INTERNATIONAL TELECOMMUNICATION UNION

ITU-T H.610

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(07/2003)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband and triple-play multimedia services –
Broadband multimedia services over VDSL

Full service VDSL – System architecture and customer premises equipment

ITU-T Recommendation H.610

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
SYSTEMS AND TERMINAL EQUIPMENT FOR AUDIOVISUAL SERVICES	H.300–H.399
SUPPLEMENTARY SERVICES FOR MULTIMEDIA	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	**H.610–H.619**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation H.610

Full service VDSL – System architecture and customer premises equipment

Summary

This Recommendation specifies the system architecture (SA) and customer premises equipment (CPE) architecture for the delivery of video, data and voice services across a VDSL access network to an in-home environment, known as a Full Service VDSL network. This Recommendation specifies the SA and CPE architecture at a high level, independent of the underlying broadband physical layer transport mechanism. VDSL is referenced throughout this Recommendation as the physical layer technology; however, the architectural specifications contained herein could be equally applicable to CPE and Access Networks employing other broadband physical layer technologies.

This Recommendation defines an architecture that enables the provisioning of a bundle of triple-play services in a reliable way, with minimal user intervention, respecting the key requirements of security and conditional access to the content and at a cost compatible with mass market deployment.

Source

ITU-T Recommendation H.610 was approved on 14 July 2003 by ITU-T Study Group 16 (2001-2004) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation H.610

Full service VDSL – System architecture and customer premises equipment

1 Scope

This Recommendation specifies the system architecture (SA) and customer premises equipment (CPE) architecture for the delivery of video, data and voice services across a VDSL access network to an in-home environment, known as a Full Service VDSL network. This Recommendation specifies the SA and CPE architecture at a high level, independent of the underlying broadband physical layer transport mechanism. VDSL is referenced throughout this Recommendation as the physical layer technology; however, the architectural specifications contained herein could be equally applicable to CPE and Access Networks employing other broadband physical layer technologies.

This Recommendation defines an architecture that enables the provisioning of a bundle of triple-play services in a reliable way, with minimal user intervention, respecting the key requirements of security and conditional access to the content and at a cost compatible with mass market deployment.

This Recommendation is limited to the use of IPv4. Use of IPv6 is for further study.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

2.1 Normative references

[1] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[2] ATM Forum af-tm-0056.000 (1996), *Traffic Management 4.0*.

[3] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

[4] IEEE Standard 802.1D (1998) | ISO/IEC 15802-3:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common Specifications – Media Access Control (MAC) bridges*.

[5] ITU-T Recommendation H.611 (2003)*, Full service VDSL – Operations, Administration Maintenance & Provision aspects*.

[6] IETF RFC 2684 (1999), *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.

[7] IETF RFC 2516 (1999), *A method for transmitting PPP over Ethernet (PPPoE)*.

[8] ITU-T Recommendation I.363.5 (1996), *B-ISDN ATM Adaptation Layer specification: Type 5 AAL*.

[9] ATM Forum af-ilmi-0065.000 (1996), *ILMI Integrated Local Management Interface*.

[10] ISO/IEC 13818-6:1998, *Information technology – Generic coding of moving pictures and associated audio information – Part 6: Extensions for DSM-CC. See Chapter 10, U-N Switched Digital Broadcast – Channel Change Protocol, and Annex H (informative), Switched Digital Broadcast Service*.

[11] ATM Forum af-nm-0122.000 (1999), *Auto-configuration of PVCs*.

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

[13] ITU-T Recommendation J.82 (1996), *Transport of MPEG-2 constant bit rate television signals in B-ISDN*.

[14] IEEE Standard 802.3 (2002), *Information technology – Telecommunication and 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*.

[15] ITU-T Recommendation I.361 (1999), *B-ISDN ATM layer specification*.

[16] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.

[17] IETF RFC 2364 (1998), *PPP Over AAL5*.

[18] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

[19] IETF RFC 2453 (1998), *RIP Version 2*.

[20] IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)*.

[21] IETF RFC 1877 (1995), *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*.

[22] ETSI TR 101 290 v1.2.1 (2001), *Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems*.

[23] IETF RFC 2326 (1998), *Real Time Streaming Protocol (RTSP)*.

[24] IETF RFC 2279 (1998), *UTF-8, a transformation format of ISO 10646*.

[25] IETF RFC 2863 (2000), *The Interfaces Group MIB*.

[26] IETF RFC 2515 (1999), *Definitions of Managed Objects for ATM Management*.

[27] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.

[28] IETF RFC 3004 (2000), *The User Class Option for DHCP*.

[29] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[30] IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP)*.

[31] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.

[32] IETF RFC 1334 (1992), *PPP Authentication Protocols*.

[33] IETF RFC 1994 (1996), *PPP Challenge Handshake Authentication Protocol (CHAP)*.

2.2 Informative references

[I-1] ITU-T Recommendation FS-VDSL Focus Group Technical Specification, Part 4 (2002), *Physical layer specification for interoperable VDSL systems*.

[I-2] ITU-T Recommendation G.783 (2000), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.

[I-3] ITU-T Recommendation I.630 (1999), *ATM protection switching*.

[I-4] ITU-T H-series Recommendations – Supplement 3 (2003), *Operator requirements for full service VDSL in ITU-T Recommendations H.610 and H.611*.

[I-5] ATM Forum af-sig-0061.002 (2002), *ATM User Network Interface (UNI) Signalling Specification Version 4.1*.

[I-6] ITU-T Recommendation I.363.2 (2000), *B-ISDN ATM Adaptation Layer specification: Type 2 AAL*.

[I-7] IETF RFC 3350 (2003), *RTP: A transport protocol for real-time applications*.

[I-8] ATM Forum af-vmoa-0145.000 (2000), *Loop Emulation Service Using AAL2*.

[I-9] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[I-10] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP*.

[I-11] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

[I-12] FIPS 180-1, *Secure hash standard*.

[I-13] IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

3 Definitions

This Recommendation defines the following terms:

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

3.2 access network operator: The AN Operator operates the physical access system. Encompassing the domain between the U-R and V reference point of the system reference model (see clause 6).

3.3 content provider: The Content Provider generates content such as video copies in various digital or analogue 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.

3.4 core network operator: The Core Network Operator maintains and manages the core network beyond the V reference point and the OLT physical interface.

3.5 digital broadcast network: A multicast Network that is used to distribute point to multi-point traffic such as digital TV and radio.

3.6 Element Management System (EMS): The system allowing the AN management.

3.7 Functional Processing (FP): A point of signal transformation or processing.

3.8 Functional Processing and Decoding (FPD): A point of application layer processing of video, audio or data.

3.9 interactive A/V network: A unicast network used to deliver point-to-point video and audio services such as VoD.

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

3.11 InterWorking to Core Network (IWCN): 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, this Recommendation only covers the AN requirements up to the V reference point.

3.12 M: Reference point used between the AN and the EMS.

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

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

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

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

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

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

3.19 POTSR/ISDNR: Interface between narrowband terminals and the PS splitter at the customer premises side.

3.20 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.

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

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

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

3.24 residential centralized model: When mentioned in this Recommendation, refers to the use of the VTPD as the decoding unit.

3.25 residential distributed model: When mentioned in this Recommendation, refers to the use of multiple FPDs that are connected to the VTP through the residential LAN.

3.26 residential network: Digital network used in an in-home environment for delivering FS-VDSL services.

3.27 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.

3.28 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.

3.29 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.

3.30 $\mathbf{T_{CN}}$: The output (input) of the digital port(s) of the VTP/D toward (from) the digital Network at the customer premises.

3.31 terminal: A physical entity hosting an FPD, e.g., set-top box (STB), PC, IP phone.

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

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

3.34 **U-R**: The network side of the PS located at the customer premises.

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

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

3.37 **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.

3.38 **VDSL Termination Processing (VTP)**: 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 residential network.

3.39 **VTP and Decoding (VTPD)**: Refers to a unit that operates the video decoding function as well as the VTP functions and interfaces. From the point of view of the access network, the functionalities and interfaces of the VTPD are identical to a VTP.

3.40 **VTP/D**: When mentioned in this Recommendation, refers to both the VTP and the VTPD.

3.41 **VTU-C**: VDSL Termination Unit. VDSL transmission unit at the ONU.

4 Abbreviations

This Recommendation uses the following abbreviations:

A/V	Audio/Video
AAL	ATM Adaptation Layer
AIS	Alarm Indication Signal
AN	Access Network
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BAS	Broadband Access Server
BER	Bit Error Ratio
BLES	Broadband Loop Emulation Service
BPID	Broadcast Program ID
CA	Conditional Access
CAC	Call Admission Control
CBR	Constant Bit Rate
CC	Continuity Check
CCF MIM	Channel Change Function Management Information Model
CDV	Cell Delay Variation
CHAP	Challenge Handshake Authentication Protocol
CMIP	Common Management Information Protocol
CO	Central Office

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
DVB	Digital Video Broadcasting
DVD	Digital Versatile Disc
EAS	Emergency Alert System
EMS	Element Management System
EPD	Early packet Discard
ER	Edge Router
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FPD	Functional processing and Decoding
FSAN	Full Service Access Network
FS-VDSL	Full Service VDSL
FTP	File Transfer Protocol
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
HW	Hardware
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPCP	Internet Protocol Control Protocol
ISDN	Integrated Services Digital Network
IWCN	InterWorking to Core Network
LAN	Local Area Network
LCP	Link Control Protocol

LT	Line Termination
MAC	Medium Access Control
MCM	Multi-Carrier Modulation
MIB	Management Information Base
MPEG	Moving Picture Experts Group
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NSP	Network Service Provider
NT	Network Termination
OAM	Operation and Management
ODN	Optical Distribution Network
OLT	Optical Line Termination
ONU	Optical Network Unit
OSI	Open Systems Interconnection
OTU-C	Optical Terminal Unit – Central Office side
OTU-R	Optical Terminal Unit – Remote side
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBX	Private Branch Exchange
PCR	Peak Cell Rate
POTS	Plain Old Telephone Service
PPD	Partial Packet Discard
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
PS	POTS or ISDN Splitter
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
QoS	Quality of Service
RDI	Remote Defect Indication
RFC	Request for Comment (IETF standard)
RIP	Routing Information Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SAR	Segmentation And Reassembly
SCM	Single Carrier Modulation

SCSI	Small Computer System Interface
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPTS	Single Program Transport Stream
STB	Set Top Box
SVC	Switched Virtual Circuit
SW	Software
TDM	Time Division Multiplexing
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TM	Transmission and Multiplexing (ETSI Technical Committee)
UBR	Unspecified Bit Rate
UPC	Usage Parameter Control
USB	Universal Serial Bus
UTOPIA	Universal Test and Operational PHY Interface for ATM
VBR	Variable Bit Rate
VBR-nRT	Variable Bit Rate non-real time
VBR-RT	Variable Bit Rate 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 or VTPD
VTPD	VDSL Termination Processing and Decoding
VTPD	VTP and Decoding
VTU-C	VDSL Terminal Unit – Central Office
VTU-R	VDSL Terminal Unit – Remote

5 Terminology

The following words are used throughout this Recommendation to signify requirement levels.

"SHALL" This word or the adjective "required," means that the definition is an absolute requirement of this Recommendation.

"SHALL NOT" This phrase means that the definition is an absolute prohibition of this Recommendation.

"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, shall be interoperable with another implementation that does include the option.

6 Reference model

The aim of the reference model in Figure 1 is to clearly define the interfaces and reference points that are used in an FS-VDSL environment.

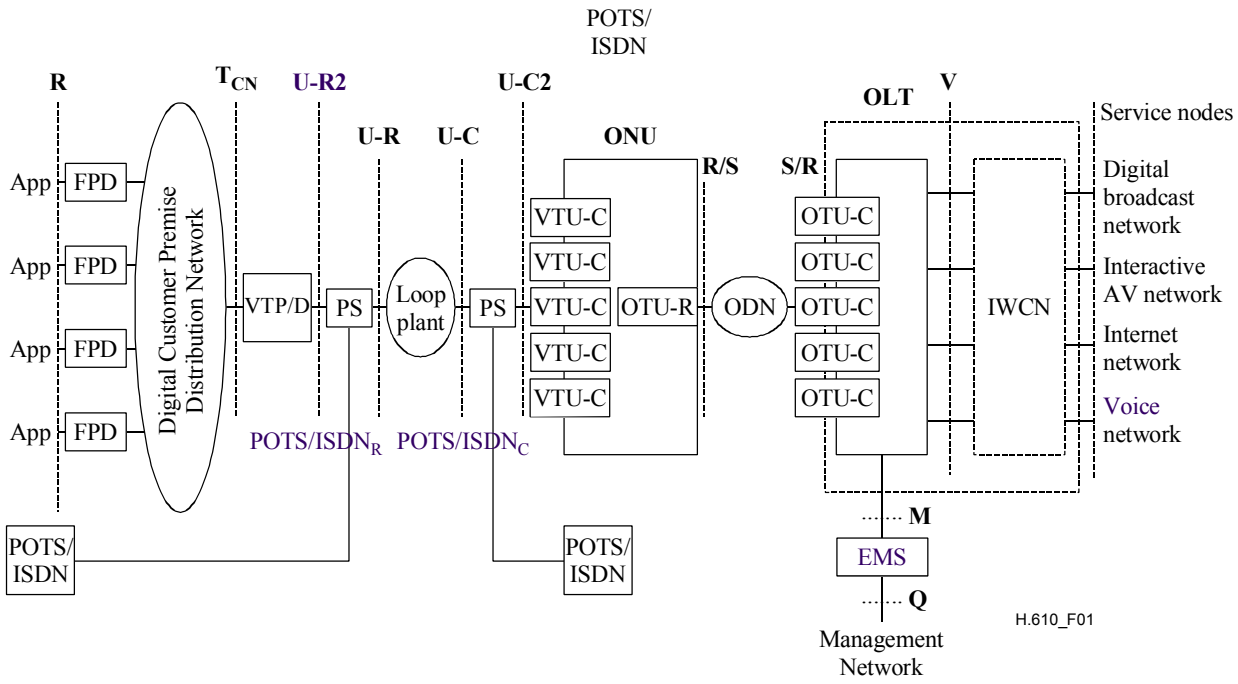


Figure 1/H.610 – FS-VDSL reference model

6.1 Residential architectures

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

- ***Distributed*** refers to an architecture in which several FPD elements are interconnected together as shown in Figure 2. These elements contain functional processors and possibly the residential appliance itself. The VTP element contains the VDSL modem, together with a protocol and functional processor.

- ***Centralized*** refers to an architecture in which most if not all processing and decoding is performed within the same physical box termed VTPD as shown in Figure 3. Internal to this box, functional processing and digital signal distribution through busses is also taking place.

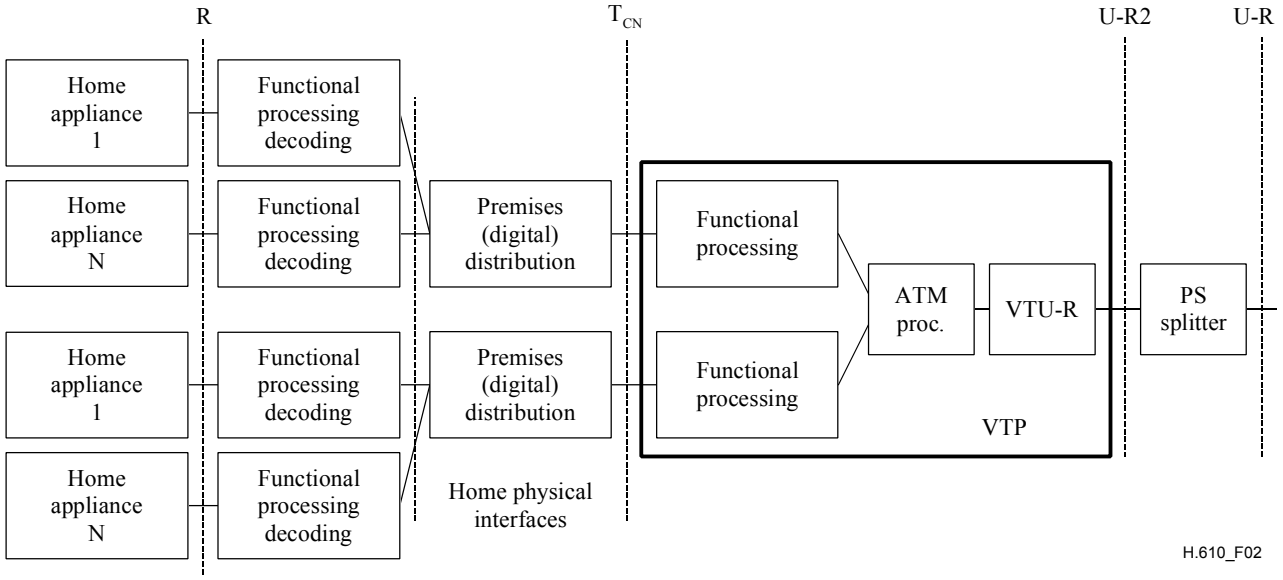


Figure 2/H.610 – VTP grouping which implements a fully distributed CPE approach

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

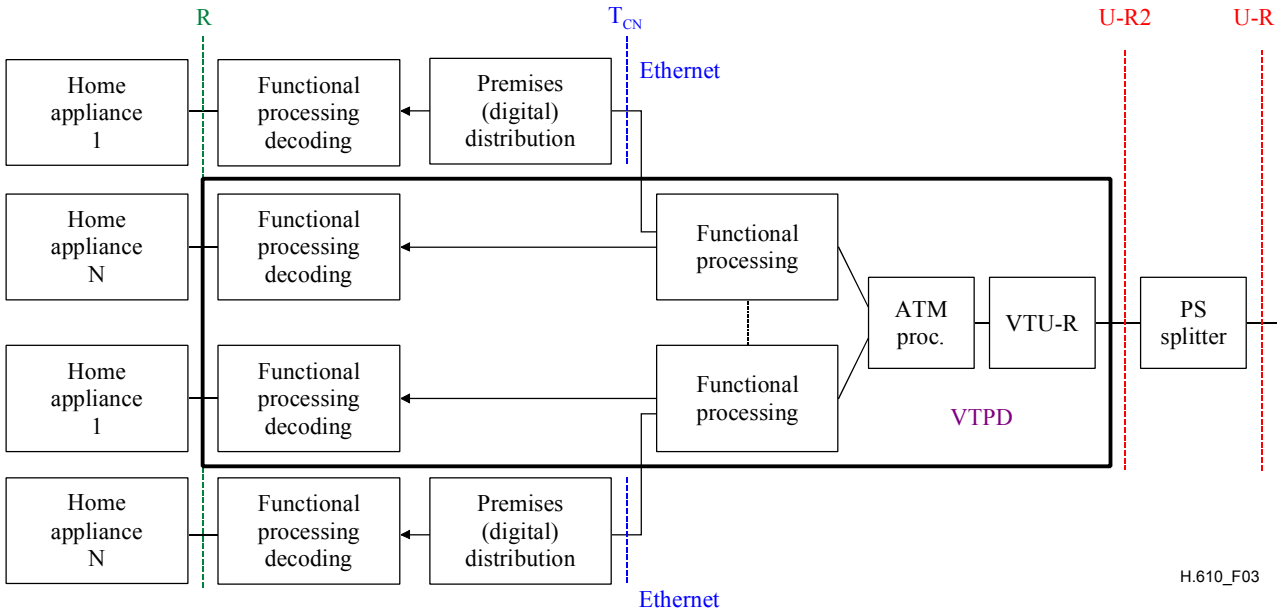


Figure 3/H.610 – VTPD grouping which implements a centralized CPE approach with optional distributed FPs

6.2 Focal reference points

The relevant architecture reference points are described in Table 1.

Table 1/H.610 – Focal reference points

Reference point	Location
T_{CN}	The output (input) of the digital port(s) of the VTP/D towards (from) the digital network at the customer premises
U-R2	The network side input of the DSL Modem
V	The reference point located between the ATM-based AN and any IWCN function connecting the AN to a Core Network
M	The interface between the OLT and the EMS

6.2.1 T_{CN} reference point

The T_{CN} shall present to the VTP/D's protocol processing modules an 802.3 frame as defined in IEEE 802.3 with the Type/Length field specifying the MAC client protocol type. This, however, does not imply that the residential network shall use the 802.3 MAC layer or an Ethernet physical layer. Different types of MAC and physical layers may be used. Where the term 'Ethernet' is used in this Recommendation, within the context of a layer in a protocol stack, it refers to the 802.3 frame format as defined above.

6.2.2 U-R2 reference point

At the U-R2 interface, the VTP/D protocol layers shall be as follows:

- The physical layer shall be a standard DSL layer transporting ATM.
- The ATM layer shall be implemented in accordance to subclause 8.3.
- The upper layers implementation shall comply with clause 9.

6.2.3 V reference point

This reference point is located between the ATM-based AN and any IWCN function connecting the AN to a Core Network.

This reference point shall provide an ATM layer in accordance to ITU-T Rec. I.361.

6.2.4 M reference point

This logical interface enables the OLT to be remotely managed by the EMS, as specified in ITU-T Rec. H.611.

7 General overview

This clause describes the general architecture of an FS-VDSL network and is provided for information. No mandatory requirements are defined in this clause. The architecture is designed for providing the infrastructure for delivering data (typically Internet access), video (broadcast and on demand) and voice services, as further detailed in ITU-T Supplement 3 to H-series Recommendations.

7.1 Access network architecture

7.1.1 Access network overview

This Recommendation is designed for DSL based AN. The physical layer may be VDSL, ADSL or any other existing or future DSL technology that fulfils the service requirements. The choice of a DSL type for a specific implementation derives from the specific service bundle, e.g., the offered services and the required bit rate.

The AN may be composed of several equipments, depending on the network topology. For example, the CO equipment may or may not include the DSL line cards and the physical links

between the AN components may be point-to-point or point-to-multipoint. It is also possible to have a combination of the two schemes in the same network. Figure 4 illustrates these basic configuration options for the AN.

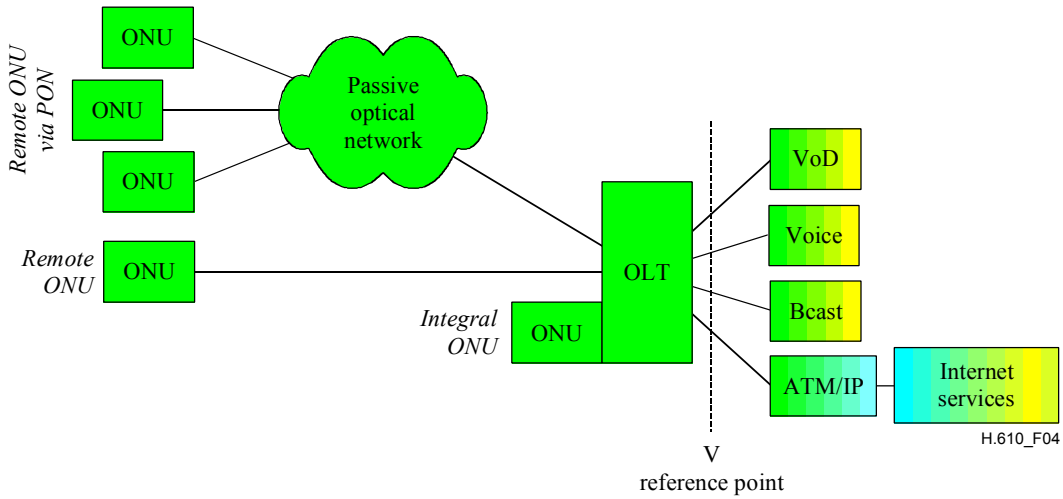


Figure 4/H.610 – Access network topology options

7.1.2 OLT

The OLT operates as an aggregator for a number of ONUs. In the upstream direction, the OLT aggregates the ATM traffic coming from the ONUs towards the V reference point; while in the downstream direction, it performs the opposite, de-multiplexing 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 are present in the unified physical box.

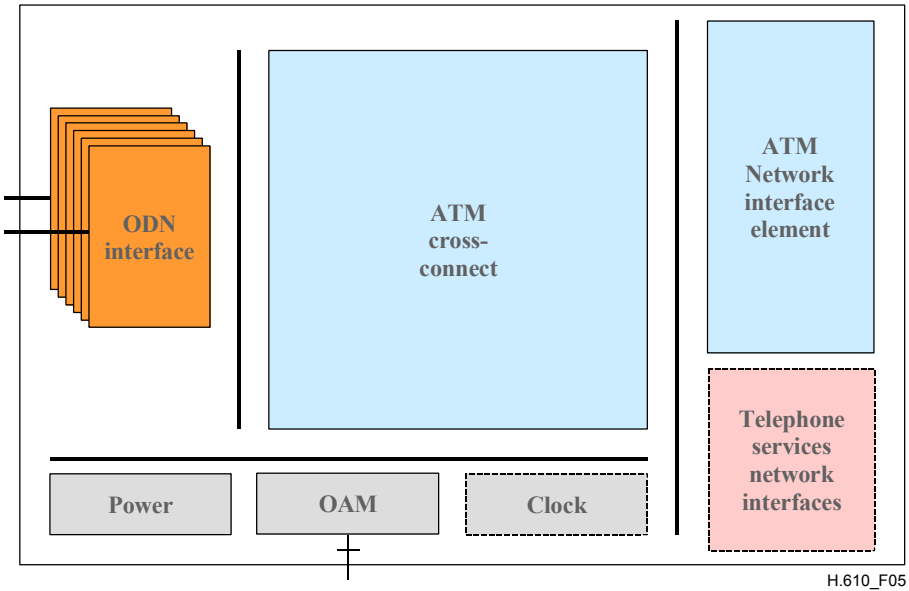


Figure 5/H.610 – OLT functional blocks

7.1.2.1 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 non-ATM core networks are deployed, the network interface

element performs the protocol conversion between ATM and the core network technology. Multiple Network Interface Elements, supporting unidirectional or bidirectional ATM transmission, may exist in a single OLT.

7.1.2.2 Telephone service network interfaces

The OLT may contain a Telephone Interface Element enabling the OLT to interface the voice network by performing the required protocol adaptations. The Telephone Interface Element may support TDM, ATM or IP voice transports and the associated signalling.

7.1.2.3 ATM cross-connect

This block performs VP/VC cross-connection to and from the appropriate interfaces. Besides an ATM layer, this block should provide higher layer protocol functions like channel change processing, access control and management.

7.1.2.4 Optical Distribution Network interface (ODN)

The block performs the ATM and PHY layer functions of the OLT's interface connecting the OLT to the ONUs through the ODN. The physical layer technology may conform to various optical transmission standards or may be vendor specific.

7.1.2.5 OAM block

The OAM block provides operation, administration and management of the AN via the M interface.

7.1.2.6 Power block

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

7.1.2.7 Clock block

Depending on the implementation of other blocks, an external clock interface may be implemented.

7.1.3 ONU

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

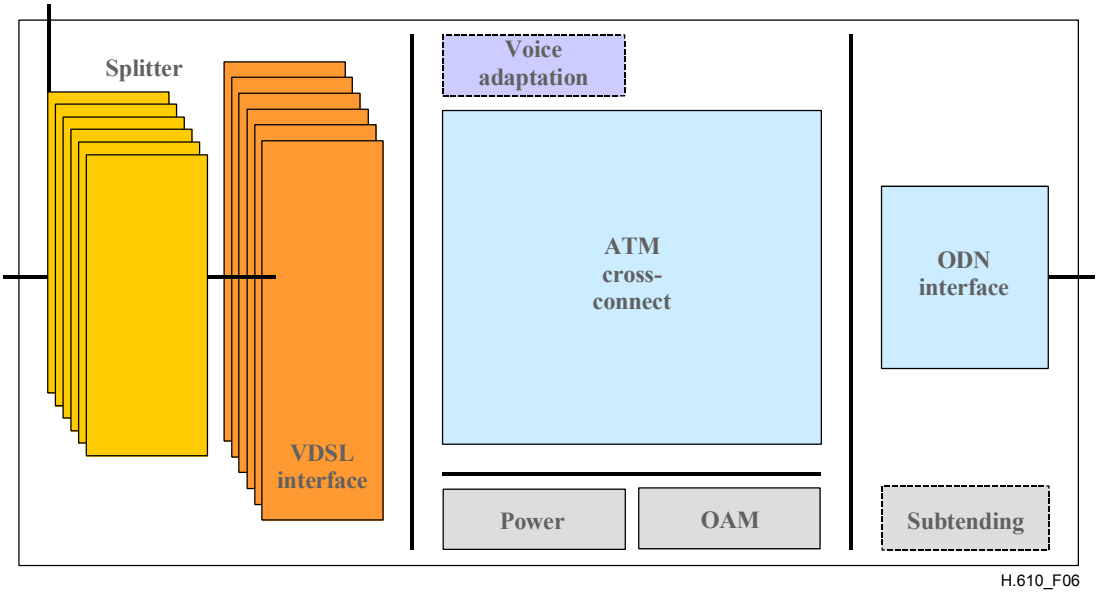


Figure 6/H.610 – ONU functional blocks

7.1.3.1 ODN interface

This block performs the ATM and PHY layer functions on the interface connecting the ONU to the OLT through the ODN.

7.1.3.2 Voice adaptation

The ONU may contain a voice adaptation element that performs mapping of base-band voice signals to voice over packet, voice over ATM or voice over IP.

7.1.3.3 ATM cross-connect

This block performs VP/VC cross-connection to and from the appropriate interfaces. This block may perform higher layer protocol functions like channel change processing.

7.1.3.4 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.

7.1.3.5 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.

7.1.3.6 OAM block

The OAM block enables operation, administration and management of the ONU, including the DSL drops. OAM tasks are performed using an in-band ATM connection.

7.1.3.7 Power block

The power block supplies the appropriate voltage and current to all the electronic circuits of the ONU. As the ONU may be installed in an outdoor facility, the power block may supply power to both cooling fans and to battery backup circuitry. In addition, if in existence, the ONU Power Block may provide power for environmental sensors or external alarm circuits.

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

7.1.3.8 Subtending

The ONU may include a subtending block connecting additional secondary ONUs.

7.2 Core network architecture

In different deployment cases, the AN may be connected to the service nodes using core networks of different topologies and technologies. The core network is used to flexibly interconnect the AN to various Service Nodes. The core network provides the following capabilities:

- Sufficient bandwidth capacity to support the traffic between the AN and the Service Nodes.
- Support for the appropriate QoS for the various services.
- Routing/Switching of traffic between the AN 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.

The following subclauses describe possible deployment scenarios.

7.2.1 ATM core network scenario

In many network deployments the service nodes are located in a centralized location, e.g., a network operation centre, and therefore, a core network is needed to connect the OLT to the service nodes. As the OLT functions as 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 reference point and the core network. This scenario is illustrated in Figure 7.

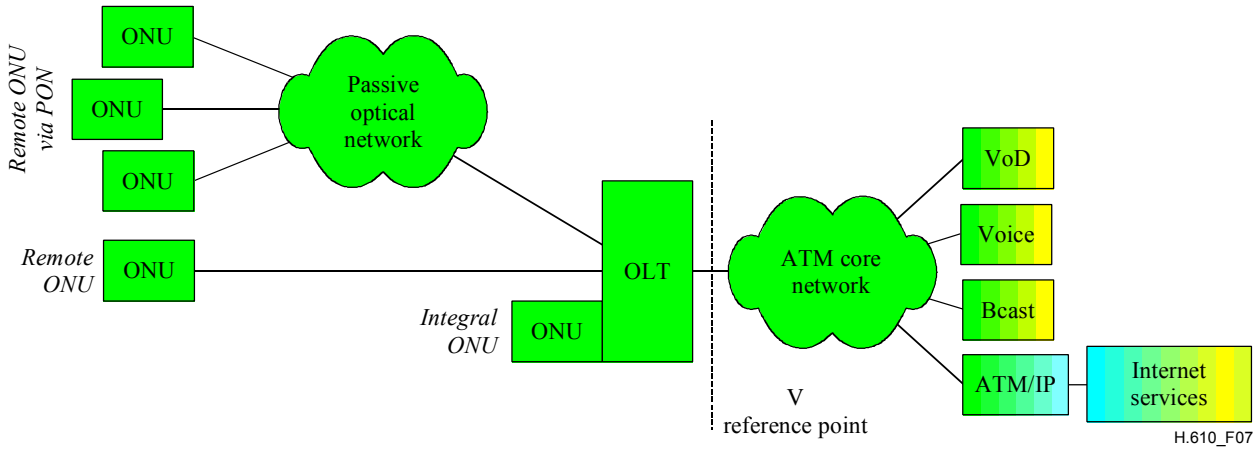
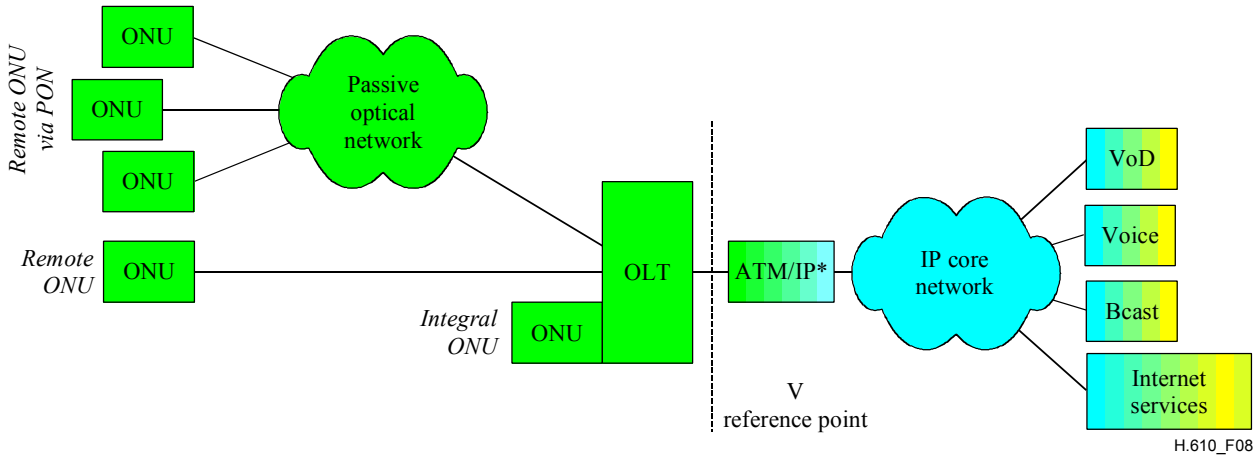


Figure 7/H.610 – ATM core network

7.2.2 IP core network scenario

This Recommendation details IP-based architecture for each one of the required FS-VDSL services, for some a native ATM solution is also specified. This means that although the AN is ATM based, the protocols used by the endpoints (i.e., service nodes and residential equipment) for service delivery are from the IP suite. This implies that in many deployment cases the traffic crossing the V reference point is 100% IP PDUs. It is therefore possible to terminate the ATM layer at the V reference point and to connect the OLTs to the service nodes using an IP network. This scenario is illustrated in Figure 8.



* A local ATM/IP service node may be implemented in the same equipment as the OLT.

Figure 8/H.610 – IP core network

This scenario introduces some technical challenges, mostly concerned with maintaining coherent QoS characteristics within the two networks.

7.2.3 Other core network scenario

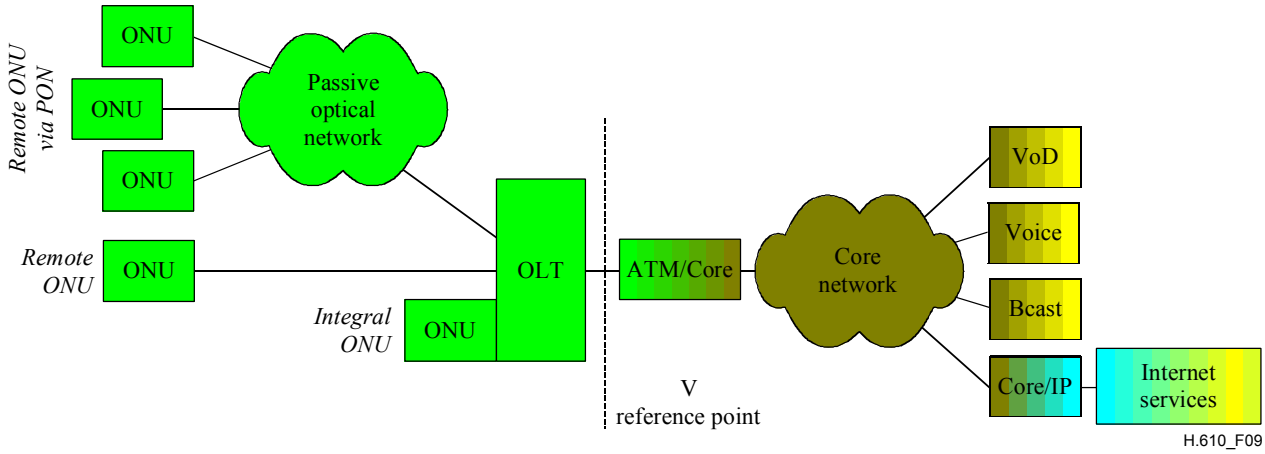
This Recommendation does not limit the core network technology only to ATM or IP. Other network protocols/technologies are possible such as SONET/SDH, Ethernet and MPLS. As the OLT is an ATM device, interworking is required between the OLT and the core network. There are three general ways that the interworking function can work.

Encapsulate and multiplex one or more of the ATM VCs at the V reference point 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 original VC characteristics are met.

Emulate the ATM VC with the transport entity of the network. In this case, the core network will be a layer-2 network like ATM. This emulation must be done in such a way that all the original VC connection characteristics 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 Figure 9. It is assumed that the service node will contain sufficient functionality to terminate the core network protocol as well as the service protocol stack.

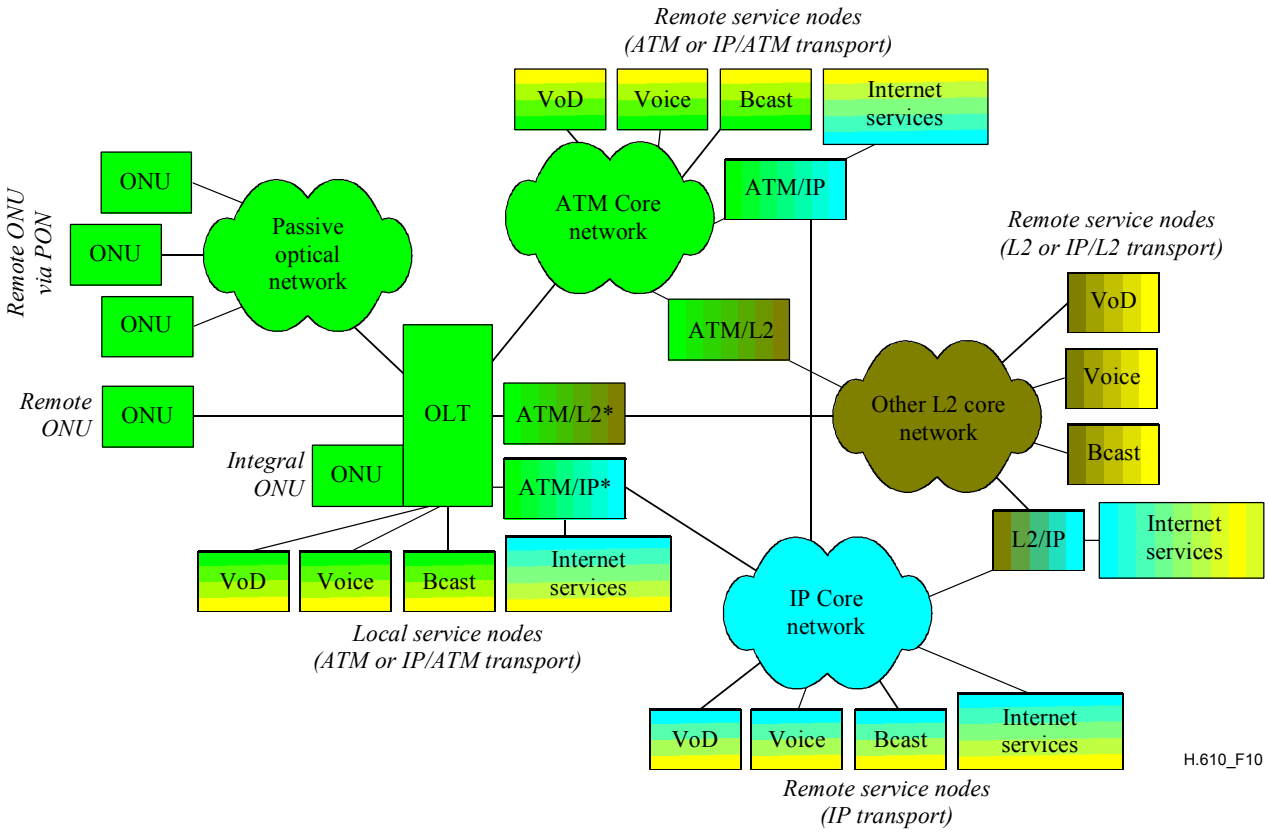


* A local ATM/Core service node may be implemented in the same equipment as the OLT.

Figure 9/H.610 – Optional core network

7.2.4 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 Figure 10.



* 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 10/H.610 – Hybrid core network

7.3 Residential environment

The following types of functionality may be present in an FS-VDSL customer premises environment:

- A service splitter electrically separates the DSL signals from other low frequency services (such as POTS or ISDN). The PS is shown in Figure 1 between the UR and U-R2 interfaces.
- A customer premises VDSL modem, VTU-R (see [1]). The VTU-R function is contained in a VTP or VTPD.
- Protocol processing and in-home distribution interfaces. This is contained by the VTP function.
- MPEG Decoding units for viewing broadcast video and VoD. This is covered by the VTPD and FPD functions.
- PCs and other customer premises IP devices connected to IP data services. These are covered by the FP and FPD functions.
- Analogue or digital voice devices that connect to VoATM or VoIP services. These are also covered by the FPD functions.
- Home appliances, such as TV sets, that are the final destination of the processed and decoded audio/video information. Examples of the interface between the FPD and home appliance are given in Table 2.

Table 2/H.610 – Example interfaces between home appliance and FPD

Coaxial Cable (RF modulated composite video)
S-Video
Composite Video
Component Video
SCART
Dolby Digital/AC-3
L/R Stereo
Telephone line
Ethernet
USB
IEEE 1394
5-channel analogue audio
SCSI
LPDT parallel
RS-232 serial
Bluetooth
IR Emitter (for control of IR controlled devices)
IEEE 802.11b
HomeRF

As reflected in the above list, the FP category covers very diverse functions. An example of FP and FPD functions is given in Table 3.

Table 3/H.610 – Example functional processing

MPEG-1 or 2 video decoding
MPEG-4 video decoding
H.323 Video
MPEG audio/MP3decoding
Dolby Digital (AC-3/AAC)
Decryption and De-scrambling
Conditional Access processing
Rights Management processing
Application processing
Middleware
IP Data processing
Remote Control and Management
RF
IR
64 kbit/s PCM for derived voice services

7.4 Service nodes

Figure 11 proposes schematic description of the Service Nodes in an FS-VDSL system.

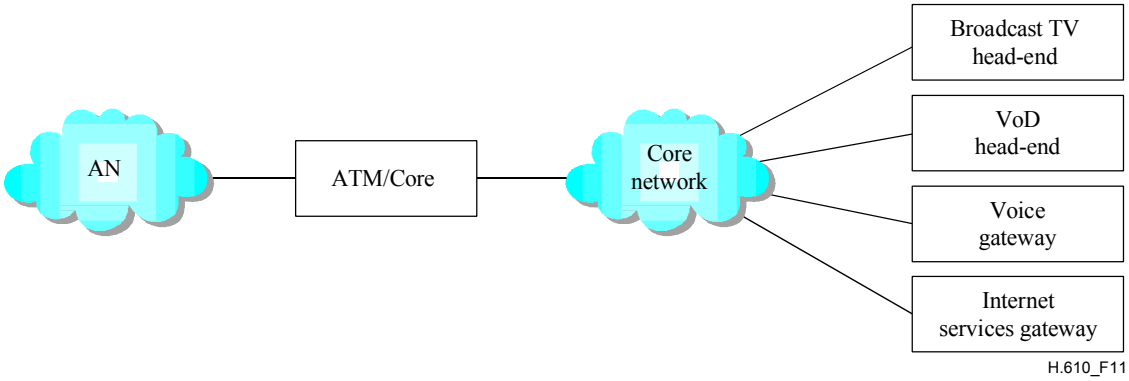


Figure 11/H.610 – FS-VDSL service nodes

7.4.1 Broadcast TV Head-end

The Head-end system receives video streams in various formats, reformats and encapsulates the video streams, interfaces the core network and transmits the video signal over the core network towards the access network. This Recommendation does not aim to specify any restriction on the video acquisition mechanism applied by the Head-end system.

7.4.2 VoD Head-end

The VoD Head-end is comprised of multiple elements, which may include:

- Back office management including asset management, subscriber management, session management and digital rights management (DRM).
- A "server farm" containing the digital content.
- Transport and access network facilities that can insure QoS.
- Compelling server application software in support of the VoD service.

7.4.3 Voice gateway

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

The main functions of the gateway include:

- Termination of the TDM voice circuits to interface the PSTN/ISDN.
- Termination of the PSTN/ISDN signalling.
- Call and bearer control.
- AAL 2 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 signalling termination.
- Connectivity to the PSTN/ISDN via an open interface.

- V5.2 support for ETSI and GR-303 support for ANSI.

7.5 IP engineering

In order to facilitate multiple services through multiple service operators to specific subscribers, several IP addressing schemes may need to coexist simultaneously at the subscriber residential Network. Network Operators and/or Service Operators must provide guidelines to ensure consistency of all IP addressing schemes. This includes ensuring that all subnetworks that could be simultaneously accessed by a specific VTP/D do not have conflicting IP address ranges.

The following constraints dictate the IP engineering scheme, which could be 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, such as point-to-point gaming and voice over IP, either public address space or private address space may be used.
- The customer is likely to make multiple logical connections to multiple networks within the residential network environment.
- A service or network provider supplying residential equipment, such as STB and Internet appliances, will need to be able to communicate with those devices. This may be for upgrade purposes, reconfiguration or initialization.

Figure 12 illustrates the addressing schemes considered:

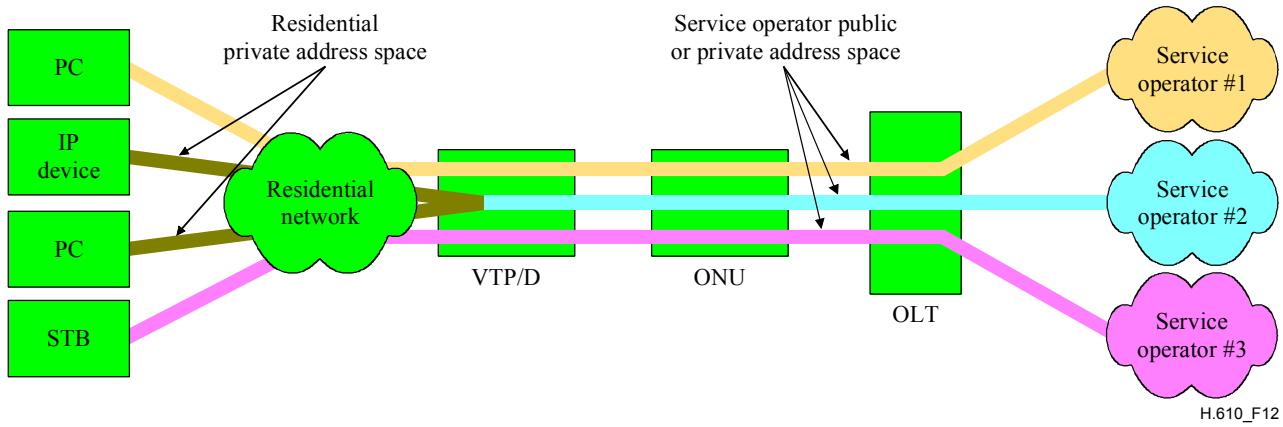


Figure 12/H.610 – Network addressing schemes

There may be up to four simultaneous distinct IP addressing schemes:

- VTP/D T_{CN} addressing scheme.
- VTP/D U-R2 addressing scheme.
- Terminal session based service operator addressing scheme.
- Terminal non-session based service operator addressing scheme.

7.5.1 VTP/D T_{CN} addressing scheme

In this scheme the VTP/D allocates designated terminals a private IP address through its DHCP IETF RFC 2131 server. Optionally, this scheme can be implemented by static IP configuration. However, the use of static IP configuration in this scheme is not recommended.

7.5.2 VTP/D U-R2 addressing scheme

In this scheme, the service operator implements the below methods to assign the VTP/D with an IP address. Multiple IP addresses may be simultaneously assigned to a single VTP/D by different Service Operators for distinct IP interfaces. In such case, the routing function of the VTP/D must manage the correct forwarding of IP packets to the appropriate IP interface:

- Session based – The VTP/D initiates a PPP session with the service operator edge router.
- Non-session based – The VTP/D obtains an IP address from the Service Operator's DHCP/BOOTP server.
- Static configuration – Static configuration is possible but is not recommended.

7.5.3 Terminal session based 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 simultaneously to connect to the same or to different service operator(s).

7.5.4 Terminal non-session based service operator addressing scheme

In this scheme, the service operator assigns IP addresses to the residential terminals using one of the following methods.

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

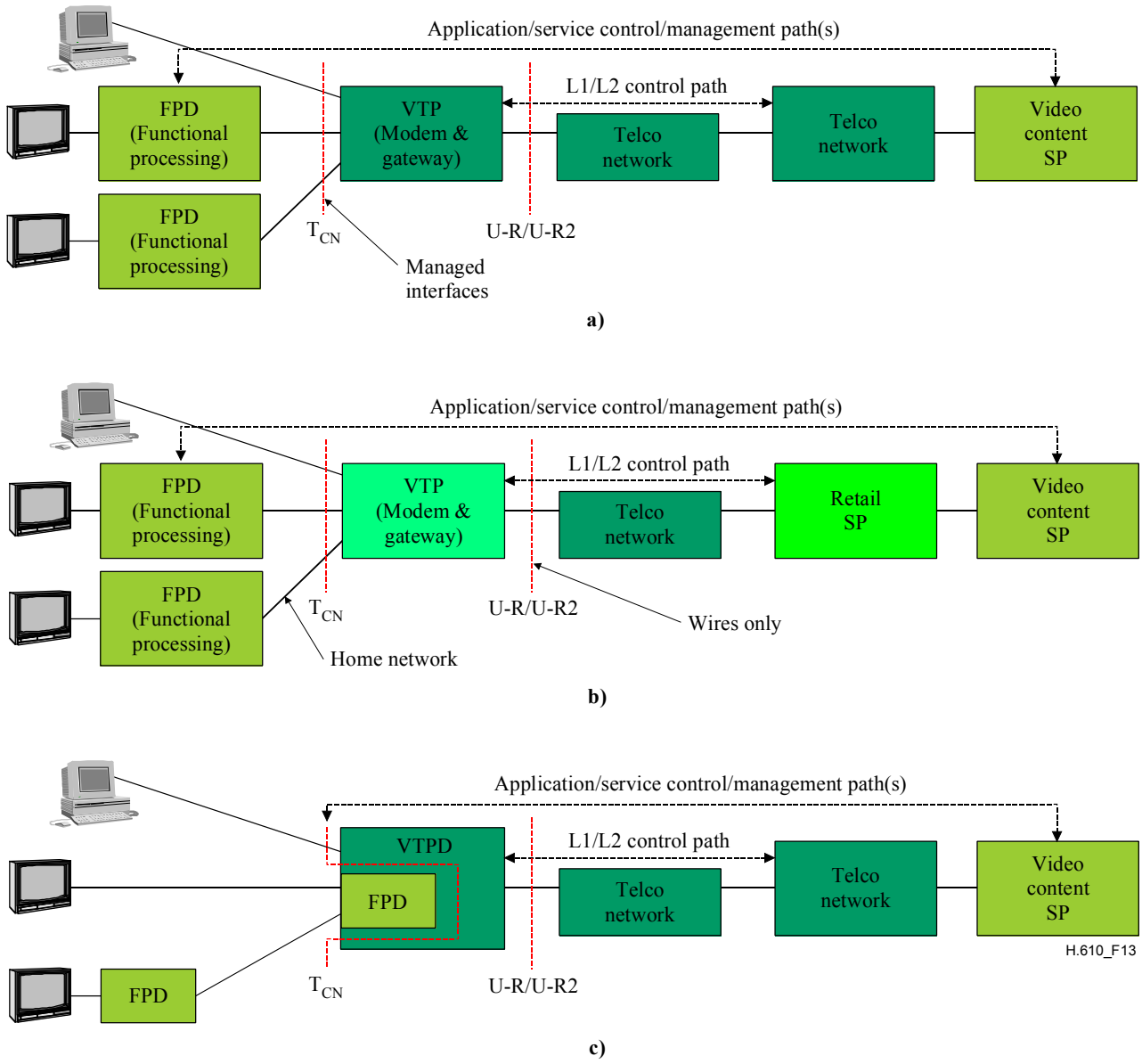
Multiple residential terminals can use this scheme simultaneously to connect to the same or to different service operator(s).

7.5.5 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 some constraints on the residential network side and on the Service Operator side to guarantee the addressing scheme integrity. This issue is further detailed in 10.3.4.

7.6 Demarcation points

Some providers may include the equipment providing the residential CPE as part of their service offering. This is illustrated in parts a) and c) in Figure 13. Alternatively, network providers may provide a service at the U-R or U-R2 differentiation point and, therefore, the VTP or VTPD functions are provided by the service providers. The VTP case is shown in part b) in Figure 13. Interface U-R2 includes the cabling from the splitter U-R interface up to the VTP connector. Control by the provider for QoS and Management may extend to the T_{CN} interface or even to the R interface, depending on the implementation. The residential service delivery control extends through the FPD. The demarcation points may vary based on network operator and regulatory requirements.



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

Figure 13/H.610 – Reference model showing business solutions

8 ATM requirements

The following subclause describes the OLT, ONU and VTP/D ATM functional requirements.

The DSL physical layer shall support ATM transport.

8.1 Access network

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

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

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

– The AN shall be able to act as an ATM OAM endpoint, as described in ITU-T Rec. I.610 [1], for VC and VP connections (i.e., F5 and F4, respectively) that terminate on it.

– The AN shall be able to act as an OAM segment point for the VC or VP connections that are cross-connected through it.
– The AN shall support ATM point-to-multipoint connections by which the broadcast TV streams are replicated according to the channel change function.
– The AN shall support traffic policing (i.e., UPC) of user connections as described in the ATM Forum Traffic Management Specification Version 4.0 [2].
– The AN shall support the following ATM Service Categories: CBR, VBR-RT, VBR-nRT, UBR as defined in ATM Forum Specification af-tm-0056.000 [2].
– The AN shall support frame based discard (i.e., EPD, PPD) on a per connection basis designated for AAL 5 traffic.
– The AN may support Switched Virtual Connections (SVCs).
– If the AN supports SVCs, it shall support ATM User Network Interface (UNI) signalling ATM Forum Specification af-sig-0061.002 [I-5].

8.1.1 OAM F4 and F5 support

The following requirements apply to the OAM implementation as specified in ITU-T Rec. I.610 [1]. 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 shall respond to OAM loop-backs.
– The AN shall generate defect indication messages (i.e., AIS, RDI).
– The AN should report detected defect indication messages to the OAM blocks.
– The AN should be function as a continuity check (CC) sink point.

8.2 OLT

The OLT should support shaping of VP connections towards the Network (i.e., at the V reference point).

8.2.1 F4 and F5 support

The following requirements apply to the OAM implementation as specified in ITU-T Rec. I.610 [1]:

• 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 loop-back cells (LB) towards the Access Network.

8.3 VTP/D

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

– The VTP/D shall support ATM adaptation layer 5 (as per ITU-T Rec. I.363.5 [8]) and ATM segmentation and reassembly (SAR) function.
– A VTP/D that supports voice over ATM (VoATM) service shall support ATM adaptation layer 2 (as per ITU-T Rec. I.363.2 [I-6]) for that purpose.
– A VTP/D shall support the termination of permanent virtual path connections (PVPs).
– A VTP/D shall support the termination of permanent virtual circuit connections (PVCs).
– A VTP/D may support switched virtual circuit connections (SVCs).
– A VTP/D supporting SVCs shall comply with ATM Forum Specification af-sig-0061.002 [I-5].

– A VTP/D shall support at least the CBR, VBR-nRT and UBR traffic types as defined in [2]. The VTP/D shall be able to shape these traffic types in the upstream (i.e., network) direction. The VTP/D shall support a UBR service with a specified PCR.
– A VTP/D shall support priority based queuing and scheduling of ATM cells in the upstream direction.
– A VTP/D shall support packet-based discard of AAL 5 PDUs, namely it shall not transmit to the network incomplete AAL 5 frames.

8.3.1 OAM F4 and F5 support

The following requirements apply to the OAM implementation as specified in ITU-T Rec. I.610 [1]:

– A VTP/D shall support ATM OAM flows of the F4 and F5 levels.
– A VTP/D shall support end-to-end ATM OAM.
– A VTP/D shall support ATM OAM loop-back function.
– A VTP/D shall support ATM OAM defect indications, AIS and RDI.
– A VTP/D should support ATM OAM continuity check (CC) sink function. Activation and deactivation may be performed by sending an activation/deactivation cell or by remote management (i.e., TMN).
– A VTP/D may support ATM OAM performance monitoring (PM) backward reporting (BR) function.
– A VTP/D should be able to receive AIS cells over point-to-multipoint connections. In such a case, the VTP/D will enter a defect state as specified for a point-to-point connection (except for the transmission of cells).

9 Connections and service flows

Different services may require different connection characteristics. In the following, an ATM connection type is determined by the higher layer protocol processing that is associated with it at the endpoints. A full service network shall simultaneously support the following connection types, as defined in the subclauses below:

• Bridge connection (subclause 9.1).
• PPPoE connection (subclause 9.2).
• Translated routed connection (subclause 9.3).
• Non-translated routed connection (subclause 9.4).
• Channel change connection (subclause 9.5).
• Digital broadcast connection (subclause 9.6).
• VTP/D remote management connection (subclause 9.7).
• BLES connection (subclause 9.8).

These connections are initiated at the VTP/D and may extend to the V reference point. The traffic that is transmitted and received by the endpoints on a specific connection type is named respectively a *flow*, for example the Bridge flow, the PPPoE flow and so on. While the first 4 connection types in the above list are generic in the sense that they can be used to transport a wide range of services, the last 3 connection types are dedicated for a specific function or service.

9.1 Bridge connection

This connection type supports the bridging of Ethernet frames between the residential network and a service node. Multiple bridge connections may be initiated on a single VTP/D, so that different services may simultaneously use different connections. Every instantiation is identified as a **Bridge**

Connection. The Network shall have the capability to support multiple bridge connections per DSL line. The bidirectional flow of PDUs received and transmitted on the Bridge connection is identified as the **bridging flow**.

The two bridge points shall ensure security by explicitly preventing VC-to-VC forwarding. The Ethernet encapsulation at the V reference point and U-R2 interface shall be in accordance with RFC 2684 bridge mode using LLC/SNAP without FCS as described in IETF RFC 2684.

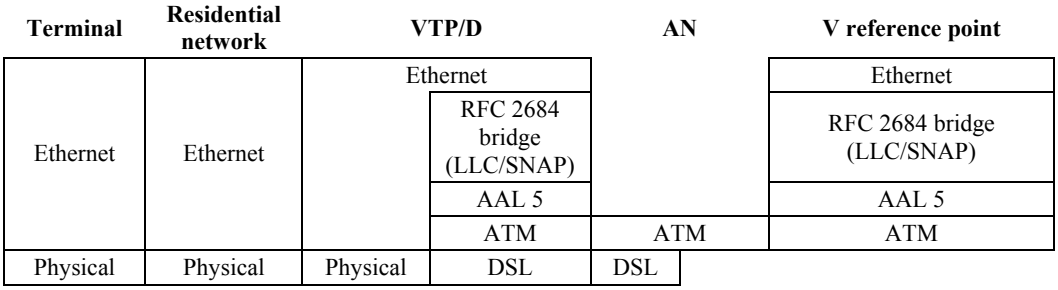


Figure 14/H.610 – Bridge connection protocol stack

9.2 PPPoE connection

This connection type supports the transport PPPoE traffic between designated residential terminals and a service node. Multiple PPPoE sessions may be established onto the same ATM VC. The bidirectional 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 shall be in accordance with IETF RFC 2516 [7]. The Network shall have the capability to support one PPPoE connection per DSL line.

The encapsulation at the U-R2 and V reference point of the PPPoE connection shall be in accordance with RFC 2684 bridge mode using LLC/SNAP without FCS. Figure 15 depicts the end-to-end protocol processing associated with a PPPoE connection.

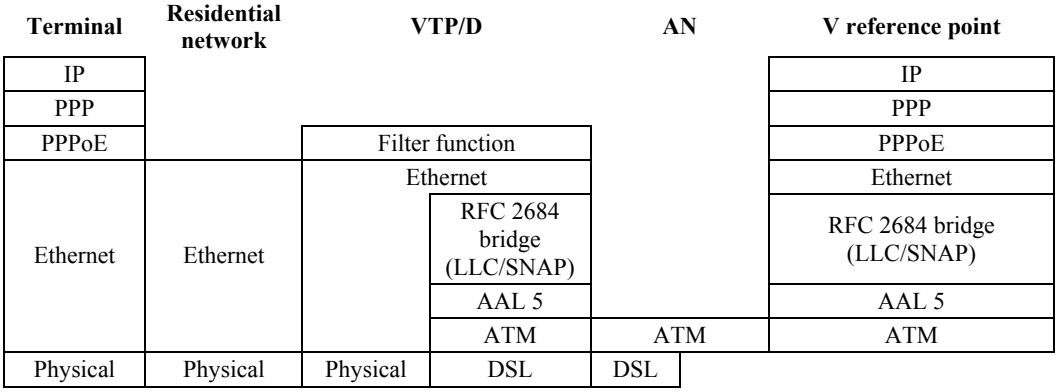


Figure 15/H.610 – PPPoE connection protocol stack

9.3 Translated routed connection

This connection type allows sharing of a single IP address for accessing the public Network by multiple end devices. It supports a routed connection between the VTP/D and a service node. The IP addresses of the residential terminals are mapped using a NAT (network address translation IETF RFC 3022 [16]) function to the VTP IP address assigned by the service operator. 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 shall have the capability to support one translated routed connection per DSL line.

Both the VTP/D and the service node terminating the ATM VC shall support PPP as defined in RFC 1661. PPP transport can be done using PPPoA in accordance with RFC 2364 [17] using the VC-multiplexing encapsulation option or PPPoE in accordance with RFC 2516 using RFC 2684 bridge mode using LLC/SNAP without FCS.

The bidirectional flow of PDUs received and transmitted on the translated routed connection is identified as the translated routed flow. Figures 16 and 17 depict the end-to-end protocol processing associated with a translated routed connection.

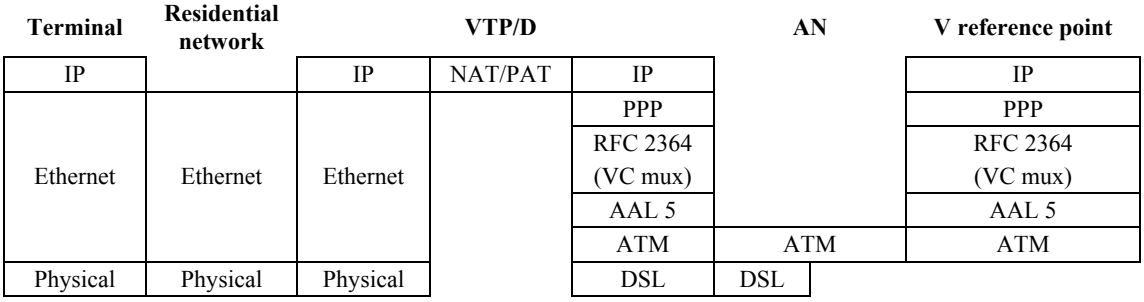


Figure 16/H.610 – Translated routed connection protocol stack with PPPoA

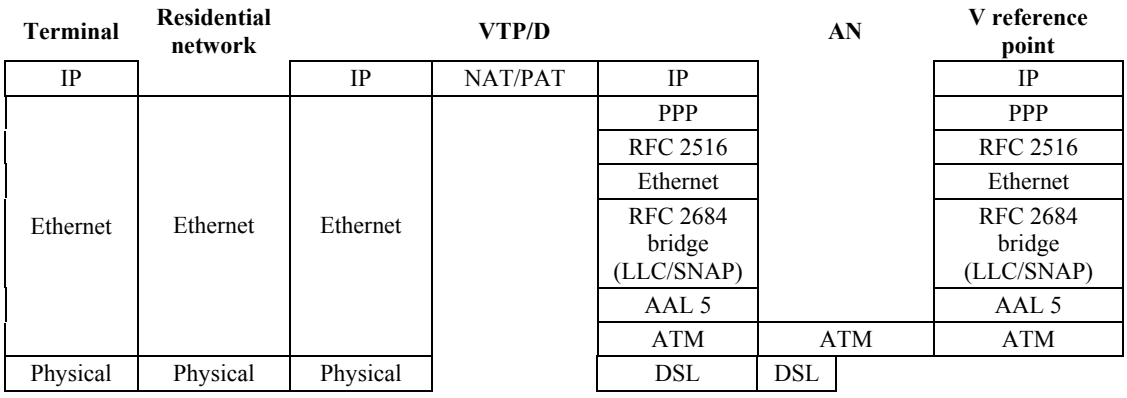


Figure 17/H.610 – Translated routed connection protocol stack with PPPoE

9.4 Non-translated routed connection

This connection type supports a routed connection between the VTP/D and a service node. Every connection is identified as a **Non-translated Routed Connection**. The Network shall support multiple such connections per DSL line. The bidirectional flow of PDUs received and transmitted on this connection is identified as the **non-translated routed flow**.

Several types of non-translated routed connections are possible. These are identified according to their IP encapsulation: IP over ATM, PPPoA or PPPoE.

9.4.1 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 shall support RFC 2684 routed mode using LLC/SNAP. Unlike all other types of non-translated routed connection, this encapsulation method does not

support inherent user authentication. Figure 18 depicts the end-to-end protocol processing associated with an IP over ATM route connection.

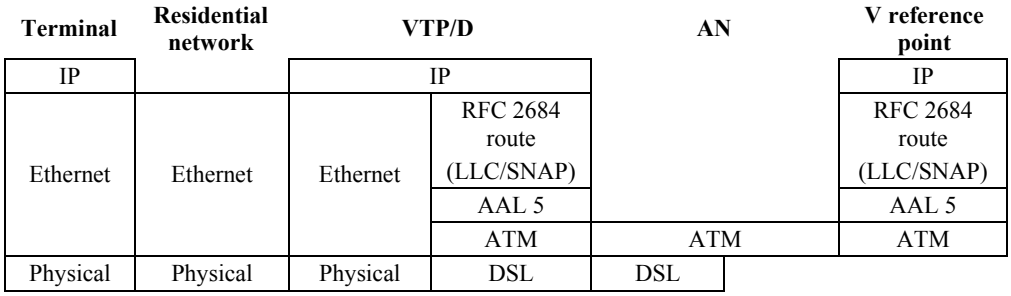


Figure 18/H.610 – IP over ATM connection

9.4.2 Non-translated routed PPPoA

This connection type supports the routing of data traffic to and from residential terminals into a PPP connection established between the VTP/D and the service node.

In order to support this type of connection, both the VTP/D and the service node terminating the ATM VC shall support PPPoA, in accordance with RFC 2364 using VC-multiplexing encapsulation option. Figure 19 depicts the end-to-end protocol processing associated with a non-translated routed PPPoA connection.

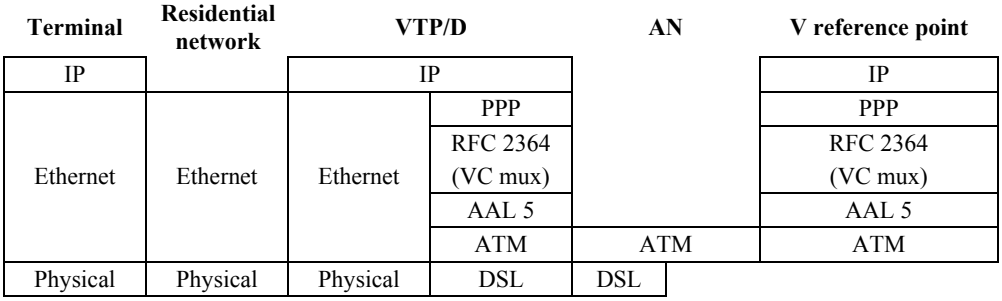


Figure 19/H.610 – Non-translated routed PPPoA connection protocol stack

9.4.3 Non-translated routed PPPoE

This connection type supports the routing of data traffic to and from residential terminals into a PPPoE connection established between the VTP/D and the service node.

In order to support this type of connection, both the VTP/D and the service node terminating the ATM VC shall support PPPoE, in accordance with RFC 2516 using LLC/SNAP encapsulation option without FCS. Figure 20 depicts the end-to-end protocol processing associated with a non-translated routed PPPoE connection.

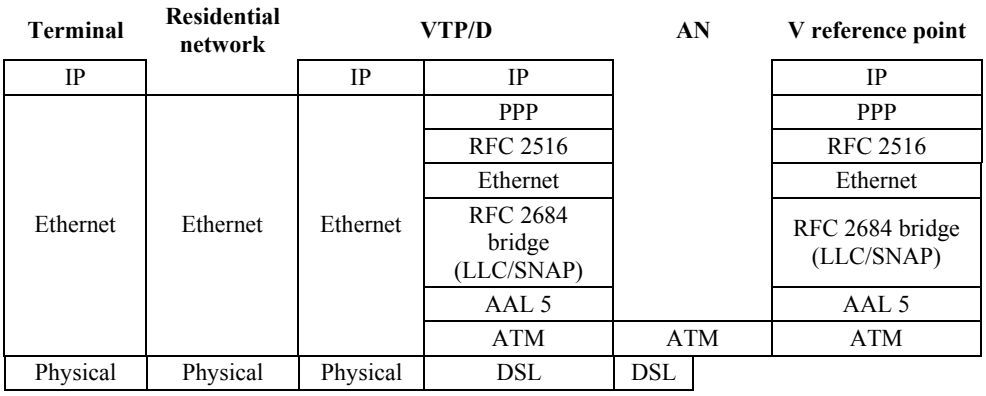


Figure 20/H.610 – Non-translated routed PPPoE connection protocol stack

9.5 Channel change connection

This connection type supports channel change messaging between the VTP/D and the access network. On this connection, channel change messages shall be IGMPv2 RFC 2236 [18] or DSM-CC ISO/IEC 13818-6 [10].

A channel change connection shall use a dedicated ATM VC between the VTP/D and the access Network. The bidirectional flow of PDUs received and transmitted on this connection is identified as the **channel change flow**.

The Network shall support one channel change connection per DSL line.

9.5.1 Use of IGMPv2

In the case that IGMPv2 is used, the encapsulation of the channel change Connection shall be in accordance with RFC 2684 routed mode using LLC/SNAP. Figure 21 describes the end-to-end protocol processing associated with an IGMP based channel change connection.

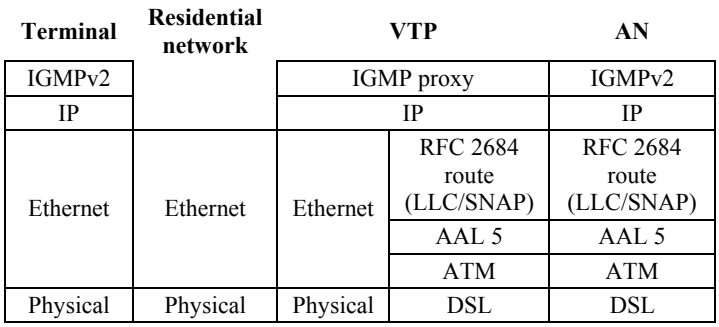


Figure 21/H.610 – IGMP end-to-end protocol stack

9.5.2 Use of DSM-CC

Figure 22 depicts end-to-end protocol processing associated with a DSM-CC based channel change connection. Note that the figure describes an IGMP to DSM-CC translation performed at the VTP. DSM-CC is encapsulated directly over AAL 5 (i.e., VC multiplexing).

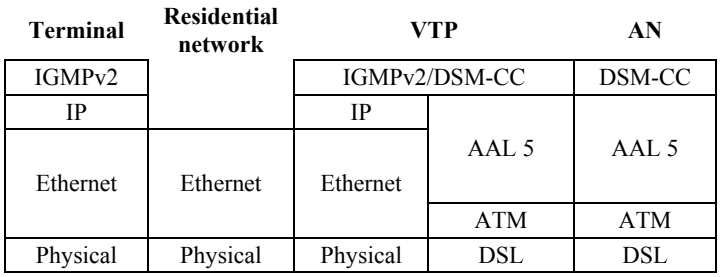


Figure 22/H.610 – IGMP to DSM-CC protocol stack

9.6 Digital broadcast connection

This connection type supports unidirectional distribution of digital broadcast information. It is implemented as a point-to-multipoint leaf VC link, which can be dynamically connected to a point-to-multipoint root in the access network. The Network shall have the capability to support multiple such connections per DSL line. The unidirectional flow of PDUs received on this connection is identified as the **digital broadcast flow**. Two methods of digital broadcast delivery are possible, MPEG-2 over AAL 5 and MPEG-2 over UDP/IP/Ethernet over AAL 5. In both cases, the network maps a single MPEG-2 SPTS to a single point-to-multipoint ATM connection.

9.6.1 MPEG over UDP/IP/Ethernet over AAL 5

In this method, MPEG-2 TS shall be encapsulated in UDP, IP and Ethernet and carried over AAL 5 using LLC/SNAP header without FCS, as per RFC 2684. Figure 23 depicts the associated end-to-end protocol processing. Note that in case of a VTPD only the three rightmost columns described in Figure 23 are applicable (the IP and upper layers shown in the Terminal column are processed in the VTPD).

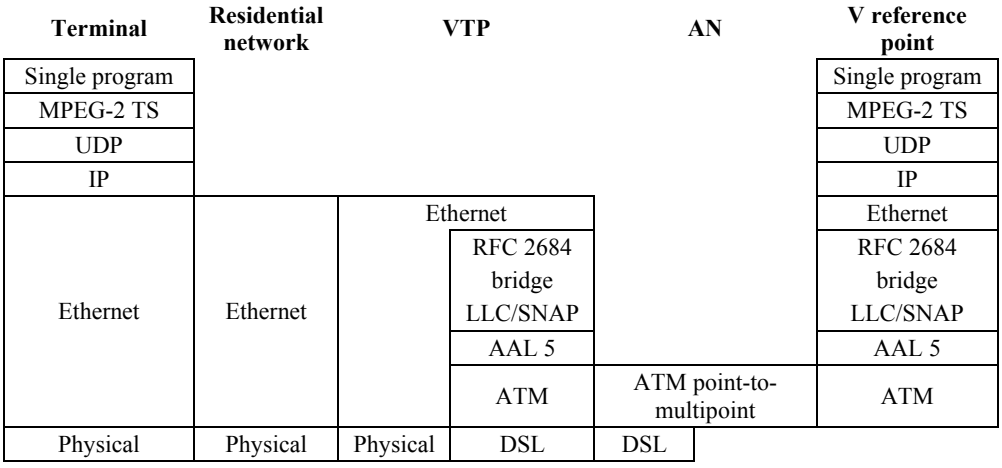


Figure 23/H.610 – MPEG-2 over UDP/IP/Ethernet over AAL 5

9.6.2 MPEG-2 over AAL 5

In this method, MPEG-2 TS shall be carried directly over AAL5 conforming to clause 8/J.82 [13]. Figure 24 depicts the associated end-to-end protocol processing. Note that in case of a VTPD only the three rightmost columns described in Figure 24 are applicable (the MPEG-2 TS and upper layers shown in the Terminal column are processed in the VTPD).

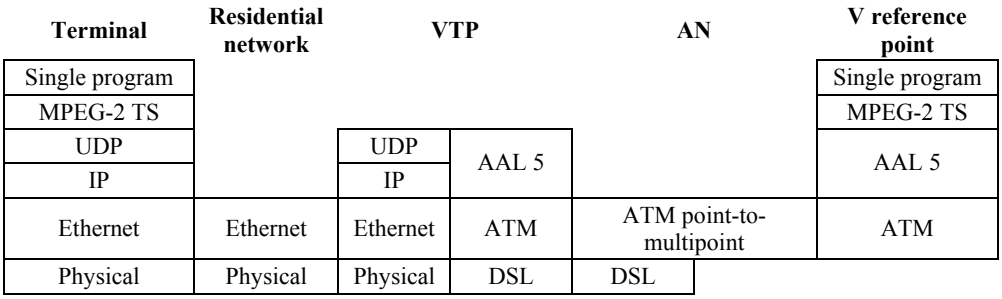


Figure 24/H.610 – MPEG-2 over AAL 5

9.6.3 Future IP-based delivery methods

The AN and VTP shall be transparent to the payload of the IP PDUs received over the digital broadcast connection. This enables future use of other IP-based delivery methods, like RTP IETF RFC 3350 [I-7] and MPEG-4, by upgrading only the endpoints (i.e., the encoder and decoder).

9.7 VTP/D remote management connection

This connection type supports bidirectional traffic flow between the VTP/D and management agents in the network. It is used for the remote management and configuration of the VTP/D. The Network shall have the capability to support one remote VTP/D management connection per DSL line.

The bidirectional flow of PDUs received and transmitted on this connection is identified as the **VTP/D remote management flow**. Figure 25 depicts the end-to-end protocol processing associated with the VTP/D remote management connection.

The VTP/D shall use DHCP IETF RFC 2131 [3] to dynamically retrieve IP configuration for this connection.

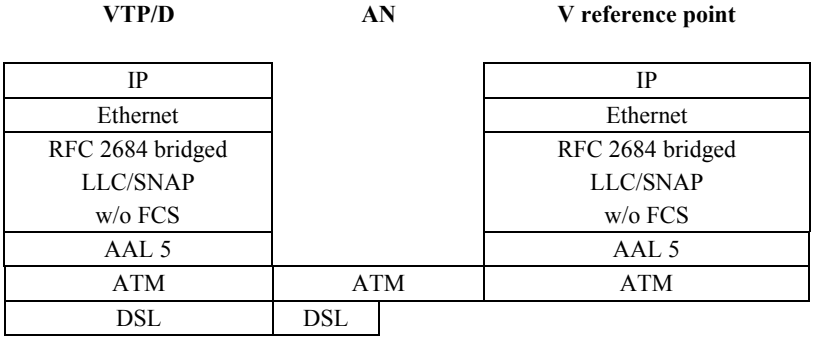


Figure 25/H.610 – VTP/D remote management connection

9.8 BLES connection

This connection type supports voice over ATM traffic between the VTP/D and a designated voice gateway. The bidirectional flow of PDUs received and transmitted on this connection is identified as the **BLES flow**. The VTP/D's and Voice gateway's implementation should be in accordance to af-vmoa-0145.000 [I-8]. Figure 26 depicts the protocol processing associated with this flow.

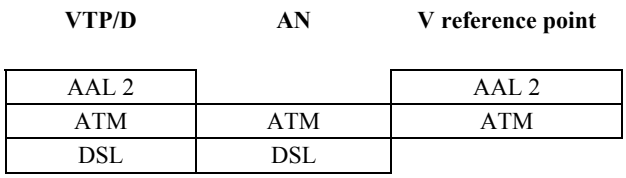


Figure 26/H.610 – BLES connection

10 VTP/D functional model

This clause specifies the functional blocks encompassing the capabilities of the VTP/D. An actual VTP/D is an implementation of a number of these functional blocks. The selection of the functional blocks for a particular implementation is determined by the flows that the VTP/D is required to support. Clause 11 specifies the functional blocks required for a baseline VTP/D. Other implementations of VTP/D are possible through alternative selections of functional blocks. In all cases, the chosen functional blocks shall comply with the specification given in this clause.

The following terms will be used throughout this clause:

- Upstream – refers to the data flowing from the T_{CN} to U-R2 interface.
- Downstream – refers to the data flowing from the U-R2 to T_{CN} interface.
- Routed flow – includes the translated and non-translated routed flows.
- Bridged flow – includes the 'Bridging' and 'PPPoE' flows.
- Routed VCs – ATM VCs carrying routed flows.
- Bridged VCs – ATM VCs carrying bridged flows.
- Routed frames – Ethernet frames arriving at the T_{CN} interface which are carrying a routed flow in the residential network and therefore, in the upstream, these are PDUs with Ethernet MAC header containing the VTP/D T_{CN} MAC address as the destination address and a unicast IP destination address.
- Bridged frames – Ethernet frames arriving at the T_{CN} interface, which are carrying a bridged flow in the residential network.

10.1 The ATM block

The *ATM* block performs the ATM and AAL layers as described in 8.3.

10.2 The DSL block

The *DSL* block implements the physical layer at the UR-2 interface.

10.3 The router block

The router block handles two packet flows, the translated routed flow and the non-translated routed flow. At the UR-2 interface, the translated flow uses the translated routed connection and the non-translated flow uses the non-translated routed connections. A router block shall support at least a single translated routed connection and at least 4 non-translated routed connections.

10.3.1 Translated routed flow

This type of packet flow carries packets that require network address translation (NAT) and port address translation (PAT) within the VTP/D. The translation is performed from IP address domains on the T_{CN} interface to one IP address on the U-R2 interface. Note that video services should not use this flow because of jitter and implementation implications. Table 4 describes how this flow is processed at the VTP/D.

Table 4/H.610 – Translated routed flow

Upstream input	Ethernet frames.
Upstream functional processing	IP Packets destined for the translated routed connection shall pass a routing function as well as Network Address Translation (NAT) and Port Address Translation (PAT) functions as per RFC 3022.
Upstream output	Routed packets whose IP destination meets the routing criteria of the NAT connection.
	If an IGMP relay function is supported (e.g., for enabling joining Internet multicast streams) by the VTP/D and bound to the translated routed connection, the output may include IGMP messages with a class D address that does not belong to the broadcast media (TV) service domain.
	If upstream forwarding of IP multicast PDUs is supported and bound to the translated routed connection, the output may contain IP multicast PDUs with a destination class D address that does not belong to the broadcast media (TV) service domain.
Downstream input	IP packets received over the translated routed connection, whose source and destination addresses are public IP addresses, and whose IP destination address matches the VTP's public IP address assigned for the NAT function.
Downstream functional processing	Packets received on the translated routed connection shall be routed to the residential network after passing the NAT and PAT functions.
Downstream output	Ethernet frame containing the MAC address that is determined by the NAT mapping from the incoming IP header to the local IP address, which is then resolved to a MAC address by the routing function.

10.3.2 Non-translated routed flow

This type of packet flow carries packets that require IPv4 routing without NAT within the VTP/D. As described in 9.4, this flow has three encapsulation options for the UR-2 interface, PPPoA, PPPoE and IPoA. However, in all cases the flow receives the same layer 3 processing, as described in Table 5.

Table 5/H.610 – Non-translated routed flow

Upstream input	Ethernet frames.
Upstream functional processing	Incoming packets shall pass a routing function. Each routed connection defines a separate routing interface.
Upstream output	Routed packets whose IP destination met the routing criteria of a specific non-translated route connection.
	If IGMP relay function is supported (e.g., for enabling joining Internet multicast streams) by the VTP/D and bound to one of non-translated route connections, the output may include IGMP messages with a class D address that does not belong to the broadcast media (TV) service domain.
	If upstream forwarding of IP multicast PDUs is supported and bound to one of the non-translated route connections, the output may contain IP multicast PDUs with a destination class D address that does not belong to the broadcast media (TV) service domain.

Table 5/H.610 – Non-translated routed flow

Downstream input	Non-translated routed connections carrying IP packets.
Downstream functional processing	Routing function.
Downstream output	Ethernet frames containing the MAC address that is resolved by the routing function.

10.3.3 Routing function

The router block shall support static routing, namely routing table that can be modified only using a management channel.

The router block should support dynamic routing, using RIPv2 RFC 2453 [19].

10.3.4 DHCP

The router block shall implement a DHCP server RFC 2131 [3] for the residential network.

DHCP servers other than the one in the VTP should not be present on the residential network.

The DHCP server in the VTP/D should ignore DHCPDISCOVER and DHCPREQUEST messages carrying User Class or Vendor Class Identifier options (number 77 and 60 respectively) of the syntax described in 12.2.

10.4 The bridge block

The bridge block handles two packet flows, the bridged flow and PPPoE flow. At the UR-2 interface, the bridged flow uses the bridge connections and the PPPoE flow uses the PPPoE connection. A bridge block shall support at least a single PPPoE connection and at least 4 bridge connections.

10.4.1 The bridge flow

This flow carries frames that require IEEE 802.1D bridging [4] bridge block. Upstream and downstream frames are forwarded according to a learning bridge MAC address table. Each bridge connection defines a separate bridge port. Table 6 describes how this flow is processed at the VTP/D.

Table 6/H.610 – The bridge flow

Upstream input	Ethernet frames.
Upstream functional processing	Incoming frames shall pass a bridging function as defined in IEEE 802.1D. Only self-learning bridge functionality [4] (subclauses 7.7 – 7.9) is mandatory.
Upstream output	Frames with destination MAC address meeting the bridging criteria for the output VC and frames with a destination MAC address not matching the VTP MAC address (on the T_{CN} interface) and not containing an IGMP message with a class D address assigned to the broadcast media (TV) service and not carrying a PPPoE Ethernet type (as long as the PPPoE filter is on).
Downstream input	Bridge connections carrying Ethernet frames.
Downstream functional processing	Valid Ethernet frames are bridged to the residential network. VC-to-VC bridging is not allowed.
Downstream output	Ethernet frames.

10.4.2 The PPPoE flow

This flow carries only PPPoE RFC 2516 [7] frames. Upstream frames received via the T_{CN} reference point are filtered to a dedicated VC if and only if they have one of the PPPoE Ethernet types (0x8863 or 0x8864).

Table 7/H.610 – The PPPoE flow

Upstream input	Ethernet frames.
Upstream functional processing	Filtering of PPPoE frames.
Upstream output	Frames carrying PPPoE Ethertype (0x8863 or 0x8864) and that the destination MAC address is not the same as the VTP MAC address.
Downstream input	The PPPoE connection carrying Ethernet frames.
Downstream functional processing	None.
Downstream output	Ethernet frames.

10.4.3 Filtering

The bridge block shall support PPPoE filtering. The PPPoE filter shall be either remotely enabled or pre-configured (i.e., by the manufacturer). In case that ILMI is supported, the PPPoE filter can be remotely activated by binding the PPPoE flow to an ATM PVC (see clause 18).

10.5 The broadcast block

The broadcast block handles two packet flows, the broadcast flow and channel change flow. At the UR-2 interface, the broadcast flow uses the digital broadcast connections and the channel change flow uses the channel change connection. A broadcast block shall support exactly one channel connection and at least 4 broadcast connections. The implementation of the broadcast block is dictated by the broadcast delivery method chosen, IP based delivery or ATM based delivery. Table 8 describes the implementation aspects of two possible broadcast delivery methods.

Table 8/H.610 – Broadcast compatibility

Delivery method	Broadcast stream encapsulation	Channel change protocol between VTP/D and the AN	Possible CPE architectures	Impacts on the VTP
IP based	MPEG/UDP/IP/ Ethernet/AAL 5	IGMPv2	Distributed	–
			Centralized	–
ATM based	MPEG/AAL 5	DSM-CC	Distributed	The VTP shall convert IGMPv2 to DSM-CC. The VTP shall also adapt MPEG/AAL 5 to MPEG/UDP/IP/Ethernet.
			Centralized	–

In the case where the residential distributed model is implemented, and the ATM based delivery is chosen, the VTP shall perform the IP re-encapsulation, to conform to the protocol stack described in 9.6.1, 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 shall be 1970.

10.5.1 Broadcast flow

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

Table 9/H.610 – The broadcast flow

Upstream input	Ethernet frames.
Upstream functional processing	Block all packets.
Upstream output	None.
Downstream input	Broadcast connections carrying MPEG-2 TS.
Downstream functional processing (VTP)	***ATM based delivery***: The payload of one or several AAL 5 frames is encapsulated as one IP multicast packet in a single Ethernet frame.
	IP based delivery: The LLC/SNAP header is removed and no further processing is required.
Downstream output	Ethernet frames carrying IP multicast packets.

10.5.2 Channel change flow

The VTP/D shall implement a 'channel change proxy', namely an IGMP server (i.e., router) function towards the T_{CN} interface and an IGMP or DSM-CC client function towards the U-R2 interface.

Table 10/H.610 – The channel change flow

Upstream input	Ethernet frames.
Upstream functional processing	Channel change proxy. The Channel change proxy function accepts frames that contain an IGMP message with a class D address assigned to the broadcast media (TV) service. The channel change proxy function generates corresponding channel change messages towards the access network. In case of ATM based delivery, IGMP to DSM-CC protocol conversion is performed.
Upstream output	**ATM based delivery**: DSM-CC messages.
	IP based delivery: IGMPv2 messages.
Downstream input	PDU received over the channel change connection.
Downstream functional processing (VTP)	**ATM based delivery**: Channel change proxy (DSM-CC client and IGMP router) state machine.
	IP based delivery: IGMPv2 proxy state machine.
Downstream output	Ethernet frames containing IGMP Queries.

10.6 Voice block

This functional block is required if VoATM service is to be supported. The voice block handles the BLES flow that carries Voice over ATM related PDUs (i.e., AAL 2 cells), as described in Table 11. A voice block shall support at least one BLES connection.

Table 11/H.610 – The BLES flow

Upstream input	Analogue voice signal.
Upstream functional processing	Generating BLES Flow.
Upstream output	AAL 2 cells carrying telephony signals.
Downstream input	AAL 2 cells carrying telephony signals.
Downstream functional processing	Terminating BLES Flow.
Downstream output	Analogue voice signal.

10.7 Management block

The management block handles the VTP/D Remote Management Flow allowing the configuration management of the VTP/D. This block handles also the local management of the VTP.

The management block shall support the functions described in clause 18.

10.7.1 IP configuration

The VTP/D shall implement a DHCP client RFC 2131 [3] enabling dynamic configuration of the IP parameters of the management interface. The VTP/D shall support DHCP options 66 (TFTP server name) and 67 (Bootfile name) described in RFC 2132 [27], enabling retrieval of locations and names of files consisting specific VTP/D configuration details. (This is in addition to the possibility of receiving these parameters in the 'sname' and 'file' fields.)

10.7.2 Remote file download

The VTP/D shall implement a TFTP client as defined in RFC 1350 [20]. This capability enables remote software/firmware upgrade and download of configuration files to the VTP/D.

10.8 Home networking block

The home networking block provides the adaptation between the T_{CN} interface and the physical residential network.

11 Baseline VTP/D implementation

This clause describes the implementation of a baseline VTP/D. This implementation is designed as a residential multi-service solution providing broadcast TV, VoD, Internet access and optionally voice services.

Figure 27 shows the VTP/D functional blocks required for the baseline VTP/D implementation. Mandatory blocks are circled in a solid line and optional blocks are circled in a dotted line. A dashed line indicates that it is mandatory to implement at least one of the encircled blocks. The *decoder* block is mandatory only for a VTPD and handles the MPEG decoding and the distribution of the decoded A/V contents to the different TVs.

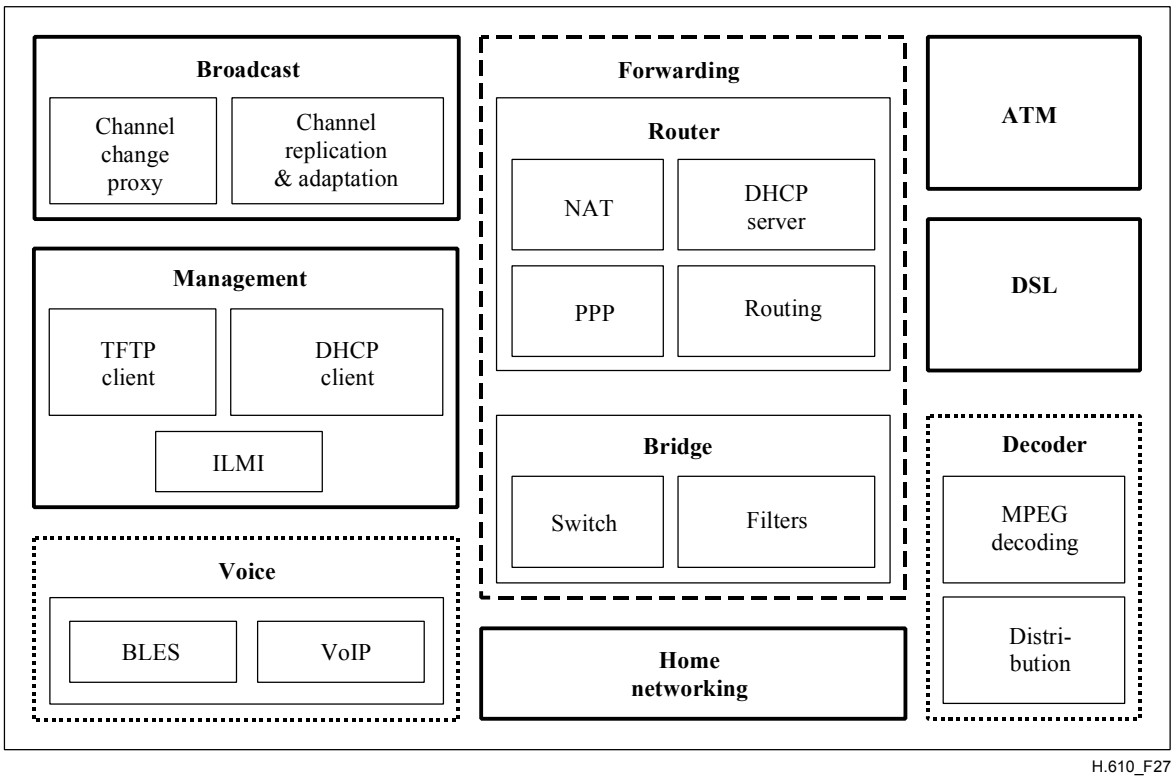


Figure 27/H.610 – VTP functional blocks

The forwarding block includes two blocks, the router block and the bridge block. A baseline VTP/D shall implement at least one of these blocks. A baseline VTP/D implementing the router block is considered as a layer-3 device, whereas a baseline VTP/D implementing the bridge block is considered as a layer-2 device. A baseline VTP/D implementation may choose to provide both blocks and is then considered a hybrid device.

12 IP configuration of the CPE

It is expected that a majority of deployments will consist of a single IP subnetwork for the residential network and a single (translated or non-translated) external route. Such scenarios are described as standard scenarios.

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

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

The support of the standard scenarios is mandatory. The support of the advanced scenarios is optional. Advanced scenarios are described in Appendix IV.

This clause assumes a VTP/D implementation that includes the router block. Throughout this clause, the term PPP is used to signify PPPoA or PPPoE.

12.1 Standard IP processing scenarios

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

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

- An exclusive private address space for the residential network, e.g., 192.168.0.0.
- A subnetwork of an externally routable address space. The residential subnetwork may be a subnetwork of:
  - The public Internet using a subnetwork of public (globally registered) address space.
  - A wider private network using private address space, e.g., 10.0.0.0 private address space.

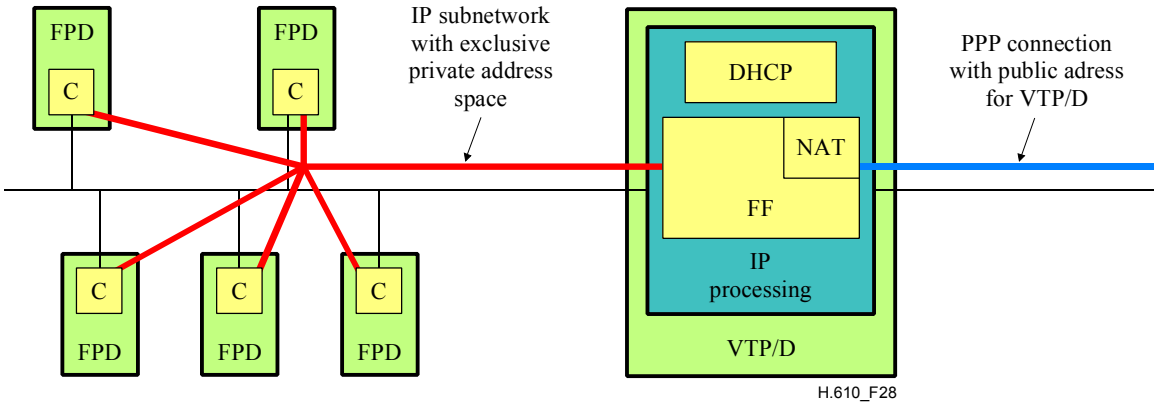
IP networking within the IP subnetwork of the home network is achieved using the Ethernet MAC layer capabilities with the IP address to MAC address mapping maintained using ARP in a standard way.

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

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

12.1.1 Default configuration of exclusive private address space

The configuration of this standard scenario is illustrated in Figure 28. The residential network uses exclusive private address space (default is 192.168.0.0/24) and since this address range is known independently of the connection to the wider network, the IP subnetwork parameters and the DHCP server parameters can be configured before the network connection is created and configured.



C Client
FF Forwarding Function

Figure 28/H.610 – Standard IP processing scenario with exclusive private address space

12.1.1.1 Default configuration action sequence

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

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

12.1.1.2 Default IP subnetwork and DHCP server configuration

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

The parameters defining the residential private address subnetwork are given in Table 12 together with their default and/or derived values. The third column specifies what alternative methods of configuration are available for this parameter.

Table 13 defines the DHCP server parameters for configuring hosts within the subnetwork.

Table 12/H.610 – Default subnetwork parameters for an IP subnetwork with exclusive private address space

Parameter	Default	Alternative configuration
Subnetwork mask (m.m.m.m)	Static – 255.255.255.0	Static value through management interface
Subnetwork address (x.x.x.x)	Static – 192.168.0.0	Static value through management interface
Default gateway	Derived – 192.168.0.1	No – calculated as x.x.x.x and m.m.m.m + 0.0.0.1
Broadcast address	Derived – 192.168.0.255	No – calculated as x.x.x.x and m.m.m.m + not m.m.m.m
Primary DNS server address	Derived – IPCP RFC 1332 extension per RFC 1877 from service node (see PPP parameter below)	Static value through management interface or the VTP may implement a DNS relay and/or caching function
Secondary DNS server address	Derived – IPCP extension per RFC 1877 from service node (see PPP parameter below)	Static value through management interface
Intra subnetwork address resolution	ARP	–
Address of VTP/D within the Subnetwork	192.168.0.1	No – calculated as x.x.x.x and m.m.m.m + 0.0.0.1

Table 13/H.610 – Default DHCP server parameters for an IP subnetwork with exclusive private address space

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

12.1.1.3 Default external connection configuration

The following default parameters, given in Table 14, are used to configure the external connection to the IP subnetwork as well as negotiate parameters with the edge router in the network.

Table 14/H.610 – Default parameters for external connection to IP subnetwork with exclusive private address space

Parameter	Default	Alternative configuration
Encapsulation	PPP	No
LCP keep alive rate	Static – 1 minute	Static value through management interface
Authentication	PAP [RFC 1334]	CHAP [RFC 1994]
IPCP VTP address offered by VTP	0.0.0.0	Static provision using the management interface
IPCP VTP address offered by service node	Accept address x.x.x.x offered	Ignore address
IPCP service node address offered by service node	Ignore address (PPP link is default route)	No
IPCP service node address offered by VTP	Do not offer address	No
IPCP primary DNS server address offered by service node	Accept address x.x.x.x offered	Ignore address
IPCP secondary DNS server address offered by service node	Accept address x.x.x.x offered	Ignore address

12.1.1.4 Default IP forwarding function configuration

The routes in the IP forwarding function are those of a trivial forwarding function. The main outgoing routes are to the residential network and the external connection, which is the default route. This default route also includes the NAT/PAT function. In addition to these routes, the VTP/D should implement a loop-back route. The default routes are shown in Table 15. The default parameters for the NAT/PAT function are given in Table 16.

Table 15/H.610 – Default IP forwarding function parameters for an IP subnetwork with exclusive private address space

Destination address range		Masquerading	Outgoing Layer 2 interface
Destination address	**Subnet mask**		
x.x.x.x (derived from subnetwork parameters)	s.s.s.s (derived from subnetwork parameters)	No	Residential network interface, e.g., eth0
127.0.0.0	255.0.0.0	No	VTP/D – loop-back route
Default route		Yes	External connection, e.g., ppp0

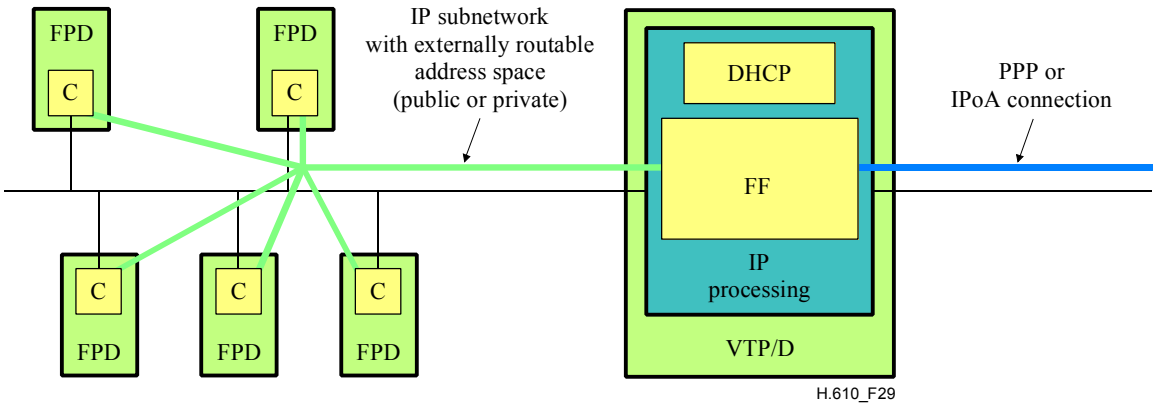
Table 16/H.610 – Default NAT/PAT parameters for an IP subnetwork with exclusive private address space

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

12.1.2 Default configuration of the standard scenario with externally routable address space

The configuration of this standard scenario is illustrated in Figure 29. In this standard scenario, the default address range is assigned by the network through the edge router, either using PPP or DHCP. (Note that this DHCP transaction is between the VTP/D as DHCP client and the edge router as DHCP server.)

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



C Client
FF Forwarding Function

Figure 29/H.610 – Standard IP processing scenarios with external routable address space

12.1.2.1 Default configuration action sequence

The default configuration is initiated by the VTP/D following the establishment of the external non-translated routed connection.

This triggers the following actions if the non-translated routed connection uses PPP:

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

If the non-translated routed connection is IPoA, then the following actions are triggered:

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

12.1.2.2 Default external connection configuration

If the external connection to the IP subnetwork uses PPP, the default parameters are given in Table 17 whereas, if the external connection uses IPoA, the default parameters are as given in Table 18. These are used to configure the external connection as well as to negotiate with the edge router.

Table 17/H.610 – Default parameters for external PPPoA connection to IP subnetwork with externally routable address space

Parameter	Default	Alternative configuration
Encapsulation	PPP	No
LCP [RFC 1661] keep alive rate	Static – 1 minute	Static value through management interface
Authentication	PAP	CHAP
IPCP VTP address offered by VTP	0.0.0.0	Static provision using the management interface
IPCP VTP address offered by service node	Accept address x.x.x.x offered	Ignore address
IPCP service node address offered by service node	Ignore address (PPP link is default route)	No
IPCP service node address offered by VTP	Do not offer address	No
IPCP primary DNS server address offered by service node	Accept address x.x.x.x offered	Ignore address
IPCP secondary DNS server address offered by service node	Accept address x.x.x.x offered	Ignore address

Table 18/H.610 – Default parameters for external IPoA connection to IP subnetwork with externally routable address space

Parameter	Default	Reconfiguration
Encapsulation	IPoA (RFC 2684 routed mode with LLC/SNAP)	No
Configuration protocol	DHCP	None – i.e., configuration protocol
Routing Protocol	None	Enabling of optional RIPv2

12.1.2.3 Default IP subnetwork and DHCP server configuration

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

This default derivation of the address range uses the following rules when the external connection uses PPP:

- Where the IPCP component of PPP can allocate subnetwork mask, this should be used for the subnetwork.
- If no subnetwork mask is allocated by IPCP, the subnetwork should assume subnetwork mask of 255.255.255.248.

  NOTE – This requires that the edge router and RADIUS servers are also aware of this convention and configured accordingly.

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

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

The parameters defining the IP subnetwork are give in Table 19 together with their default and/or derived values. The third column specifies what alternative methods of configuration are available

for this parameter. Table 20 defines the parameters for the DHCP server in the VTP/D associated with the IP subnetwork.

Table 19/H.610 – Default parameters for IP subnetwork with externally routable address space

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

Table 20/H.610 – Default parameters for DHCP server for IP subnetwork with externally routable address space

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

12.1.2.4 Default IP forwarding function configuration

The routes in the IP forwarding function are those of a trivial forwarding function. The main outgoing routes are to the residential network and the external connection, which is the default route. In addition to these routes, the VTP/D should implement a loop-back route. The default routes are shown in Table 21.

Table 21/H.610 – Default IP forwarding function parameters for an IP subnetwork with externally routable address space

Destination address range		Masquerading	Outgoing Layer 2 interface
Destination address	**Subnet mask**		
x.x.x.x (derived from subnetwork parameters)	s.s.s.s (derived from subnetwork parameters)	No	Residential network interface, e.g., eth0
127.0.0.0	255.0.0.0	No	VTP/D – loop-back route
Default route		No	External connection, e.g., ppp0 or ipoa0

12.2 DHCP

DHCPDISCOVER and DHCPREQUEST messages, issued by FS-VDSL compliant terminals shall include a Vendor Class Identifier option (subclause 9.13 of IETF RFC 2132 [27]) specifying the terminal type. The value of this option shall be interpreted as a string of UTF-8 IETF RFC 2279 [24] characters with the 4-field format described below.

<FSVDSL><Service Type><Manufacturer ID><Model Number>

- **<FSVDSL>** is the constant 6-character string "FSVDSL" followed by the dot ('.') character.
- **<Service Type>** is a variable length string indicating the service supported by the terminal. This field shall contain exactly one dot character as the last character.
- <**Manufacturer ID>** is a variable length string that uniquely identifies the manufacturing vendor. It is recommended that this field will be encoded as the OUI allocated to the vendor by the IEEE. This field shall contain exactly one dot character as the last character. Appendix X gives the current method to obtain an OUI from IEEE.
- <**Model Number>** is a variable length string that uniquely identifies the terminal type within the scope of this vendor. Model numbers shall be allocated and published by the terminal vendors.

Where the Vendor Class Identifier Option cannot be used by the terminal, the User Class Option IETF RFC 3004 [28] shall be used instead, with the same syntax as defined above. This option shall be also used in cases where multiple service types have to be indicated by the terminal.

A DHCP server in the network should be configured such that it only replies to DHCP messages that contain identification with a valid syntax as described herein. Otherwise, the DHCP server should discard the message and not respond. This enables, for example, to configure the DHCP server to respond to terminals requesting IP parameters for a specific service or to terminals from specific vendor or model.

The DHCP server in the VTP/D should ignore DHCPDISCOVER and DHCPREQUEST messages carrying User Class or Vendor Class Identifier options of the above syntax, in order to allow controlling IP addressing for advanced services to be from the network (i.e., service operator).

The following basic service types are defined for the usage of FS-VDSL terminals (additional types may be used):

- "VOICE" – for derived voice services;
- "VIDEO" – for digital broadcast and VoD services;
- "DATA" – for data only service.

13 Data service

Data service shall be provided using one or more of the following:

- Bridge connection as described in 9.1 associated with the bridge flow as described in 10.4.1.
- PPPoE connection as described in 9.2 associated with the PPPoE flow described in 10.4.2.
- Non-translated route connection as described in 9.4 associated with the non-translated routed flow described in 10.3.2.
- Translated routed connection as described in 9.3 associated with translated routed flow described in 10.3.1.

The respective IP configuration shall conform to clause 12.

14 Broadcast service

This clause provides 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 service offered by a satellite or a cable operator.

14.1 Delivery options

The A/V content shall be encapsulated in MPEG2-TS regardless of the encoding technique used (e.g., MPEG-2, MPEG-4, etc.).

Prior to transmission of the A/V content over the V reference point, appropriate encapsulation shall be performed. Two delivery options are possible, "ATM based delivery" and "IP based delivery" as described in 10.5. Choosing one delivery option dictates the MPEG2-TS encapsulation and the VTP/D to AN channel change protocol.

In both options it is required that the A/V content be transmitted in a SPTS. The transport of A/V content in the AN shall be transparent to the choice of encapsulation option.

Encapsulation methods are PCR unaware.

14.1.1 ATM based delivery

In ATM based delivery, MPEG-2 Transport Stream shall be encapsulated as described in 9.6.2 and the channel change protocol shall be DSM-CC.

At the launch of DBTV services at the Head-end, the encapsulation shall be 2 MPEG Transport Stream packets per AAL 5 PDU at the V reference point.

14.1.2 IP based delivery

In IP based delivery the MPEG-2 Transport Stream shall be encapsulated as described in 9.6.1 and the channel change protocol shall be IGMPv2.

At the launch of DBTV services at the Head-end, the encapsulation shall be 7 MPEG Transport Stream packets per IP packet in an AAL 5 PDU when MPEG-2/IP/ATM is used at the V reference point.

14.2 Broadcast TV IP addressing scheme

In case of IP based delivery, each broadcast stream received on the V reference point shall have a unique class D IP address as its IP destination.

In case of ATM based delivery and distributed residential environment, the IP multicast encapsulation is performed only at the VTP. The class D IP address assignment in this case is described in 10.5 and 14.4.1.

The default Class D IP subnet allocated for broadcast streaming shall be 239.192.0.0/14.

14.3 Transport

14.3.1 Channel replication and ATM cross connect

The OLT shall replicate and the ONU may replicate the incoming broadcast streams (channels) to all users that simultaneously access 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. A user's channel change request causes a user side VC link to be cross-connected to the appropriate point-to-multipoint root.

14.3.2 Encryption

The AN and the residential network shall be transparent to the implementation of encryption based conditional access.

14.3.3 Administrative channel

The administrative channel includes all messaging and data flows between FPD and the broadcast service management platform. Administrative messaging may include STB boot files, software upgrade, Electronic Program Guide data, etc. This administrative channel shall use a bridged, PPPoE or non-translated routed connection.

14.3.4 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 assumes guarantees on packet delivery, correct packet sequencing, and bound on packet delay variation and Program Clock Reference jitter. The network engineering for both the core network and AN shall 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 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 Program Clock Reference jitter of the delivered service as indicated below. A detailed definition of Program Clock Reference jitter and measurement techniques for Program Clock Reference jitter are contained in clause 5.3.2 and Annex I of ETSI TR 101 290.

14.3.4.1 Head-end

The Head-end (together with the contribution of any intervening core network) shall not contribute more than 5 ms of Program Clock Reference jitter to the delivery of the MPEG SPTS packets measured at the V reference point.

14.3.4.2 AN

The AN configuration and dimensioning between the V reference point and the U-R2 interface shall support a peak-to-peak cell delay variation as defined in ATM Forum Specification af-tm-0056.000 to be less than 2 ms. The sum of the cell error ratio and cell loss ratio shall be less than 10^{-8}.

14.3.4.3 VTP and residential network

The residential network shall not contribute more than 5 ms of Program Clock Reference 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 Program Clock Reference within the IP frame or ATM cell by using the average bit rate of the stream and the knowledge of the position of the Program Clock Reference bearing MPEG Transport Stream packet.

NOTE – The 'positional jitter' of the Program Clock Reference is of increasing importance as the bit rate of the stream is reduced (as enabled by MPEG-4 and other proprietary compressions).

14.3.4.4 FPD

The FPD shall be able to tolerate Program Clock Reference jitter of at least 12 ms. The ratio of 10^{-8} stated in 14.3.4.2 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.

14.4 Channel change signalling

14.4.1 IGMPv2 and DSM-CC use for channel change control

Using ATM based delivery in the case of the distributed residential model requires an IGMPv2 to DSM-CC translation at the VTP. This translation implies that the VTP implement both IGMP and DSM-CC state machines, and that class D addresses are converted to BPIDs (Broadcast Program IDs used in the DSM-CC CCP signalling). The use of identical numbering schemes for the class D addresses and the BPIDs eliminates the need for any computed translation. For further details on IGMPv2 to DSM-CC translation, see Appendix II.

14.4.2 IGMPv2 end-to-end for broadcast channel change control

The IGMP protocol was not originally intended for use as a channel zapping protocol, and some of the default values for timers, etc., would yield unacceptable performance for this application. This subclause describes a number of suggested modifications to default behaviours and also suggests alternate default timer values in order to optimize the performance.

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 Recommendation, only the network delay is addressed, and a target below 500 ms is pursued.

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 following list reports the recommended timer values.

In the following, an unsolicited IGMPv2 report message is denoted as *join* and an IGMPv2 leave message is denoted as *leave*.

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, where the smaller the value the faster the release of unused resources.

RFC 2236 default value: 1 s

Recommended value: 100 ms

LastMemberQuery count

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

RFC 2236 default value: 2

Recommended value: 1

UnsolicitedReport 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, RFC 2236 recommends that it be repeated once or twice after short delays (Unsolicited Report Interval).

RFC 2236 default value: 10 s

Recommended value: 100 ms

The FPDs and VTPs should support recommended values, and shall interwork with other equipment using these values. However, the use of the recommended values is not mandatory. Parameters for which no optimization is recommended shall default to the values specified in RFC 2236.

14.4.2.1 STB requirements

The STB shall implement the RFC 2236 host processing including the following additional requirements:

- Every time a channel is left the STB shall send a leave message.
- During a channel change, the leave message shall always be sent before the join message, with the exception of multiple channels reception (e.g., for picture-in-picture).
- During a channel change, the STB shall send a join message only after a period of *joinDelay* from the previously sent leave message in order to ensure that the order between leave and join messages is maintained when these messages are proxied by the VTP/D to the AN.
- The value of *joinDelay* should be configurable. The recommended value is 100 ms.
- The STB shall be able to reply to specific queries with a maximum response time of 100 ms.
- The STB should generate 2 (or 3) unsolicited reports at the UnsolicitedReport interval.

14.4.2.2 VTP requirements

The VTP shall implement the RFC 2236 querier process at the residential network interface and relay IGMPv2 requests (join and leave messages) to the access network. When a report message is received for a channel that has no members, the VTP shall relay this message towards the OLT. The VTP shall 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 100 ms.
- The VTP should be able to set the *LastMemberQuery* count to 1.

14.4.2.3 AN requirements

The AN shall react to a join message by connecting the requested channel to the proper DSL port and shall 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 RFC 2236. The AN shall implement the "general query" mechanism in order to recover from leave message losses. This last process may be started periodically (as per RFC 2236) or triggered by a specific event.

14.4.3 IP source addresses used in IGMP messages

The IP destination address of the IP packets carrying 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 residential 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 reference point, but rather it is terminated within the AN.
- All broadcast channels are expected to be received by the OLT. However, for future expansion of this Recommendation, signalling 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.
- FPD, VTP/D and AN shall process IGMP messages regardless of their source IP address.

14.5 Information model for the channel change function within the AN

This clause applies exclusively to the M interface. The functions defined below 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 30 depicts the management information model that shall be implemented at the AN. This management information model is referred to as the Channel Change Function Management Information Model (CCF MIM). Figure 30 describes 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 Annex B.

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

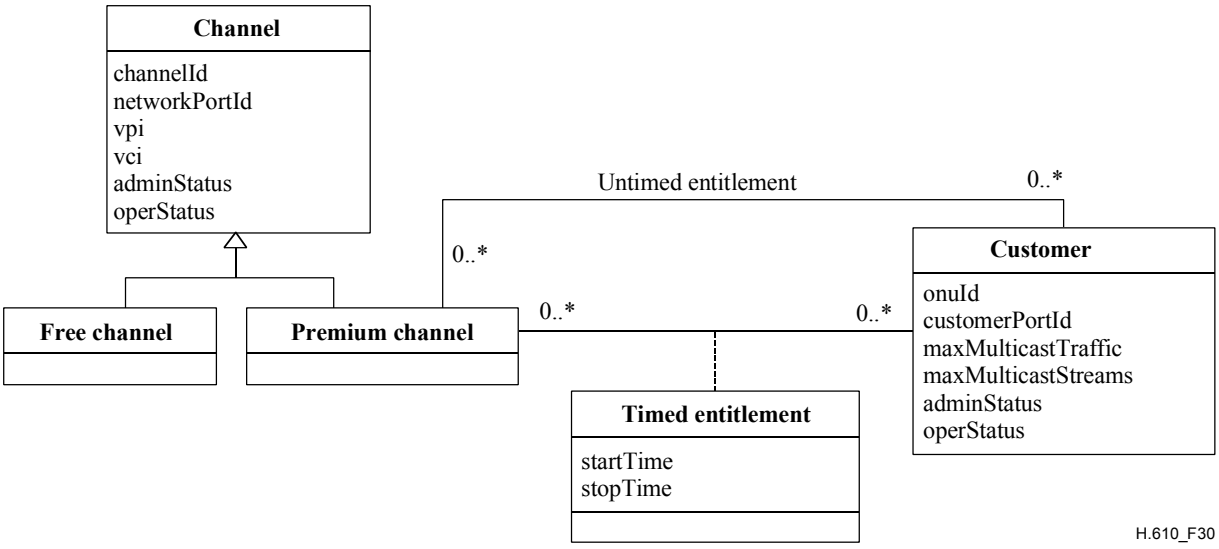


Figure 30/H.610 – Channel change function management information model

14.5.1 Channel change

The channel change function makes 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 Broadcast Program ID. In addition, it defines at the V reference point the networkPortId, VPI and VCI values.

The **Customer** object is used to describe each DSL 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.

14.5.2 Connection Admission Control (CAC)

The Customer object defines the attributes maxMulticastStreams and maxMulticastTraffic. maxMulticastStreams specifies the maximum number of separate streams that can be simultaneously active across the Customer's DSL link. 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.

14.5.3 Conditional access at the AN

For conditional access the model needs to support the following:

- a distinction between channels that require conditional access and those that do not;
- 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 modelled using the Free Channel object. Premium channels do require conditional access to be applied and these are modelled 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 modelled 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 AN. 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 AN shall be synchronized in time with the entity setting the entitlement. The way this synchronization is achieved is outside the scope of this Recommendation.

Together the Untimed relationship, Timed relationship and the maxMulticastStreams attribute of the Customer object provide all the required information for performing the CA function at the AN. 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.

15 VoD service

This clause defines requirements for Video-on-Demand (VoD) service in an FS-VDSL system. VoD service is an on-demand service that delivers multimedia assets such as video, audio, and games[1]. VoD service requires a high quality of service and guaranteed bandwidth. It delivers broadcast quality video, and allows for interactivity to support functions such as "pause" and "fast-forward".

An implementation of VoD service typically requires:

- Back office management.
- A "server farm" containing interesting content.

[1] A "VoD" service can also deliver non-video assets. 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 Recommendation without further clarification or explanation.

- Transport and AN facilities that can ensure QoS.
- Compelling client server application software.
- Coordination of key network resources between VoD service providers and the network operator.

An FS-VDSL system shall provide the ability to deliver multiple VoD sessions per DSL line.

15.1 VoD back office management

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

Back office components are illustrated in Figure 31. Content and associated metadata arrive to the Asset Manager, which places them onto the servers ("content distribution"), and, with input on scheduling and pricing, populates the "content directory".

Content may be stored in an encrypted form on the video server; in this case rights information shall be 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 shall communicate with the Digital Rights Manager to determine the rights information and shall communicate them to the client; and the Digital Rights Manager shall communicate with the video server to apply the proper encryption keys.

The Subscriber Manager shall create accounts for users and shall maintain current account status. At the end of a billing cycle, the Subscriber Manager shall provide billing records to the customer care system. The Asset Manager shall collect purchase information.

The consumer selects content from the Content Directory for purchase. Session and Connection Establishment are invoked when a client wishes to view a VoD asset. These are described below.

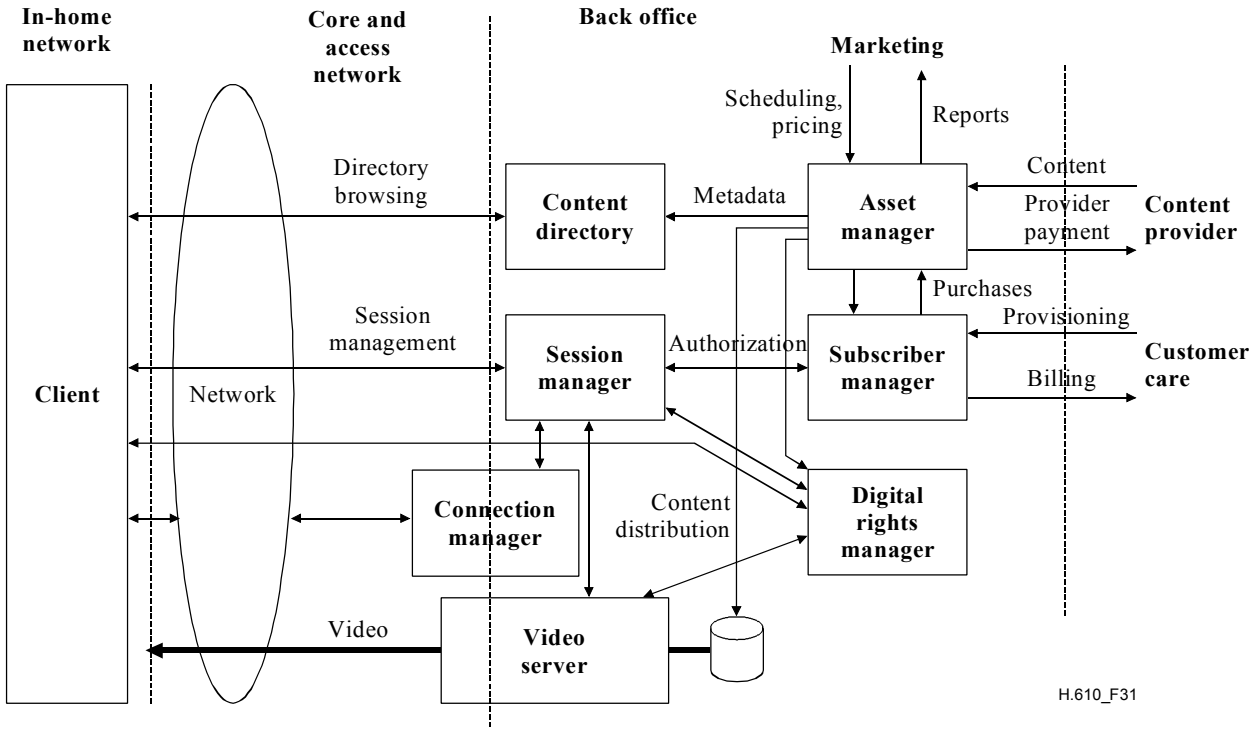


Figure 31/H.610 – VoD back office management

15.2 VoD network engineering

15.2.1 Centralized and distributed VoD server farms

VoD server hardware may be "centralized", where VoD servers provide content to a large population of users from a single site. Alternately, a "distributed" approach may be used, where there are several sites hosting a smaller number of servers that serve a smaller population of users.

15.2.2 Two-way administrative traffic

An FPD shall be able to perform directory browsing, interact with the DRM Head-End, and perform VoD session establishment and stream control. IP protocols shall be used to communicate with the VoD application servers.

A bridged, PPPoE, or non-translated routed connection, as defined in clause 9, shall be provided for the VoD administrative traffic. The application servers that support these functions may be in a separate physical network than the public Internet and data service.

This two-way administrative traffic should share the connection with the Broadcast Service administrative channel defined in 14.3.3.

15.2.3 One-way video traffic

A one-way transport capacity shall carry the VoD content between the video server and the VTP/D.

The administrative traffic may be multiplexed with the downstream video traffic (e.g., using "in-band" signalling). However, this may introduce MPEG jitter and complicate VoD server design.

The administrative traffic should use "out of band" signalling. This approach allows the network operator to optimize for the one-way nature and QoS requirements of the video traffic.

Three main approaches may be taken for bandwidth management and the network engineering of the VoD transport network:

- 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 also possible. The approach taken has an impact on connection establishment procedures, which are described in 15.5.

15.2.4 QoS requirements for VoD video traffic

The transport network shall not allow undue packet loss, introduce excessive packet jitter, or allow packet reordering. The detailed QoS requirements for VoD service are identical to those for broadcast service (see 14.3.4).

15.2.5 Encapsulation of VoD video traffic

The video stream encapsulation options are identical to those required for broadcast service as described in 9.6.1 and 9.6.2.

15.3 VoD content browsing

The subscriber shall be able to browse the Content Directory in order to purchase content. The two-way administrative channel described in 15.2.2 shall be used for this purpose.

No specific requirements are placed on how the Content Directory is managed or how browsing is performed, but it may use techniques such as HTML.

Once a selection has been made by the user, the Content Directory shall provide the identifier for the VoD asset (e.g., RTSP URI) 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.

15.4 VoD session establishment

Session Management signalling shall be performed between the FPD application and the VoD session management entity. RTSP RFC 2326 shall be used as the session management protocol.

The RTSP SETUP message shall contain the following fields:

- A unique identifier of the FPD shall 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 shall be provided. This information shall come from the Content Directory.

The RTSP SETUP message may contain the following fields:

- A VoD session manager identifier. 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 to further identify the physical location of the FPD.
- QoS information such as desired encoding rate.

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 may be invoked at this time to grant the user the necessary rights, and to provide key and access information back to the FPD for decryption.

The RTSP SETUP REPLY may contain the following fields:

- Connection and QoS information. This information could include a class D multicast address or DSM-CC BroadcastProgramId.
- DRM rights or key information.

Once the session has been established, the user can use RTSP stream control within the session to start, pause or play the movie.

When the client has finished viewing the movie, it shall release the session by the RTSP TEARDOWN command. This releases both session and connection resources. The server can also release the session if necessary.

15.5 VoD connection establishment

This clause 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, bandwidth is not established between the VTP/D and the server and connection establishment procedures shall be invoked at the time of session establishment.

15.5.1 Pre-established bandwidth end-to-end

This subclause describes the case where bandwidth is pre-established between VoD server and VTP/D.

In this case, bandwidth is typically "overbooked" in the AN and on the DSL line; the subscriber bandwidth is shared among broadcast video service and data. The FPD software and the back office VoD components shall 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 only at the VoD server; core network and AN are unaware of the session.

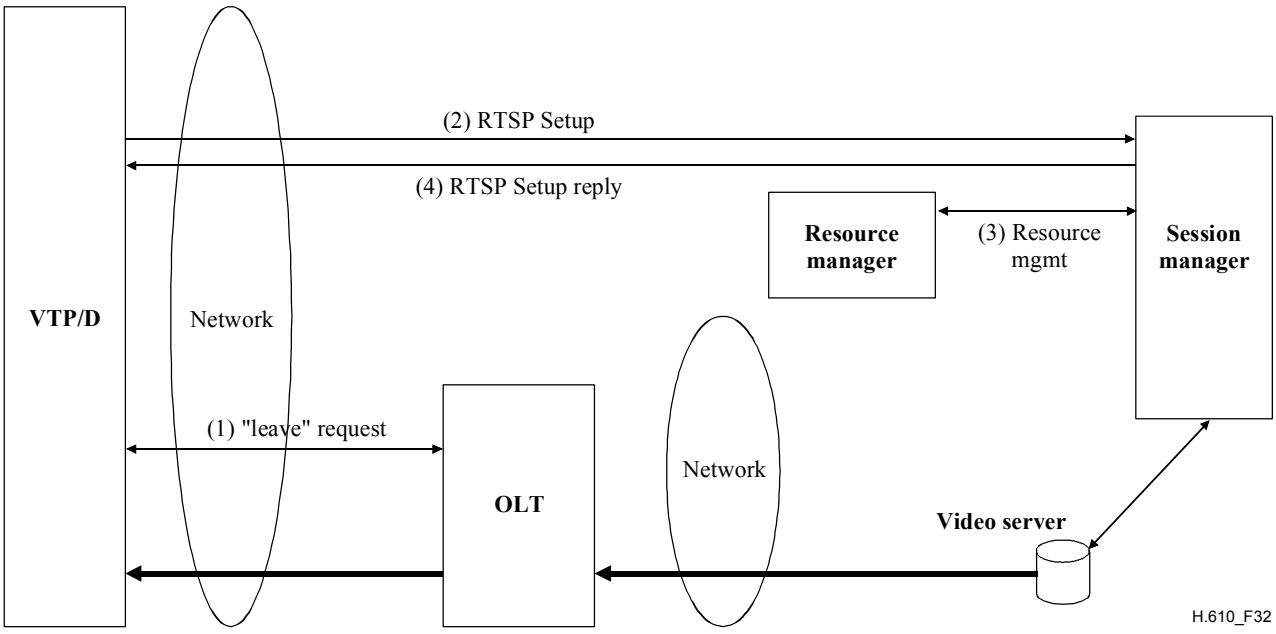


Figure 32/H.610 – VoD session establishment – Pre-established bandwidth end-to-end

Figure 32 illustrates the message flow to establish a VoD session.

Step 1. The client "leaves" an existing broadcast channel in order to free bandwidth for the VoD channel.

Step 2. VoD Session signalling is performed between the FPD and the Session Manager.

Step 3. VoD server resources shall be allocated. In the diagram above, the Session Manager invokes the Resource Manager. At minimum, the Resource Manager will need to identify and allocate the appropriate video server resources such as output port. To do this, it may need to know the identity of the VTP/D (or the OLT), and also the desired video asset.

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

15.5.2 Bandwidth bottleneck in the transport network

This subclause describes the case where bandwidth is not pre-established between VoD server and VTP/D. Connection establishment procedures are, therefore, required.

Figure 33 provides an overview of VoD session and connection establishment procedures in this case.

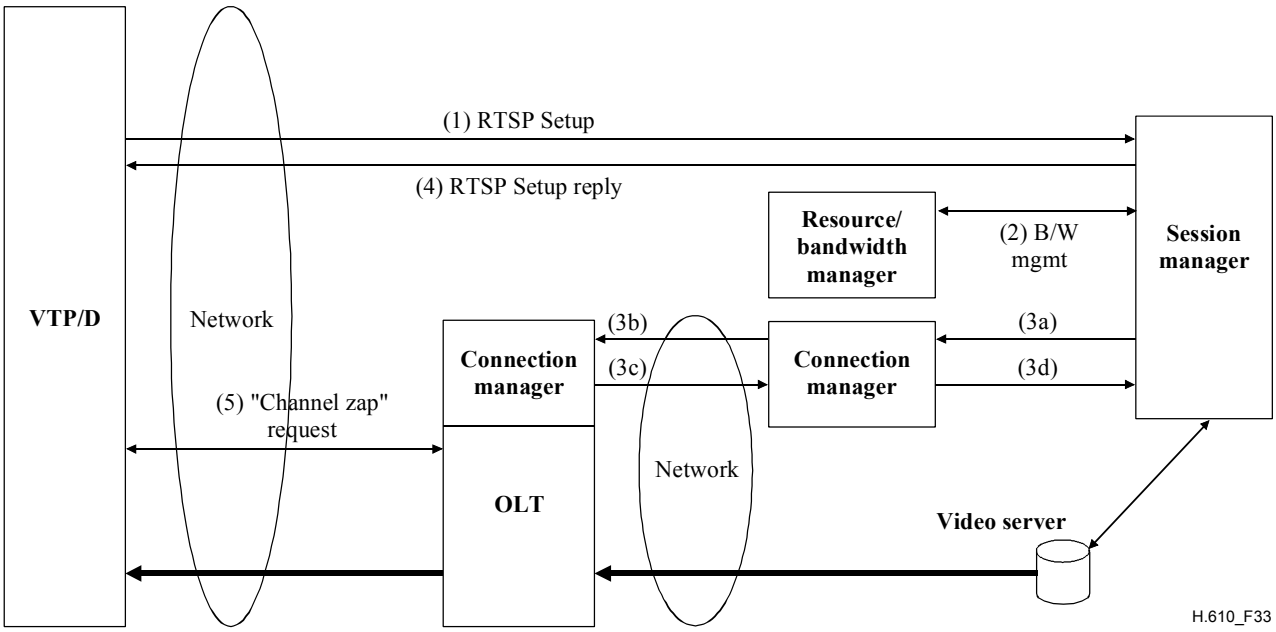


Figure 33/H.610 – VoD session establishment – Concentration in access network

Step 1. VoD session signalling is performed between the FPD and a Session Manager.

Steps 2 and 3a. Allocation of VoD server resources and network bandwidth is required. The Session Manager will invoke the Resource Manager and the Connection Manager to establish a connection from video server to FPD. The required bandwidth management can be performed either as part of connection signalling (i.e., by the Connection Manager), or it can be a function of the Resource Manager.

Step 3b. Connection establishment procedures are used to reserve bandwidth for the downstream video connection. The Connection Establishment entity in the Session Manager shall map the VTP/D identity to AN OLT to determine the route of the connection. There are a few possible methods for retrieving the OLT location from the VTP/D or FPD identification:

- Local configuration of the OLT id in the FPD.
- 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.
- Other means of configuration.

If access control procedures are used in the access network, the connection establishment procedures shall create the connection with the necessary permissions.

Steps 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 FPD.

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

15.5.3 Connection establishment protocol requirements

The connection establishment protocol should be performed out of band.

The connection establishment protocol should be server initiated, as server initiated signalling is more secure than FPD initiated signalling.

The connection establishment protocol should be "hard state." This approach creates a well-defined path to ensure QoS for the life of the session. Hard State connections also eliminate the need for per-connection "keepalive" traffic. RSVP RFC 2205 [I-9], for example, is a "soft state" protocol and is not recommended as a long-term solution.

15.5.4 Connection establishment protocol options

The choice of connection establishment protocol depends upon the transport network.

For IP transport networks, RSVP-TE RFC 3209 [I-11] or CR-LDP RFC 3212 [I-10] may be used.

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 may 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).

Alternately, ATM signalling may be terminated on the access network and complemented by channel change signalling from the FPD.

15.5.5 IP address assignment for downstream VoD

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

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 signalling), and allows the OLT to participate in the bandwidth management.

16 Guidelines for voice over DSL

Voice over DSL shall be provided using VoATM or VoIP. Informative guidelines on Voice over DSL implementations may be found in Appendix IX.

16.1 VoATM

VoATM shall be provided using BLES in accordance with 9.8 and 10.6.

16.2 VoIP

The underlying IP connectivity may be established using one of the following:

- A Bridge connection as described in 9.1 and 10.4.1.
- A PPPoE connection as described in 9.2 and 10.4.2.
- A non-translated routed connection as described in 9.4 and 10.3.2.
- A translated routed connection as described in 9.3 and 10.3.1.

17 Management of the AN

17.1 OLT

The OAM functions of the AN shall be performed through the OLT via the M interface (see Figure 1). Remote operation and management of the AN shall be possible through an in-band connection to the OAM block, and may be possible through an out-of-band connection. The M interface may be vendor specific. However, an industry accepted management protocol, (e.g., SNMP, CORBA, CMIP) should be supported for operator specific management systems accessing the OAM block directly.

Access control MIB for digital broadcast service is described in 14.5.3 and in Annex B.

The OLT management shall be compliant with ITU-T Rec. H.611 [5].

17.2 ONU

The OAM block enables operation and management control of the ONU including the DSL drops. Operation shall be performed through an in-band connection.

The ONU management shall be compliant with ITU-T Rec. H.611 [5].

18 Management of the VTP/D

18.1 VTP/D management model

The VTP/D management model consists of classes with attributes that may require configuration within the VTP/D. The management model is expressed using the Unified Modelling Language (UML). The shaded areas in Figure 34 enable the management model to be related back to the VTP/D functional model blocks defined in clause 10. The classes with a dashed border are outside the scope of this Specification and are only shown here for completeness.

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

The DSL interface contains one or more **ATM PVC**s (Permanent Virtual Connection). If the ATM PVC uses AAL 2 or AAL 5, then the appropriate **AAL 5 Descriptor** or **AAL 2 Descriptor** is associated with the PVC, respectively. Each PVC is nominated to transport a particular type of flow which are defined in clause 9. This is indicated by an inheritance relationship to a flow class. A flow class may have attributes associated with it to provide configuration parameters related to that flow. In some cases a flow class may be empty and exists solely to provide an indication of the type of flow carried by an ATM PVC. The following additional relationships are exposed in terms of the management aspect of flows:

- The **Routed flow** can be of type **PPP** or **IPoA**. It can be translated or not translated.
- The **Bridged flow** can have zero or more **Bridge Filters** associated with it in order to support filtering of packets received on the flow. For example, a filter based on a packet being a PPPoE packet.

The VTP/D has a **DHCP Server,** which is used to allocate IP addresses to terminals on the residential network.

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

The following subclauses provide a description of the attributes associated with a selection of these classes.

The following subclauses provide a partial list of the managed attributes related to key classes of the management model. Only configuration related attributes are considered. Elements described in ITU-T Rec. H.611 [5] shall also be taken into account.

The definition of an FS-VDSL specific MIB is for further study.

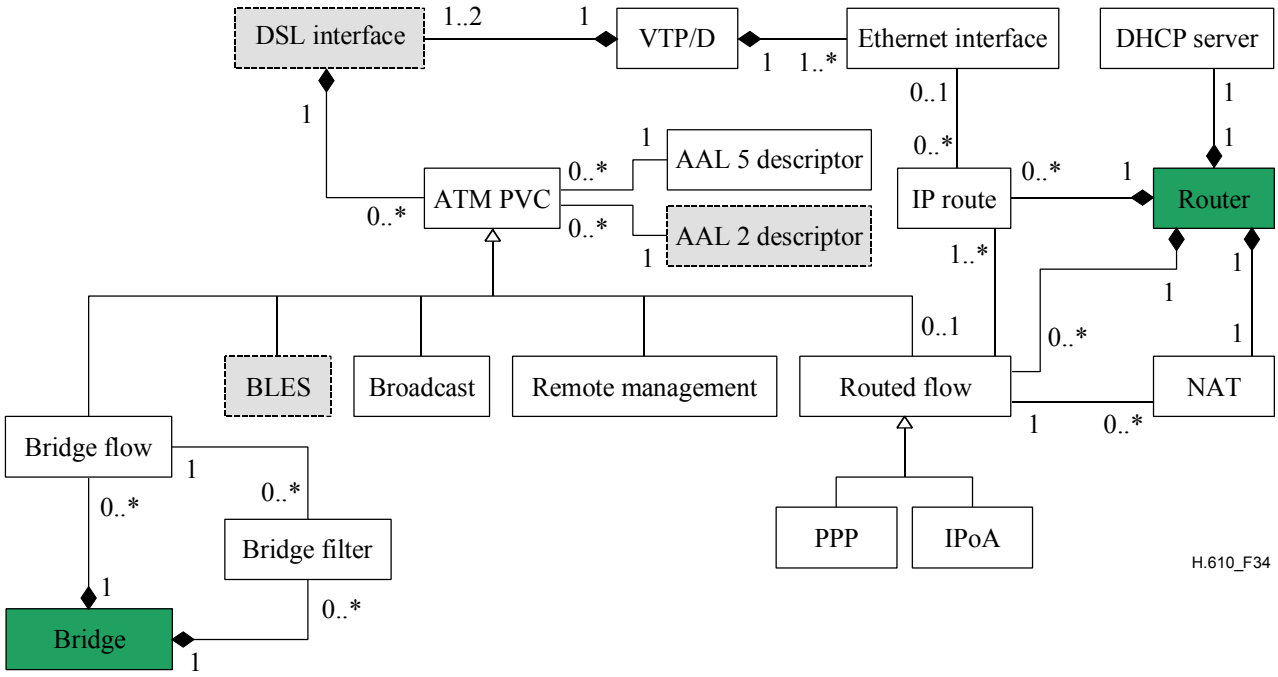


Figure 34/H.610 – VTP/D management information model

18.1.1 ATM PVC class

The attributes given in this subclause relate to the configuration management of the ATM PVC class. Note that when ILMI is available, most of the parameters in Table 22 will be redundant.

This is used to configure the traffic parameters for an ATM PVC as per ATM Forum Specification af-tm-0056.000 [2].

Table 22/H.610 – ATM PVC class

Attribute	Value	Note
DSL Interface	Fast, Interleaved	–
VPI	0-255	–
VCI	32-65535	–
F5 function	Endpoint, Segment, both, none	See ITU-T Rec. I.610
F4 function	Endpoint, segment, both, none	See ITU-T Rec. I.610
F4ccsink	On, off	–
F5ccsink	On, off	–
Encapsulation type	LLC/SNAP, VCMUX	–
AAL Type	AAL 2, AAL 5	–
ATM service category	CBR, UBR, VBRrt, VBRnrt	–
Peak cell rate	Any (Cells/s)	–
Sustainable cell rate	Any (Cells/s)	For VBR service only
Maximum burst size	Any (Cells)	For VBR service only

18.1.2 Broadcast class

The attributes given in Table 23 refer to the configuration management of the digital broadcast service function of the VTP/D.

Table 23/H.610 – Broadcast class

Attribute	Value	Note
IGMP Last Member Query Interval	1-100 (multiples of 100 ms)	See 14.4.2
IGMP Last Member Query Count	1-10	See 14.4.2
IGMP Unsolicited Report Interval	1-100 (multiples of 100ms)	See 14.4.2
Broadcast TV IP address	Any (class D IP address)	See 14.2
Broadcast TV IP mask	Any (IP address)	See 14.2
Channel change protocol	IGMPv2, DSMCC	See 9.5
MPEG Encapsulation	MPEG2AAL5, MPEG2UDP	–

18.1.3 Bridged flow class

The attributes related to the configuration management of a Bridge flow class are given in Table 24.

Table 24/H.610 – Bridged flow class

Attribute	Value	Note
VLAN tagging	On, off	–
Default VLAN tag	Any (Integer)	–

18.1.4 Bridge filter

The attributes related to the configuration management of the bridge Filter are given in Table 25.

Table 25/H.610 – Bridge filter

Attribute	Value	Note
Filter	On, off	–
Bridge Port	A reference to a bridge port	–

18.1.5 PPP class

The attributes related to the configuration management of a PPP class are given in Table 26.

Table 26/H.610 – PPP class

Attribute	Value	Note
PPP type	PPPoA, PPPoE	–
PPPoE Service-Name Tag	Any (text)	See RFC 2516. Not applicable if PPP Type is 'PPPoA'
PPPoE AC-Name Tag	Any (text)	See RFC 2516. Not applicable if PPP Type is 'PPPoA'
PPP default authentication protocol	None, CHAP, PAP	–
LCP echo request interval	Any (seconds)	–
PPP username	Any (text)	–
PPP password	Any (text)	–

18.1.6 IPoA class

The attributes related to the configuration management of an IPoA class are given in Table 27.

Table 27/H.610 – IPoA class

Attribute	Value	Description
IP Configuration	Dynamic, static	If the value is dynamic then the configuration is done using DHCP and the following two DHCP parameters are used in the DHCP messages.
DHCP Vendor Class Identifier option	Any (text)	See 12.2
DHCP User Class option	Any (text)	See 12.2
RIP v2	On, off	–

18.1.7 IP Route class

The attributes related to the configuration management of an IP route class are given in Table 28.

Table 28/H.610 – IP route class

Attribute	Value	Note
IP destination address	Any (IP address)	–
IP destination subnet mask	Any (IP address)	–
Interface	Reference to either a PPP class or an IPoA class or an IP interface on the residential network.	–
Metric	Any (Integer)	–

18.1.8 NAT class

The attributes related to the configuration management of the NAT class a re given in Table 29.

Table 29/H.610 – NAT class

Attribute	Value	Note
Downstream Port Type	UDP, TCP	–
Downstream Port Number	1-65535	–
Destination IP Address	Any IP address in the residential network (IP address)	–
PPP port identifier	Reference to a PPP port	–

18.1.9 DHCP server class

The attributes related to the configuration management of the DHCP Server are given in Table 30.

Table 30/H.610 – DHCP server class

Attribute	Value	Note
Subnet Address	Any (IP address)	–
Subnet Mask	Any (IP address)	–
IP address pool	Any within subnet defined above (IP address)	–
Primary DNS	Any (IP address)	–
Secondary DNS	Any (IP address)	–
DNS relay	On, off	This is needed where the primary and secondary DNS fields are not yet filled in and so cannot allocate to terminals in the residential network.

18.2 Configuration methods

The following are possible ways to configure a VTP/D. Different deployment scenarios may find different configuration schemes to be best fitted for their needs. Moreover, some deployment scenarios may require multiple configuration methods to co-exist. Clearly, the proposed configuration methods introduce a trade-off between the level of flexibility and the effort (i.e., complexity and overhead) associated with the configuration. Unless specifically specified, a method can be used to provide all layers of VTP/D configuration.

18.2.1 Pre-set configuration

The VTP/D shall be able to boot up and work with a pre-set configuration. This includes the cases of configuration set by the manufacturer for the first installation and a dynamic configuration stored on the unit's non-volatile memory before its last reset. This attribute enables the VTP/D to work in static environment where the network does not support dynamic means of configuration. In order to facilitate interoperability in the early stages of FS-VDSL deployments, a default FS-VDSL ATM configuration is defined. The default ATM configuration is specified in Table 31.

18.2.2 ILMI

ILMI ATM Forum Specification af-ilmi-0065.0000 is a tool dedicated and limited to ATM layer configuration. ILMI can define ATM connections and associate each one with essential ATM layer parameters like a traffic class, traffic descriptor, AAL type, encapsulation and even a service type. Since this Recommendation focuses on permanent VCs, the VTP/D shall support the ATM Forum and DSL Forum ILMI extensions for PVC as described in Specification af-nm-0122.000 and TRF 037. ILMI utilizes a predefined VC connection (i.e., 0,16) between the VTP/D and the Access Network.

The association between a PVC and specific functional processing (i.e., traffic flow) is achieved using the ILMI MIB field atmfAtmServiceName, which is a part of a service type object. The following are the FS-VDSL service names representing the 8 connection types described in clause 9 (with the same order).

- FS-VDSL-BRIDGE
- FS-VDSL-PPPOEFILTER
- FS-VDSL-TRANSROUTE
- FS-VDSL-NONTRANSROUTE
- FS-VDSL-CHANNELCHANGE
- FS-VDSL-BROADCAST
- FS-VDSL-RMMANAGE
- FS-VDSL-BLES

In addition, a few service sub-names values are defined in order to enhance the service definition. This is done using the atmfAtmServiceSubName, which is also part of the service type object in the ILMI MIB.

– DSMCC – relevant only for the FS-VDSL-CHANNELCHANGE flow.

– IGMPv2 – relevant only for the FS-VDSL-CHANNELCHANGE flow.

– MPEG2AAL5 – indicates that MPEG2 over AAL 5 encapsulation is used (i.e., ATM based delivery). Relevant for FS-VDSL-BROADCAST flow only.

– MPEG2UDP – indicates that MPEG2 over UDP encapsulation is used (i.e., IP based delivery). Relevant for FS-VDSL-BROADCAST flow only.

18.2.3 Remote management channel

A dedicated ATM VC is available on every VTP/D for the purpose of remote management, as defined in 9.7 and 10.7. The following configuration methods may be used over this connection.

18.2.3.1 SNMP

SNMPv2 IETF RFC 3416 may be used for remote management and configuration of the VTP/D. SNMP is a well-known full-scale management protocol suitable for a highly dynamic management environment. SNMP provides the ability to set and query the value of specific objects within a large set of database tables. It also supports means for the managed entities to initiate notifications (i.e., SNMP Traps) towards the management systems indicating faulty conditions. SNMP operations are based on a common knowledge of the internal organization of the database tables, called SNMP MIBs, residing in the managed entities.

This Recommendation does not define a specific SNMP MIB for the VTP/D. Thus, an SNMP implementation for the VTP/D should use as far as possible the relevant existing standard MIBs, such as MIB II IETF RFC 1213 [I-13] for basic interface and system definitions, the Interface MIB IETF RFC 2863 [25] for logical and physical interfaces definition and the AToM MIB IETF RFC 2515 [26] for ATM layer definitions.

18.2.3.2 Configuration file

Unlike SNMP, this method is not intended for a step-by-step configuration but rather for performing bulk configuration operations. The configuration file is downloaded to the VTP/D using TFTP.

An FS-VDSL configuration file format is specified in Annex A. The format is based on TLV (Type, Length, Value) definitions and includes all parameters needed for the basic configuration of the VTP/D. The format also provides the possibility for vendors to extend the basic configuration options with vendor specific attributes.

18.2.3.3 Other methods

Other methods, such as Local management, may be used as described in ITU-T Rec. H.611 [5].

18.3 VTP/D configuration sequence

One straightforward way to configure the VTP/D is bottom-up according to the protocol stack layers. Namely, at first the physical layer, DSL, is configured. Second, the ATM layer is configured. Third, the Ethernet and IP, and the services (e.g., digital broadcast etc.) are last. However, this sequence cannot be performed when using the remote management channel for configuration (e.g., SNMP, file, etc.) because the IP configuration of the VTP/D remote management connection (i.e., DHCP) shall be completed before a file transfer or an SNMP transaction can be invoked. This emphasizes the need for the default remote management connection to always be present.

Another issue concerning the configuration sequence is the order of precedence between several management tasks that may configure the same protocol layer. The following subclause discusses this issue with respect to the ATM layer.

18.3.1 ATM configuration sequence

Since multiple management processes may be running simultaneously on the VTP/D and each could be used to configure the ATM parameters on the VTP/D, then the state machine shown in Figure 35 shall be used in order to avoid conflict for ATM layer configuration. The state machine specifies that ILMI based configuration can override remote management flow based ATM configuration during the operation of the VTP/D. However, the reverse is not true, i.e., when ILMI connectivity has been established once the VTP/D shall never accept an ATM configuration via the remote management channel even if subsequently ILMI connectivity is lost. The only manner in which the VTP/D can be forced to retry an ATM configuration via the remote management channel is by restarting the VTP/D.

Note also that a local management interface shall be disabled for ATM layer configuration if ILMI or a downloaded configuration file is used.

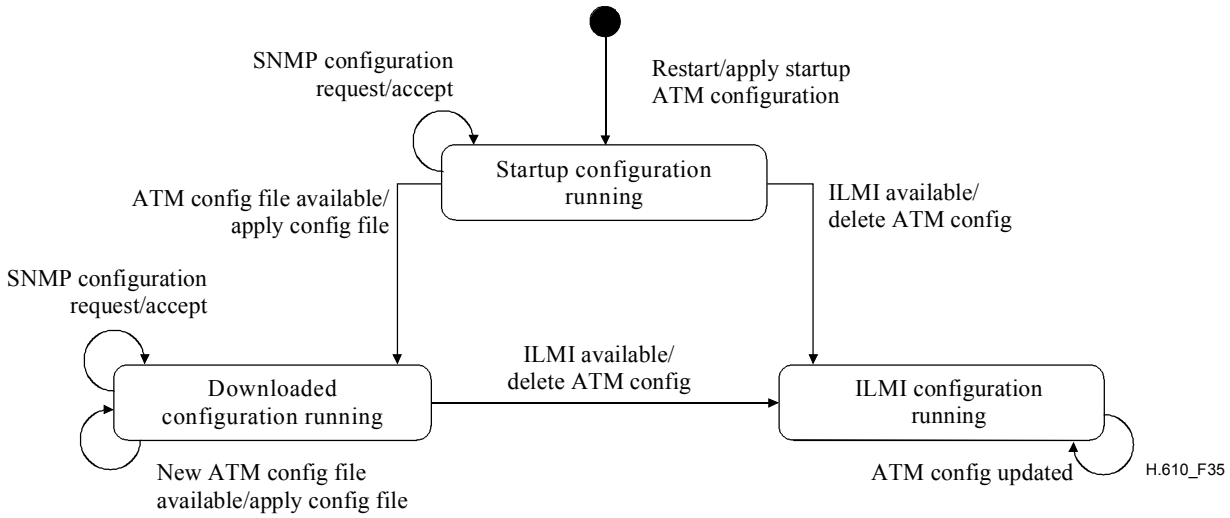


Figure 35/H.610 – State machine for the VTP/D ATM layer configuration

The states and transitions are described below.

Initial state: This represents the VTP/D in the down state. There is only one transition from this state.

- *Restart*: The VTP/D is restarted. As a result the start-up configuration is applied. The start-up configuration may either be the last running configuration (if there was one) or in the case of an initial start up, the default configuration given in Table 31 shall be used. The VTP/D then moves to the Start-up configuration running state.

Start-up configuration running state: This state represents a running ATM layer, which was configured using a start-up configuration. In this state the higher layers associated with any configured and available VCCs may be manipulated. There are three possible transitions from this state.

- *ILMI available*: If ILMI connectivity is established, then the existing ATM configuration is deleted and the VTP/D transitions to the ILMI configuration running state.
- *ATM config file available*: If an ATM configuration file is downloaded across the remote management flow, then this configuration is applied (overwriting the existing configuration) and the VTP/D moves to the Downloaded configuration running state.
- *SNMP configuration request*: If an SNMP configuration request is received, then this shall be accepted according to the SNMP protocol and rules of the VTP/D MIB. The VTP/D remains in this state.

ILMI configuration running state: This state represents a running ATM layer configured using ILMI. In this state the higher layers associated with any configured and available VCCs may be manipulated. Once in this state the VTP/D cannot use the remote management channel for configuration of the ATM layer, even if the ILMI connectivity is lost. ILMI has many states. Only one is shown to clarify that ILMI can be used to update ATM layer configuration once it is in this state.

Downloaded configuration running state: This state represents a running ATM layer configured using a configuration file received across the remote management flow. In this state the higher layers associated with any configured and available VCCs may be manipulated. There are three possible transitions from this state.

- *SNMP configuration request*: If an SNMP configuration request is received, then this shall be accepted according to the SNMP protocol and rules of the VTP/D MIB. The VTP/D remains in this state.
- *New ATM config file available*: If a new ATM configuration file is downloaded across the remote management flow, then this configuration is applied (overwriting the existing configuration) and the VTP/D remains in this state.
- *ILMI available*: If ILMI connectivity is established, the existing ATM configuration is deleted and the VTP/D transitions to the ILMI configuration running state.

Table 31/H.610 – Default ATM configuration scheme

Connection type	ATM traffic descriptor	Details
Broadcast	VPI/VCI = 1/33 Traffic Type: CBR uni-d	Default values are required only for IGMP based channel change.
Broadcast	VPI/VCI = 1/34 Traffic Type: CBR uni-d	Default values are required only for IGMP based channel change.
Broadcast	VPI/VCI = 1/35 Traffic Type: CBR uni-d	Default values are required only for IGMP based channel change.
Broadcast	VPI/VCI = 1/36 Traffic Type: CBR uni-d	Reserved for non-video traffic. Default values are required only for IGMP based channel change.
Channel change	VPI/VCI = 1/32 Traffic Type: CBR bi-d sym PCR = 42 cells/s	–
Bridged	VPI/VCI = 0/32 Traffic Type: UBR bi-d	–
Bridged	VPI/VCI = 0/33 Traffic Type: UBR bi-d	–
Bridged	VPI/VCI = 0/34 Traffic Type: UBR bi-d	–
Bridged	VPI/VCI = 0/35 Traffic Type: UBR bi-d	–
PPPoE	VPI/VCI = 0/62 Traffic Type: UBR bi-d	–
Non-translated routed	VPI/VCI = 0/42 Traffic Type: UBR bi-d	–
Non-translated routed	VPI/VCI = 0/43 Traffic Type: UBR bi-d	–
Non-translated routed	VPI/VCI = 0/44 Traffic Type: UBR bi-d	–
Non-translated routed	VPI/VCI = 0/45 Traffic Type: UBR bi-d	–
Translated routed	VPI/VCI = 0/63 Traffic Type: UBR bi-d	–

Table 31/H.610 – Default ATM configuration scheme

Connection type	ATM traffic descriptor	Details
BLES	VPI/VCI = 0/40 Traffic Type: CBR bi-d sym PCR no default value is specified.	This VC is optional.
ILMI channel	ATM Forum defaults for ILMI channel (VPI/VCI = 0/16 bi-d sym)	–
Remote management channel	VPI/VCI = 0/50 Traffic Type: VBRnrt bi-d sym PCR = 100 cells/s SCR = 50 cells/s MBS = 50 cells	–
NOTE – bi-d = bidirectional connection, uni-d = unidirectional connection, sym = symmetric bandwidth parameters.		

Annex A

Configuration file format

In this annex the format and use of the VTP/D configuration file is defined. The configuration file can be used to configure the VTP/D from a remote management system through the remote management connection.

The configuration file shall be in TLV (Type, Length, Value) format. The TLV types and subtypes providing basic VTP/D configuration are described in Table A.1. Proprietary extensions to the definitions given here are allowed through the use of a special TLV type (127).

The configuration file is regarded as a sequence of octets, where the least significant bit of the octet is bit 1 and the most significant bit is bit 8.

The following general rules apply when dealing with a configuration file:

1) TLV Type and SubTLV Type fields are 1 byte long.
2) TLV Length and SubTLV Length fields are 1 byte long.
3) If a TLV type is not present in the configuration file, the default value for the parameter specified by that TLV type shall be retained.
4) Each TLV definition can contain only one occurrence of a certain sub TLV.
5) Sub TLVs in a TLV are ordered by increasing sub TLV type.
6) Not all sub TLVs of a certain TLV type are mandatory; some combinations may even make no sense. However, no guidelines are given here except for the use of common sense.
7) TLV definitions can be repeated to define more entities of the same type.
8) Parameters are set in the order they occur in the configuration file.
9) Values of *index* sub-TLVs shall be unique per TLV type.
10) Unrecognized TLVs or sub-TLVs shall be silently ignored.

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes
Pad			0	N.A.			N.A.	This special TLV has no Length nor Value fields. Used to pad the file to an integral number of words, if necessary. It is placed after the end of data field (TLV type = 255).
ATM Traffic Descriptor			1	Variable (Sum of sub TLV fields)			Composition of sub TLVs	This TLV is repeated once per ATM Traffic Descriptor definition
	Index				1	1	Any	
	ATM Traffic Class				2	1	0..3 (0 = CBR, 1 = UBR, 2 = VBRrt, 3 = VBRnrt)	
	PCR	*[Cells/s]*			3	1..3	Any	
	SCR	*[Cells/s]*			4	1..3	Any	
	MBS	*[Cells]*			5	1, 2	Any	
ATM Port			2	Variable (sum of sub TLV fields)			Composition of sub TLVs	This TLV is repeated once per ATM Port definition.

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes
	Index				1	1	Any	
	Path				2	1	0, 1 (0 = Fast, 1 = Interleaved)	
	VPI				3	1, 2	0..4095	
	VCI				4	1, 2	0..65535	
	ATM Traffic Descriptor				5	1	Any	
	F4 ccsink				6	1	0, 1 (0 = disabled, 1 = enabled)	
	F5 ccsink				7	1	0, 1 (0 = disabled, 1 = enabled)	
	AAL type				8	1	2, 5	
	Encapsulation				9	1	0, 1 (0 = VCMUX, 1 = LLC/SNAP)	
	Protocol				10	1	0..3 (0 = Ethernet, 1 = IPoA, 2 = PPPoA, 3 = PPPoE)	

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes	
	Connection type				11	1	0..7 (0 = Bridge, 1 = PPPoE, 2 = translated route, 3 = non-translated route, 4 = channel change, 5 = management, 6 = broadcast, 7 = BLES)		
	Connection subtype				12	1	0..3 (0 = DSM-CC, 1 = IGMPv2, 2 = MPEG2AAL5, 3 = MPEG2UDP)		
Router Port			3	Variable (Sum of sub TLV fields)			Composition of sub TLVs		This TLV is repeated once per Router port definition
	Index				1	1	Any		
	ATM port index				2	1	Any		
	IP configuration				3	1	0, 1 (0 = Static, 1 = Dynamic)		
	IP static address				4	4	Any		
	IP static mask				5	4	Any		

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes	
	PPP default authentication protocol				6	1	0..2 (0 = none, 1 = PAP, 2 = CHAP)		
	LCP echo interval	*[Seconds]*			7	1	Any		
	IPCP VTP address offered by VTP				8	4	Any		
	PPP login ID				9	Any	Any text	UTF-8 encoded text IETF RFC 2279 [24]	
	PPP password				10	Any	Any text	UTF-8 encoded text IETF RFC 2279 [24]	
	PPPoE service name				11	Any	Any text	UTF-8 encoded text IETF RFC 2279 [24]	
	PPPoE access concentrator name				12	Any	Any text	UTF-8 encoded text IETF RFC 2279 [24]	
	NAT/PAT activation				13	1	0, 1 (0 = enable, 1 = disable)		

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes
	RIP activation				14	1	0, 1 (0 = enable, 1 = disable)	
	MTU size				15	1, 2	0..1500	
NAT/PAT downstream port to local address mapping			4	Variable (Sum of sub TLV fields)			Composition of sub TLVs	This TLV is repeated once per port-address mapping.
	Downstream port number				1	1, 2	Any	
	Local IP address				2	4	Any	
Bridge Port			5	Variable (Sum of sub TLV fields)			Composition of sub TLVs	This TLV is repeated once per Bridge Port definition.
	ATM Port index				1	1	Any	
	Filter actions				2	1	0, 1 (0 = none, 1 = PPPoE)	
	VLAN tagging				3	1	0, 1 (0 = enable, 1 = disable)	
	Default VLAN tag				4	4	Any	

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes
Routing			6	Variable (Sum of sub TLV fields)			Composition of sub TLVs	
	Destination address				1	4	Any	This TLV is repeated once per static route definition.
	Destination mask				2	4	Any	
	Next hop address				3	4	Any	Sub TLVs 3 and 4 are mutually exclusive.
	Router port index				4	1	Any	
	Metric				5	1	Any	
DHCP server			7	Variable (Sum of sub TLV fields)			Composition of sub TLVs	
	Subnet address				1	4	Any	
	Subnet mask				2	4	Any	
	Pool base IP address				3	4	Any	
	Number of pool IP addresses				4	1, 2	Any	

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes
	DNS relay activation				5	1	0, 1 (0 = enable, 1 = disable)	
	Primary DNS				6	4	Any	
	Secondary DNS				7	4	Any	
Channel Change engine			8	Variable (Sum of sub TLV fields)			Composition of sub TLVs	
	Channel change protocol				1	1	0, 1 (0 = DSM-CC, 1 = IGMPv2)	
	Last Member Query Interval	*[1/10 seconds]*			2	1	Any	
	Last Member Query Count				3	1	Any	
	Unsolicited Report Interval	*[1/10 seconds]*			4	1	Any	
	Broadcast channels Class D IP subnet				5	4	Any	
	Broadcast channels Class D IP netmask				6	4	Any	

Table A.1/H.610 – Configuration file format

Name	Sub-name	Units	Value of TLV type tag	Value of TLV length tag	Value of SubTLV type tag	Value of SubTLV length tag	Value of (Sub)TLV value tag	Notes	
Vendor specific options			127	Variable (Sum of sub TLV fields)			Composition of sub TLVs		This TLV is repeated per each set of vendor specific attributes. It can be included as sub TLV of TLV types 1 to 8.
	Vendor code				1	6	Any	IEEE assigned Organization Unique Identifier (see Appendix X); if not available, this sub TLV shall not be used	
	Vendor option 1				2	Vendor specific	Vendor specific		
	Vendor option n				n + 1	Vendor specific	Vendor specific	$n \leq 254$	
Conf file integrity check			254	20			Any	The value field is the 160-bit SHA FIPS 180-1 hash of all preceding bytes of the configuration file. It is placed just before the End of data marker (TLV type = 255)	
End of data marker			255	N.A.			N.A.	This special TLV has no Length nor Value field. It is placed at the end of the file, before any pad fields (TLV type = 0).	

Annex B

SNMP MIB for the channel change function

This annex defines the SNMP IETF RFC 3416 [29] 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 14.5.

B.1 Relationship to other MIBs

The CCF MIB contains references to the following SNMP MIBs:

- The interface MIB IETF RFC 2863, used by the OLT to describe the V reference point 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.
- The ATM MIB IETF RFC 2515, used by the OLT to describe the ATM VCC replication points for the broadcast entertainment services at the V reference point. The channelTable makes reference to the ATM VCC in order to enable the CAC function to check the bandwidth requirements of a broadcast channel.

B.2 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  18479  }
        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 shall 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 shall 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 shall
         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 shall 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 shall
         be zero (0)."
    ::=  {  customerEntry  1  }


customerPortIdOBJECT-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 shall 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 shall be an integer multiple of 10kbps
         and shall 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 shall 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 2047
         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 shall be 1. In order to revoke entitlement to channel with
         entitlementIndex y, the value of bit y in this bitmap shall 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 shall 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 shall
         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
         shall be immediately disconnected and further join requests from this customer
         shall 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
        less 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
        shall 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 shall 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 shall
        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 shall 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 shall 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 I

VTP implementation examples

This appendix provides an example of VTP implementation.

I.1 Upstream protocol processing

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

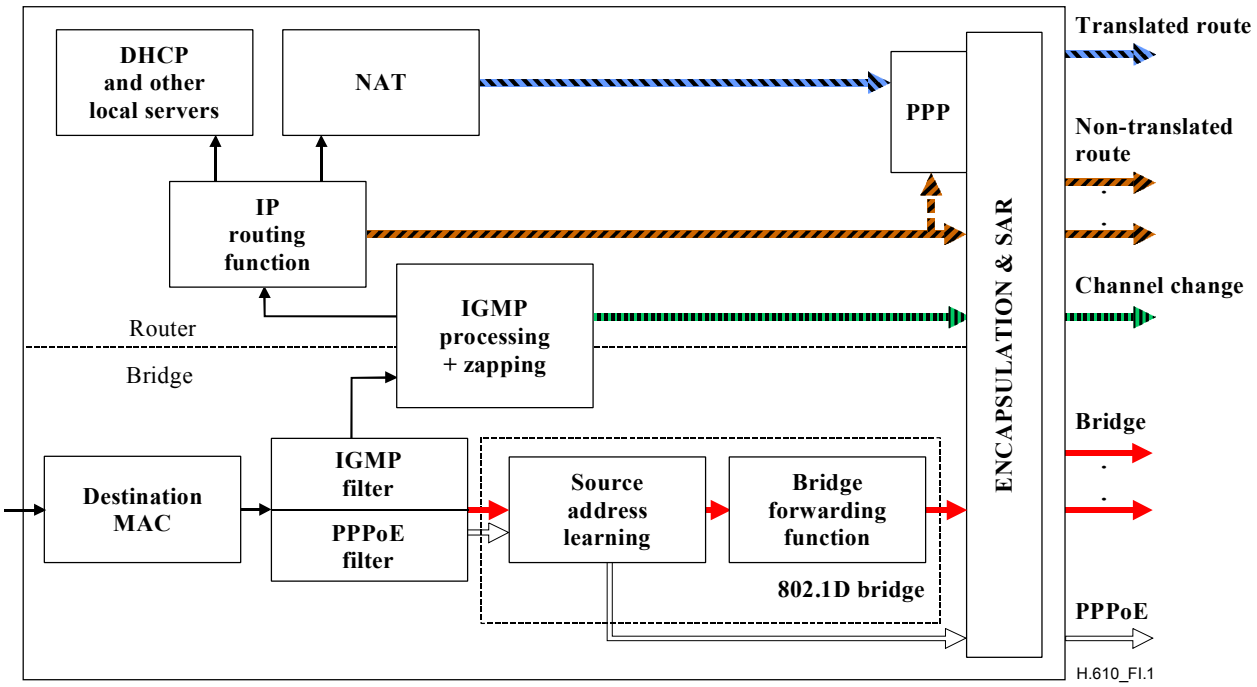


Figure I.1/H.610 – VTP upstream protocol processing

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

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

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

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

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

I.2 Downstream protocol processing

Figure I.2 describes the protocol processing that is performed in the downstream direction. The first block is the Encapsulation and SAR block, which performs the ATM reassembly, the AAL sublayer processing and the RFC 2684 de-capsulation. The ATM VCs of the broadcast TV are relevant only to the downstream, since they are unidirectional (i.e., point-to-multipoint ATM VCs). Frames received on the digital broadcast VCs are sent directly to the MAC driver for transmission. Frames coming from the PPPoE VC are forwarded to the Bridge forwarding block (i.e., this is required when multiple physical ports are available towards the residential network). Frames from Bridged VCs are first passed through the Bridging function (i.e., forwarding and learning) and then sent for transmission. Routed packets are handled by the IP routing function (e.g., ARP etc.) and then forwarded to the MAC driver. The same treatment is given to locally generated packets, like DHCP responses. The PPP block handles the PPP sessions running over the routed connections. Packets at the output of the PPP block are sent to the routing function either directly or through the NAT block, which performs network and port address translations.

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

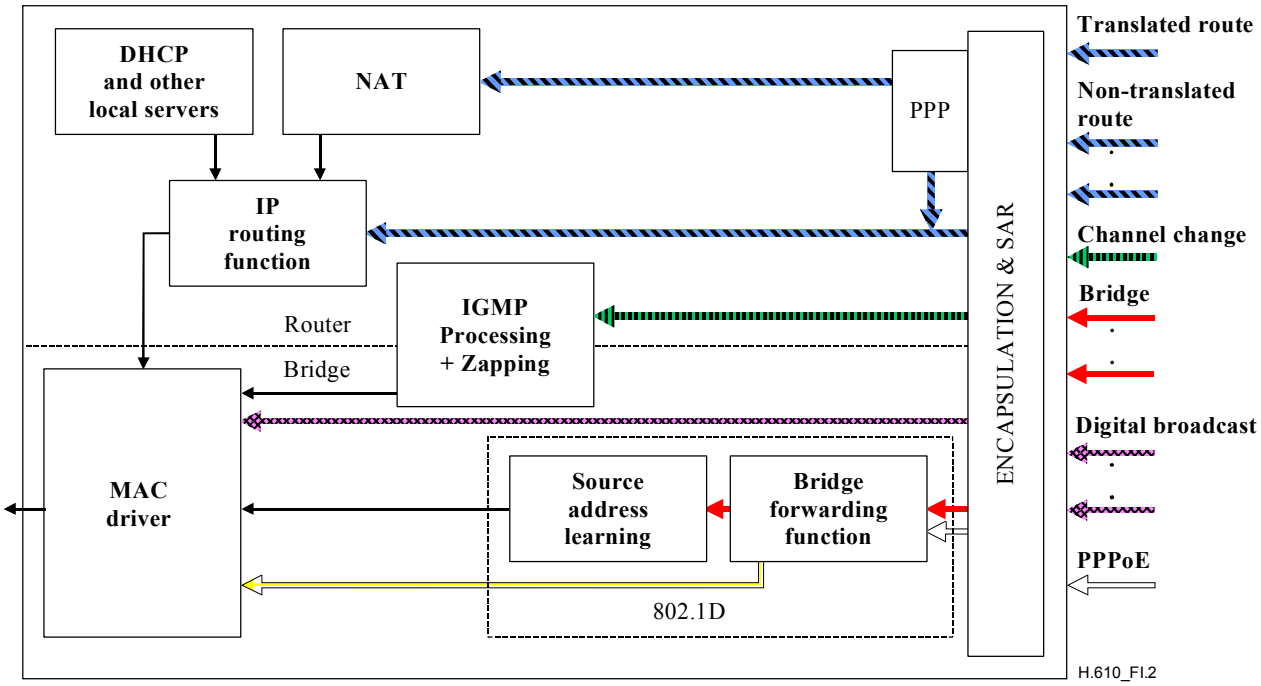


Figure I.2/H.610 – VTP downstream protocol processing

Appendix II

IGMPv2 to DSMCC translation function

This appendix describes how the VTP/D may interwork with the two channel change protocols, IGMPv2 and DSM-CC. The interworking would be performed by an IGMPv2-DSM-CC interworking function within the VTP/D as described in Figure II.1 below.

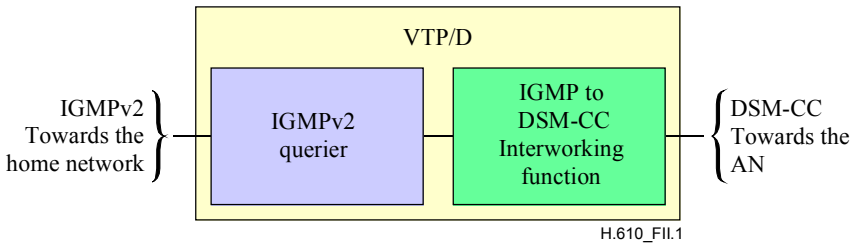


Figure II.1/H.610 – VTP/D DSM-CC channel change functional architecture

For the purpose of the following discussion, it is assumed that all IGMPv2 messages processed by the IGMPv2 Querier are related to the digital broadcast service.

The IGMPv2 Querier function keeps track of the state of each active multicast channel as defined in clause 14. 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 provide a faster channel change and thereby may improve the overall channel change switch over time. Also, it may improve 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 is started. This timer may have a default value of a 200 ms.
- If a Join message is received while the "Join_Anticipation" timer is running, then the timer will be cancelled. This will be followed by the generation of a DSM-CC ProgramSelect message specifying the session identity associated with the old channel and the new Broadcast Program Id (BPID) that is required. Note that this behaviour might not be optimal for deployment scenarios where multiple multimedia streams are simultaneously transmitted to the same VTP/D.
- 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 specifying the session identity associated with the channel that is no longer required and a BPID of "0".

NOTE – The BPID is determined from the IP class D multicast address.

The optimization described above enables multiple digital broadcast streams to be received simultaneously.

Appendix III

VDSL dual latency channel support

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 2 ms), but a higher Bit Error Ratio (BER) that can be caused by impulse noise in comparison to an "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.

For 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 Table III.1 below provides a possible mapping of applications to the VDSL dual latency channel. Selecting one latency channel or the other clearly presents a trade-off between delay and bit error sensitivity.

Table III.1/H.610 – Typical mapping of applications to VDSL dual latency channels

Application	Delay sensitive	Bit Error Ratio (BER) sensitive	VDSL dual latency channel
Voice	Yes (Note 1)	No (Note 2)	Fast channel preferred.
Channel Change	Yes	Yes	Neither channel is ideally suitable. A trade off must be made as to whether delay or bit error ratio is the more significant factor.
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 ratio is the more significant factor.

NOTE 1 – It is commonly agreed that up to 150 ms mouth to ear delay can be tolerated with virtually no quality degradation, if echo cancellation 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, packetization delay, queuing delay, etc.

NOTE 2 – Depending on chosen voice codec.

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 is then 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 is 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 has to 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. Note that it is not mandatory for the VTP/D and ONU to support more than one latency channel.

Appendix IV

Advanced IP scenarios

This appendix describes advanced scenarios for the residential network configuration and complements to what is described in clause 12.

IV.1 Advanced IP processing scenarios

If the VTP/D has more than one external routed connection and/or there are more than one IP subnetwork in the residential network, the IP processing scenario can no longer be configured as one of the standard scenarios. This subclause describes the default configuration of advanced scenarios, which can include a wide variety of IP networking situations.

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

For the IP forwarding function, these default configurations basically work as follows:

- If there is only one IP subnetwork, each additional external connection will result in at least one additional route in the forwarding table.
- If there is more than one IP subnetwork, the IP forwarding function uses the concept of virtual routers to separate the routes in the forwarding table so that each route is only associated with one IP subnetwork.

  NOTE – This requires that each external connection is uniquely associated with an IP subnetwork.

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

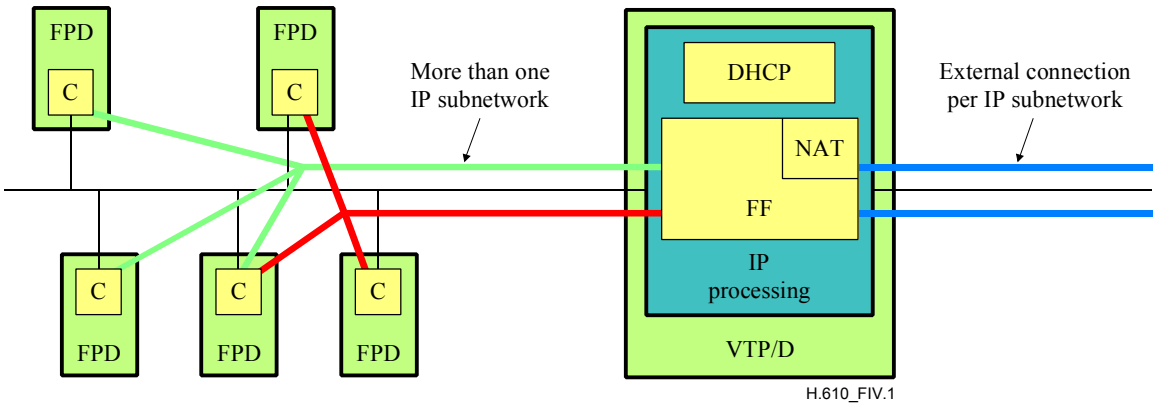
IV.1.1 Adding of an additional IP subnetwork

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

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

Each IP subnetwork is therefore treated as if it were a standard scenario from the default configuration point of view with the exception that the trigger to create any additional IP subnetwork cannot be wholly automated and will require some external stimulus. While some

intelligent interpretation could be made from parameters negotiated over an external connection using PPP or DHCP, the expectation is that this trigger will ultimately come from the management interface.



C Client
FF Forwarding function

Figure IV.1/H.610 – Advanced scenario – Adding an IP subnetwork

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

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

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

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

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

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

Table IV.1 shows the example of the forwarding table resulting from the addition of an external routable IP subnetwork to a standard scenario with an IP subnetwork with exclusive private address space and Table IV.2 shows the associated access control lists for each virtual router.

Table IV.1/H.610 – Example forwarding table with IP subnetwork added to a standard exclusive private address space scenario

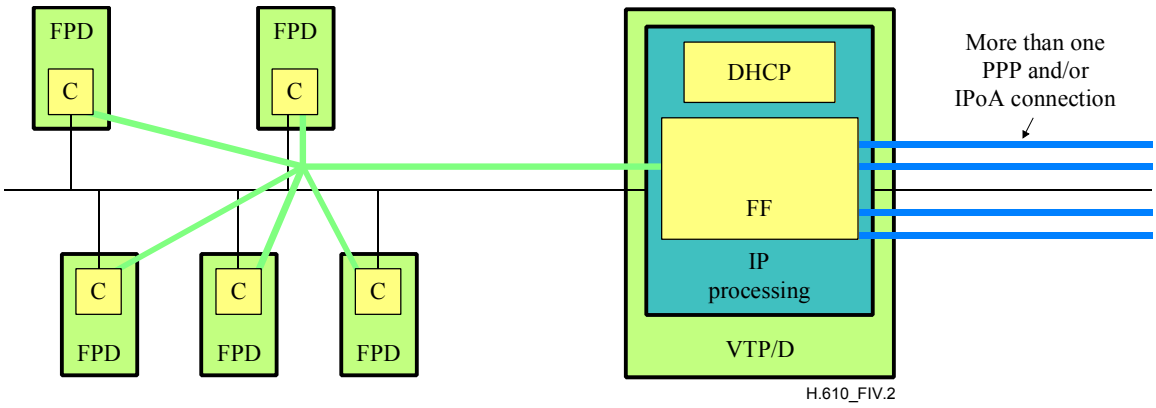
Virtual router ID	Destination address range		Masquerading	Outgoing Layer 2 interface
	Destination address	Subnet mask		
0	192.168.0.0	255.255.255.0	No	Residential network interface, e.g., eth0
0	127.0.0.0	255.0.0.0	No	VTP/D – loop-back route
0	Default route		Yes	External translated routed connection, e.g., ppp0
1	x.x.x.x (derived from IPCP or DHCP)	s.s.s.s (derived from default, IPCP or DHCP)	No	Residential network interface, e.g., eth1
1	127.0.0.0	255.0.0.0	No	VTP/D – loop-back route
1	Default route		No	External non-translated routed connection, e.g., ppp1 or ipoa0

Table IV.2 /H.610 – Example access control lists with IP subnetwork added to a standard exclusive private address space scenario

Source address range		Incoming Layer 2 interface	Virtual router ID
Source address	Subnet mask		
192.168.0.0	255.255.255.0		0
		External translated routed connection, e.g., ppp0	0
x.x.x.x (derived from IPCP or DHCP)	s.s.s.s (derived from default, IPCP or DHCP)		1
		External non-translated routed connection, e.g., ppp1 or ipoa0	1

IV.1.2 Adding of an additional external connection to an IP subnetwork

The first scenario to consider is the case of adding additional connections to a standard scenario IP subnetwork. This is illustrated in Figure IV.2 below.



C Client
FF Forwarding function

Figure IV.2/H.610 – Adding additional connections to an IP subnetwork

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

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

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

The consequence of the above rules for adding addition external PPP connections for the PPP parameters and negotiation with the far end is captured in Table IV.3.

Table IV.3/H.610 – Default configuration parameters for a subsequent PPP connection to an IP subnetwork

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

An example of forwarding table is shown in Table IV.4. This example is where the IP subnetwork has externally routable address space, the external connection uses PPP and its IPCP does pass a subnetwork mask.

Table IV.4/H.610 – Default IP forwarding function parameters after the addition of a PPP external Connection to an IP subnetwork with externally routable address space

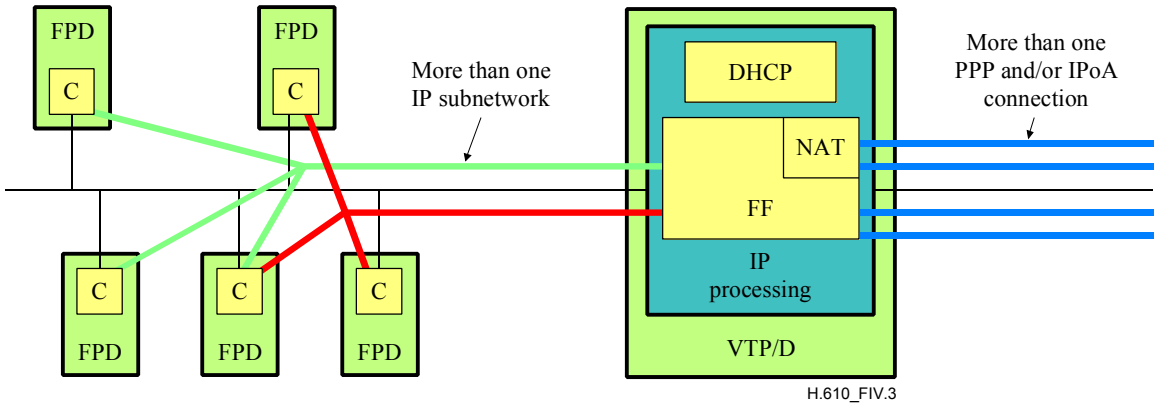
Destination address range		Masquerading	Outgoing Layer 2 interface
Destination address	Subnet mask		
x.x.x.x (derived from subnetwork parameters)	s.s.s.s (derived from subnetwork parameters)	No	Residential network interface, e.g., eth0
y.y.y.y (derived from address passed by IPCP on additional connection)	y.y.y.y (parameter passed by IPCP on additional connection)	No	Additional external connection, eg ppp1
127.0.0.0	255.0.0.0	No	VTP/D – loop-back route
Default route		No	External connection, e.g., ppp0 or ipoa0

If IPoA is used for an additional connection to an IP subnetwork, then the default is that no new entries are automatically added to the forwarding table and all additions are added using static provisioning through the management interface. The default parameters for the additional connection using IPoA are given in Table IV.5.

Table IV.5/H.610 – Parameters for subsequent IPoA connection to a subnetwork

Parameter	Default	Reconfiguration
Encapsulation	IPoA (RFC 2684 routed mode)	No
Configuration protocol	None	No
Routing Protocol	Static routing	Enabling of optional RIPv2

Further scenarios are created when there is more than one IP subnetwork as illustrated in Figure IV.3 below.



C Client
FF Forwarding function

Figure IV.3/H.610 – Adding additional connections to an IP subnetwork when there is more than one IP subnetwork

Using the rules for creating additional subnetworks, these scenarios can be described as multiple instances of the first scenario shown in Figure IV.1, as the IP subnetworks are kept entirely separate using virtual routers.

Appendix V

Message sequence charts

This appendix proposes a set of example message sequence charts (MSCs) describing several common scenarios that the VTP and the FS-VDSL network are required to support.

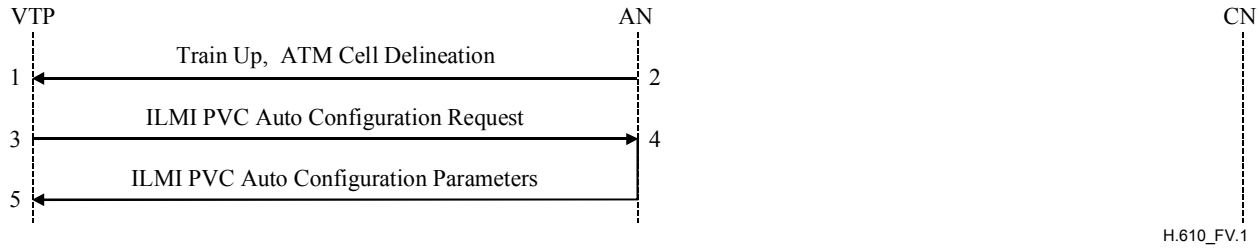
Each of the MSCs is annotated to provide a description of the high level procedures to assist in the understanding of the MSCs.

V.1 Start-up of the VTP

The scenario describes the flow that occurs when a VTP undergoes 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 cells 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 configured and the traffic descriptor associated with each of these ATM VCs.

4 The AN responds with the ATM VC configuration parameters. See Specification af-ilmi-0065.00 for further details of the procedures.

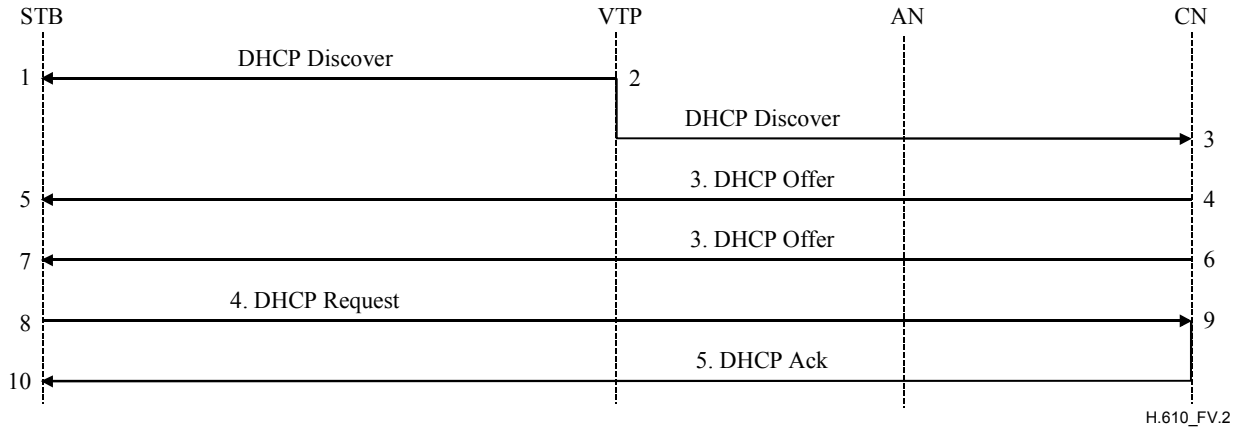
5 The VTP stores the ATM configuration parameters that identify the ATM VCCs that have been set up and their corresponding traffic descriptors.

V.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 as described in 10.3.4.

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 is received and 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 as described in 10.3.4. 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 recognizes its 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:

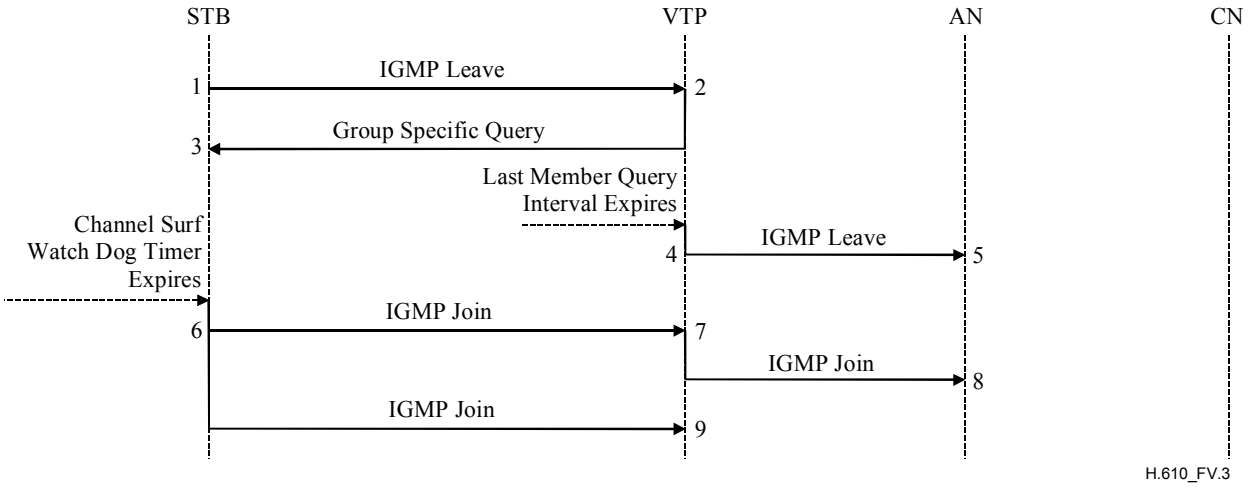
- Download its software image using mechanisms such as TFTP/FTP.
- Broadcast TV and VoD channel selection as described in the latter MSCs.
- Internet browsing.

V.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 boot-up 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 that 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 performs channel surfing.

NOTE 1 – The running and the value of this timer is implementation dependent and is outside the scope of the Recommendation.

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 to generate a second IGMP in order to cover the case the first one is lost (as specified by the robustness variable in IETF RFC 2236).

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 DSL 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 DSL drop for the specified channel. If there is 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.

NOTE 2 – The VTP filters any IGMP messages received over the T_{CN} interface that match any of the multicast addresses associated with the broadcast TV stream.

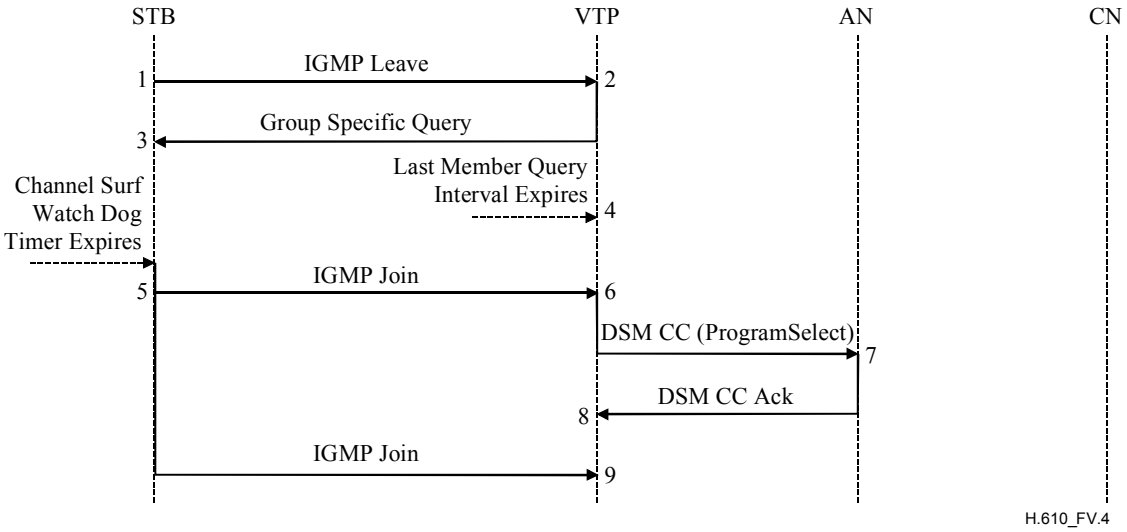
NOTE 3 – IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

V.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 boot-up of the VTP and STB.
- The STB is receiving a broadcast TV channel.



1 As per step 1 of sequence V.3.

2 As per step 2 of sequence V.3.

3 As per step 3 of sequence V.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 its existing multicast group and re-connects the broadcast ATM VC to the new multicast group. This optimizes the performance of the AN.

To achieve the optimization the "JoinAnticipation" timer has to be chosen to be greater than the "Channel Surf Watch Dog" timer run by the STB.

5 As per step 6 of sequence V.3.

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 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 T_{CN} interface.

9 As per step 9 of sequence V.3.

NOTE 1 – The VTP filters any IGMP messages received over the T_{CN} interface that match any of the multicast addresses associated with the broadcast TV stream.

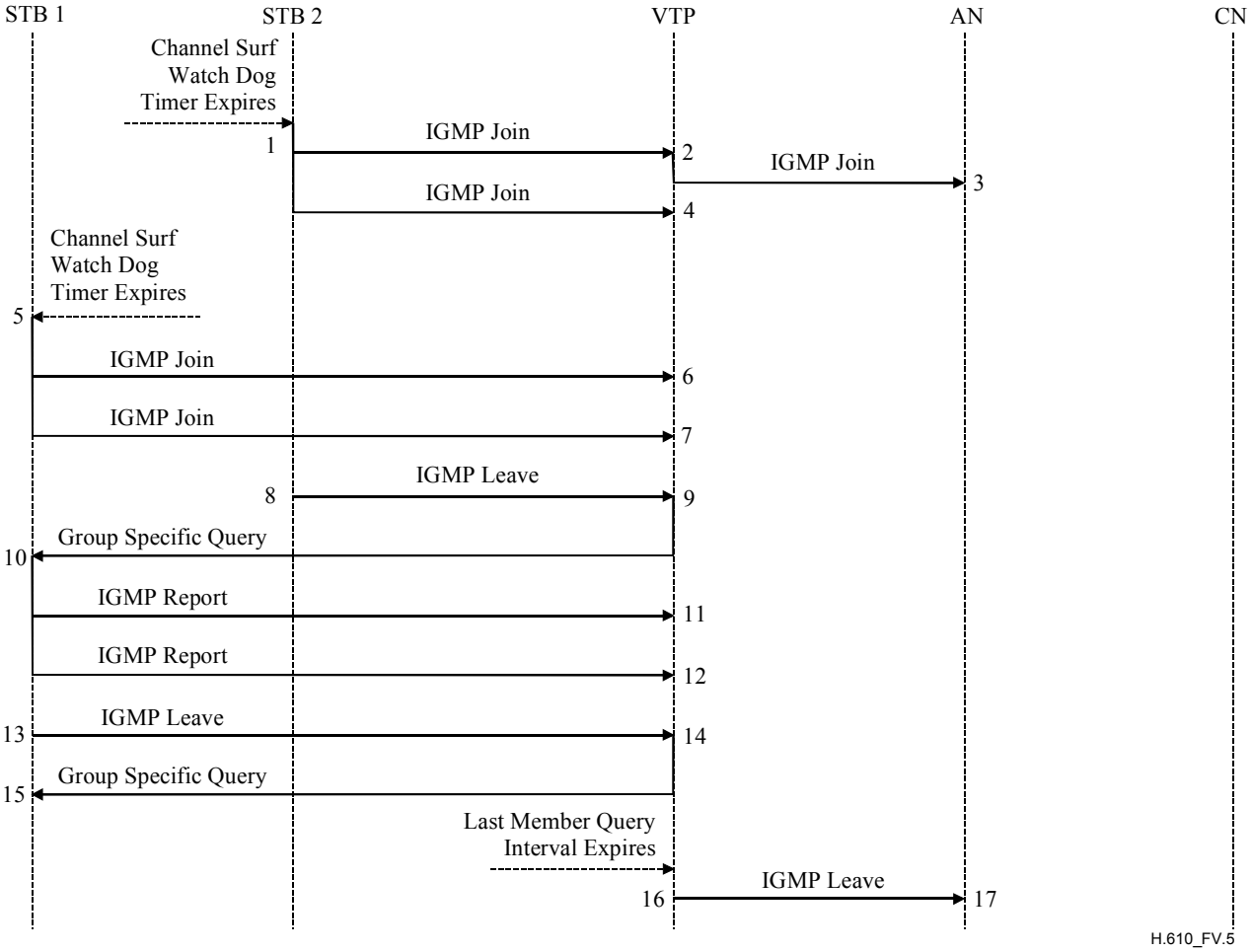
NOTE 2 – DSCM CC messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

V.5 Multiple STB broadcast TV surfing – IGMP between VTP and AN

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

Pre-conditions:

- Successful boot-up 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 RFC 2236).

2 As per step 7 of sequence V.3.

3 As per step 8 of sequence V.3.

4 As per step 9 of sequence V.3

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 RFC 2236).

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 step 6 of sequence V.3.

8 End User 2/STB2 disconnects from broadcast TV channel. STB 2 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 in 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 RFC 2236).

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/STB 1 disconnects from broadcast TV channel. STB 1 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.

NOTE 1 – The VTP filters any IGMP messages received over the T_{CN} interface that match any of the multicast addresses associated with the broadcast TV stream.

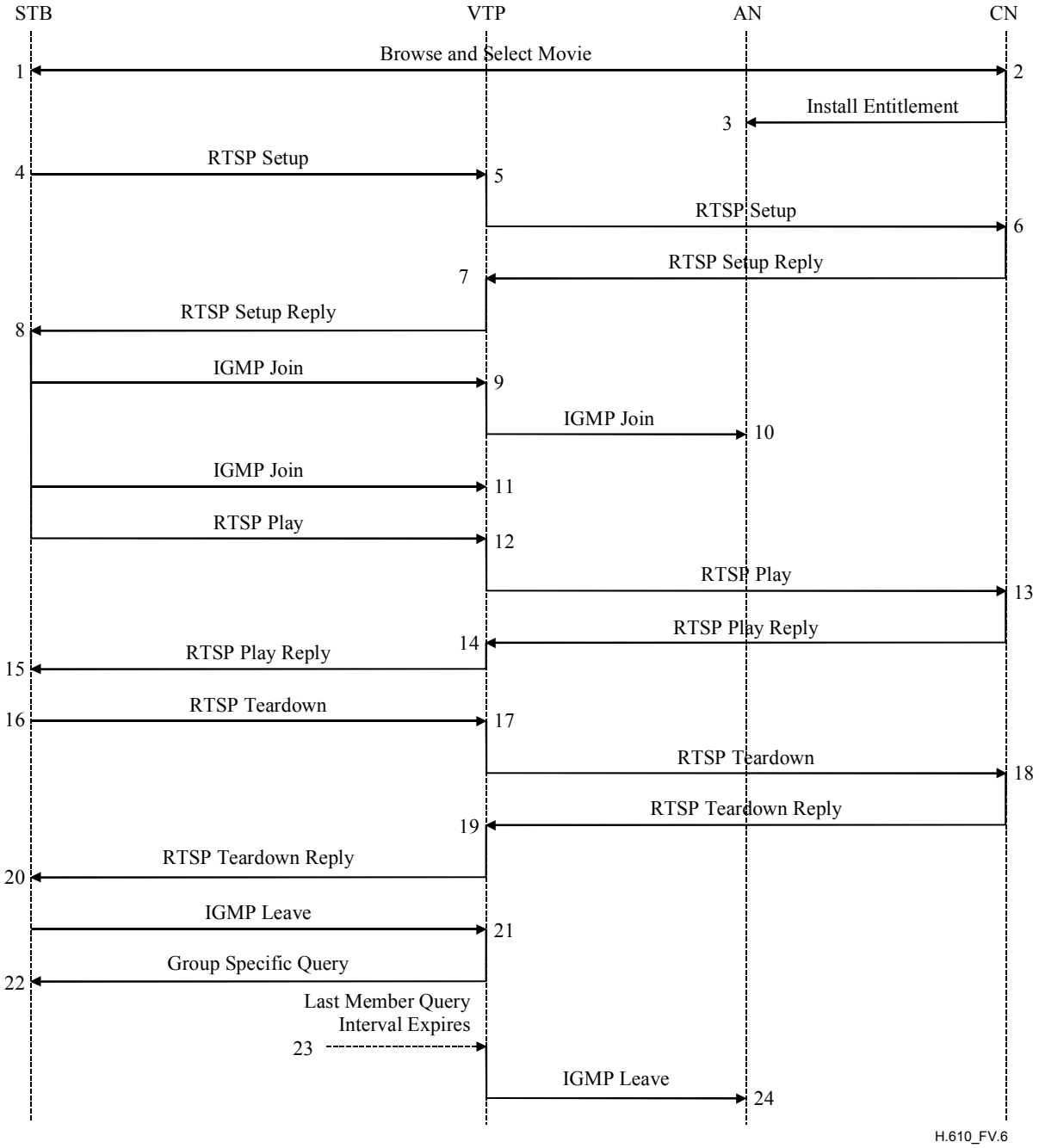
NOTE 2 – IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

V.6 VoD movie selection – IP multicast delivery

This scenario describes the message flow when a user selects a VoD movie that 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 its end.

Pre-conditions:

- Successful boot-up 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 residential 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 RFC 2236).

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 step 8 of sequence V.3.

11 As per step 9 of sequence V.3.

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 residential 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 an 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 an RTSP Teardown reply.

19 The VTP will forward the request towards the residential network.

20 The STB generates an 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 STBs 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.

NOTE 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.

NOTE 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.

NOTE 3 – The VTP filters any IGMP messages received over the T_{CN} interface that match any of the multicast addresses associated with the broadcast TV/VoD stream.

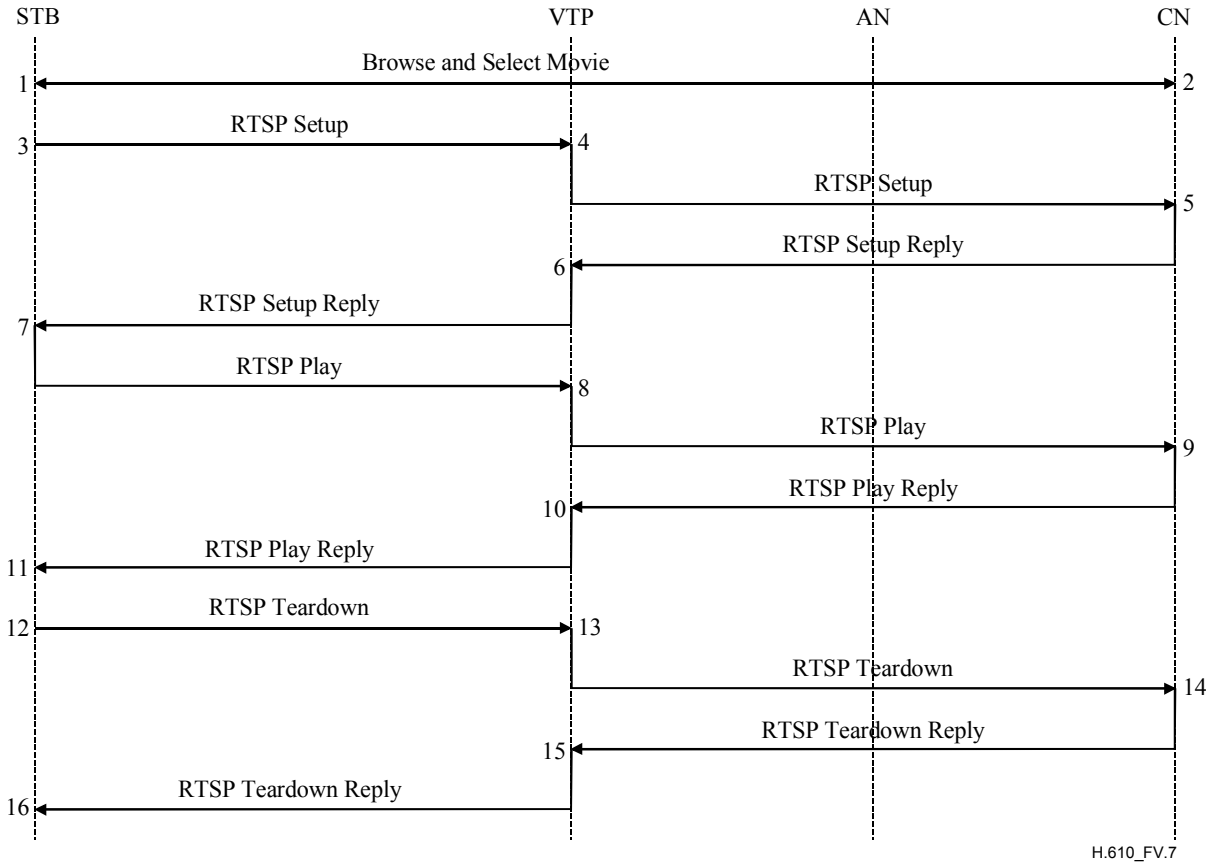
NOTE 4 – IGMP messages sent between the VTP and the AN are carried on a dedicated channel change ATM VCC.

V.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 its 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 residential network.

7 The STB sends 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 residential 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 residential network.

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

NOTE 1 – RTSP messages and the VoD movie stream 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.

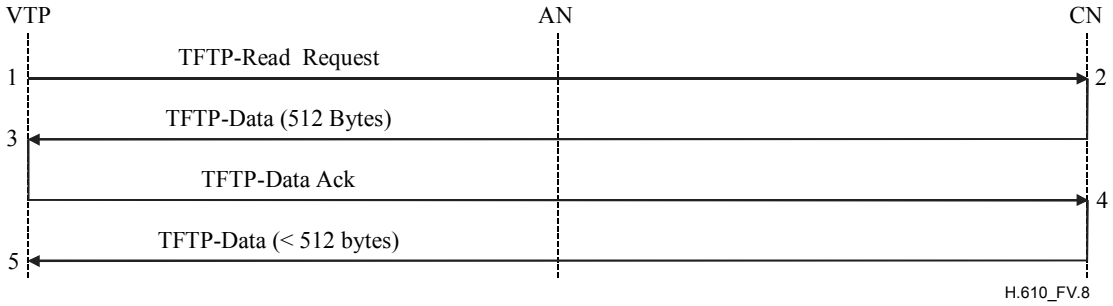
NOTE 2 – The AN does not intercept the RTSP messages or the VoD movie stream, these are just transparently forwarded as a result of the AN performing ATM cell relay.

V.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 boot-up 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 is ready to use the new downloaded software image.

NOTE 1 – The VTP receives TFTP messages on the VC that is designated for remote management.

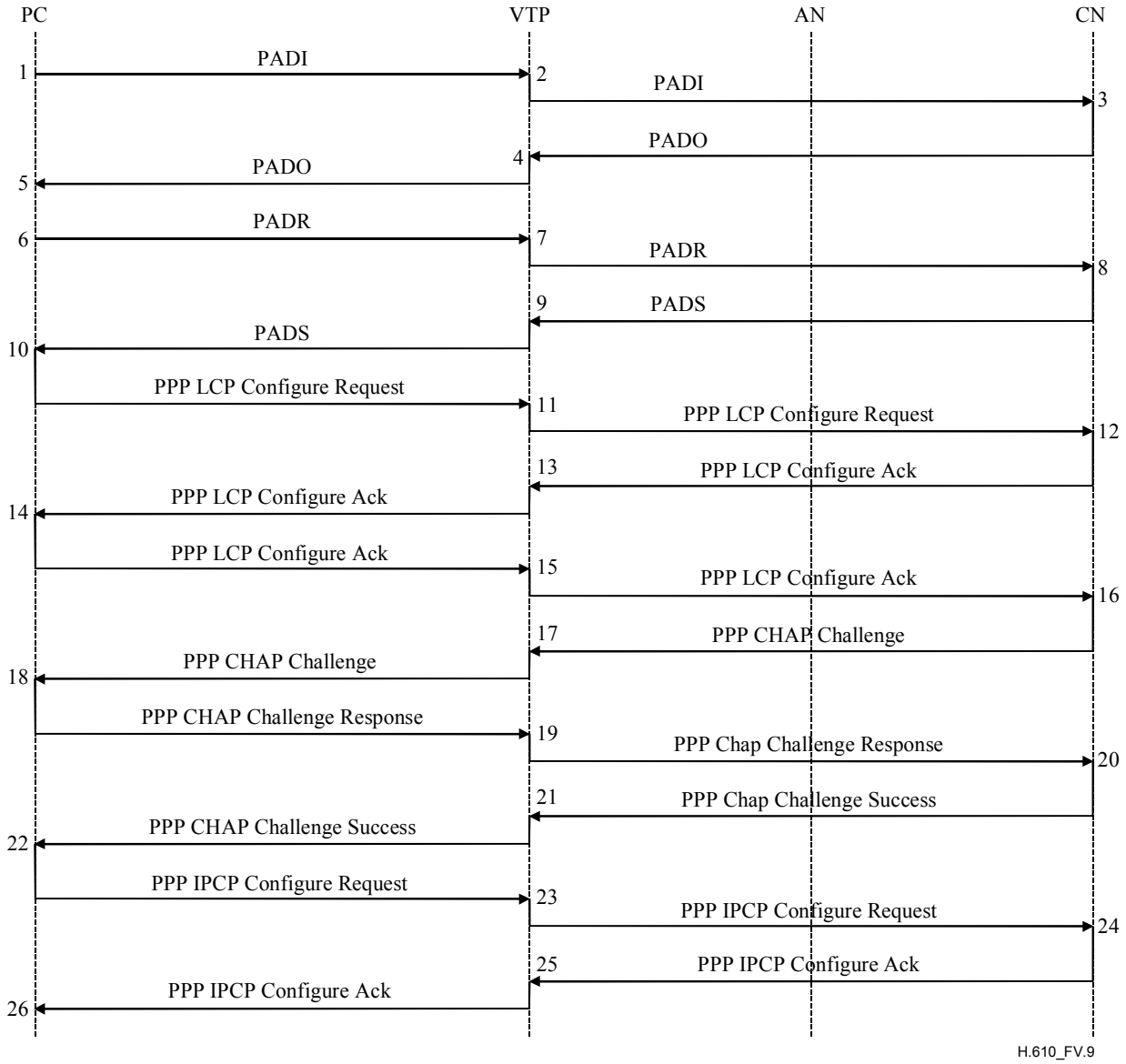
NOTE 2 – The AN does not intercept any of the TFTP messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.

V.9 Internet browsing using PPPoE from a terminal

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 boot-up 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 residential 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 to 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 on 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 residential 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 residential 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 residential 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 residential 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 residential network.

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

NOTE 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.

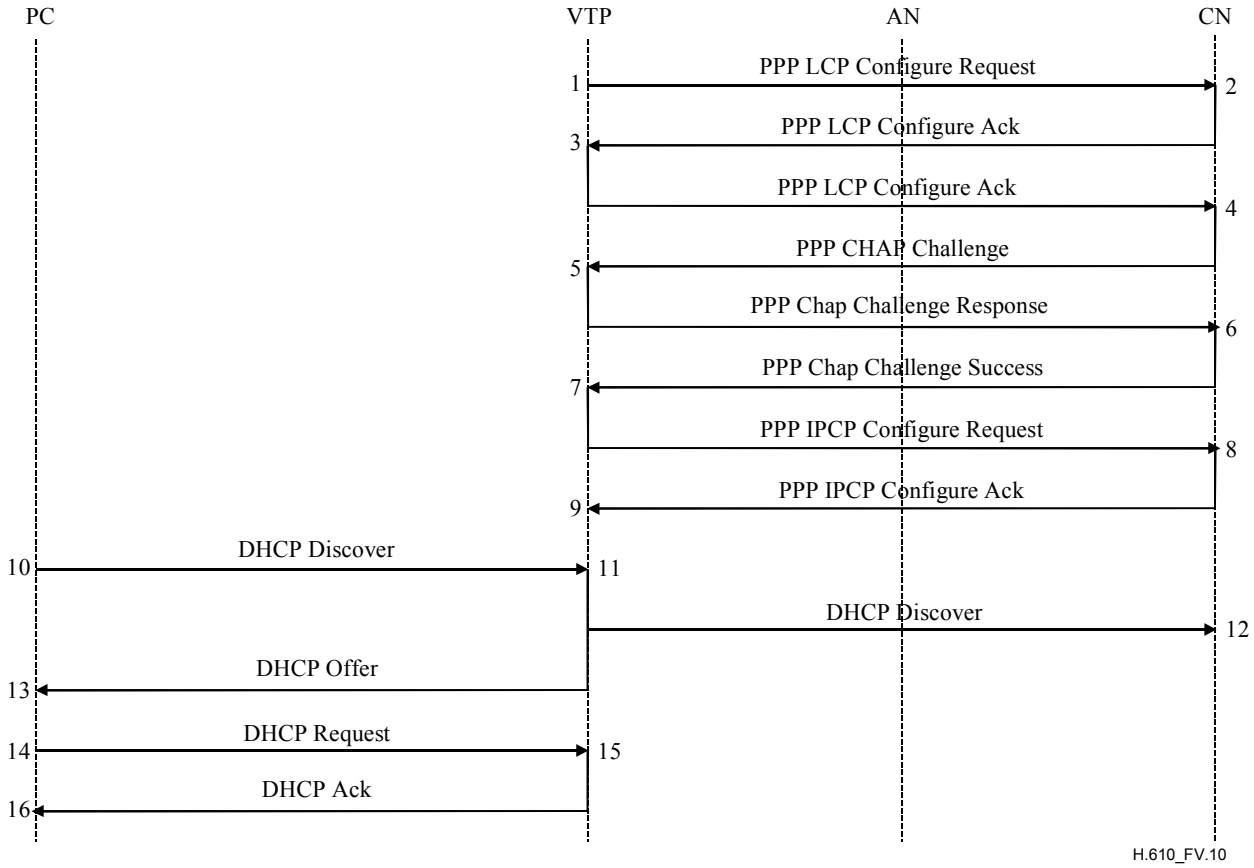
NOTE 2 – The AN does not intercept any of the PPPoE messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.

V.10 Internet browsing using PPP from the VTP

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

Pre-conditions:

- Successful boot-up of the VTP.



1 The VTP initiates a PPP 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 PPP 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 residential 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 DHCP server/relay 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 if 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 recognizes its 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 PPP).

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 translated routed connection.

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

NOTE – The AN does not intercept any of the PPP messages, they are just transparently forwarded as a result of the AN performing ATM cell relay.

Appendix VI

FPD File download using multicast TFTP

Following IP connectivity establishment, FPDs that support video services may download some software, meta-data and additional configuration information from the network. This ensures that following FPD restart, the FPD has the latest software and data for the video applications. As part of the IP connectivity establishment phase, a filename is passed to the FPD (using DHCP) informing it of the location and name of the file containing the FPD software. There are several mechanisms for the FPD to download this file such as:

- Multicast Trivial File Transfer Protocol (M-TFTP) – The standard TFTP is defined in RFC 1350 and the multicast option is defined in RFC 2090. Together they describe a mechanism for file transfer optimized for a one-to-many file distribution scenario. It is a request-response protocol utilizing IP multicast for transmitting the data.
- Coherent File Distribution Protocol (CFDP). This is defined in RFC 1235 and provides a similar architecture to M-TFTP.
- Proprietary file carousel – This mechanism would be similar to the DSM-CC Object Carousel defined by DAVIC. This is a push mechanism and would push the data into the network without a specific request from an FPD. There is not a standard that currently exists which defines such a carousel for an FS-VDSL network.

Unicast TFTP is well utilized for file download in customer premises equipment deployed today and network infrastructure already exists for such a solution. Therefore the easiest migration step to a more scaleable file transfer mechanism, from the above choices, is M-TFTP. Choosing a single mechanism and its consistent implementation across multiple FPDs will result in improved interoperability in a multiple FPD vendor environment.

This appendix describes how M-TFTP can be used to download the FPD software prior to its booting. This protocol may also be used subsequent to the FPD boot for downloading any meta-data and configuration information required by the IP TV applications. A typical usage of M-TFTP is shown in Figure VI.1, where a file consisting of 2×512 Byte blocks is downloaded by two FPDs simultaneously.

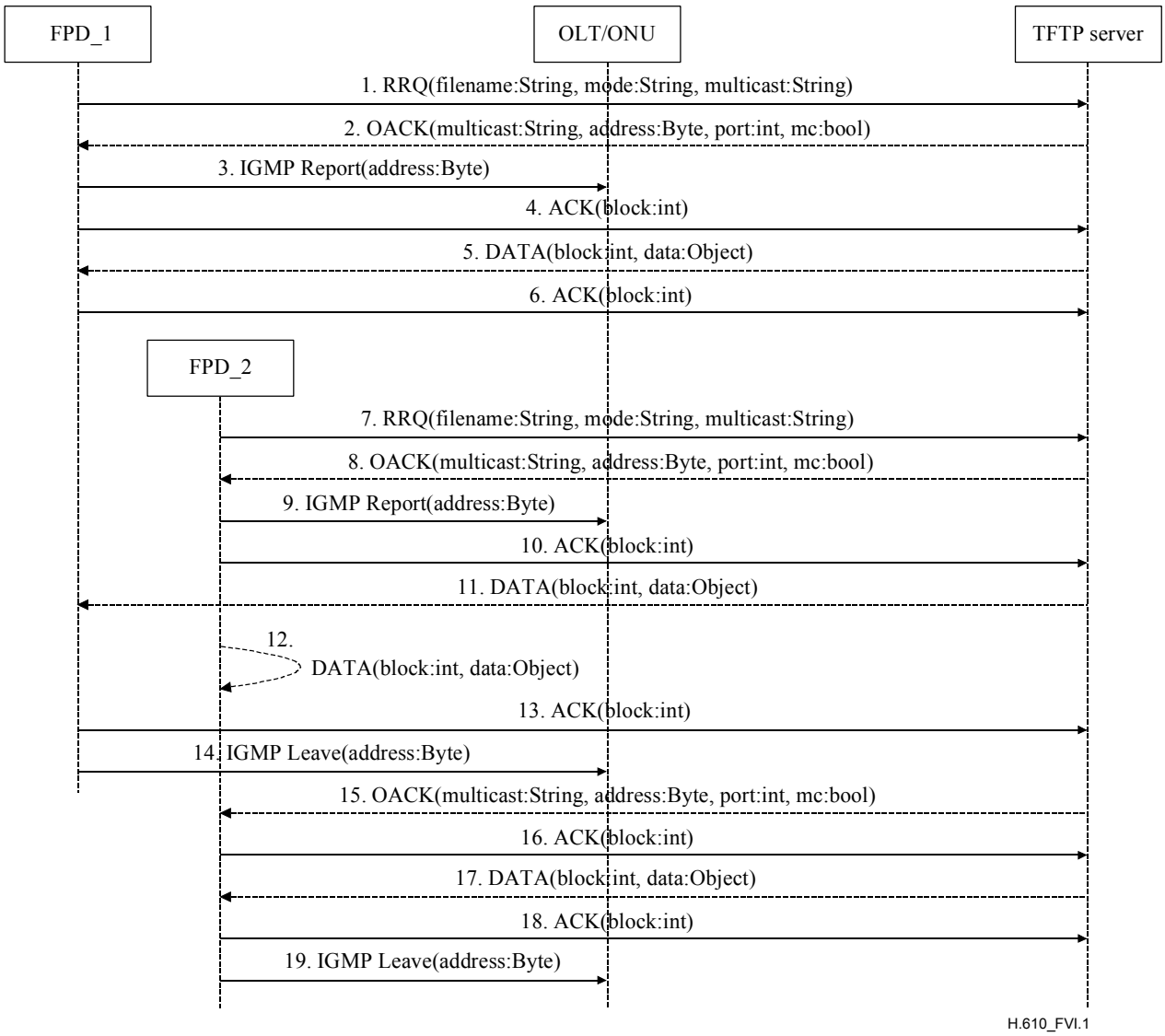


Figure VI.1 /H.610 – Multicast TFTP file download

The steps involved are as follows:

FPD_1 issues a Read Request (RRQ) for the file that was specified during the IP connectivity establishment phase via DHCP. The RRQ requests a file transfer mode of octet and contains the multicast option.

The TFTP server recognizes and supports the octet mode of file transfer and the multicast option and therefore sends and Option Acknowledgement (OACK) specifying the multicast address, port number and mc = 1 indicating that FPD_1 is the master client, responsible for acknowledging TFTP DATA packets.

FPD_1 joins the multicast group specified in the OACK using an IGMPv2 Report message OLT/ONU to and starts listening on that multicast group and port number for TFTP packets.

FPD_1 then issues an ACK with the block parameter set to zero (0). This specifies to the TFTP server that it is requesting block one (1).

The TFTP server sends a DATA packet containing block number 1.

FPD_1 sends an ACK with the block parameter set to one (1). This specifies to the TFTP server that it is requesting block (2).

Then FPD_2 sends a RRQ for the same filename specified to it during the IP connectivity establishment phase via DHCP. The RRQ contains the multicast option.

Since the file transfer is already in progress to FPD_1, the TFTP server sends an OACK specifying the same multicast address and port number as it did to FPD_1 but with mc = 0, indicating that another FPD is the master client and that FPD_2 should not send ACKs in response to DATA packets it receives.

FPD_2 joins the multicast group specified in the OACK using an IGMPv2 Report message and starts listening on that multicast group and port number for TFTP packets.

FPD_2 acknowledges the OACK with an ACK with the block parameter set to zero (0).

The TFTP server sends a DATA packet containing block number 2, in response to step 6.

FPD_2 also receives this DATA packet because it is listening to the same multicast group and port number as FPD_1.

FPD_1 sends an ACK with the block parameter set to (2). This specifies to the TFTP server that FPD_1 has completed receiving the file.

FPD_1 leaves the multicast group specified in the OACK using an IGMPv2 Leave message.

The TFTP server sends an OACK to FPD_2 now with the same parameters as specified in step 8 but with mc = 1, indicating to FPD_2 that it is now the master client and should start sending ACKs in response to DATA packets.

FPD_2 sends an ACK with the block parameter set to zero (0). This specifies to the TFTP server it is requesting block one (1).

The TFTP server sends a DATA packet containing block number 1.

FPD_2 having already received block two (2), then sends an ACK with the block parameter set to two (2). This specifies to the TFTP server that FPD_2 has completed receiving the file.

FPD_2 leaves the multicast group specified in the OACK using an IGMPv2 Leave message.

Appendix VII

FPD IP Configuration using PPPoE and DHCP

When an FPD supporting video services (i.e., Set-top-box) first starts up, it needs to obtain an IP address, default gateway and DNS in order to obtain IP connectivity onto the video service provider's network. Such FPDs primarily utilize the Dynamic Host Configuration Protocol (DHCP) for obtaining such IP connectivity. The exclusive use of DHCP for this purpose together with the necessary DHCP options and associated nomenclature is defined in the normative part of this Recommendation.

However, in a network environment where broadband DSL services of Internet are already deployed, there may already be in existence an IP connectivity establishment infrastructure based on the Point-to-point Protocol (PPP). In this case, it would be cost-effective to reuse the same infrastructure for FPD IP connectivity, and then employ DHCP only for additional configuration that is beyond PPP capabilities. The normative part of this Recommendation does not define this scenario and the aim of this appendix is to specify how the FPD may utilize PPPoE to obtain IP connectivity to the video service provider's network and then DHCP to obtain further configuration parameters.

The first phase, establishing basic IP configuration using PPPoE, is described in Appendix V (scenario 9). Once the PPPoE session and PPP link are established, then the IP connectivity establishment phase is complete. The next phase is retrieval of the FPD software filename and location. This is done using DHCP Inform messages from the FPD to the DHCP server residing in the video service provider's network as shown in Figure VII.1. The steps involved are the following:

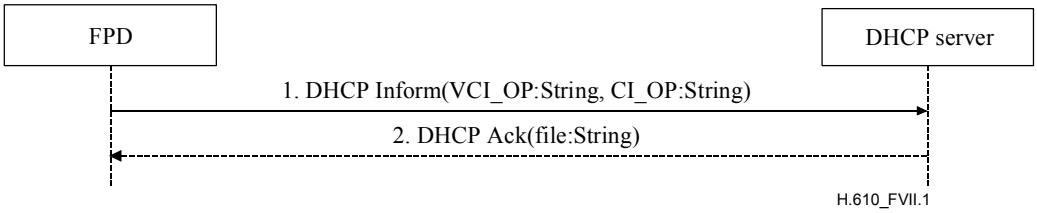


Figure VII.1/H.610 – DHCP Inform for FPD software filename

The FPD sends out a DHCP Inform message following the IP connectivity establishment phase using PPP. The DHCP Inform message is sent on the broadcast Ethernet address. In addition to the standard parameters, the DHCP Inform message contains the DHCP options as described in 10.3.4.

The DHCP Server, which receives the DHCP Inform message, responds with a DHCP ACK message containing the appropriate FPD configuration parameters only if it is responsible for the CLIENT_TYPE as provided in the Inform message. Otherwise, the DHCP server silently discards the DHCP Inform message and does not respond. The DHCP ACK message also contains the IP address for the TFTP server (where TFTP is used for file download) in the *sname* parameter, and a fully qualified directory-pathname, in the *file* parameter of the DHCP message, pointing to location and filename, respectively, of the software[2] for the FPD of type CLIENT_TYPE. The DHCP server does not allocate a new address, check for an existing binding, fill in *yiaddr* or include lease time parameters in the DHCP ACK message, as all these aspects were handled by the BAS during the PPP IP connectivity establishment phase. This completes the retrieval of the FPD software location and filename using DHCP and completes the scenario where a combination of PPPoE and DHCP are used for FPD IP connectivity establishment.

[2] Note that standard DHCP only allows one filename to be provided as part of the DHCP message. This must contain the filename of the software that is required by the FPD to boot. Where the FPD requires additional files, e.g., for meta-data, then the software itself may contain the appropriate vendor specific DHCP options that allow the FPD to subsequently download these additional files following boot. This keeps the baseline DHCP implementation simple and as standard as possible, whilst allowing flexibility by different FPD software vendors to implement their own extensions should they wish.

Appendix VIII

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 minimize 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 utilizes 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 ITU-T Rec. G. 783 [I-2] for further details).
- ATM protection switching – This scheme utilizes 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 ITU-T Rec. I.630 [I-3] 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 standardized or proprietary protection scheme is suitable.
- The V reference point 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.

Appendix IX

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 appendix provides a general overview of relevant standard VoDSL technologies specified by different bodies such as ATM forum, DSL forum, IETF, ITU-T study groups 15/16 and ETSI.

VoDSL can be characterized by the following:

- Voice services digitally emulated by a 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 analogue phone interfaces are correspondingly called "derived voice lines". The derived voice lines usually 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) are enabled.
- Since usually a VoDSL VTP/D offers multiple service interfaces, the VoDSL VTP/D is referred to as the Integrated Access Device (IAD).
- VoDSL can support voice quality that is equal to other forms of digital telephony like ISDN. Indeed, impairments of analogue 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.

In the following, two different voice over DSL architectures are described. The first architecture takes use of AAL 2 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 af-vmoa-0145.000 [I-8]. The second architecture relies on IP to transport the voice packets and will be referred to as voice over IP.

The items 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.

IX.1 BLES

Loop Emulation Service (LES) has been defined by the ATM Forum and has been adopted by the DSL Forum. In the context of VoDSL, it is sometimes referred to as Broadband Loop Emulation Service (BLES). BLES uses ATM/AAL 2 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).

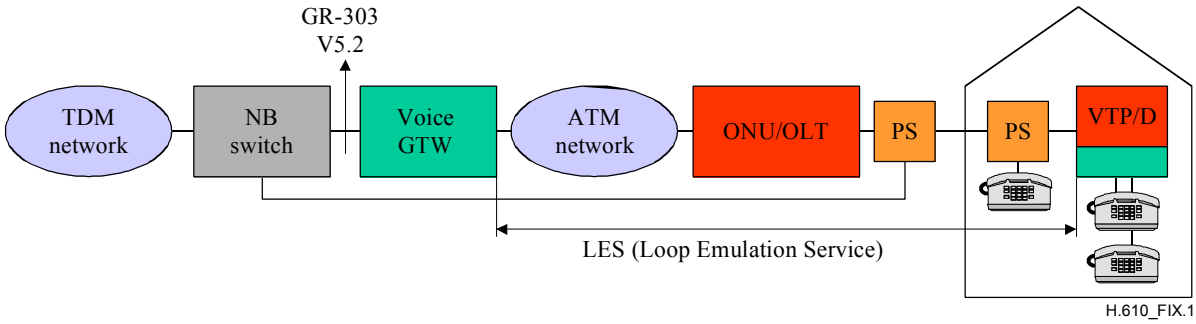


Figure IX.1/H.610 – VoDSL network elements

The following principles apply:

- VoDSL is 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 AAL 2 voice connection, performs the (de-) coding function and supports the necessary signalling 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 analogue voice band end-user interfaces, 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 signalling.

IX.2 Voice over IP (VoIP)

This method suggests that both the voice signal and the voice signalling messages are carried within IP packets. VoIP has been specified in different standardization forms and industry consortia, such as IETF, ITU-T study groups 15/16, 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 for the encapsulation of the (compressed or uncompressed) voice frames.
- The H.323 suite for call setup.
- SIP (Session Initiation Protocol) for call setup.
- SDP (Session Description Protocol).
- H.248 and MEGACO.

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 analogue phone interfaces 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 residential 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 providing 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.

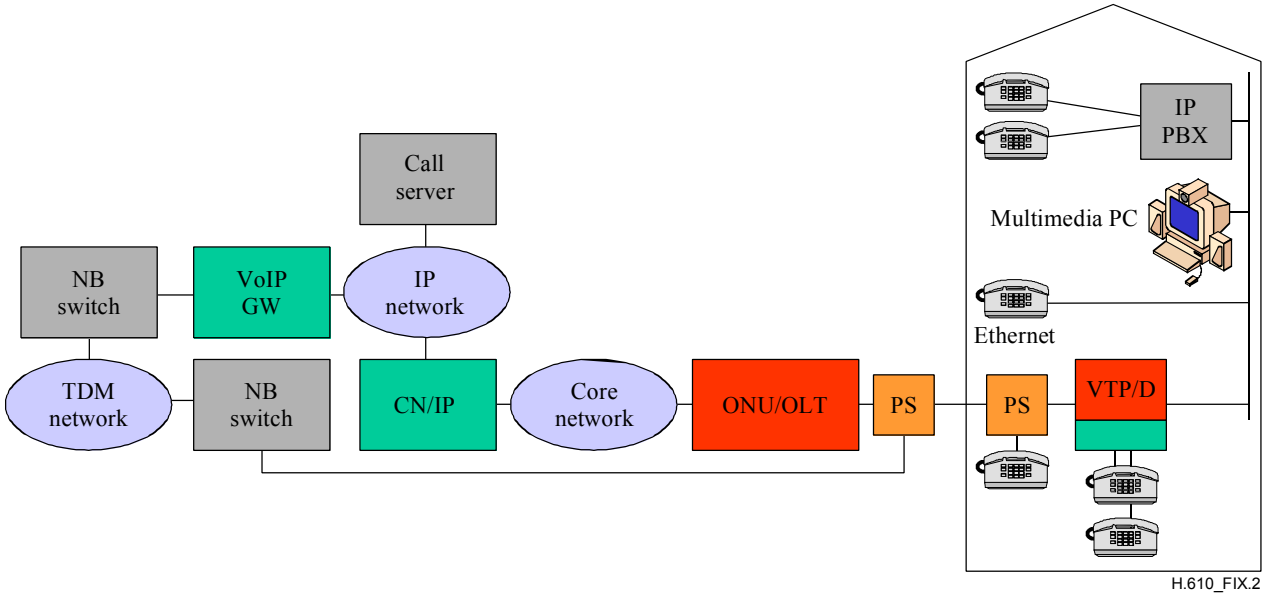


Figure IX.2/H.610 – VoIP network elements

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 implemented 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 analogue voice band end-user interfaces to VoIP and vice versa. This VoIP conversion includes speech compression, packetization, RTP encapsulation and VoIP signalling, such as H.323, SIP or H.248. 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 Ethernet, IP or ATM QoS mechanisms.

- If the VoIP traffic is routed through the translated routed 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 Signalling 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 phone 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 X

IEEE process of obtaining OUI

OUI numbers are administrated by the IEEE organization. Application for OUI may be submitted on the IEEE web site (http://standards.ieee.org) using the following URL, http://standards.ieee.org/regauth/oui/forms/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure, Internet protocol aspects and Next Generation Networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004