INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FS-VDSL
FGTS

Full-Service VDSL

Focus Group
Technical Specification

Part 1: Operator requirements

Version 1.0.0
5 June 2002

FULL-SERVICE VDSL FOCUS GROUP

FOCUS GROUP TECHNICAL SPECIFICATIONS SERIES

FOCUS GROUP TECHNICAL SPECIFICATIONS	
FULL-SERVICE VERY HIGH-SPEED DIGITAL SUBSCRIBER LINE	**Version control:**
Part 1: Operator Requirements	Version 1.0.0 / 5 June 2002
Part 2: System Architecture	Version 1.0.0 / 5 June 2002
Part 3: Customer Premises Equipment	Version 1.0.0 / 5 June 2002
Part 4: Physical Layer Specification for Interoperable VDSL Systems	Version 1.0.0 / 5 June 2002
Part 5: Operations, Administration and Maintenance & Provision aspects for FS-VDSL Services	Version 1.0.0 / 5 June 2002

FOREWORD

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

ITU-T FS-VDSL Focus Group Technical Specification 1

PART 1: OPERATOR REQUIREMENTS

Summary

This document positions the FS-VDSL specification documents and provides information on operators' requirements for services and infrastructure deployment. This information has been summarised to assist vendors to implement common products that can be offered in all the markets represented by the sponsoring operators, thereby achieving economies of scale.

CONTENTS

ITU-T FS-VDSL Focus Group Technical Specification 1

Part 1: Operator Requirements

1. Scope

The FS-VDSL work has been scoped to ensure that only the elements that need to be specified to achieve an interoperable low cost platform are included in these specifications. The FS-VDSL Committee has been careful not to over-specify as this would constrain innovation, or to specify at too high a level of detail which would lead to delay. The FS-VDSL Committee believe this "light" approach is the best way to achieve rapid progress; moreover it has ensured that each service provider can define and evolve a distinct portfolio of competitive services using the 'bricks' defined in the specifications with downloadable software configuration.

2. References

The following references contain provisions, which, through reference in this text, constitute provisions of this Technical Specification. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Specification are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

[1] ANSI Working Group Contribution T1E1.4/2000-009R1 "Very-high-bit-rate Digital Subscriber Line (VDSL) Metallic Interface, Part 1: Functional Requirements and Common Specification", August 2000

[2] ANSI Working Group Contribution T1E1.4/2000-011R1 "VDSL Technical Specification, Part 2: Technical Specification for a Single-Carrier Modulation (SCM) Transceiver", August 2000

[3] ANSI Working Group Contribution T1E1.4/2000-013R2 "Very-high bit-rate Digital Subscriber Lines (VDSL) Metallic Interface, Part 3: Technical Specification of a Multi-Carrier Modulation Transceiver", August 2000

[4] ETSI TS 101 270-1 V1.2.1 "Transmission and Multiplexing (TM); Access transmission systems on metallic access cables; Very high speed Digital Subscriber Line (VDSL); Part 1: Functional requirements", 1999-10-21

[5] ETSI draft TS 101 270-2 V1.1.1 "Transmission and Multiplexing (TM); Access transmission systems on metallic access cables; Very high speed Digital Subscriber Line (VDSL); Part 2: Transceiver requirements", 1999-12-03

[6] FS-VDSL Specification Part 2 (2002): System Architecture Specification

[7] FS-VDSL Specification Part 3 (2002): Customer Premises Equipment Specification

[8] FS-VDSL Specification Part 4 (2002): Physical Layer Specification for Interoperable VDSL Systems

[9] FS-VDSL Specification Part 5 (2002): OAM & P Specification

[10] ETS 300 019-1-3, Equipment Engineering (EE); Environmental conditions and environmental test for telecommunications equipment; Part 1-3: Classification of environmental conditions – Stationary use at weatherprotected locations

[11] ETS 300 019-1-4, Equipment Engineering (EE); Environmental conditions and environmental test for telecommunications equipment; Part 1-4: Classification of environmental conditions – Stationary use at non-weatherprotected locations

[12] ITU-T Recommendation K.34 (1996), Classification of electromagnetic environmental conditions for telecommunications equipment – Fast transient and radio-frequency phenomena

[13] ITU-T Recommendation K.43 (1998), Immunity requirements for telecommunication equipment

[14] ITU-T Recommendation K.45 (2000), Resistibility of access network equipment to over voltages and over currents

[15] ITU-T Recommendation K.50 (2000), Safe limits of operating voltages and currents for telecommunication systems powered over the network

[16] EURESCOM Project P917 BOBAN – Broadband cabinet survey, specification and demonstration

[17] CISPR 22, Information Technology Equipment - Radio Disturbance Characteristics - Limits and Methods of Measurement, 1997

[18] CISPR 24, Information Technology Equipment - Immunity characteristics - Limits and methods of measurement, 1998

[19] Telcordia Technologies GR-1089-CORE, Electromagnetic Compatibility and Electrical Safety Generic Criteria for Network Telecommunications Equipment

[20] Telcordia Technologies GR-487, Generic Requirements for Electronic Equipment Cabinets

3. Definitions

This specification defines the following terms:

ONU

Strictly speaking the ONU would designate only the optical termination. However in this document the term ONU is used as an overall concept that includes the switching matrix, VDSL line terminations, powering circuitry, and it may also include POTS/ISDN splitters, environmental sensors, back up batteries and wire cross connection jumpers.

4. Abbreviations

This specification uses the following abbreviations:

AAL	ATM Adaptation Layer
ADSL	Asymmetrical Digital Subscriber Line
ANSI	American National Standard Institute
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BER	Bit Error Ratio
BLES	Broadband Loop Emulated Service
BRAS	Broadband Remote Access Server
CAM	Conditional Access Module

CBR	Constant Bit Rate
CCS7	Common Channel Signalling #7
CCTV	Closed Circuit TV
CLASS	Customer Local Area Signalling Services
CLEC	Competitor Local Exchange Carrier
CO	Central Office
CPCM	Copy Management and Copy Protection
CPE	Customer Premises Equipment
CSA	Carrier Serving Area
DAVIC	Digital Audio-Visual Council
DBA	Dynamic Bandwidth Allocation
DBS	Digital Broadcast Satellite
DBTV	Digital Broadcast TV
DHCP	Dynamic Host Configuration Protocol
DLC	Digital Loop Carrier
DLEC	Distribution Local Exchange Carrier
DRM	Digital Rights Management
DSA	Distribution Serving Area
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ECM	Entitlement Control Message
EMC	Electro-Magnetic Compatibility
EMS	Element Management System
ETSI	European Telecommunication Standards Institute
EPG	Electronic Programming Guide
FPD	Functional processing and Decoding block
FSAN	Full Service Access Network
FS-VDSL	Full Service VDSL
FTTB	Fibre To The Building
FTTCab	Fibre To The Cabinet
FTTCurb	Fibre To The Curb
FTTEx	Fibre To The Exchange
FTTH	Fibre To The Home
GbE	Gigabit Ethernet
HDTV	High Definition TV
HTML	Hyper Text Mark-up Language

IAD	Integrated Access Device
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
ILMI	Integrated Local Management Interface
IM	Instant Messaging
IoTV	Internet on TV
IP	Internet Protocol
IPSec	IP Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPEG	Moving Pictures Experts Group
MTVF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAT	Network Address Translation
NTSC	National Television Standards Committee
OAM	Operation, Administration and Maintenance
ODN	Optical Distribution Network
OLT	Optical Line Termination
ONU	Optical Network Unit
OPI	Outside Plant Interface
OTU-C	Optical Termination Unit – Central Office
OTU-R	Optical Termination Unit – Remote
PAL	Phase Alternation Line
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PON	Passive Optical Network
POTS	Plain Old Telephony Service
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPV	Pay Per View
PS	Pots or ISDN Splitter
PVR	Personal Video Recorder

QoS	Quality of Service
RFT-C	Remote Feeding Telecommunication – Current limited
RFT-V	Remote Feeding Telecommunication – Voltage limited
ROW	Right Of Way
SDH	Synchronous Digital Hierarchy
SECAM	Sequential Coleur Avec Memoire
SME	Small-Medium Enterprise
SNR	Signal to Noise Ratio
SNMP	Simple Network Management Protocol
SOHO	Small Office – Home Office
SONET	Synchronous Optical Network
STB	Set Top Box
TDM	Time Division Multiplexing
VBI	Vertical Blanking Interval
VBR	Variable Bit Rate
VC	Virtual Connection
VDSL	Very high bit rate Digital Subscriber Line
VLAN	Virtual LAN
VoATM	Voice over ATM
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
VTPD	VDSL Termination Processing and Decoding
VTP/D	VTP and/or VTPD
VTU-C	VDSL Termination Unit - Central Office
VTU-R	VDSL Terminal Unit – Remote
WDM	Wavelength Division Multiplexing

5. The FS-VDSL Committee

The decision to create the Full Service-VDSL Committee was taken in July 2000 when a group of telecommunication operators met with vendors to propose a forum to accelerate standardization of a video-centric network based on VDSL (Very high-speed Digital Subscriber Line) technology. It was formed because no other body was progressing toward standardization of an end-to-end platform

based on VDSL. Competitive solutions were required quickly to address emerging market and to allow the delivery of a large set of services.

The standardisation of the piece-parts for such a network, including VDSL, were (and are) being progressed in isolation by different bodies, but in an uncoordinated way; and they are progressing at different speeds. Hence, service providers were extremely concerned that a cost-effective platform would not emerge from this situation, or would not emerge in time to meet their aspirations for deployment. Having already successfully co-operated via the Full Service Access Networks initiative (FSAN), the formation of the FS-VDSL Committee as a sub-committee of FSAN was a logical step.

To date, 15 telecommunication operators have been involved in the FS-VDSL specifications and support publication of the specifications documented herein. These network operators are: Belgacom, Bell Canada, Bezeq Israel Telecom, British Telecommunications, Deutsche Telekom, Eircom, France Telecom, KT, KPN, Qwest Communications International, SBC, Swisscom, Telecom Italia, Telefonica and Telenor.

Over 60 major equipment and software vendors have provided input to these discussions and the published specifications represent the consensus of all the FS-VDSL member organisations.

This document is intended to position the FS-VDSL specification documents and provides important information on the operators' requirements for services and infrastructure deployment. The FS-VDSL committee has tried to maximise commonality of the operators' requirements to help vendors to implement common products, which can then be offered in all international markets thereby achieving economies of scale.

The FS-VDSL work has been progressed according to the organisation shown below:
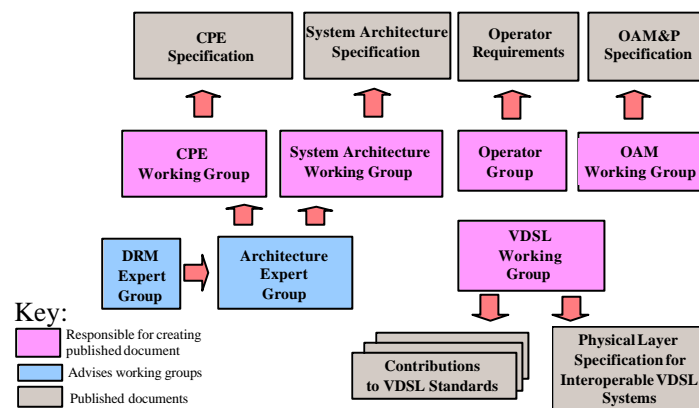
It can be seen from the figure above that five working groups are each responsible for one of the published specification documents. Given that the forum has grown rapidly, two expert subgroups were convened to accelerate discussions on the detail of the system architecture and to address issues for protection of digital content.

Typically, all working groups met in parallel at plenary sessions convened at three-month intervals to align their work. Discussion was progressed via dedicated email reflectors, teleconferences and interim meetings of the working groups to ensure that momentum was maintained between plenary sessions.

In this way, the FS-VDSL Committee has completed its work in an extremely short time frame (less than two years) compatible with the perceived window of opportunity.

6. Architecture and services

6.1. Introduction

VDSL stands for Very high-speed Digital Subscribers Line. Similar to the well-known ADSL, VDSL capabilities are dependent on the distance between the end-customer and the operator equipment and the condition of the existing copper plant supporting the services. In all cases, as ADSL, the idea is to use the telephone copper pairs to transport high bandwidth services to the customers.

In its design, VDSL is able to support various bit rates, in asymmetrical and symmetrical mode, depending upon loop conditions.

Operators have expressed their interest for the bit rates reported in Table 1.

Table 1 – Minimum bitrates of interest for the Operators

	Asymmetric profiles	Symmetric profiles
North America	22 Mbps / 3 Mbps	13 Mbps 6 Mbps
Europe	ETSI A4 (23 Mbps / 4 Mbps) ETSI A4 (14 Mbps / 3 Mbps)	ETSI S3 (14 Mbps) ETSI S1 (6.4 Mbps)
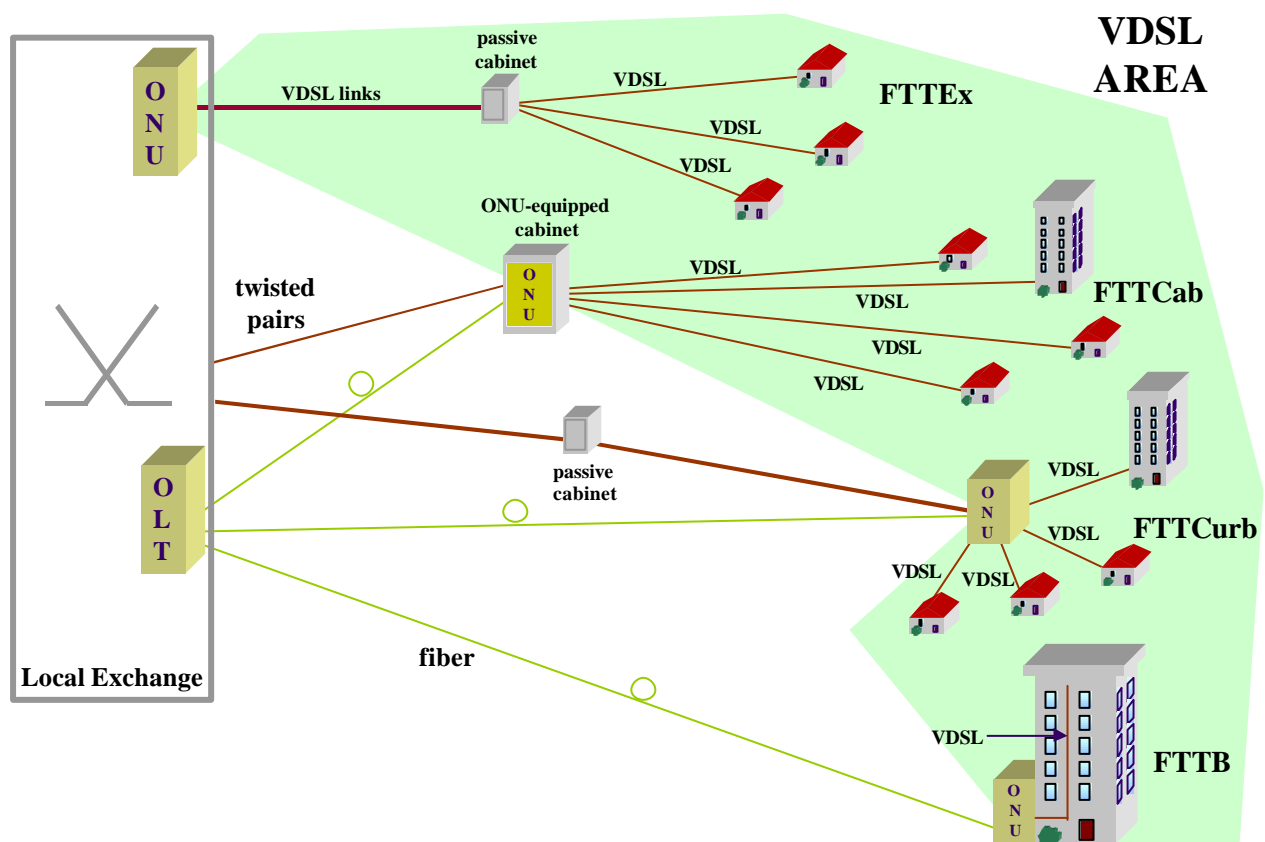
Figure 1 – Architecture of the VDSL access system in the operator network

Both asymmetrical and symmetrical services are expected to be deployed in each market served. Asymmetrical services are mainly focused to the residential market, whereas symmetrical services are typically targeted at the SME/SOHO markets.

In asymmetrical mode, the available bandwidth allows for the delivery of voice services, high-speed Internet, interactive applications and various video centric services to the end users, all this simultaneously on the same copper pair. This mode is well suited for the residential market.

The symmetrical mode, on the other hand, is better suited for the business market where flow of information is more than likely to be bi-directional for data and file transfers and web access.

6.2. The FS-VDSL platform architecture

Figure 3 gives a pictorial representation of the FS-VDSL network configuration. As shown, the various services (Internet, POTS/ISDN and video) are aggregated at the Optical Line Termination (OLT) which then distributes the content via a fibre link to the subtending Optical Network Units (ONU) connected to it.
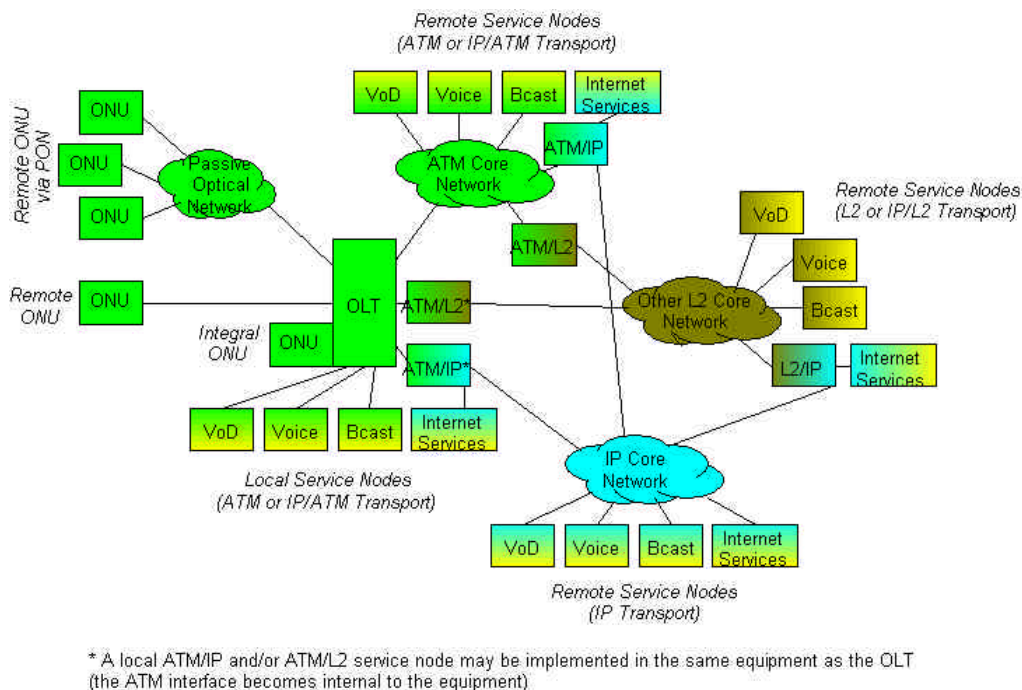
Figure 2 – FS-VDSL platform architecture

It should be pointed out that the same manufacturer typically provides the OLT/ONU combination, because the OLT/ONU design often includes transport of proprietary information on the fibre link in addition to the standard service content. Proprietary information can be for maintenance purposes or for more effectively managing the flow of information between the two entities. In reality, the OLT/ONU combination should be viewed logically as a single identity. The fibre link between both is simply an extension between both backplanes.

In order to keep the data rate manageable across the platform; multicasting should be applied at the appropriate points.

6.3. Services description

The bandwidth available with VDSL enables bandwidth-hungry video services to be offered to customers. Several services, available on copper pairs by different home appliances, are reported in the following sections.

Based on the number of simultaneous TV channels to be offered, the system should be capable of dynamically allocating bandwidth to either TV or PC-based services. This is referred to as Dynamic Bandwidth Allocation (DBA).

6.3.1 TV Based Service Descriptions

This section discusses the services that could be deployed as part of the TV based services offering. The list is not all-inclusive, however represents the majority of the features currently provided or planned on competitive networks.

In order not to over increase the complexity and the costs of the FS-VDSL platform, some technical constraints have been taken into account in the implementation of the services offering.

Note that patents may have been filed associated with the services and features as described.

6.3.1.1 Broadcast TV

Broadcast TV is traditional digital television channel service comprising a single video stream as well as one or more stereo audio streams (multiple languages). The industry standards for encoding should be followed (e.g. MPEG). The signals are transported over the VDSL platform and decoded at the VTPD or at the set top box(es). The TV signal is decoded back to its original state being analog form, e.g. NTSC/PAL/SECAM with Dolby AC3 or Musicam audio. These requirements may be required for all Video/Audio content delivery services as described in this section.

Certain content and features must also be "passed through" such as VBI data (for Close caption text etc.) and Macrovision copy protection for analog channels. These requirements may also be required for all Video/Audio content delivery services as described in this section.

The broadcast signals typically comprise Local (e.g. local city, community or closed circuit), National (e.g. Fox, Speedvision) and International TV channels (e.g. BBC, CNN).

Due to local and regulatory restrictions the system must be able to control the "black-out" of certain programs (usually sporting events). The "black-out' area is typically defined by billing address or geographical location.

The system must also be capable of offering packages of channels based on local interest as well as thematic/genre groups such as News, Sports and Kids channels. Certain channels can also be offered individually such as the Playboy Channel.

6.3.1.2 High Definition TV

HDTV content is becoming more readily available as mandated by the FCC in the USA. At the moment there is little content available other than some Network feeds, Sporting events and Movie/PPV content. HDTV requires HD encoders and set top box decoders. The standards dictate 19.2 Mb/s encoding however as this is not very practical for carriers, innovative encoding has led to pseudo accepted rates of ~13 Mb/s enabling 3 channels per 6MHz carrier on HFC plant for the cable industry.

Due to these high bit rates and low demand for HDTV, VDSL may be limited to a single channel (plus data and voice) per VDSL copper loop.

6.3.1.3 Broadcast Audio

This stereo audio service is delivered similar to Broadcast TV, however the video signal is typically replaced with artist and song/album text information. DMX is an example of this service. The text information can be encoded in MPEG or delivered by other more cost-effective means to the set top box (data stream).

6.3.1.4 Pay Per View

This service involves streaming Movies or Special Events (e.g. WWF, Boxing, and Football). These signals are typically MPEG based digital broadcast channels and hence the customer does not have VOD controls. A request is made to join the session and granted at the scheduled start time. Some providers may allow a cancellation period and a buy window (before and after start).

NearVOD is also another method of delivering PPV. In this case, a movie is streamed on several channels with start times staggered every 15 to 30 minutes. The end user can navigate between these channels to jump ahead or jump back during the movie within a predetermined NVOD viewing window.

PPV should not be limited to a single program or channels. A PPV purchase could also include multiple events (e.g. complete set of StarWars movies over a weekend) and multiple channels (NCAA playoffs).

In order to prevent unauthorized purchases, the system (EPG) should include a "Purchase PIN" in addition to the "Parental Control PIN".

6.3.1.5 Video on Demand

In a true VOD service, the end user accesses the movie from a library directory. The library may include a search engine and movies listing descriptions and ratings. Parental and Purchase PINs must be included to avoid unauthorized purchases. As with PPV, the encoding is typically based on MPEG digital video.

VOD controls typically include "VCR type" controls (Pause, Play, Fwd, Rwd) as well as additional "DVD type" controls (skip ahead, back, nX fast forward) and features (additional info, interviews, angles and clips).

Access to the movie is usually controlled by business rules such as predetermined VOD viewing window or number of plays allowed per purchase.

6.3.1.6 On-screen Navigator

With all these new services on the TV set, an on-screen Navigator is usually essential enabling the customer to easily navigate between the various Broadcast/PPV/VOD service segments, the EPG, the interactive TV applications and the system configuration and customization screens.

6.3.1.7 Electronic Program Guide

A large multi-channel environment renders the traditional paper TV guide impractical. A user friendly EPG could enable the customer to quickly scroll through programming, view program descriptions and ratings, search for a title, actor or key word, set reminder (force tune or record), set parental controls and PIN numbers, view purchases, view account and service provider information and alter account subscription. A typical EPG will include up to 7 days of programming information.

The EPG may also provide a PIP (Picture In Picture) video window and audio pass through capability.

6.3.1.8 Picture in Picture

The inclusion of a PIP feature as part of the VTPD (multiple decoder STB that includes the VDSL Modem) may be desirable.

The simplest method is to enable two broadcast signals from the Set Top Box to connect to a customer's PIP dual tuner TV set.

The VDSL VTPD solution however has the added capability of overlaying two of the broadcast streams and decoding to a single output stream. In this case a PIP capable TV set is not required. The customer could also have the capability to reverse the video feeds, disable/enable PIP feature, change channels in one or both windows, resize the PIP window and move the PIP around the screen. One touch toggle control would be preferred for ease of use.

Creative methods of displaying the content in the PIP window are encouraged to minimise bandwidth required.

6.3.1.9 Picture in Browser

Similar to PIP, this feature enables the end user to set to TV signal in a window overlaid onto, or designed into, the browser page.

As with PIP, the end user should be able to disable, resize, change the channel and move the window around the screen. One touch toggle control would be preferred for ease of use.

6.3.1.10 Personal Video Recorder:

The PVR can be used for many opportunities. This section will only describe customer controlled "VCR like" features.

Typical PVR functionality includes the ability to program the Set Top Box to record programs from the broadcast TV service. This is similar to a typical home VCR with the following exceptions: the PVR Hard Disk Drive (HDD) is included as an inherent component within the VTPD or Set Top Box, the customer uses the EPG to select the program to record (either one time or multiple times) and a filing system is included for easy movie management. DRM may need to be considered as content is stored digitally onto the PVR.

Due to the high bandwidth capabilities of the VDSL system, a network server based PVR solution may also be a desirable solution.

6.3.1.11 Interactive TV

iTV can include many internet based convergent applications. These make use of the high-speed data connectivity and always on features of the data service. These may also integrate into services offered by an ISP/ASP on a common customer account.

The Picture in Browser feature could be enabled with these services so that the end user can continue to watch/listen a smaller program window and toggle to full screen in a one-touch command.

For iTV services, the use of a user-friendly remote control and wireless keyboard is essential.

- **TV Telephony features**

  Simple display of CLASS services on screen. This could include Caller number ID and Caller name ID, Caller log, web-activated calls. The end user should be able to enable/disable the display.

- **TV Web Browser**

A TV based browser must run persistently (always on) when enabled. This will allow the customer to toggle between the TV programming and the web without having the re-launch the browser. The browser and set top box must include TV friendly features that make browsing on the TV a value add service. These may include anti-aliasing color correction, anti jitter, text resizing, margin wrapping, scroll bars, zoom features and some of the more traditional browser features. The browser should be compatible with many of the Internet plug-ins especially those focused on entertainment and graphics/animation.

- **TV E-mail**

  A TV friendly e-mail client would include most of the typical PC features however must be designed with the TV in mind. Compatibility with "attachments" must be considered.

  The persistent connection should advise the customer of incoming messages. An end user should also be capable of setting several accounts for the home.

  This service may either be server based (IMAP, POP) or Web Based. The TV e-mail service may be linked to an ISP service hence creating convergence across the PC and TV appliances. The system should be compatible with popular web based mail systems such as hotmail.

- **TV Instant Messaging**

  As with e-mail, the Instant Messaging client could be closely linked to an ISP service or can be treated independently. In order to maximize customer value, the IM service should be compatible with current web based IM services.

  The persistent connection should advise the end user of incoming messages as well as identify on-line buddy lists.

  The ability to run IM with PIP video window may lead to interesting service capabilities bridging discussion with a TV program.

- **TV Notification**

  The system should take advantage of the always on high-speed connection and render on-screen notification messages associated with incoming e-mail and Instant Messages. The end user should have the ability to enable/disable.

- **TV Chat**

  TV Chat is similar to and compatible with existing Chat services on the Internet today (Chat rooms, News groups, dialog boxes, etc). The content rendering must be suitable for TV viewing.

  The ability to run TV Chat with PIP video window may lead to interesting service capabilities bridging discussion with a TV program.

- **TV Interactive Games**

  Interactive games could represent single player and multi-player games. These should be server based and either downloaded or played directly from a network server.

  The simplest Interactive Games solution includes a walled garden selection of pre-loaded games on the set top box.

  The VTP/D and set top capabilities (CPU, RAM, HDD, Flash, Graphics engine, etc) will determine how compelling each game is played.

DRM rules will need to be considered.

- **Music Juke Box**

   This service would enable the playback of audio titles selected from a library. The content may be downloaded to a hard disk or played back directly from a network or in-home server. DRM requirements should be considered. Several popular audio codec formats exist such as MPEG2, MP3, Real Networks and WMP.

Table 2 – TV focused services

TV focused Services	Typical bandwidth (downstream)	note
Broadcast TV – e.g. MPEG2	3 to 6 Mb/s	1
High definition TV – HDTV	12 to 19 Mb/s	
Pay Per View and NVOD – e.g. MPEG2	2 to 6 Mb/s	1
VOD – e.g. MPEG2	2 to 6 Mb/s	1
Navigator and EPG (can be locally launched and updated in non real time)	Less than 0.5 Mb/s	
Picture in Picture – two MPEG2 channels	Up to 12 Mb/s	1, 2
Picture in Browser – one MPEG2	Up to 9 Mb/s	1, 2
Personal Video Recorder PVR – replay MPEG2 file off hard disk	3 to 6 Mb/s local	1
ITV - TV telephony features	Less than 64 kb/s	
- TV browser (same as Internet access rates)	Up to 3 Mb/s	
- TV e-mail (same as Internet access rates)	Up to 3 Mb/s	
- TV Instant Messaging (same as Internet access rates)	Up to 3 Mb/s	
- TV Chat (same as Internet access rates)	Up to 3 Mb/s	
- TV on-screen notification	Less than 64 kb/s	
- TV interactive games (same as Internet access rates)	Up to 3 Mb/s	
- TV Audio Juke Box	Less than 128 kb/s	
NOTES:		
1) expect that video compression techniques will advance to enable lower bandwidth for digital video encoding (2 to 3 Mb/s)		
2) more efficient solutions could be available		

6.3.2   PC Based Service Descriptions

This section briefly discusses the services that could be deployed as part of the PC based services offering.

6.3.2.1   High Speed Internet Access

This service provides end user with access to the Internet. Several service options based on downstream and upstream bit rates and aggregated monthly bandwidth (Bytes) may be delivered. This service is typically "always on". End users would access all web based applications through this service (Webmail, Chat, Instant Messaging, web browsing, FTP, etc). An ISP may also offer value-added services such as firewall, virus detection, parental controls, VPN corporate network access, etc.

6.3.2.2   E-mail access

Traditional IMAP or POP mail service offered by the ISP.

6.3.2.3   Live TV on PC
This service would involve the delivery of live video/audio media though the network. The content is typically encoded using standard web codecs such as Windows Media Player (WMP), Real

Network, MPEG variants, AVI, MIDI, etc. The client PC typically uses a software codec to decode the media streams.

6.3.2.4   Video on Demand
This represents a true VOD solution and can entail either real time streaming or download to HDD. DRM will need to be taken into consideration.

6.3.2.5   Video conferencing
This represents a bidirectional service between two or more end users, exchanging real time video and audio contents.

6.3.2.6   Interactive Games
This could include both local and network based games and could be either single or multiple player games. In most cases, a portion of the game is downloaded to the client PC. DRM will need to be taken into consideration.

Table 3 – PC focused services

PC focused Services	Typical bandwidth (downstream)	note
High Speed Internet Access (browsing, IM, Chat, FTP, VPN access, etc)	Residential: Up to 3Mb/s	1
	SME/SOHO: Up to 6Mb/s	2
Server based E-Mail	As above	
Live TV on PC	300 to 750 kb/s	
Video on Demand	300 to 750 kb/s	
Video Conferencing	300 to 750 kb/s	
Interactive Games	300 to 750 kb/s	
NOTES:		
1) typically asymmetrical with lower upstream rates such as 128, 256, 640 kb/s		
2) typically symmetrical service		

6.3.3   Voice services descriptions

VDSL system shall not disturb the lifeline telephony as it is to be carried on the copper loop within the current standard spectral frequencies using splitting filters. This includes all existing and planned CLASS features. The lifeline telephony service can be either POTS or ISDN BRA.

Derived voice can be implemented in different ways, e.g. over IP (VoIP), over ATM (VoATM) or over DSL (VoDSL). It is envisaged that for residential customers up to 4 voice channels will be required, while 30 channels are probably adequate for business customers. Appropriate quality of service is required to meet the needs of customer's e.g. low cost, average quality service for residential customers, high quality, high availability for business customers.

Service features equivalent to existing CLASS features, Centrex, etc. are required to be supported.

7.   Service offering

Various combinations of services can be offered to customers. They are discussed within this section. It should be noted that in all cases the POTS/ISDN service is also present on the copper loop infrastructure: existing standard POTS/ISDN frequencies and service features (example: CLASS, indicators, ring tones, dial-up modems, etc.) are assumed to be unaffected by the VDSL spectrum and services.

The communication services that can be offered are the ones described in the section 6.3, and can be classified as Voice services, Data Services or Video/media services. These services can be bundled in various combinations to suit the needs of the end customers.

This section assumes that the services can be offered either individually or aggregated in bundled offers. It should be noted that FS-VDSL systems will support the different service types over multiple appliances.

The following subsections show examples of possible service scenarios and their implementations.

7.1. PC/Internet only service

This segment represents the traditional ISP/ASP services. The service management facility will be responsible for providing for the setting of bit rates in both upstream and downstream directions individually. This offering would consist of a VDSL connection providing a PC Internet access service alone for customers who are not interested in TV/Entertainment segment of services, or SOHO and SME locations.

Bit rates could range from hundreds of kbit/s up to tens of Mbit/s depending on the specific service (e.g. Home working, point to point leased lines, …).

A number of PC and IP appliances may be simultaneously "on line".

PPPoE, PPPoA, Firewall and VPN software are assumed to be loaded within the IP appliance, PC or Internet Gateway products and not necessarily included within the VTP/D products.

7.2. Broadcast content and EPG

An FS-VDSL system must give the possibility to the end user to get the main video services traditionally offered by a cable or DBS service provider in combination with additional services feasible by such a system.

There shall be the possibility to control the number of channels being delivered simultaneously i.e. One stream service, Two stream service etc. This offering would provide digital broadcast channels comprising digital Video and Audio programming. An electronic program guide (EPG) is essential to navigate and control activities. This guide should enable the end user to view future program listings (typically including titles, actors, producers, start-end-duration times, and program ratings). The EPG should also enable the user to operate search, reminder and record functions. The EPG is assigned to either a stream or a TV set location hence a separately controllable EPG is required for each TV stream in the customers' home

Parental control should also be supported.

These services are typically similar to those provided by the cable or DBS companies and hence, in certain countries, may require regulatory approval. The business model may consist of various channel packaging options ranging from large thematic groups (Locals, News, Sports, etc.) to individual channels (speciality programming, etc.).

On Screen display of Telephony CLASS information should be considered as part of this first basic service bundle. This is provisioned as a chargeable feature so it must be controllable by the system.

Note that text overlays may be required for the audio services showing for example artist and song information.

Basic VBI information and application must be supported within the broadcast service offering for Closed Captioning, teletext interactivity triggers etc.

Note that iTV systems that embed information in the VBI, may need to be transported and compatible with the VDSL systems. These may include Wink, ATVEF and HMP.

The addition of a Pay Per View service may be essential to compete with the Cable/DBS industry. PPV is a stream that is purchased by the consumer via the EPG system. The EPG listings must hence include a complete listing and purchase PIN code system.

The PPV purchase may be limited to a single event (i.e. a movie), multiple events on one or more channels and may also extend for a predetermined period of time (i.e. World Cup).

7.3. Broadcast plus Video on Demand

It should be noted that VoD refers to the unicast provision of various content, (e.g. Video, Music, Games) following a user request.

VDSL is capable of supporting network based Video on Demand service along with the broadcast TV services. Although technologically the TV channel and the VoD channels are different, mainly one being broadcast (or multicast) while the other is on demand (or unicast) and fully controllable by the end user (stop, pause, play, ffwd, rwd). It is expected that the VoD channel will require similar bandwidth (video streams) to a typical broadcast TV channel, and as such, can share the same bandwidth on the VDSL line. For example a customer on a 3 TV stream system can simultaneously watch 1 VoD program and 2 broadcast channels, or 2 VoD programs and 1 broadcast channel, etc.

The purchased events must be authorised prior to viewing and tracked both on the EPG and back to the billing system.

7.4. Broadcast plus Internet on TV services

Ideally the IoTV service will be available on multiple sessions/appliances. For example a single stream service could access one session… a three stream service could access three IoTV sessions i.e. three impressions of the browser running independently. In order to create an effective service and customer experience, the IoTV applications must be capable of running persistently in the VTPD or Set Top Boxes. This will enable toggling for TV to IoTV (without relaunching the browser) as well as allow for addition value added features such as e-mail, Chat, IM and notification while watching a TV program.

7.5. Combined TV/Entertainment and PC/Internet

This offering is a combination of the above-mentioned services.

7.6. PC/Internet and derived voice services

This offering is a combination of the above-mentioned data services combined with derived voice services. For the consumer market a full service offering consisting of video, data and voice services is conceivable.

8. Digital content protection

As mentioned in the previous chapters, the VDSL access is designed to support the delivery of valuable content across the network. The service may include broadcast TV and other on-demand services such as Video-On-Demand, Pay Per View, etc. All content will be transported digitally. This chapter is to identify the security requirements for the types of service proposed in the FS-VDSL specifications.

8.1. Purpose

This is to ensure that the FS-VDSL specifications will meet the content owners' expectations, regulatory rules about commercial availability, as well as budgetary constraints. Security, in the form of digital content protection, is basically an economic exercise. It is a balancing art striking for

equilibrium amongst the value of the content, the cost of providing the level of security desired, and the effort required for breaking the protection in order to gain access to the content without paying for it.

8.2. Goals

The general goals of the FS-VDSL digital content protection specification and any implementation thereafter should possess the following objectives:

- **Content Protection** – Content must be protected to ensure integrity as well as not be accessed illegally for purpose from simple viewing to more severed illegal copying

- **Subscriber Management** – To ensure only the legitimate users may access the content, FS-VDSL security must be capable of supporting processes such as user identification, authentication and authorization

- **Secure Network Communications** – Transmission must be safe from eavesdropping, unauthorized modification, insertion, deletion or replays

- **Reasonable cost** – the cost and complexity to implement the security must be reasonable

- **Network element interoperability** – Network elements, including CPEs, from multiple vendors must inter-operate and support the security requirements

- **System Renewability** – Any security implementation must support system renewability of security methods and algorithms when required

- **Associative Business Rule Capability** – The ultimate goal would be to associate the business rules and use policy with the content

8.3. Security Threats

The following summarizes the possible security threats that are relevant to the FS-VDSL proposed system architecture and video services:

- **Network Element Clones** – One or more network elements may be masqueraded in order to redirect the content to illegal or fraudulent recipients. Although this is highly unlikely but nonetheless it is possible. Network elements must therefore support remote surveillance and be monitored continuously via certain control paths to ensure that the entire network is secured and intact. In addition, network elements should always be located in a physically secured environment.

- **Protocol Attacks** – A weakness in the proposed FS-VDSL access protocol, if any, may be manipulated to allow illegal access to the content. This may include replay, eavesdrop and man-in-the-middle attacks.

- **CPE Clones** – CPE may be masqueraded as another CPE by duplicating its permanent identity and keys.

- **CPE Attacks** – The CPE identity or the secret cryptographic keys may be obtained by either breaking the physical security of the CPE or by employing cryptanalysis. Further, the CPE data path, memory and/or storage may be broken into, digital content redirected and usage information removed.

- **CPE Output Copying** – Digital content may be copied illegally if output of "clear" digital content is allowed.

- **Repudiation** – customer may repudiate a particular service (e.g. PPV based VOD service) and deny responsibility for paying for it. As aforementioned statement of content protection being a

balancing art, this type of fraudulent claim is usually not worth the effort to prevent. Most service providers rely on the service agreement contract the users signed when they subscribe to the service, and frequent billings to avoid the users from running up a substantial amount of outstanding charges.

8.4. FS-VDSL Security Model

The goal of FS-VDSL security model is to protect digital video content from illegal use. Other services such Internet access, voice over IP (or packet) and the traditional POTS services are considered to be outside of the scope of the current chapter.

8.4.1   FS-VDSL System Architecture Re-visit

The following diagram depicts the proposed FS-VDSL system architecture. For details, refer to FS-VDSL System Architecture Specification.
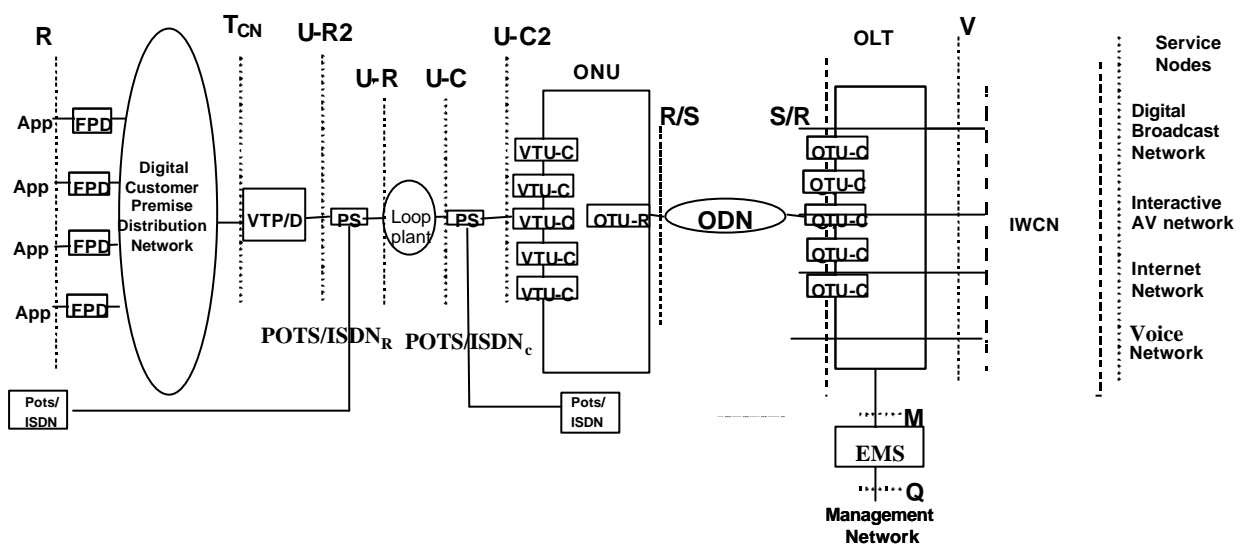
Figure 3 –   Schematic Diagram Depicting the FS-VDSL Reference Model

8.4.2   The Security Model

Based on the proposed VDSL access architecture model as depicted, the security model can be described to have the following functional components relevant to the targeted video services:

1. Digital Broadcast Network

2. Interactive AV Network

3. OLT

4. ODN

5. ONU

6. VDSL Loop Plant

7. VTP/D

8. Digital Customer Premise Distribution Network

9. FPD

The Digital Broadcast Network and the Interactive AV Network are outside the scope of the FS-VDSL specifications. The other functional components and their respective security threats may be grouped together into security blocks as follows:

- **Network elements –** This includes the OLT, ODN and ONU. The possible threats are mainly Network Element Cloning and Network Level Protocol Attacks. OLT and ONU are vendor specific network devices. Even though they are expected to be interoperable, the cost of cloning such devices and the effort required to insert them into the dedicated ODN network without alarming the system operation will be extremely high. Physically, the locations of the OLT and ONU are secured, and logically, ATM as transport protocol is extremely difficult and costly to break into. Still, it is important that the OLT and ONU provide continuous remote monitoring, surveillance and mechanised management capability to prevent such attack to take place.

- **Access Loop –** This includes the VDSL Loop Plant. The possible threat is Network Level Protocol Attack. Since ATM is the transport protocol, same argument will hold that it will be expensive to attack the content by tapping into the ATM virtual circuits. Nonetheless the threat of such attack is real. Since there is no possible way to physically shield the copper pair from tapping, this kind of attack can be less obvious and may not even cause any alarm to the system operation. There are two reasons why this kind of attack has not been widely tried. Firstly, the cost of a protocol analyzer for tapping into the ATM VCs can be expensive. It can be as high as tens of thousands of dollars. Secondly, the content is not worth nearly as much. Obviously then, when operators start to transport valuable content such as first run movies over VDSL, other means of protection such as encryption of the content may be required.

- **CPE –** This includes the VTP/D, Digital Customer Premise Distribution Network and FPD. Based on the proposed CPE architecture and the two recommended video delivery mechanisms (i.e. MPEG/ATM and MPEG/IP/ATM), the CPE security block may be further subdivided into the following two models:

- **Centralized Model –** For the centralized model, the VTPD functions as an end point of the ATM virtual circuits as well as the end point of the digital content delivery. The content is then decoded immediately. The output of the VTPD is in analog TV (such as PAL, NTSC, etc.) or other analog video formats. No content in digital format will be forwarded from the VTPD, over the Customer Premise Distribution Network, to FPD or any other devices. In the centralized model, the possible security threats are the CPE Cloning, CPE Attacks and CPE Output Copying. These threats can be counteracted by the requirements listed in the "CPE Protection" section.

- **Decentralized Model –** For the decentralized model, the VTP, functioning as an ATM VC end point, terminates the ATM transport. The VTP, however, then forwards the content in its original digital format, over the Ethernet (with IP as the transport) continuously to other devices over the Customer Premise Distribution Network within the household. Security threats in the decentralized model are the network level Protocol Attacks, CPE Cloning, CPE Attacks and CPE Output Copying. Since the content is transported in its original digital format over the Customer Premise Distribution Network, over IP and Ethernet, protocol attack can be achieved much more easily and IP protocol analyzers are much less expensive than ATM protocol analyzers. In fact, a personal computer with the proper software can function as an IP protocol analyzer. For decentralized model, content protection by means of encryption has become a definite requirement.

8.5. Security Mechanisms

8.5.1 CPE Protection

The following protection mechanism enables CPE (such as VTP/D and FPD) to properly protect the content and meet the necessary security requirements:

- Each CPE must have its own unique identity.

- For CPE that requires supporting and deciphering encrypted content, the C PE must have its own decryption key that is somehow wrapped with its own unique identity.

- The design and manufacture of the CPE must be tamper proof:

- CPE's own unique identification, any non-public keys, cryptographic algorithms or other secrets/confidential information can never be revealed.

- Change of the embedded unique identification cannot be attempted.

- The design of the CPE shall not allow switches, buttons, jumpers or traces be cut or altered.

- The design of the CPE control functions and service menus shall not allow the content protection technologies be defeated.

- The design of the CPE shall not allow the protected content be exposed to unauthorized copying.

- The design of the CPE shall not allow the core security functions be circumvented or defeated by using general tools such as screwdrivers, jumpers, clips and soldering irons or specialized electronic or software tolls such as EEPROM readers and writers, debuggers or de-compilers.

- The design of the CPE shall render the CPE useless if attempt to remove or replace the hardware components that implement security functions is detected.

- The design and manufacture of the CPE shall support the following content and key management and functions:

- Protected content shall not be present on any user accessible buses in unprotected analog or in unencrypted, compressed digital form.

- Keys used to support content encryption and/or decryption shall not be present on any user accessible buses in unencrypted form.

- Keys, key generation and cryptographic functions shall be embedded in silicon circuitry or firmware that cannot be easily read.

- Software implementations of security functions shall be designed to perform self-checking of the integrity of its component parts and be designed to result in a failure of the security function to provide authorized authentication and/or decryption in the event of unauthorized modification.

- Failure of a security function shall cause the CPE to stop receiving and playing back the protected content.

- The resource of the CPE shall be sufficient to support content decryption and rules processing.

- The design and manufacture of the CPE shall support system enhancements through renewability for any changes of underlying security algorithms and/or processes, or future compatibility with other security recommendations and works in progress.

- The design and manufacture of the CPE must have an embedded system logging function and be able to support any client/server based audit trail application.

- The design and manufacture of the CPE must support remote diagnostics.

8.5.2   Access Control

A second method of digital content protection is provided by "access control". Different from the "Content Encryption" methods, Access control transports the content in the clear and uses "Subscriber Management" capability, either in the network or in the CPE, to ensure that only legitimate users may access the content. Access control, however, does not prevent a malicious user from stealing the content via a legitimate user account. This is especially true and tempting in the

case of "Decentralized CPE" deployment scenario. Access control must therefore be used only in the "Centralized CPE" deployment, and even that, it must be coupled with "CPE protection" to provide a reasonable level of security.

8.5.3 Content Encryption

The third method of digital content protection is by encryption. Encryption techniques can be roughly segregated into two classes: symmetric and asymmetric encryptions. Symmetric encryption is efficient in terms of system resource demand and file size compactness, whereas asymmetric encryption is effective in terms of strong security and key uniqueness. For video encryption, which means huge file sizes and high bandwidth processing, security industry in general employs both techniques, i.e. symmetric encryption for the content itself and asymmetric encryption for the key managements.

The following summarize the implementation requirements for content encryption recommended for FS-VDSL:

- Uses industry accepted algorithms and key lengths to encrypt the content data payload. The encryption algorithm and technique deployed must be video format agnostic and be able to support both non-real-time video such as VOD service, and real time event such as sport event with "on-the-fly" encryption of live video streams.

- Best to encrypt the content at source of origination (e.g. encoding house, post production facility, studio) prior to distribution whenever possible.

- Content to remain encrypted in storage on network, distribution to consumer end users and in storage at consumer premises.

- Content decryption keys should be wrapped, delivered and stored separately from content.

- The encryption implementation, for mainly the key and not necessary the content, must be flexible to allow easy and seamless integration with 3rd party e-commerce and subscriber management systems.

- Best to make use of network based subscriber management system as well as CPE's unique identification.

- The encryption system deployed should be interoperable with other industry security architectures such as 5C, CPCM, etc.

8.5.3.1 Conditional Access

The term "Conditional Access" can be traced back to the analog TV broadcast era. Analog-based conditional access is still being used by most cable systems for protecting their premium channels. Basically, it tries to confuse the receiver by removing synchronization information or manipulate the gain control. For FS-VDSL, quite obviously, "Conditional Access" means the use of cryptography for controlling the access to the digital content.

The basic principle of cryptographic conditional access is as follows: The content is encrypted at the video head-end site by a symmetric encryption technique known to both the encryption and decryption devices. The encryption key plus certain other encryption related information together is called ECM (Entitlement Control Message). When the encrypted packet arrives at the receiver (i.e. the VTP/D or FPD), it is first sent through the CAM (Conditional Access Module) for decryption. CAM can be built directly into the receiver or in a secure device like smartcard. The implementation of CAM must be governed by the CPE protection guidelines. Symmetric encryption is not a strong encryption if key length is short (e.g. 64 bits), therefore the key needs to be changed over time. Key change frequency is implementation specific but usually it should proportional to how secure the

encryption is. The general principle is to change the key before the content can be attacked by the brute force cryptanalysis.

The symmetric keys are wrapped by an asymmetric encryption technique (e.g. PKI) in order to provide user authentication and non-repudiation capability. The actual implementation of the key and subscriber management systems is implementation specific, and is outside the scope of the current document. Most service providers prefer Conditional Access, as they inherently become the gatekeepers of the key management, hence owning the business relationship with the end users.

Technically speaking, the encryption based Conditional Access and the Digital Rights Management (DRM, to be discussed in the following section) are similar. The differences between them are four folds.

- Firstly, it is the system flow within the receiving device. Conditional access functions like a secure conduit (similar to the concept of IPSec) and content is in the clear before entering and after departing from the conduit, whereas in the Digital Rights Management system, content stays encrypted all the time and is decrypted only when displayed. Because of this fundamental difference, Conditional Access is not recommended when copying of content from one device to another at the consumer location is allowed (e.g. super-distribution of content).

- Secondly, it is the core network security. Conditional Access provides the secure delivery but it does not protect the distribution of the content before it enters the Conditional Access's system. In order to ensure core network security, operators may need to extend the head end of the Conditional Access to the content source, resulted in unnecessary complicated OAM&P issues.

- Thirdly, it is the digital content cache in the network. Conditional Access is not designed to support network caching and has no concept of allowing content to stay encrypted within the pipe. As such, digital cache must be handled as if it is a content source, resulted in unnecessary cumbersome encryption process, and complicated user management issues.

- Fourthly, it is the key management. Conditional access is meant for secure delivery of the content across a network. Digital rights management, on the other hand, is meant for securing the content and not necessary the delivery of it.

8.5.3.2   Digital Rights Management

Digital Rights Management (DRM) is an emergent technology that allows digital content to be published on an unsecured network and content owners (or their representatives) to maintain the copyright. Most DRM implementations are application level cryptographic solutions. As such, the intent of the FS-VDSL specifications is not to specify what DRM implementation should be. Rather, the current document is to detail the essential requirements to ensure that the VDSL system will support whatever the DRM implementation will be.

The following summarizes a set of guidelines on how to support DRM systems:

- CPE protection as specified in section 4.5.1 must be fully enforced.

- CPE identification must be made available for and retrieved easily by DRM applications.

- CPE is capable of supporting and seamlessly integrating with any 3rd DRM solutions.

- CPE is capable of supporting the coexistence of more than one DRM applications, although these DRM applications may not need to be instantiated and run concurrently.

- CPE vendor may choose to support DRM at firmware or hardware level. However, this should not jeopardize the support of other DRM applications to run at application level.

- CPE, as specified in the CPE protection section, must provide a secured storage for keys.

- CPE system log files must be easily retrievable.

- The solution should cover the encryption and content distribution directly from the owner sites, user and key management system, e-commerce for royalty and fee payments, and most importantly, the CPE management.

- The system should separates the rights information from the encryption and delivery of content.

- The system should store the rights information on the network and be able to deliver the rights information for decryption of the content on demand. However, for broadcast TV support, on-demand delivery of rights information may not be fast enough for channel zapping.

- The DRM solution should be format-agnostic.

9. Requirements for deployment

This chapter is dealing with the deployment of active equipment in the outside plant. In the case of an FS-VDSL network, this active equipment is represented by the ONUas shown in Figure 8.

A study of ONU requirements for the deployment of VDSL networks has been carried out inside FS-VDSL operators to help vendors in designing the most suitable solutions. The operators have provided valuable data on their present access copper plants and outlined some required features for a Optical Network Unit designed to operate in their access networks. The results of this activity are reported in the following paragraphs.

9.1. Access network for VDSL deployment

The VDSL technology allows the reuse of existing copper networks to carry broadband services to residential customers and SME. Since VDSL performance suffers degradation due to crosstalk and cable attenuation, a careful analysis of existing access networks is required to understand the level of VDSL penetration while minimizing investments in new infrastructures (for example, large investments in laying fibre in early stages of deployment). Given this intention, some information about network characteristics of FS-VDSL operators has been gathered. The network survey has focused on areas where operators think VDSL will be deployed initially.

9.1.1 Today's copper networks

Two general models of typical access networks are represented in Figure 4 and Figure 5: the former applies mainly in Europe, while the latter is more suitable for North America. These schemes generally apply since many similarities exist.
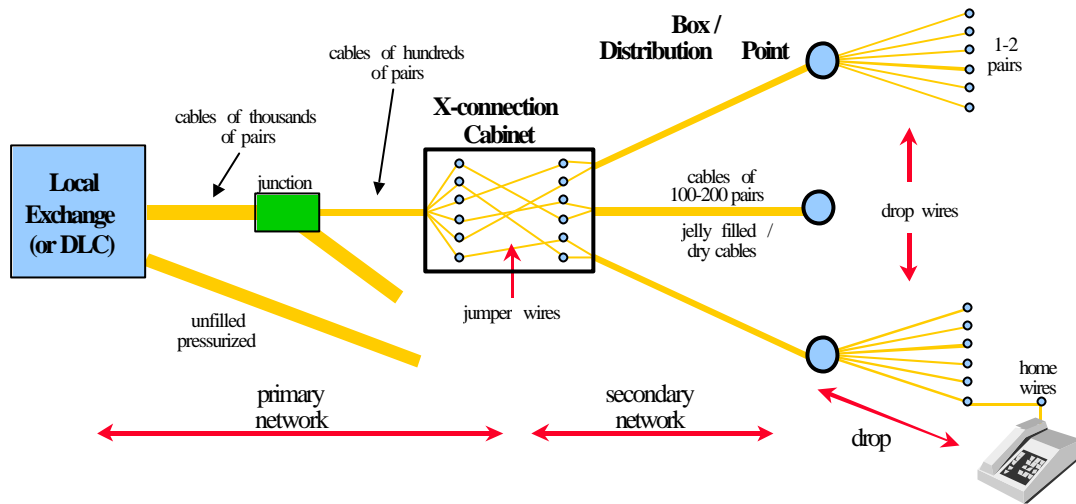
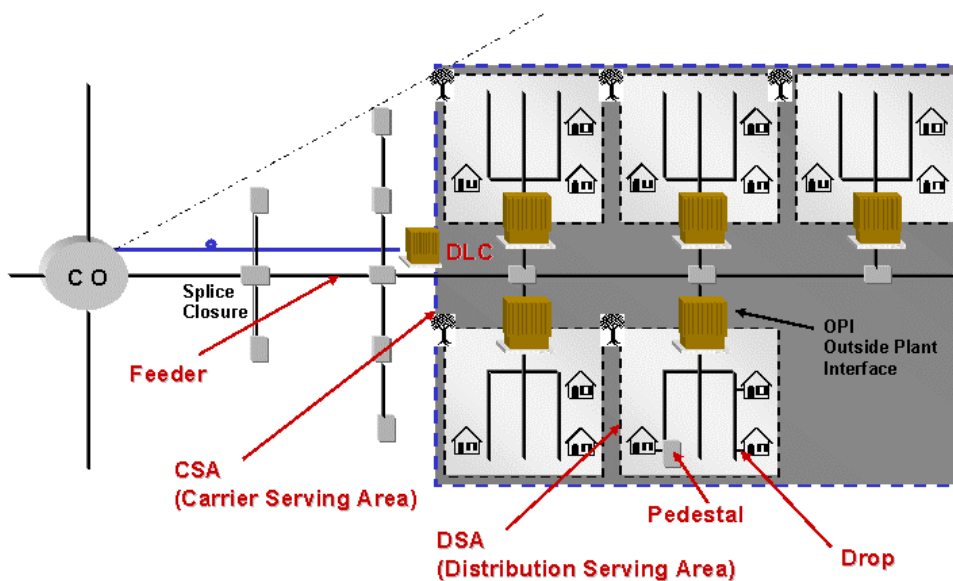**Figure 4 – General model of an access network (Europe)**

Figure 5 – General model of an access network (North America)

Hereafter some definitions of various entities of the access network are reported:

- **Cabinet / Optical Plant Interface (OPI) -** The cabinet/OPI is a major passive flexibility point where it is possible to access the twisted pairs cables for a significant number of customers. Typically the cabinet is within 100 to 1500 metres of the customer building. The cabinet location is an interesting point to collocate the ONU because of the large number of potential homes served.

- **Terminal box –** The terminal box represent the nearest telco-owned flexibility point to the customer. Typically the box would either be within the building or in the external plant and it is also known as the distribution point or pedestal. The box and the cabinet/OPI form part of the

network operator-owned infrastructure and are subject to regulatory constraints. Sometimes in-building infrastructures are owned and managed by the building owner and not subject to regulatory constraints. Some operators are considering installing the ONU within an enhanced enclosure, maybe located in a controlled environment, able to feed a certain number of boxes or cabinets.**DLC -** The Digital Loop Carrier (DLC) is an active device usually located at the entrance of the Carrier Serving Area (CSA) to provide POTS services to the community. DLCs were deployed by operators to serve customers too far from the Central Office (CO) and are fed by fibre or DS-1 lines from the CO. DLCs can also serve the data function provided by the ONU, if so equipped.

- **CSA -** Carrier Serving Areas (CSAs) are geographical areas that delimit the ability by an operator to provide POTS service to a community. CSA definition has evolved with time to include the ability to provide DSL service. CSAs typically vary from within 1 km long (in dense areas) to 3 km (in suburban areas) in the residential segment to offer maximum service flexibility and provide data services without special loop engineering. The DLC is usually located at the entrance of a CSA.

- **DSA -** The Distribution Serving Area (DSA) represents a geographical area where the last outside plant point of physical interconnection between the CO and the residential customers is located. At the entrance of the DSA, there is the OPI that can provide interconnection service to between 300 and 700 residential customers and is the interface point between the feeder and distribution facilities.

Obviously the deployment strategy of each FS-VDSL operators will be affected by the characteristics of the operator's access network. Some interesting figures provided by operators about their access network coverage is reported in Figure 6 and Figure 7. The values are referred to the zones where VDSL will be deployed in first stages, not to all the access network coverage.

In Figure 6 the primary network length refers to the section between the CO/DLC and the cabinet/OPI (primary network/CSA); in Figure 7 the secondary network length refers to the section between the cabinet/OPI and the box (secondary network/DSA).
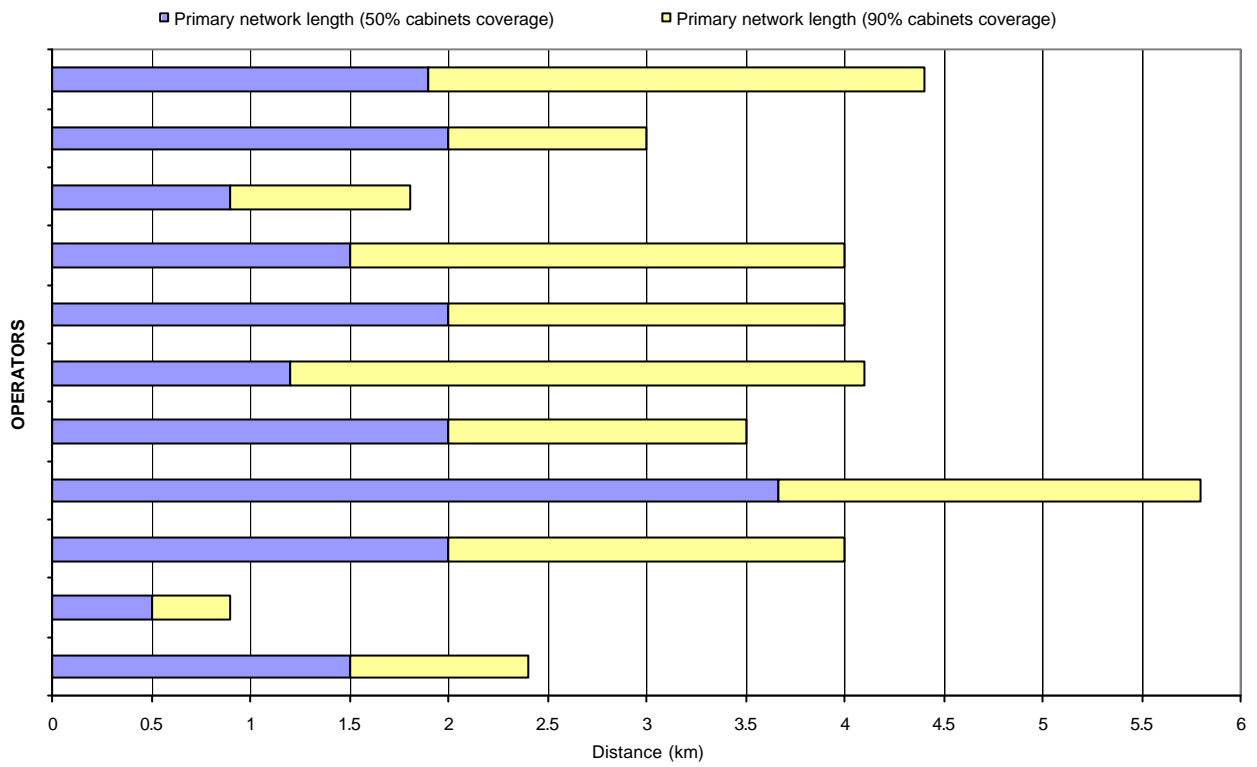
Figure 6 – Primary/CSA network coverage for FS-VDSL operators
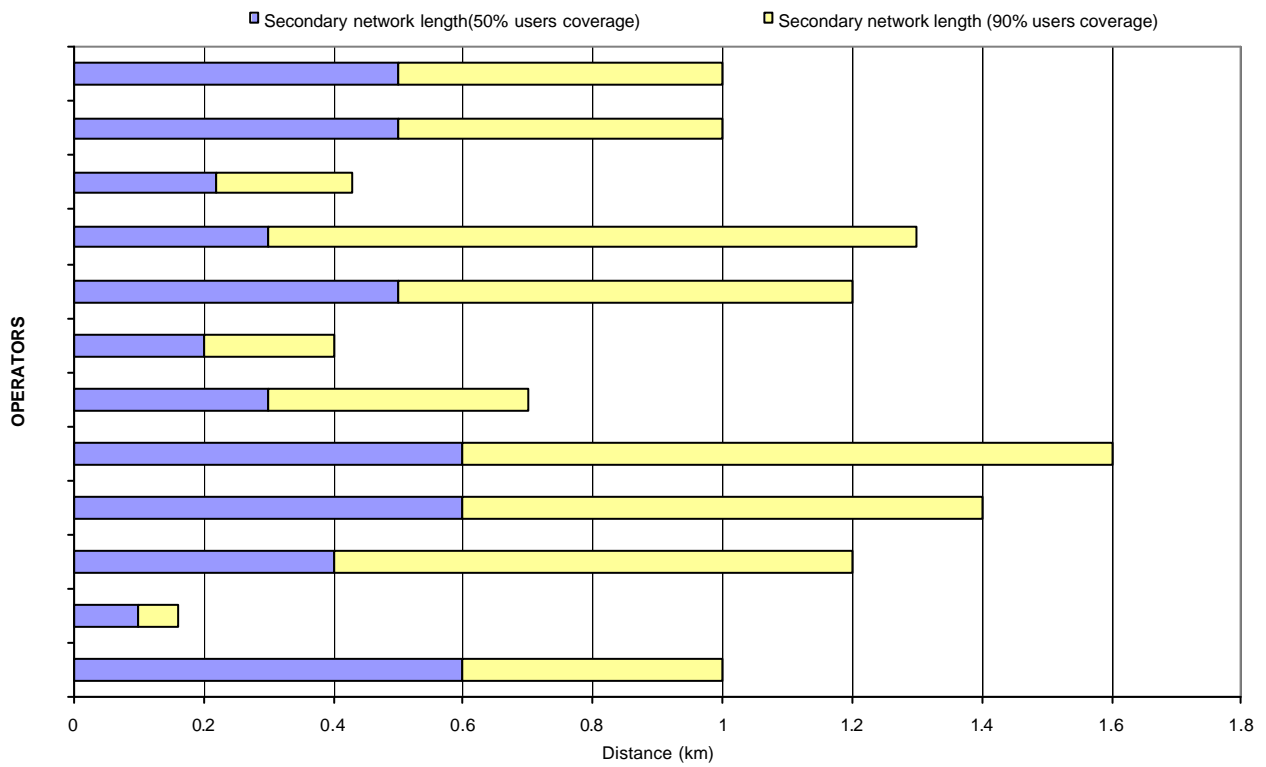
Figure 7 – Secondary/DSA network coverage for FS-VDSL operators

Another interesting figure is the average number of households that can be served from a terminal box, a cabinet/OPI or a DLC, as reported in Table 4.

Table 4 – Average number of household served at various points of the access network

|	OPERATORS											
OPI/Cabinet	250	600	250	500	250	200	350	500	400	200-400	350	110
Terminal Box	20	25	20	8	4	12	7	8	4	N/A	10	7
DLC	N/A	1890	250	N/A	N/A	200	N/A	2000	2000	600-900	450	N/A

9.2. ONU deployment issues

Although the individual needs of FS-VDSL operators vary widely because of their different regulatory, business and structural environment, the structure of access networks is similar and it is possible to define a common platform specification based on requirements from operators.

The Optical Network Unit is the most important network element for the deployment of VDSL in the access network and some information on the desired features of a FS-VDSL ONU have been gathered among operators. These requirements are intended to represent some guidelines to assist vendors in designing the most suitable solutions for the operators, in order to obtain volume cost reductions. Complete detailed specifications for the ONU are not provided, but some highly desirable characteristics from the operators' point of view are outlined.

9.2.1 ONU general scheme

The ONU serves as an ATM cross-connect between the VDSL lines and the Optical Distribution Network. A general diagram of ONU functional blocks is represented in Figure 8. In addition to the blocks which perform the functions described above, there are other blocks necessary to power the equipment, manage the alarms, interface the fibres and the copper pairs and so on.
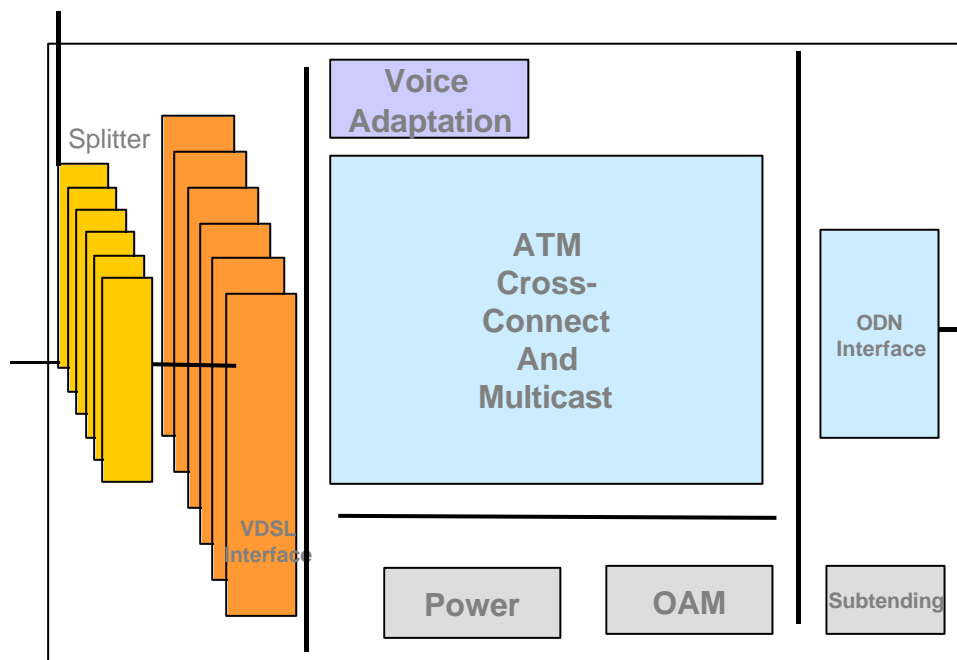
Figure 8 – ONU functional blocks

9.2.2 Powering

The issue of powering an ONU is strictly related to its size and varies widely between a small ONU serving tens of customers at the building and a large cabinet ONU intended for hundreds of customers. The power consumption is determined in the first place by the number of VDSL ports. The power drained by an ONU is expected to be no more than 3 Watts per VDSL port, including all of its functional blocks, such as the optical section, fans, the alarm equipment etc.

Several schemes have been considered for ONU powering. An ONU with 100 ports and more, is expected to be locally powered, and its back up power (where implemented) is planned using batteries.

Battery autonomy from 2 to 8 hours at 25 °C is considered adequate by the majority of the operators. Since very low temperature can highly decrease this value, it's important to keep batteries at a suitable temperature. Also the lifetime of batteries is affected by the temperature variation and a minimum useful lifetime of 10 years in standard conditions (+25 °C) is recommended.

It's also strongly recommended to use batteries requiring no maintenance and having low gas emission (and ensure that ONU enclosure is capable of dissipating emissions).

An optional scheme using remote powering is also being considered, particularly for FTTCab architecture, i.e. for outdoor located ONU, where it could be more difficult to access the main electricity network and manage batteries. For remote power feeding two options are envisaged:

a. Using dedicated power feed: since usually there will be a need to lay a fiber to the street cabinet, it might be possible to lay a power cable with the fiber. With this approach it is expected to deliver about 200 Watts up to 3 km.

b. Using regular telco pairs: according to the limitations imposed by RFT-C and RFT-V circuit (ITU-T K.50). This solution seems to be suitable for small ONU, requiring few pairs for feeding.

This approach is attractive because no batteries are required at the ONU, so that it's possible to relay on centralized feeding and backup capabilities, reducing significantly the size of the ONU and the operational costs (no battery management).

Other powering schemes have been discussed, such as solar panels and reverse powering from user side, but they have not currently considered viable for feeding the ONU by the operators.

9.2.3 Dimensions

The number of VDSL users that an ONU must be able to support is typically very different in a FTTCab or in an FTTB architecture. The target number of lines that an ONU should be able to serve at the Cabinet or at the Box in operators' opinion is reported in Table 5.

Table 5 – Number of VDSL lines served by an ONU

	OPERATORS							
FTTCab	800	60-90	200-300	80-140	48-64 4-8 8-16	40	100-200	128-160	12-48
FTTB	50	4-30	20-40	20-40	8-16	20	100+	128-160	4-12

Typically the ONU could serve the same number of users served today by a passive cabinet/OPI or terminal box; however some operators are planning to have centralized ONU serving a larger number of users, being connected to more than one cabinet or box. This could typically affect the configuration of wiring blocks.

The physical size of the ONU is related to factors such as the achievable number of VDSL ports, the total power consumption, and the power dissipation and temperature issues. Also, accessibility to internal equipment for installation and maintenance is a consideration. Reducing the size of the ONU (compatibly with required functionalities) must be a driving point in designing the equipment since operators, especially in FTTCab scenario, could have difficulties in finding space and obtaining Right of Way / easements from local authorities or private land owners.

9.2.4 Expandability

It is required for an ONU to have a certain degree of modularity regarding the number of VDSL lines that it can support. It must be possible to reach the maximum number of lines by adding VDSL cards when necessary. In this way operators can save extra-costs, buying only the number of cards that they really need and having the possibility of expansion by the simple addition of new cards.

The suitable number of ports per card has been estimated to be 8-12 for a small ONU and 16 (or higher, if a high-density integration will be feasible) for a large ONU. These values allow a certain level of integration without giving up flexibility.

An ONU may include a subtending block to connect additional secondary ONUs to the OLT through the primary ONU ODN interface. This feature, considered optional, would allow a further degree of flexibility and expansion capacity.

9.2.5 Environment

An ONU is required to operate in the following environmental conditions:

- Class 3.2 of ETS 300 019-1-3 for stationary use at partly temperature-controlled locations is suitable for ONUs intended for FTTEx and FTTB (inside the building) deployment

- Class 4.1 of ETS 300 019-1-4 for stationary use at non-weatherprotected location is required for ONUs intended for FTTCab (outside environment) deployment

In some countries Class 4.1E (non-weatherprotected locations – extended) of ETS 300 019-1-4 could be requested for ONUs designed for FTTCab (outside environment) deployment.

The temperature and humidity ranges of the three classes are reported in the Table 6.

Table 6 – Parameters of different environmental classes

Class	Unit	3.2	4.1	4.1E
Low air temperature	°C	-5	-33	-45
High air temperature	°C	45	40	45
Low relative humidity	%	5	15	8
High relative humidity	%	95	100	100

Passive cooling (with non-forced heat transfer from inside the ONU to the outside) is the preferred solution, because it has lower costs, minimum maintenance and mitigates noise issues.

9.2.6 EMC and protections

The ONU must be compliant with the following specifications about EMC and protections:

- ITU-T K.34

- ITU-T K.43

- CISPR 22 for emission
- CISPR 24 for immunity
- ITU-T K.45 for resistibility
- GR-1089-CORE for EMC and electrical safety for telecommunications equipment

More severe national requirements could be requested by operators.

9.2.7   Availability

Operators require an availability of the access network of 99.99%. This corresponds to a maximum downtime of 53 min/yr for the access network section (this figure comprise the ONU/OLT, ODN, and copper pairs).

This 53 min/yr should be allocated to the active equipment and the network according to

Table 7.

Table 7 – Downtime per access network element

Access Network Element	Max. Downtime/yr/channel
OLT	10 min
Network (cables etc)	17 min
ONU	26 min

It is assumed that the failed hardware is a field replaceable plug-in unit. To calculate the Mean Time Between Failures (MTBF) of the active equipment it's necessary to define the Mean Time to Repair (MTTR) for each kind of device. The MTTR is assumed to be:

- 2 hours for the OLT
- 6 hours for equipment outside the central office building (ONU)

The requirements on Mean Time Between Failure (MTBF), calculated according to the following formula:

$$MTBF = \frac{MTTR}{Downtime/yr}$$

are the followings:

- OLT MTBF = 12.0 years
- ONU MTBF = 13.8 years

Each ONU and OLT manufacturer should, when requested, supply design documentation showing component MTBF calculations and describing how component MTBF and component redundancy are used to meet operators' availability objectives.

9.2.8   Summary Table

According to the considerations discussed in precedent paragraphs, specifications for three different types of ONU are reported in Table 8 as an example and summary of the FS-VDSL operators' requirements.

Table 8 – Characteristics of three type of ONU

	Large-sized ONU	Medium-sized ONU	Small-sized ONU
Number of lines served	300	100	24
Local powering arrangements	230 V 50 Hz AC (Europe) 110 V 60 Hz AC (North America)		
Remote powering	No	Optional with dedicated power cable	Optional with telco pairs (RFT-C/RFT-V) or dedicated power cable
Battery autonomy	Optional 2-8 hrs		
Add-on cards modularity	32	32	12
Subtending module	Optional		
Environmental conditions	ETS 300 019-4 Class 4.1 (Class 4.1E could be required) for FTTCab ETS 300 019-3 Class 3.2 for FTTB		
Cooling	Active	Active/passive	Passive
Heating	Optional (see environmental conditions)		
Availability (MTBF)	13.8 years		
Dual homing	Optional	Optional	No
Alarms	Required (see OA M specification)		
Metallic test access	Optional (see OA M specification)		
EMC and protections	ITU-T K.34 ITU-T K.43 CISPR 22 CISPR 24 ITU-T K.45 GR-1089-CORE		
Optical interface	See section 9		

10. Optical Access Network Requirements

This chapter discusses the segment of access network between R/S and S/R reference points of the FS-VDSL architecture. These are the interfaces between the OLT and the ONU, as described in Figure 9.
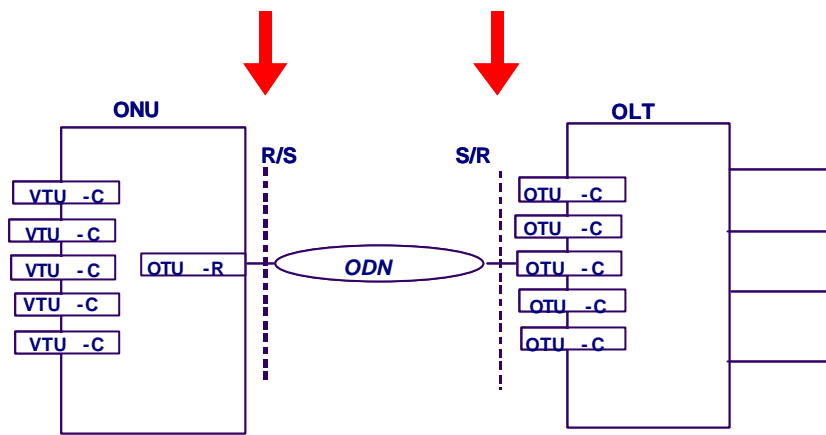
Figure 9 – Optical interfaces between ONU and OLT

The meaning of this chapter is not to specify the architecture of the optical part of the access network, but to provide specific requirements for the optical interfaces between the ONU and OLT.

Use of standardized interfaces (STM-1/4, OC-3/12, G.983, 1 Gbps interfaces) is preferred as it takes advantage of standards (with complete technical description), which are known by operators for deployment, implementation and measurement issues.

Since interoperability is not strictly required between the ONU and OLT from different manufacturers, use of proprietary interfaces may represent an opportunity for technical issues and cost effectiveness. It is also important to understand how these proprietary interfaces could evolve towards standardized ones.

In the case of proprietary optical interfaces, between R/S and S/R reference points of the FS-VDSL architecture, the operators have considered necessary to outline a minimum set of requirements at the Physical Medium Level which proprietary interfaces must satisfy.

These requirements are given hereafter:

- Network architecture (point to point or point to multipoint)
- Fibre type
- Bit rates for Downstream / Upstream directions
- Bidirectional transmission (1 fibre WDM or 2 fibres)
- Operating wavelength
- Minimum optical attenuation range between S/R and R/S reference points
- Supported split ratio (point to multipoint)
- Optical connectors.

No requirements are given about:

- Maintenance Wavelength
- Launched power at the S/R and R/S points
- Sensitivity at the S/R and R/S points
- Equipment reflectance at the S/R and R/S points

Operators have expressed their preferences on the above requirements for proprietary optical interfaces. The results of this survey are given in Table 9.

Regarding the proprietary interfaces, it should be noticed that, at the physical layer, the operators' preferences are very closed to existing standardized ones (G.983) with the needs to consider evolutions towards 1 Gbps interfaces.

Table 9 – Operator survey regarding optical interfaces

Requirement	Value	Operators' answer
Architecture	P2P	Y
	P2MP	Y
Fiber type	G.652	Y
Bit rate downstream	622.08 Mbps	Y and higher rates
Bit rate upstream	155.52 Mbps	Y and higher rates
Bidirectional transmission mode	1 fibre WDM	Y
	2 fibres	Y
Optical Wavelength	2 fiber Up : 1.26-1.36 μm Down : 1.48-1.58 μm	Y
	2 fiber 1.26-1.36 μm	Y
Minimum attenuation range between S/R and R/S points	10 dB for P2P	Y
	25 dB for P2MP	Y
P2MP supported split ratio	32	Y and possibly others
Optical connectors	Standardized connectors	Y