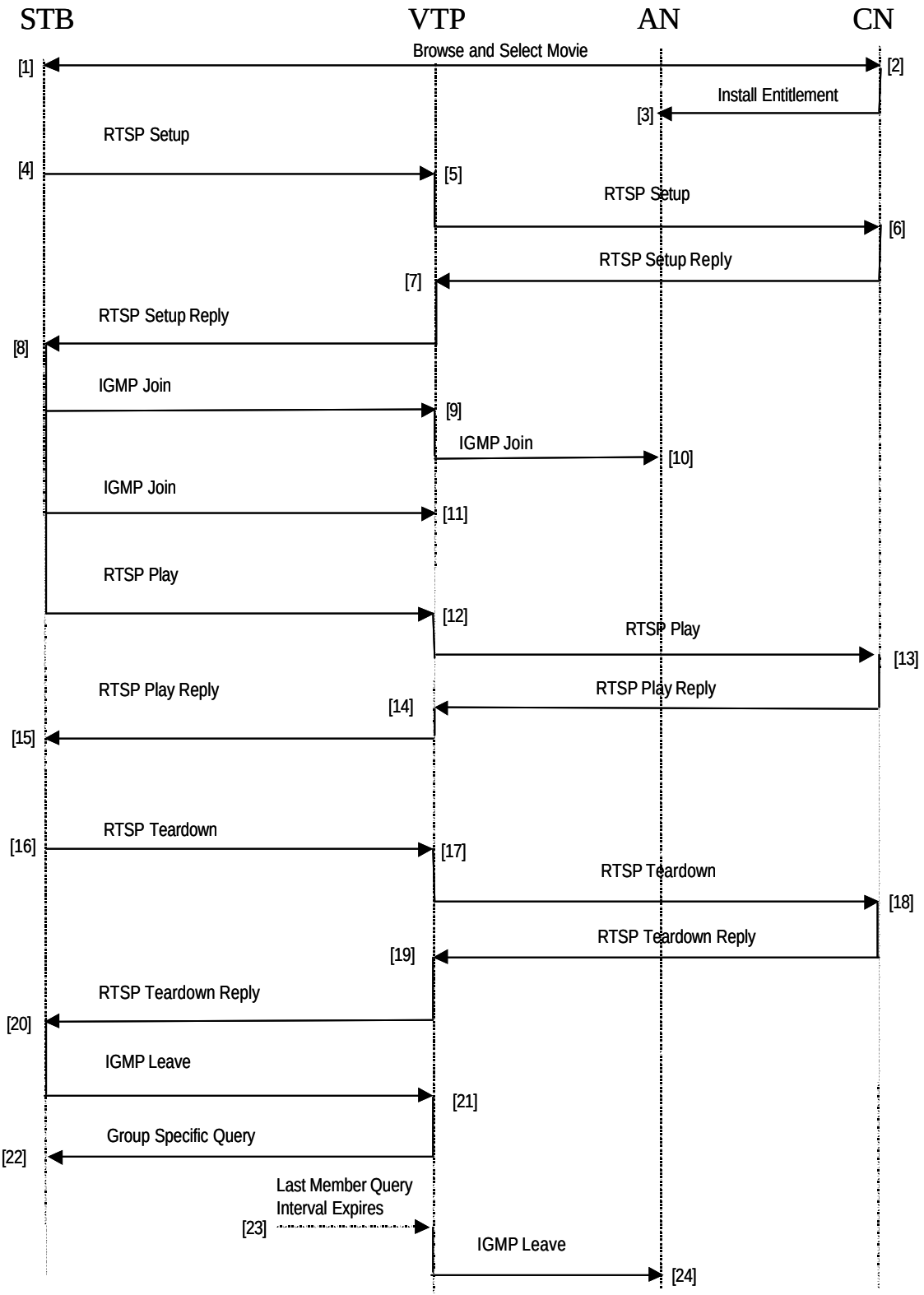
1. The VTP filters any IGMP messages received over the Tcn interface that match any of the multicast addresses associated with the broadcast TV stream
2. IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

6. VoD movie selection – IP multicast delivery

This scenario describes the message flow when a user selects a VoD movie and is delivered using IP multicast. The movie is then completed as a result of the end user either terminating the movie or the movie completes to it's end.

Pre-conditions:

- Successful bootup of the VTP and the STB.
- The STB is not already receiving a VoD movie.



[1] The end user browses the content directory and selects a VoD movie.

[2] The TV Manager within the core network authenticates the user, accepts the purchase and returns a valid URI for the movie to the STB. If conditional access is performed by the AN, then the entitlement for the selected VoD movie will be installed in the AN.

[3] The AN grants access to the specified multicast address for the customer.

[4] The STB sends a RTSP Setup message specifying the Unified Resource Indicator of the selected movie.

[5] The VTP will forward the request towards the AN.

[6] The VoD server will perform connection admission control to ensure that there is sufficient bandwidth to support the VoD Channel. If connection establishment is necessary, then this will be performed. Appropriate resources will be allocated and reserved for playing of the selected VoD movie. It will then send an RTSP Setup Reply containing the multicast group address to use for the VoD movie.

[7] The VTP will forward the request towards the home network.

[8] The STB will generate an IGMP Join specifying a copy of the received multicast group address of the selected VoD movie. The STB also generates a second IGMP in order to cover the case the first one is lost (as specified by the robustness variable in RFC2236).
In addition the STB also sends a RTSP Play request to inform the VoD server to start playing the VoD movie.

[9] The VTP determines that there is no existing member of the same multicast group and forwards the IGMP Join to the AN.

[10] As per 2.3 [8]

[11] As per 2.3 [9]

[12] The VTP will forward the request towards the AN.

[13] The VoD Server will start now playing the movie that was requested earlier using the multicast group address specified previously in the RTSP Play Reply.

[14] The VTP will forward the request towards the home network.

[15] The STB notes that the VoD movie is now being played.

[16] The VoD movie now either completes to the end or the user terminates the movie. This results in the STB issuing a RTSP Teardown request.

[17] The VTP will forward the request towards the AN.

[18] The VoD server stops playing the VoD movie, de-allocates any resources and tears down any connections that were dynamically established. It finally sends a RTSP Teardown reply.

[19] The VTP will forward the request towards the home network.

[20] The STB generates a IGMP Leave message to the VTP indicating the multicast group address that it no longer requires.

[21] Upon receipt of the “IGMP Leave” the VTP checks to see if other STB are still interested in receiving the multicast channel by sending an IGMP Group Specific Query and starting the “lastmemberquery” interval timer.

[22] The Group Specific Query is ignored by all STBs, since none of them are members of the multicast group specified within the message.

[23] The “lastmemberquery” interval timer expires and the VTP generates an IGMP Leave to the AN specifying the multicast group that has no members listed.

[24] Upon receipt of the “IGMP Leave” the Access Network stops sending the specified multicast channel stream to the VTP.

Notes;

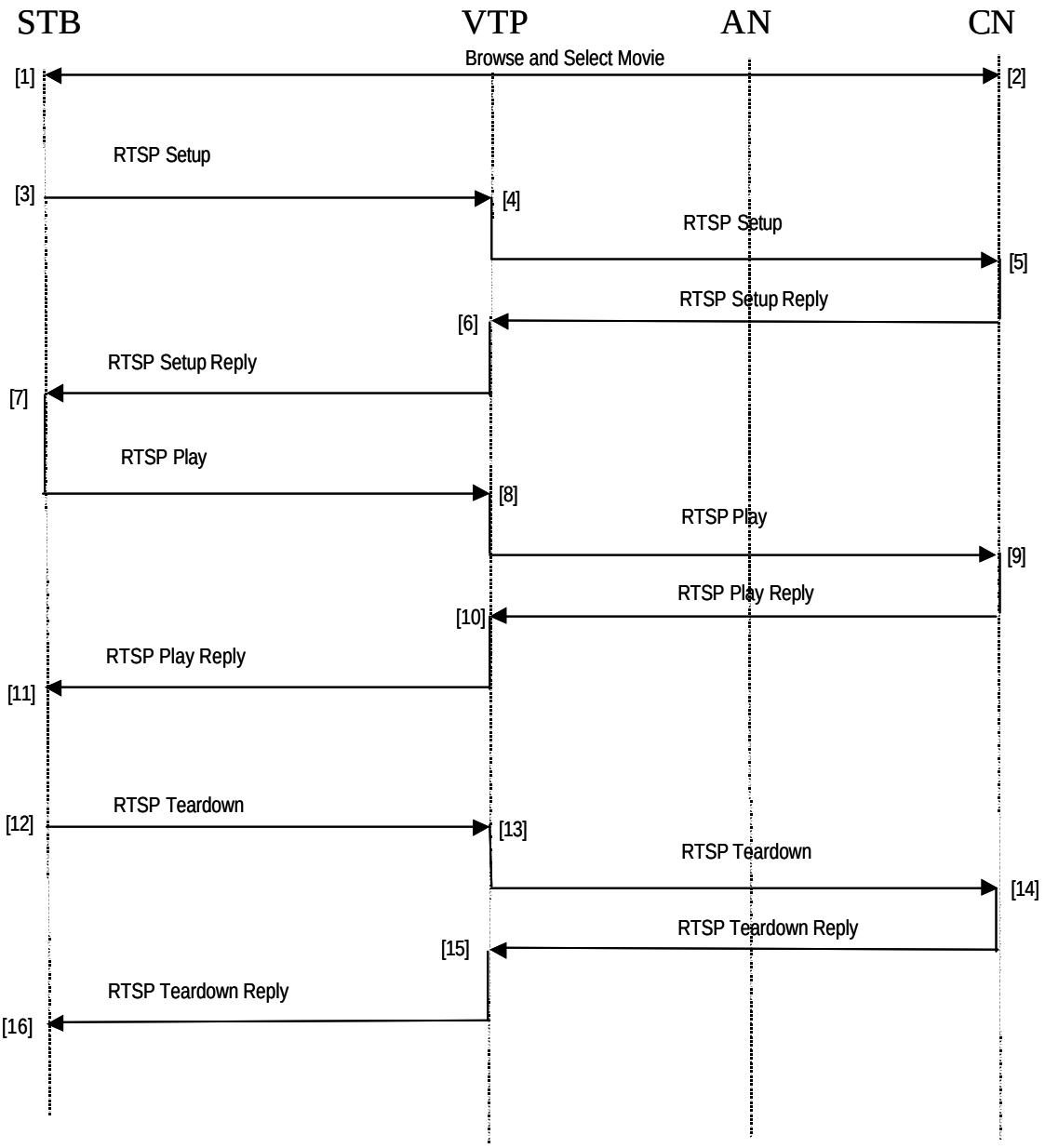
1. RTSP messages may be sent over a bridged, routed or PPPoE ATM VCs by the VTP. The choice is dependent upon the network architecture. The actual ATM VC used does not affect the overall sequence described above.
2. The AN does not intercept any of the RTSP messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.
3. The VTP filters any IGMP messages received over the Tcn interface that match any of the multicast addresses associated with the broadcast TV stream
4. IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

7. VoD movie selection – IP unicast delivery

This scenario describes the message flow when a user selects a VoD movie and it is delivered using IP unicast. The movie is then completed as a result of the end user either terminating the movie or the movie completes to it’s end.

Pre-conditions:

- Successful bootup of the VTP and the STB.
- The STB is not already receiving a VoD movie.



[1] The end user browses the content directory and selects a VoD movie.

[2] The TV Manager within the core network authenticates the user, accepts the purchase and returns a valid URI for the movie to the STB.

[3] The STB sends a RTSP Setup message specifying the Unified Resource Indicator of the selected movie.

[4] The VTP will forward the request towards the AN.

[5] The VoD server will perform connection admission control to ensure that there is sufficient bandwidth to support the VoD Channel. If connection establishment is necessary, then this will be performed. Appropriate resources will be allocated and reserved for playing of the selected VoD movie. It will then send an RTSP Setup Reply.

[6] The VTP will forward the request towards the home network.

[7] The STB send a RTSP Play request to inform the VoD server to start playing the VoD movie.

[8] The VTP will forward the request towards the AN.

[9] The VoD Server will start streaming the movie using the unicast IP address of the STB and generate a RTSP Play Reply.
The VoD movie will be streamed into the VTP using either a bridged, routed or PPPoE flow.

[10] The VTP will forward the request towards the home network.

[11] The STB notes that the VoD movie is now being streamed by the VoD Server.

[12] The VoD movie now either completes to the end or the user terminates the movie. This results in the STB issuing a RTSP Teardown request.

[13] The VTP will forward the request towards the AN.

[14] The VoD server stops streaming the VoD movie, de-allocates any resources and tears down any connections that were dynamically established. It finally sends a RTSP Teardown reply.

[15] The VTP will forward the request towards the home network.

[16] The STB notes that the VoD movie has been successfully terminated by the VoD Server.

Notes;

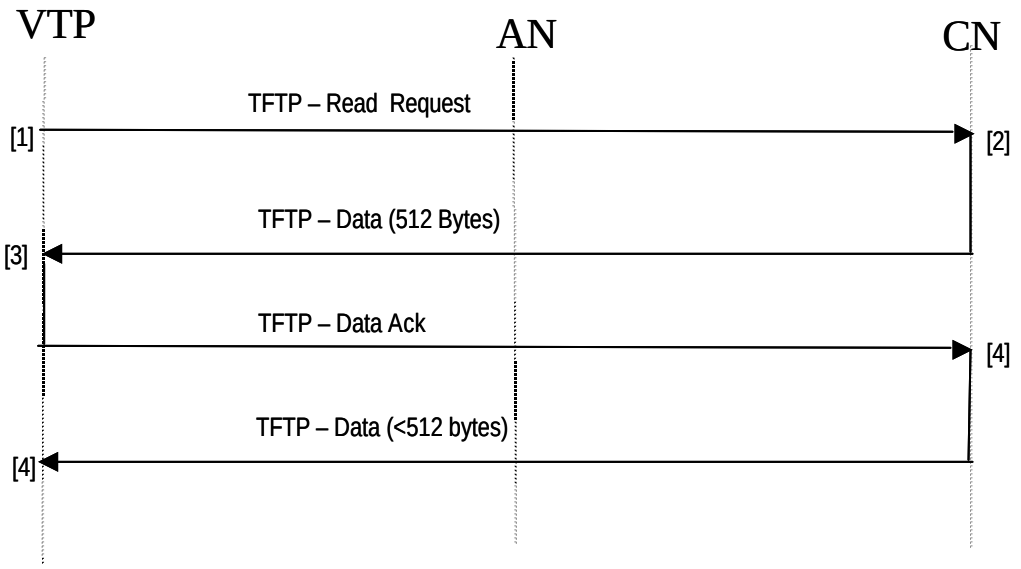
1. RTSP messages and the VoD movie strea may be sent and/or received over a bridged, routed or PPPoE ATM VCs by the VTP. The choice is dependent upon the network architecture. The actual ATM VC used does not affect the overall sequence described above.
2. The AN does not intercept the RTSP messages or the VoD movie stream, these are just transparently forwarded as a result of the AN performing ATM cell relay.

8. Remote Software Download of the VTP.

The sequence below describes the case where the software within the VTP is remotely updated. The VTP uses TFTP to retrieve a file from the core network. This action could be triggered autonomously by the VTP for example upon start up or by a remote management system.

Pre-conditions:

- Successful bootup of the VTP.
- The Remote Management Channel IP connectivity has been established.



[1] The VTP requests download of a new version of a software file. This is achieved by issuing a TFTP Read Request (RRQ).

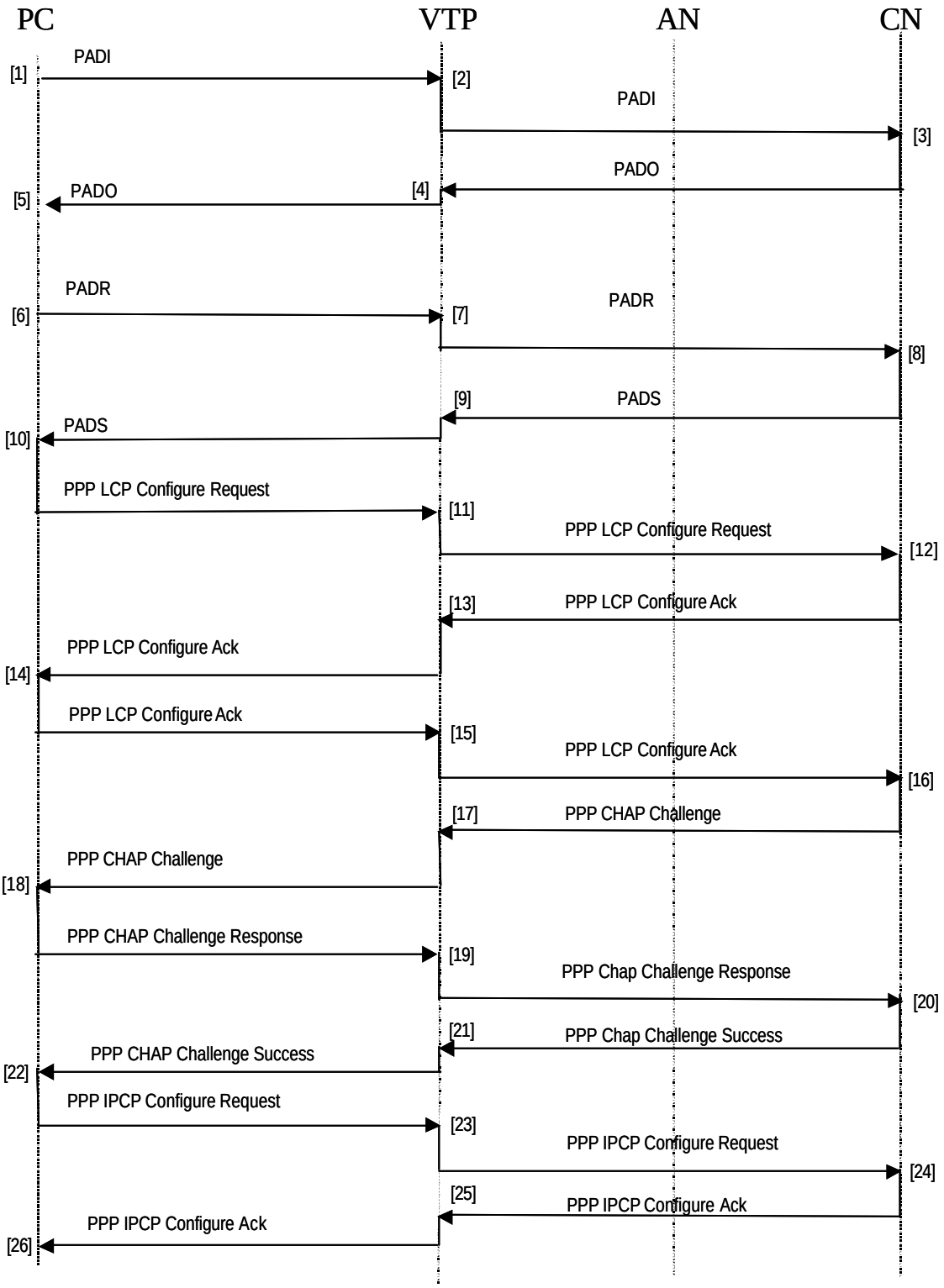
[2]	The remote management system located within the core network will acknowledge the request by sending the first 512 bytes of the file.
[3]	The VTP will acknowledge the request by sending a TFTP Data Ack packet and store the received bytes.
[4]	The remote management system located within the core network will send the final bytes of the file and since the number of bytes is <512, then this will signify the closure of the TFTP session.
[5]	The VTP will append the received bytes to those previously received and mark the end of the session. Now, the VTP ready to use the new downloaded software image.
Notes:	1. The VTP receives TFTP messages on the VC that is designated for remote management. 2. The AN does not intercept any of the TFTP messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.

9. Internet browsing using PPPoE

The sequence below describes the situation where a Personal Computer (PC) initiates a PPPoE session for connecting to the network in order to perform tasks such as web browsing and e-mail access.

Pre-conditions:

- Successful bootup of the VTP..



[1] The PC initiates a PPPoE session by sending a PADI packet with the destination ethernet address set to broadcast. The PADI packet may also contain additional information such as service name.

[2] The VTP will forward the request towards the AN.

[3] The Edge Router located within the Core Network (CN) that can serve the PADI request will respond with a PADO Packet. The PADO packet will contain the destination ethernet address of the PC as received in the PADI.

[4] The VTP will forward the request towards the home network.

[5] Since the PADI was broadcast, then it is possible to receive one or more PADO packets. Therefore the PC will run a guard timer allowing it wait for responses from other Edge Routers

the PC will run a guard timer allowing it wait for responses from other Edge Routers.

[6] Upon expiry of the guard timer the PC will choose which PADO packet to respond to. The selection criteria can be based for example the Edge Router name. The PC will generate a PADR packet containing the destination ethernet address of the selected Edge Router.

[7] The VTP forwards the request towards the AN.

[8] The Edge Router will respond with a PADS packet indicating it is prepared to begin a PPP Session. The Edge Router also allocates a unique PPPoE session identity.

[9] The VTP will forward the request towards the home network.

[10] The PC notes that the PPPoE session has been successfully established. It now initiates the PPPoE session by sending PPP LCP Configure request.

[11] The VTP will forward the request towards the AN.

[12] The Edge Router specifies the link parameters that will be used for the PPPoE session and includes these within the PPP LCP Configure Ack.

[13] The VTP will forward the request towards the home network.

[14] The PC notes the link configure parameters and sends a PPP LCP Configure Ack.

[15] The VTP forwards the request towards the AN.

[16] The Edge Router now attempts to securely authenticate the PC by sending a PPP CHAP Challenge packet.

[17] The VTP will forward the request towards the home network.

[18] The PC will encrypt the user name and password and include it within the PPP Challenge Response.

[19] The VTP will forward the request towards the AN.

[20] The Edge Router will validate the encrypted user name and password and if it is deemed to be valid, then a PPP CHAP Challenge Success will be sent.

[21] The VTP will forward the request towards the home network.

[22] The PC notes the successful authentication has occurred and now sends a PPP IPCP Configure request requesting the IP configuration parameters such as an IP address for the PC, primary and secondary DNS.

[23] The VTP will forward the request towards the AN.

[24] The Edge Router sends a PPP IPCP Configure Ack specifying the requested IP configuration parameters.

[25] The VTP will forward the request towards the home network.

[26] The PC notes the IP configuration parameters. The PPP session is now established and can be used for internet browsing.

Notes;

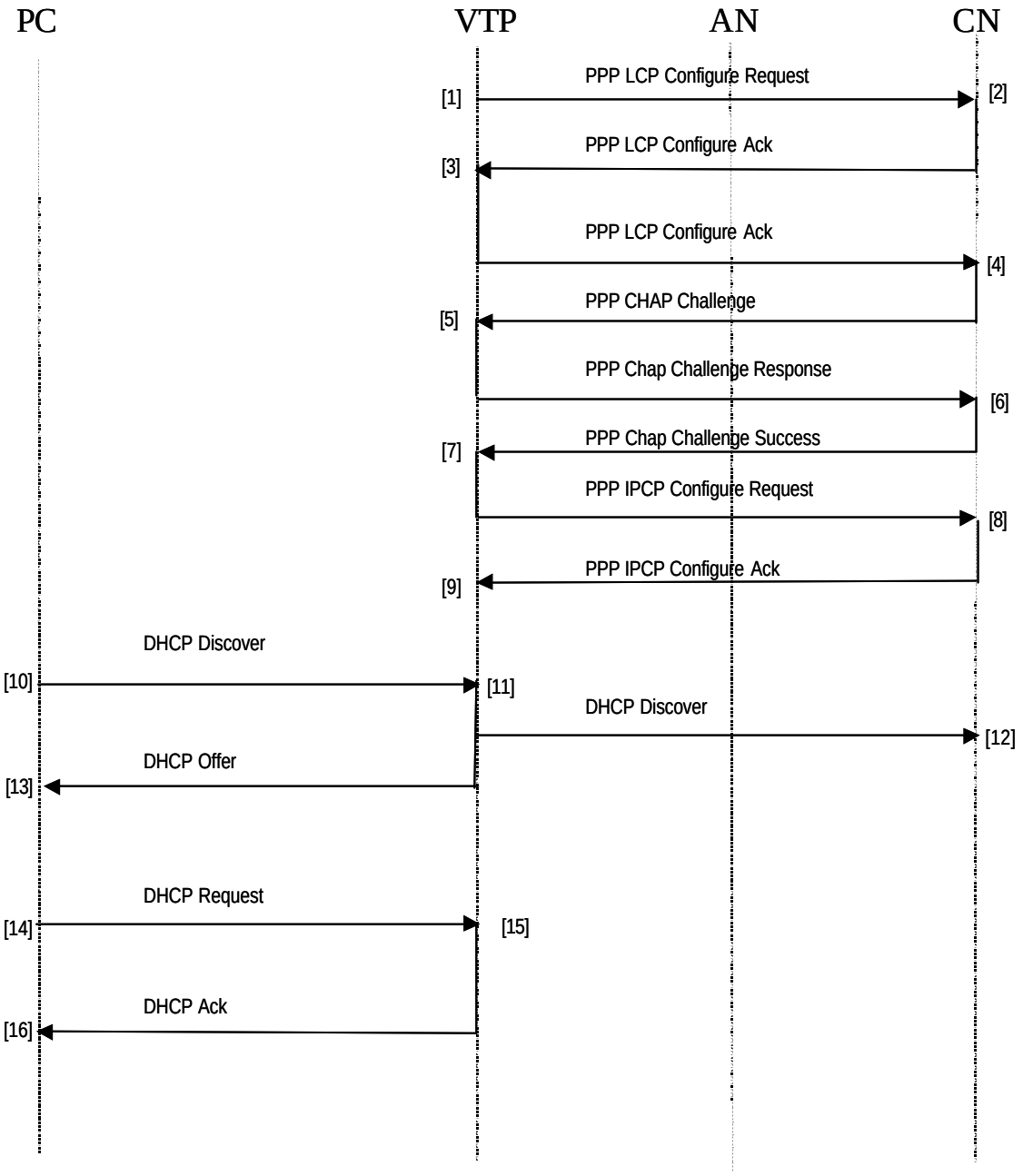
1. PPPoE messages may be filtered using the PPPoE filter and sent on an ATM VC designated solely for PPPoE. Or alternatively the PPPoE messages may be bridged and sent on a bridged ATM VC. The choice is network architecture dependent, but this choice does not affect the overall sequence described above.
2. The AN does not intercept any of the PPPoE messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.

10. Internet browsing using PPPoA

The sequence below describes the situation where the VTP initiates a PPPoA session and acts as a proxy for a Personal Computer (PC) within the home network. The DHCP server for the home network is located within the VTP/D.

Pre-conditions:

- Successful bootup of the VTP



[1] The VTP initiates a PPPoA session by sending a PPP LCP Configure request.

[2] The Edge Router which is typically a BRAS within the Core Network (CN) will specify the link parameters that will be used for the PPPoA session and includes these within the PPP LCP Configure Ack.

[3] The VTP notes the link configure parameters and sends a PPP LCP Configure Ack.

[4] The Edge Router now attempts to securely authenticate the VTP by sending a PPP CHAP Challenge packet.

[5] The VTP will encrypt the user name and password and include it within the PPP Challenge Response.

[6] The Edge Router will validate the encrypted user name and password and if it is deemed to be valid, then a PPP CHAP Challenge Success will be sent.

[7] The VTP notes the successful authentication has occurred and now sends a PPP IPCP Configure request requesting the IP protocol configuration parameters such as an IP address for the PC, primary and secondary DNS.

[8] The Edge Router sends a PPP IPCP Configure Ack specifying the requested IP configuration parameters.

[9] The VTP notes the IP configuration parameters. The PPP session is now established and can be shared by the home appliances for internet browsing etc.

shared by the home appliances for internet browsing etc.

[10] The PC issues a request to the VTP in order to request an IP address and other configuration parameters such as default gateway, primary and secondary DNS addresses. The DHCP Discover packet contains a destination IP broadcast address (255.255.255.255).

[11] The DHCP Discover broadcast packet will be processed by the DHCP server that is resident within the VTP. The DHCP server will respond with a DHCP Offer packet that includes an available IP address.

If the VTP is performing bridging as well, then the DHCP Discover broadcast packet will also be sent on the bridged ATM VCs. Otherwise no DHCP Discover packet will be sent towards the AN.

[12] The Edge Router located within the Core Network will be configured to ignore any DHCP Discovery packets that do not contain a Vendor Class Identifier attribute.

[13] The PC notes that a DHCP server has responded and runs a guard timer within which other DHCP servers may respond is the DHCP Discover packet was broadcast.

[14] The PC selects the DHCP server that has responded and this is done by sending a DHCP Request packet with a destination IP address (255.255.255.255) and the address of the target server in the "server IP address" field of the DHCP packet. The DHCP Request packet is broadcast so that non selected DHCP servers that have responded can be informed.

If the VTP is performing bridging as well, then the DHCP Request broadcast packet will also be sent on the bridged ATM VCs. Otherwise no DHCP Discover packet will be sent towards the AN.

[15] The DHCP server in the VTP recognises it's IP address in the "server IP address" field of the DHCP Request packet and responds with a DHCP Ack containing the following configuration parameters; IP address, Subnetwork Mask, Default Gateway, DNS Primary and Secondary Server addresses (assigned by PPPoA).

[16] The PC records the received parameters for the duration of the lease period. The PC is now ready to browse the internet.

All further IP packets used for internet browsing will now be processed by the VTP NAT function and sent over the NAT ATM VC.

The VTP NAT function enables multiple home appliances (e.g. Personal Computers) to have shared access to the internet, by using the IP address assigned by the PPPoA process when sending packets over the U-R2 interface.

Notes;

1. The PPP packets are sent and received over the ATM VC designated for NAT flows.
2. The AN does not intercept any of the PPPoA messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.