

Test Suite for Full-Service End-to-End Analysis of Access Solutions

Part 1: Test objectives

Rob F.M. van den Brink – TNO
Task Force leader TF4: "Lab Trials"
(e-mail: Rob.vandenBrink@tno.nl)

Kamal Ahmed - TNO
Editor M TF4.4 "Test Suite, Part 1: Test Objectives"
(e-mail: kamal.ahmed@tno.nl)

Plus TF4 Team (*see contributing authors per chapter*)

Identifier:	Deliverable D TF4.4a
Class:	Report
Version:	Final, December 2007 (V16)
Version Date:	December 20th, 2007
Distribution:	Public
Responsible Partner:	TNO
Filename:	MUSE_TestSuite_Part1

DOCUMENT INFORMATION

Project ref. No.	IST-6thFP-26442
Project acronym	MUSE
Project full title	Multi-Service Access Everywhere
Security (distribution level)	Public
Contractual delivery date	June 2007
Actual delivery date	July 12 2007 (Final Update Dec 2007)
Deliverable number	DTF4.4a
Deliverable name	Test Suite for Full-Service End-to-End Analysis of Access Solutions, Part 1
Type	Report
Status & version	Version December 2007 - V16
Number of pages	294
WP / TF contributing	TF4
WP / TF responsible	TF4
Editor(s)	Kamal Ahmed (TNO), compiled from various focus documents (*Federiko Krommendijk, TNO, from 2004 till oct 2006*)
EU Project Officer	Pertti Jauhiainen
Keywords	Testing, access networks, QoS, Quality of Service, connectivity, residential gateway, management system, xDSL, fibre.
Abstract (for dissemination)	This *test suite*, is a comprehensive document, that provides a holistic *system* view on testing to analyze the capabilities of access systems. It describes a wide range of test objectives in significant detail, and guides the reader through state-of-the-art views and many standards (when appropriate). This “part 1” of this “*test suite*” describes **what** should be tested (the objectives) while the accompanying part is dedicated on *how* the tests should be performed (the methods)

Contributing Authors per Chapter

chapter		Names
1	intro	Rob van den Brink (TNO).
2	def	All
3	class	Hervé le Bihan (THO), Rob Kooij (TNO), António Gamelas (PT), Gilbert le Houerou (FT), Federiko Krommendijk (TNO), Rob van den Brink (TNO), Pieter Liefooghe (IMEC), Brecht Vermeulen (IMEC).
4	serv	Hervé le Bihan (THO), Rob van den Brink (TNO), Georgina Galizzo (TID) + QoS-team (chapter 5).
5	qos	Rob Kooij (TNO), Jeroen van Vugt (TNO), Kamal Ahmed (TNO), Kjell Brunnström (ACR), Tanja Kauppinen (ACR), Georgina Gallizo (TID), António Gamelas (PT)
6	con/S	Pieter Liefooghe (IME), Brecht Vermeulen (IME), Björn Nagel (DT), Arnaud Riaudel (FT), Frank Geilhardt (DT)
7	con/N	Pieter Liefooghe (IME), Brecht Vermeulen (IME), Björn Nagel (DT), Arnaud Riaudel (FT), Frank Geilhardt (DT)
8	con/RG	Johannes Deleu (IBBT), Brecht Vermeulen (IBBT), Alex De Smedt (THO)
9	man	Gilbert le Houerou (FT), Federiko Krommendijk (TNO), Harold Balemans (LuNL), Hélder Alves (PTI), Bruno Veloso (PTI), Rob van den Brink (TNO).
10	xdsl	Bas Gerrits (TNO), Rob van den Brink (TNO), Mauro Tilocca (TI)
11	fibre	Andrzej Mosek (TP), Marcin Ratkiewicz (TP), Kai Habel (HHI), Klaus-Dieter Langer (HHI).

DOCUMENT HISTORY

This document has been created during a period of four years (2004-2007) and interim releases have been published various times. This version is V16, and considered as the final version delivered by MUSE.

TABLE OF CONTENTS

DOCUMENT INFORMATION **2**

TABLE OF CONTENTS **4**

EXECUTIVE SUMMARY **8**

1 INTRODUCTION **9**
1.1 Scope 9
1.2 Objectives 9
1.3 Innovation – what is new? 11
1.4 History of the creation of this document 11

2 DEFINITIONS **13**
2.1 Terminology 13
2.2 Abbreviations 17

3 CLASSIFICATION FRAMEWORK FOR E2E TESTING **24**
3.1 Purpose of this chapter 24
3.2 Classification of Services 24
3.3 Classification of Network Domains 28
3.4 Classification of Connectivity 29
3.4.1 OSI Reference Model *29*
3.4.2 TCP/IP Reference Model *30*
3.5 Classification of QoS 31
3.6 Classification of Management functions 32
3.6.1 TMN model *33*
3.6.2 e-TOM model *33*

4 INVENTORY OF SERVICE REQUIREMENTS **35**
4.1 Introduction 35
4.2 Basic Characteristics of Services 35
4.3 Basic Requirements to Enable Quality 40
4.4 Basic Requirements to Enable Security 43
4.4.1 Unauthorised reception/obtaining of information *43*
4.4.2 Unauthorised usage of resources *45*
4.4.3 Disturbing the proper functioning of services, networks, applications *46*
4.4.4 Untraceable or repudiated sending of 'bad' information *47*
4.5 Basic Requirements to Enable Connectivity 48
4.6 Basic requirements on Naming and Numbering 48
4.7 Basic Requirements on AAA 50
4.7.1 Authentication requirements *50*
4.7.2 Authorization requirements *50*
4.7.3 Accounting requirements *51*
4.8 Other Basic Requirements 52
4.9 High level requirements for advanced applications 52
4.10 "Full service" testing with a limited number of applications 56
4.10.1 E2E Service Requirements *56*
4.10.2 E2E Network Requirements *58*

5 QOS TESTING **63**
5.1 Introduction 63
5.2 Perceived service quality for end users 63
5.2.1 Perceived quality factors for Voice over IP *64*
5.2.2 Perceived quality factors for Streaming video *65*
5.2.3 Perceived quality factors for Videoconference *66*

5.2.4 Perceived quality factors for Web browsing and bulk data....66
5.2.5 Perceived quality factors for Interactive gaming....67
5.3 Measuring perceived quality....67
5.3.1 Subjective measurements....68
5.3.2 Objective measurements....68
5.3.3 Using network quality to predict user-perceived quality....68
5.3.4 Hierarchy of test methods for perceived quality....69
5.3.5 Summary....70
5.4 Measuring network quality....70
5.4.1 Network QoS parameters....70
5.4.2 Measurement framework....72
5.4.3 Proposed measurements for network quality per application....72
5.5 Summary....73
5.6 Inventory of Standards....74
5.6.1 ITU....75
5.6.2 IETF....75
5.6.3 Other standardization bodies....75
5.7 References....76

6 SERVICE CONNECTIVITY TESTING....83
6.1 Introduction....83
6.2 Test Objectives: Service VIEW....84
6.3 High-speed Internet Access Service....85
6.3.1 Description....85
6.3.2 Limiting Presumptions....85
6.3.3 Application Layer protocols....85
6.3.4 Transport Protocols....85
6.3.5 Network Protocols....85
6.3.6 High-Speed Internet Tests....86
6.4 Multicast Streaming Service....87
6.4.1 Description....87
6.4.2 Limiting presumptions....87
6.4.3 Application Layer Protocols....87
6.4.4 Transport Layer Protocols....88
6.4.5 Network Layer Protocols....88
6.4.6 Link-Layer Protocols....92
6.4.7 Multicast Streaming Tests....93
6.5 Voice over IP Service....96
6.5.1 Description....96
6.5.2 Limiting Presumptions....97
6.5.3 Application Layer Protocols....97
6.5.4 Network Layer....100
6.5.5 Voice over IP Tests....100
6.6 Inventory of standards....103
6.6.1 ITU-T....103
6.6.2 IETF....103
6.6.3 Other standardization bodies....103

7 NETWORK CONNECTIVITY TESTING....109
7.1 MUSE Architectures....109
7.2 The MUSE reference model....110
7.3 The MUSE Data Plane....111
7.3.1 Interfaces....112
7.3.2 Data Plane TESTS....115
7.4 The MUSE Control Plane....119
7.4.1 Authentication....119
7.4.2 Auto-configuration....123
7.4.3 MUSE QoS Architecture....125
7.4.4 Control Plane TESTS....130

7.5 References 135

8 CONNECTIVITY TESTING OF RESIDENTIAL GATEWAYS 140
8.1 Multicast test objectives 141
8.1.1 IGMPv3 Requirements 141
8.1.2 IGMPv3-Proxy Requirements 148
8.1.3 DSLForum Multicast RGW Requirements 149
8.2 DHCP test objectives 151
8.2.1 Sources 151
8.2.2 Message requirements 151
8.2.3 Client Requirements 163
8.2.4 Server Requirements 169
8.2.5 DHCP Options 173
8.3 VLAN 177

9 MANAGEMENT TESTING 179
9.1 Selecting a reference model for MUSE Management Tests 179
9.1.1 Fault management 181
9.1.2 Configuration Management 181
9.1.3 Accounting Management 181
9.1.4 Performance Management 181
9.1.5 Security Management 182
9.2 Management Tests Objectives 182
9.2.1 Testing Fault Management 183
9.2.2 Testing Configuration Management 196
9.2.3 Testing Account Management 209
9.2.4 Testing Performance Management 218
9.2.5 Testing Security Management 226
9.3 References 233

10 XDSL SPECIFIC TESTING 235
10.1 Introduction 235
10.1.1 Functional testing 236
10.1.2 Conformance testing 236
10.1.3 Choosing between functional and conformance testing 236
10.2 Testing management capabilities 237
10.2.1 Testing configuration management 237
10.2.2 Line configuration 237
10.2.3 Channel configuration 240
10.2.4 Testing monitoring capabilities 241
10.3 Testing Usability 243
10.4 Testing Transceiver signal characteristics 244
10.4.1 Total transmit power 244
10.4.2 Power Spectral Density 245
10.4.3 Power adaption 246
10.4.4 Power management 248
10.4.5 Power consumption 249
10.5 Testing performance under noisy stress conditions 249
10.5.1 Basic test setup and stress conditions 250
10.5.2 Testing margin under stationary cross talk noise conditions 253
10.5.3 Testing bit rate under stationary crosstalk noise conditions 254
10.5.4 Testing Reach under stationary crosstalk noise conditions 255
10.5.5 Testing performance under other noise conditions 256
10.5.6 Testing minimum required performance 257
10.6 Summary 258
10.7 References 261

11 FIBRE SPECIFIC TESTING 263
11.1 Introduction 263
11.2 Overall testing plan 267

11.3 Functional tests 267
11.3.1 Testing management capabilities 267
11.3.2 Monitoring capabilities 268
11.3.3 Security tests 269
11.3.4 Redundancy tests 272
11.4 External interface aspects 272
11.4.1 Analogue external interfaces 273
11.4.2 Framed digital external interfaces 274
11.4.3 Digital external interfaces 276
11.5 Optical technology aspects 277
11.5.1 Element specific aspects 278
11.5.2 Optical technology specific aspects 285
11.6 Inventory of standards and other documents 293
11.7 References 294

EXECUTIVE SUMMARY

Challenge State-of-the-art access networks are so complex, that it has become a real challenge to analyse their most relevant capabilities and shortcomings and to compare them with other access solutions. Nevertheless adequate analyses are vital for both operators and vendors, for different reasons:

- *For operators*: to support migration decisions, to development meaningful RFI/RFQ documents and to judge different technology platforms.
- *For vendors*: to improve/debug solutions, and to convince customers how adequate proposed solutions are.

The real challenge is to make well-balanced judgements by analysing a *system as a whole*, in stead of analysing individual elements or sub-systems. This requires a holistic top-down view on what characteristics of a system are relevant, and how to identify them.
However, to enable such an analysis, detailed expertise is required on *all* relevant properties to know "what" and "how" to analyse them by suitable tests. The way of testing physical layer aspects of individual elements is something that may be found in various product standards, but when higher layer characteristics are to be analysed the required information is scarce or even lacking.

Aim The aim of this document is to provide operators and vendors with a Test Suite, in multiple parts, that guides them to the most relevant aspects of "full-service, end-to-end" analysis of access systems. This part 1 (the "test objectives") gives guidance on "what to test", while the companion part 2 (the "test methods") gives guidance on "how to test". This Test Suite is to combine knowledge from dedicated experts, and to address a wide range of properties related to quality of service (QoS), connectivity, management and transmission. These two parts are to provide a basis for certification documents (outside the scope of this test suite).

Results The current part 1 of this test suite, is a comprehensive document, that provides a holistic *system* view on "what to test" for analyzing the capabilities of access systems. It describes a wide range of test objectives in significant detail, and guides the reader through state-of-the-art views and many standards (when appropriated). The current version provides vendors with necessary knowledge for system development, and operators with essential "tools" for complete system analysis. The test objectives that are summarized in this document, are by definition based on prior art, but from a holistic point of view this document is unique. Such a single source of reference has not created before, due to the wide range of topics that are addressed in a single source.

Recent additions A previous version of this document was published in 2005. During the second phase of MUSE (2006-2007) lots of material has been added, harmonized and refined. A new chapter on Residential Gateways was created from scratch and most of the chapter related to fibre was rewritten to make it system-oriented. The objectives for testing management systems are now fully in line with the TMN model, and elaborated in detail. The QoS chapter was refined, and the chapter related to xDSL has added several topics being introduced by VDSL2.

1 INTRODUCTION

1.1 Scope

The present document gives guidance on a common framework (test suite) for analysing *access solutions* from a *full service*, *end-to-end* point of view. End-to-end refers in this context to all connectivity between the edge of a core network (usually at a central office) and an application terminal (usually at a customer premises).

The scope covers the description of all essential aspects of testing access solutions, and covers the full width of these tests. This includes:

- A top-down identification of all properties that are relevant for testing;
- A top-level explanation for testers why (and when) these properties are relevant;
- the identification of relevant parts of existing documents (e.g. standards);
- the identification of the issues that are missing in existing documents;
- the description of possible test solutions, in case of missing issues;
- all other descriptions of "tools" to identify how adequate a specific access solution is to deliver a full set of services.

This document is focussed on *integrated* analysis of a *system* as a whole, and how the properties of individual system elements influences the overall behaviour, rather than *stand alone* testing of individual elements or components. The certification of access solution that can pass all tests described here is beyond the scope of this document.

The present document is part 1 of a multi-part deliverable, covering test suite documents for full service, end-to-end analysis, as identified below:

- **Part 1: "test objectives"**, a document that identifies what to test.
- **Part 2: "test methods", a document that identifies how to test.**

1.2 Objectives

The objective is to provide a singe source of reference, for end-to-end analysis by testing. The document is to give the means for finding answers to the question how adequate a particular access solution is for delivering a full set of services.

The aim is to cover the full width of end-to-end testing, to be as complete as possible within the limits of available expertise and resources, and to refer to relevant standards as much as possible. The remaining missing or unsolved issues in these standards are assumed to be identified in this document.
Another aim is to provide sufficient background information about all functionalities and capabilities of an access solution that are to be tested, and why these properties are relevant. The same applies to the inventory of selected standards.

A first purpose of end-to-end analysis is to provide feedback to the designers and to enable a balanced view on the capabilities, functionality, performance and maturity of an access solution. The MUSE project can use this to debug the MUSE architecture and the platforms resulting from the various sub projects. However, the list of possible application of this document is wider, and includes:

- To debug solutions that are under development (architecture, equipment,)

- To facilitate a consistent presentation of the test results
- to identify strong and weak points of a solution
- to support strategic decisions on migration scenarios
- To select one solution out of many offers from different vendors.
- to improve existing standards by identify missing or irrelevant requirements
- to provide input for the creating of additional certification documents
- To provide a well-balanced top down view on end-to-end testing, and to improve measurement skills.

The tests should give the best possible prognoses about the operation of an access solution:

- **End-to-end** testing covers, within the context of this document, everything between a service platform and an end-user application terminal, with the restriction that it can be build-up in a lab environment.
- **Full service** testing covers, within the context of this document, a range of representative services for which the solution should provide access to end users, with the restriction that it can be build-up in a lab environment. The range should include at least a voice, video and data service, and preferably services with high user interaction (e.g. gaming) as well.

Figure 1-1 illustrates the structure of the chapters in the Test Suite. Each block represents an individual chapter, and the its vertical position and height is roughly indicative for the OSI layers being covered by that particular chapter.

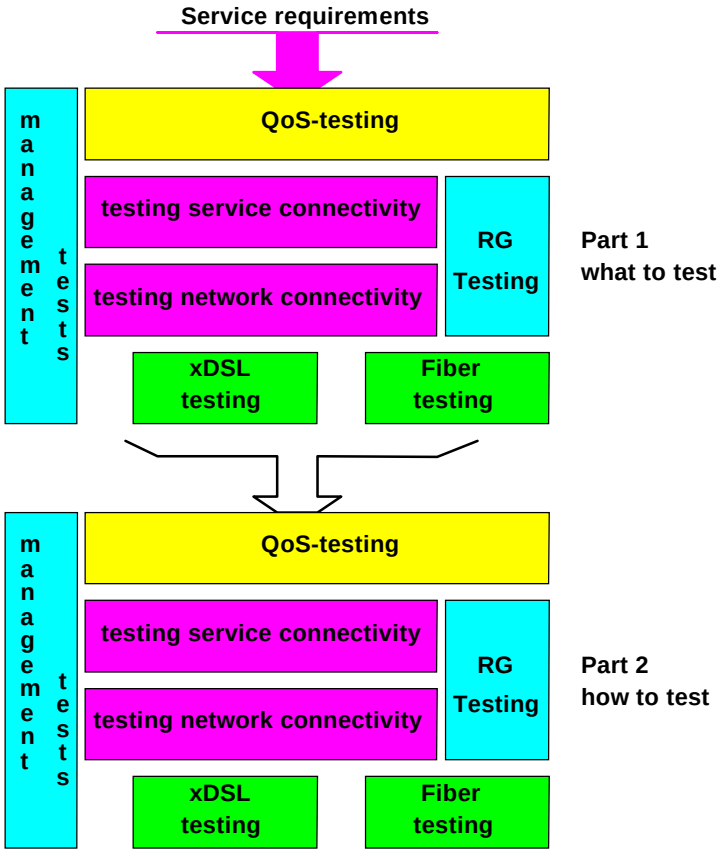


Figure 1-1: Schematic overview of various aspects of end-to-end testing

Testing means identifying or quantifying all kinds of relevant properties of an access solution. There are different ways to achieve that, and each property has its own preferred one:

- ***Measuring*** means an objective quantification of a property, such as performance, stability, delay, jitter, throughput/bandwidth, packet loss, etc. The result can be a number or a curve.
- ***Scoring*** means a subjective quantification of a property such as for security, scalability, manageability, robustness, etc. The result can be an opinion score, for instance ranging between "low", "medium" and "high".
- ***Verifying*** means an objective identification of the presence a property. For instance the capability to support multiple channels over a single link. The result can be a "yes" or "no" answer to the question if some capability is supported.

1.3 Innovation – what is new?

It is a simple question to ask how adequate a specific access solution can deliver a full set of services. The answer, however, is quite complicated. The concept of a new solution can be very future proof, but if the implementation is immature, or if a specific capability/functionality is not supported, then the solution as a whole may be inadequate for the job.
So to answer such a simple question, the access solution need to be analyzed on a variety of aspects, ranging from transport capabilities to management of the system, and from quality of service to security of the connection. But what are relevant properties to be tested for all aspects of such analysis? How to test each property to enable meaningful conclusions? What list of properties can be considered as sufficiently complete to judge a solution-under-test as adequate for the job? In other words, one has to be an expert on *all* these aspects to enable a good answer.
The answer to what and how to test cannot be found by reading only a few leading standards with chapters on testing. This is because many standards are dedicated only to a single device, a single interface or a single point of view. In addition, adequate documents on testing higher layers are limited or even lacking. This is the gap that is filled by this present document.

The *innovation* from this present document is that it is a *single* document covering such a wide range of end-to-end aspects for testing access solutions. To our knowledge, this has never done before on such a wide scale, and MUSE has enabled this by bringing a wide range of expertises together.

Recent additions
A previous version of this document was published in 2005. During the second phase of MUSE (2006-2007) lots of material has been added, harmonized and refined. A new chapter on Residential Gateways was created from scratch and most of the chapter related to fibre was rewritten to make it system-oriented. The objectives for testing management systems are now fully in line with the TMN model, and elaborated in detail. The QoS chapter was refined, and the chapter related to xDSL has added several topics being introduced by VDSL2.

1.4 History of the creation of this document

Work on this test suite started in 2004 by a multi-disciplinary team of experts that were made available for the MUSE consortium. It was clear from the beginning, that it would be impossible to define the full structure of the document in advance, since this work started

almost from scratch. Therefore a two-step approach was chosen to create this document, as illustrated in Figure 1-2.

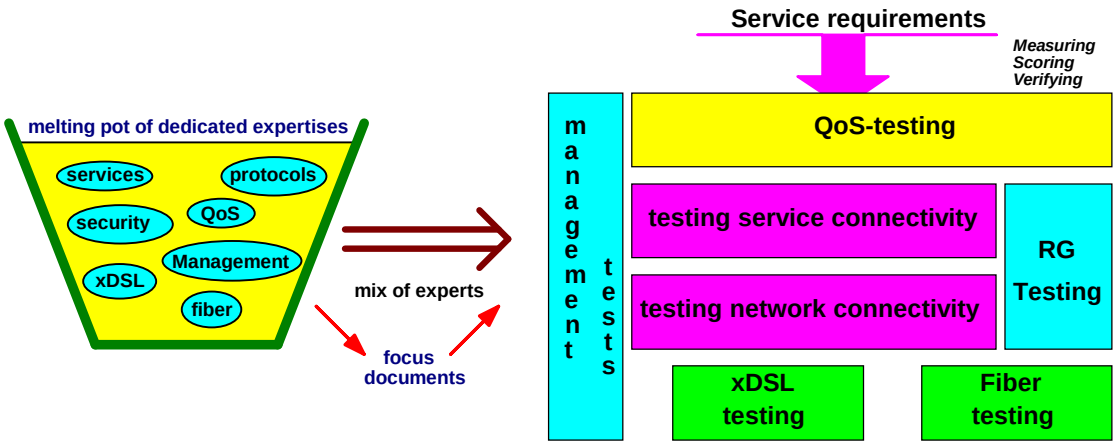


Figure 1-2: Schematic overview of the two-step approach being followed to create this part 1 of the test suite

MUSE facilitated the equivalent of a “melting pot” of a variety of experts, each of them with a different background. Small teams of experts were formed to focus on a dedicated knowledge area, and each team produced a focus document on testing. The overall structure was created later on in an iterative way from these intermediate focus documents and the current part 1 was compiled several times from the latest versions. This two-step approach, where the individual focus documents were kept leading and where the editor of the test suite gives only guidance on a common framework, has proven to be very effective. As a result, the current table of content has appeared to be different from what was expected at the beginning.

2 DEFINITIONS

2.1 Terminology

Test suite refers to a set of documents, summarizing a battery of tests. A test suite can describe a test in detail or simply refer to detailed descriptions in public documents.

Access solution refers to all hardware and software means that facilitates and controls the connectivity between the edge of a core network and an end-user application terminal. This includes transport of data, management of systems and the security of the connection.

======= *Tests* =======

End-to-end testing means, within the context of this document, a test that covers everything between a service platform and an end-user terminal, with the restriction that it can be build-up in a lab environment.

Full service testing means, within the context of this document, a test that covers a range of representative services for which the solution should provide access to end users, with the restriction that it can be build-up in a lab environment. The range should include at least a voice, video and data service, and preferably services with high user interaction (e.g. gaming) as well.

Performance tests are tests to determine how a solution operates under well defined stress conditions. A Layer-1 example is the maximum bitrate of an xDSL modem, when the transmit signal is attenuated (cable loss) and deteriorated by noise (crosstalk, ingress, etc). Higher layer examples are measurements of throughput, jitter, delay/latency, switching/routing capacity under a high number of service connections, etc.

Functional tests are aimed at verifying the system's capacity to perform a given function envisaged by the system. In particular, the actions and reactions of the system are considered from the outside, by analyzing the messages exchanged on the involved interfaces and by verifying the effects obtained on the elements under study. Each test is passed if they give the desired effects and if the exchanged messages are coherent with the service specifications.
For instance, a functional test for a telephone system might be to go off-hook on a phone set and observe how the system will respond to that. Another functional test can be to verify if modems can start-up under noisy stress conditions, which has some similarity with performance tests.

Conformance tests are tests for to determine if a specific solution (piece of equipment or software) satisfies the criteria in a specified requirement document ("standards") like an IETF RFC, DSL Forum TR, ETSI TS/TR, or an ITU Recommendation.
The result of such a test is typically that a solution is “compliant” or “not-compliant” with the mandatory requirements of such a requirement document.

Interoperability tests are tests to verify if equipment implementations from different vendors can operate when they are interconnected. It is for instance not obvious that an ADSL modem from vendor 1 is interoperable with an ADSL access node (DSLAM) from vendor 2. It

is also not obvious that they can support all functionalities under the same stress conditions as solutions from the same vendor would likely do.
Interoperability tests are primarily functional tests, but may have more overlap with the previous tests:

- If the test also verifies if specific performance requirements are met under significant stress conditions, then the test is a performance test as well.
- If such interoperability tests are specified in terms of fulfilling a requirement document, then the test is a conformance test as well.

Suitability tests (also known as *credibility tests*) are test to identify the strong and weak points of solutions and to identify if the solution is adequate for a certain network-architecture/service-paradigm. The results can support strategic decisions on product selection or migration scenarios. They can also be used to debug solutions that are under development.
Suitability tests are typically a mix between (a subset of) characteristics specified in a requirement document, and other characteristics that are seen as relevant.

======= *Services and quality* =======

Perceived QoS**:** quality of a service or application as experienced by an end-user. Recently it has become fashionable to use the term Quality of Experience (QoE) to denote perceived QoS. In this document we do not follow this trend.

Network quality**:** statements of the performance of a network in terms of delay, delay variation, packet loss and bandwidth.

Note that the end-to-end perceived QoS will depend on input signal, the network quality and on the terminal quality.

Subjective assessment of quality**:** methods for determining the perceived quality of an application through a test panel.

Objective assessment of quality**:** methods for determining the perceived quality of an application either through a cognitive/perceptual model that mimics the human audio/visual system or through a mapping from network and terminal quality.

Service**:** Family of applications with the same characteristics with respect to network requirements, i.e. interactive, error-tolerant services.

Application**:** Member of a service class, e.g. Voice-over-IP.

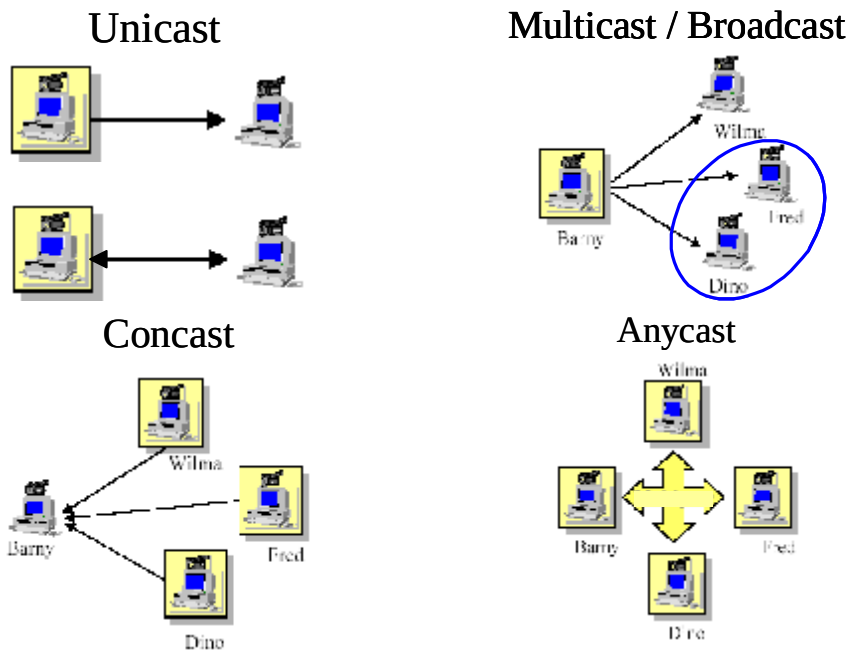
======= *Connectivity* =======

Unicast, means 1:1 communication between terminals. The dataflow can be unidirectionally (such as Video on Demand and Data Downloading) or bidirectionally (e.g. video telephony).

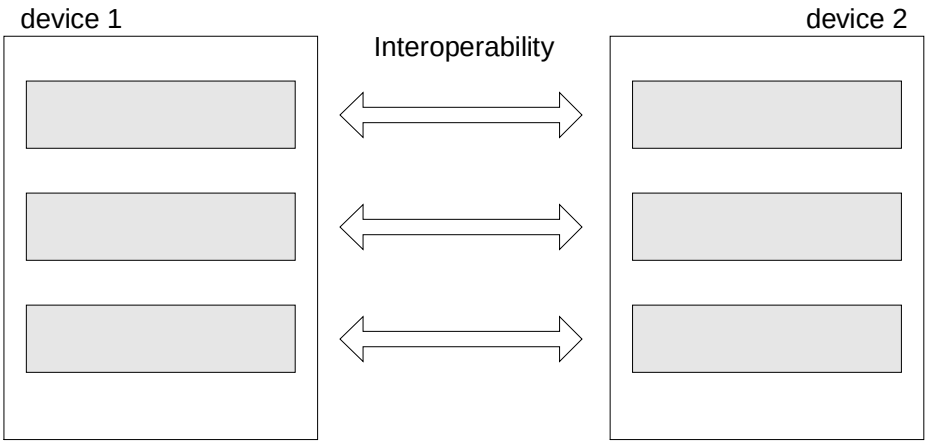
Multicast/Broadcast, means 1:n communication between one terminal and many terminals. The dataflow is unidirectional (e.g. Broadcast TV)

Concast, means m:1 communication between many terminals and one terminal. The dataflow is unidirectional (e.g. Tele-Working, Webcam, Data-Upload)

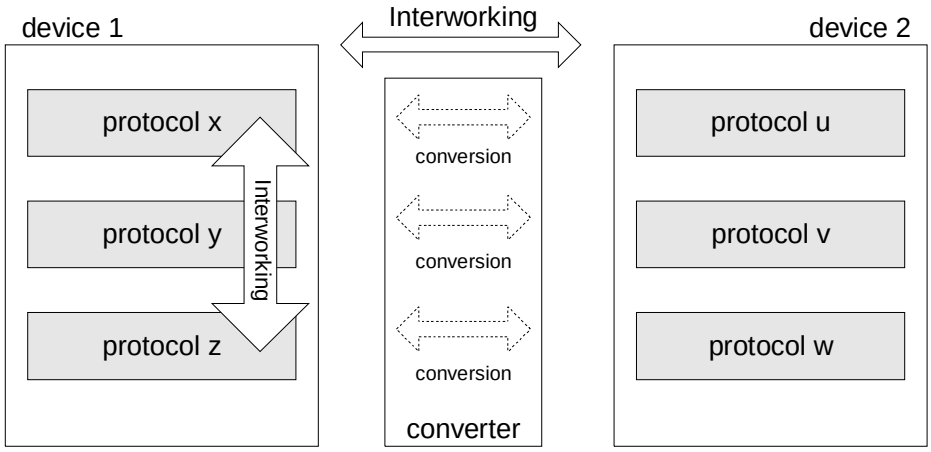
Anycast, means m:n communication between many terminals and one terminal. The dataflow is multidirectional (e.g. Video conference, Gaming).



Interoperability means that the desired communication can be established for all involved OSI layers and protocols by connecting two interfaces *directly*. This is not obvious when connecting solutions from different vendors.



Interworking means that the desired communication can be established for all involved OSI layers and protocols by connecting two interfaces *through some conversion mechanism*. This converter translates at one or more OSI-layers, such as for instance IP/ATM, IPv4/IPv6, Ethernet/ATM, etc.



======= *Transmission* =======

Noise margin: the ratio (P_{n2}/P_{n1}) by which the received noise power P_{n1} may increase to power P_{n2} until the recovered signal does no longer meet the predefined quality criteria. This ratio is commonly expressed in dB.

Signal margin: the ratio (P_{s1}/P_{s2}) by which the received signal power P_{s1} may decrease to power P_{s2} until the recovered signal does no longer meet the predefined quality criteria. This ratio is commonly expressed in dB.

Performance: is a measure of how well a transmission system fulfils defined criteria under specified conditions. Such criteria include reach, bit rate and noise margin.

PSD mask: The absolute upper bound of a PSD, measured within a specified resolution band. The purpose of PSD masks is usually to specify maximum PSD levels for stationary signals.

PSD template: The expected average values of the PSD of a stationary signal. The purpose of PSD templates is usually to perform simulations. The levels are usually below or equal to the associated PSD masks

Power back-off: is a generic mechanism to reduce the power. It has many purposes, including the reduction of power consumption, receiver dynamic range, cross talk, etc.

Power cut-back: is specific variant of power back-off, used to reduce the dynamic range of the receiver. It is characterized by a frequency independent reduction of the in-band PSD. It is used, for instance, in ADSL and SDSL.

2.2 Abbreviations

3GPP	The 3rd Generation Partnership Project
AAC	Advanced Audio Coding (MPEG)
AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACS	Auto-Configuration Server
ADSL	Asymmetric Digital Subscriber Line
AEL	Accessible Emission Limit
AEN	Access Edge Node
AF	Adaptation Function
AN	Access Node
AS	Authentication Server
ASM	Any Source Multicast
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AVC	Advanced Video Coding (MPEG-4 Part 10 or H.264)
AWG	Arbitrary Waveform Generator
AWG	Arrayed Waveguide Grating
BAP	Bluetooth Access Point
BER	Bit Error Ratio
BER	Bit Error Rate
BLES	Broadband Loop Emulated Service
B-OSF	Operations System Function block of the Business Management Layer
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
CAC	Call Admission Control
CAP	Carrierless Amplitude/Phase modulation
CCE	Call Control Element
CCS7	Common Channel Signalling #7
CCSS	Common Channel Signalling System
CD	Chromatic Dispersion
CF	Call Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CLASS	Customer Local Area Signalling Services
CNR	Carrier-to-Noise Ratio
CoS	Class of Service
CPE	Customer Premises Equipment
CPE	Customer Premises Equipment
CPG	Customer Premises Gateway
CPN	Customer Premises Network
CS	Complementary Services
CSO	Composite Second Order
CTB	Composite Triple Beat
CWDM	Coarse Wavelength Division Multiplexer
CWMP	CPE WAN Management Protocol (aka TR-69)
DARPA	Defense Advanced Research Projects Agency
DCR	Degradation Category Rating
DCT	Discrete-Cosing Transform
DGD	Differential Group Delay
DHCP	Dynamic Host Configuration Protocol

DIAMETER	An AAA (authentication, authorization and accounting) protocol, the precessor of RADIUS
DMT	Discrete Multitone modulation
DNS	Domain Name System
DOS	Denial Of Service
DPBO	Downstream Power Back-Off (see also clause 3.1 on definitions)
DRM	Digital Rights Management
DSCP	Differentiated Services Code Point
DSCQS	Double Stimulus Continuous Quality Scale
DSIS	Double Stimulus Impairment Scale
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
DTMF	Dual Tone Multi Frequency
DVD	Digital Versatile Disc
DVMRP	Distance Vector Multicast Routing Protocol
DWDM	Dense Wavelength Division Multiplexer
E2E	End-to-End
EAP	Extensible Authentication Protocol
EC	Echo Cancelled (see also under EC, in clause 3.1 on definitions)
E-OSF	Operations System Function block of the Element Management Layer
EP	Enforcement Point
EPG	Electronic Programming Guide
ERP	Enterprise Resource Planning
eTOM	enhanced Telecom Operations Map
ETSI	European Telecommunications Standardisation Institute
FDD	Frequency Division Duplexing/Duplexed
FEC	Forward Error Correction
FHR	First Hop Router
FRTV	Full Reference TV
FTP	File Transfer Protocol
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
FTTP	Fibre to the Premises
FWM	Four Wave Mixing
GbE	Gigabit Ethernet
GDMF	Guidelines for the Definition of TMN Management Functions
GPON	Gigabit Passive Optical Network
GPS	Global Positioning System
GSB	Global System for Broadband communications
H.264	MPEG-4 Part 10 or AVC
HAM	Handheld Amateur Radio
HDD	Hard Disc Drive
HDSL	High bit rate Digital Subscriber Line
HDTV	High Definition TV
HMAC	(Keyed) Hash Message Authentication Code
HSI	High-Speed Internet
HTML	Hyper Text Mark-up Language
HTR	Hard-To-Reach
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning

ICMP	Internet control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institution of Electronic and Electric Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IL	Insertion Loss
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IMIX	Internet traffic Mix
IMS	IP Multimedia Subsystem
IoTV	Internet on TV
IP	Internet Protocol
IPDV	IP Packet Delay Variation
IPER	IP Packet Error Ratio
IPLR	IP Packet Loss Ratio
IPoE	IP over Ethernet
IPoPPPoE	IP over PPP over Ethernet
IPPM	IP Performance Metrics
IPTD	IP Packet Transfer Delay
IP-TV	Internet Protocol TV
ISDN	Integrated Services Digital Network
ISMA	Internet Streaming Media Alliance
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	ITU – Telecommunication Standardization Sector
IVR	Interactive Voice Response unit
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LHR	Last Hop Router
LL	Leased Line
LLC	Link Layer Control
LSP	Label Switched Path
LT-port	Line Termination port (*commonly at central office side*)
M+N	M working units + N spare units
MAC	Media Access Control
MAC	Message Authentication Code
M-BGP	Multi-protocol extension to BGP
MFA	Management Functional Area
MGCP	Media Gateway Control Protocol
MIDCOM	MIDdlebox COMmunications
MIME	Multipurpose Internet Mail Extension
MLD	Multicast Listener Discovery Protocol
MLM	Multi-Longitudinal Mode
MM	Multi Mediq
MMS	Multimedia Message Service
MOS	Mean Opinion Scores
MPEG	Moving Picture Experts Group
MPLS	Multi-protocol Label Switching
MP-to-MP	Multi-point to Multi-point
MSDP	Multicast Source Discovery Protocol
MSE	Mean Squared Error
NAP	Network Access Provider
NAPT	Network Address/Port Translator

NAT	Network Address Translator
NE	Network Element
NE(s)	One, several or a group of Network Elements
NF	Noise Figure
NOD	News On Demand
Non-WDM	One wavelength in propagation direction
N-OSF	Operations System Function block of the Network Management Layer
NP	Network Performance
NRE	Network Routing Engine
NSP	Network Service Provider
NT	Network Termination
NTP	Network Time Protocol
NT-port	Network Termination port (*commonly at customer side*)
NVOD	Near Video On Demand
OAM	Operation Administration and Maintenance
ODN	Optical Distribution Network
OEO	Optical-Electrical-Optical
OLT	Optical Line Termination
ONU	Optical Network Unit
ORL	Optical Return Loss
OS	Operations System
OSF	Operations System Function block
OSI	Open Systems Interconnection
OSNR	Optical Signal-to-Noise Ratio
P2MP	Point-to-Multipoint
P2P	Point-to-Point
P2P	Peer To Peer
PAA	PANA authentication Agent
PaC	PANA Client
PAM	Pulse Amplitude modulation
PANA	Protocol for carrying Authentication for Network Access
PAP	Password Authentication Protocol
PAT	Port Address Translator
PBO	Power Back-Off (see also clause 3.1 on definitions)
PBX	Private Branch Exchange
PCB	Power Cut-Back (see also clause 3.1 on definitions)
PDA	Personal Digital Assistant
PDH	Plesiochronous Digital Hierarchy
PDL	Polarisation Dependant Loss
PESQ	Perceptual Evaluation of Speech Quality
PHB	Per Hop Behaviour
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
PIP	Picture In Picture
PLC	Power Line Communication
PM	Performance Monitoring (the TMN Management Function Set Group)
PMD	Polarization Mode Dispersion
PON	Passive Optical Network
POP 3	Post Office Protocol
POTS	Plain Old Telephony Service
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet

PPV	Pay Per View
PSD	Power Spectral Density (single sided)
PSNR	Peak Signal-to-Noise Ratio
PSTN	Public Switched Telephone Network
P-to-MP	Point to Multi-point
P-to-P	Point to Point
PVR	Personal Video Recorder
QAM	Quadrature Amplitude modulation
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAS	Reliability, Availability and Survivability
REIN	Repetitive Electrical Impulse Noise
RFC	Request For Comment
RMS	Root-Mean Square
RNP	Regional Network Provider
RoF	Radio over Fibre
RPC	Remote Procedure Call
RPR	Resilient Packet Ring
RPT	Rendezvous Point Trees
RRNR-TV	Reduced Reference No Reference TV
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTT	Round-trip Time
SB	Service Broker
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SDSCE	Simultaneous Double Stimulus for Continuous Evaluation
SDSL	Symmetrical (single pair high bit rate) Digital Subscriber Line
SDTV	Standard defenition TV
SEN	Service Edge Node
SFP	Small Form-factor Pluggable
SHINE	Single High level Impulse Noise Event
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Single-Longitudinal Mode
SME	Small-Medium Enterprise
SMS	Short Message Service
SMSR	Side Mode Suppression Ratio
SMTP	Simple Mail Transfer Protocol
SNI	Service Node Interface
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio (*ratio of powers*)
SNR	Signal-to-Noise Ratio
SOHO	Small Office, Home Office
S-OSF	Operations System Function block of the Service Management Layer
SpM	Spectral Management
SPM	Self-Phase Modulation
SRA	Seamless Rate Adaptation
SSCQE	Single Stimulus Continuous Quality Evaluation
SSH	Secure Shell

SSM	Single Source Multicast/Source Specific Multicast
STB	Set Top Box
SUT	System Under Test
S-VID	Stacked VLAN ID
S-VLAN	Stacked VLAN
T&L	Terminate test and Leave
TAP	Test Access Path
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TMF	Tele Management Forum
TMN	Telecommunications Management Network
ToIP	Telephony over IP
ToS	Type of Service
TR	Technical Report (DSLForum)
TTL	Time To Live
TVoIP	Television over IP
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UNI	User Node Interface
UPBO	Upstream Power Back-Off (see also clause 3.1 on definitions)
UPE	User Profile Engine
URI	Unified Resource locator
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCR	Video Content Recorder
VDSL	Very-high-speed Digital Subscriber Line
VGA	Video graphics array
VHE	Virtual Home Environment
VLAN	Virtual Local Area Network
VLC	VideoLAN Client
VLL	Virtual Leased Line
VoATM	Voice over ATM
VoD	Video on Demand
VoDSL	Voice over DSL
VoIP	Voice over IP
VPDN	Virtual Private Dial Netwok
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Segment
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VQEG	Video Quality Experts Group
VQM	Video Quality Metric
VTU-C	VDSL Transceiver Unit – Central office side
VTU-R	VDSL Transceiver Unit – Remote side (customer premises)
WINS	Windows Internet Naming Service
WMP	Windows Media Player
WT	Working Text (DSLForum)
xDSL	(all systems) Digital Subscriber Line

XPM	Cross-Phase Modulation
xTU-C	xDSL Transceiver Unit – Central office side
xTU-R	xDSL Transceiver Unit – Remote side (customer premises)
xWDM	All kinds of WDM (e.g. CWDM, DWDM, ...)

3 CLASSIFICATION FRAMEWORK FOR E2E TESTING

3.1 Purpose of this chapter

To simplify the characterization of the functionality within an access system, very different descriptions are used. The well known layered OSI model may be suitable for describing “connectivity” properties; it is not suitable to model the functionality of a management system or to model the properties that are essential to enable the different roles played by network providers, access providers and service providers. In fact each group of properties that are to be characterized by testing requires its own framework to model the associated functionality. This chapter 3 is therefore intended as an extension to the previous “definition” chapter, and defines a common framework of very different models being used within various tests. It is mainly a summary of independent definitions, and therefore the amount of explanatory text is kept as low as possible.

3.2 Classification of Services

To simplify the characterization of the functionality within an access system, very different descriptions are used. The well known layered OSI model may be suitable for describing “connectivity” properties, it is not suitable to model the functionality of a management system or to model the properties that are essential to enable the different roles played by network providers, access providers and service providers. In fact each group of properties that are to be characterized by testing requires its own framework to model the associated functionality. This paragraph summarizes a framework to classify services.

In the following, a service taxonomy based on a selected service classification of multimedia services is presented, which has been adopted for the testing of the MUSE access network in terms of QoS requirements. This constitutes a crucial point since a long chain of relations are affected, i.e., the service characteristics influence the traffic network, which in its turn puts conditions in QoS parameters, as well as in several other factors that ultimately determine the network architecture and its traffic engineering mechanisms.

The architecture and features of the IP networks, which constitute the basis of the MUSE access network, allow the deployment of a large variety of advanced multimedia services. These kind of services are characterised by some specific requirements (e.g., delay, jitter, packet-loss) that needs to be fulfilled by the networks. If a network cannot fulfil the requirements then deployment of those services can be constrained, as described in [QoS2], [QoS3], [QoS5] and [QoS6].

The variety of services forces the network designers and services developers to co-ordinate their efforts to reach the corresponding trade-offs in order to get the optimal deployment of the advanced multimedia services in networks technically feasible and based on standards. The key target is to find out the best balance among application/service design, network engineering and economic limitations.

Thus, it is first necessary to study the services (and the applications associated with them), by analysing their properties and grouping them in "classes". In a second step, it is necessary to study and find the requirements that every class demands from the network, as it is shown in [QoS5] and [QoS6]. Although the service developers must take into account the technical limitations of the networks as described above, there are a number of basic parameters, specifically associated with the services, that are also supposed to be considered if they are to be offered with the required QoS.

The first step is to group the services considering common characteristics and usage scenarios from different viewpoints and taking into account their basic parameters and technical requirements. Although many classifications are possible, see for instance in [QoS5], [QoS6], [QoS7] and [QoS8], the present document follows the classification given in [QoS7]. By considering a range of applications involving the media of voice, video, image and text, and the parameters that govern end-user satisfaction for these applications, a broad classification of end-user QoS categories is determined in [QoS5]. It is intended that these categories be used as the basis for deriving realistic QoS classes and associated QoS control mechanisms for the underlying transport networks. The services are classified according to their requirements with respect to delay and tolerance for errors. With respect to delay four types of services are identified:

- Interactive
  - Delay << 1 s
- Responsive
  - Delay ~ 2 s
- Timely
  - Delay ~ 10 s
- Non-critical
  - Delay >> 10 s,

See table 3-1.

	Interactive (delay <<1 s)	**Responsive** (delay ~2 s)	**Timely** (delay ~10 s)	**Non-critical** (delay >>10 s)
Error tolerant	Conversational voice and video	Voice/video messaging	Streaming audio and video	Fax
Error intolerant	Command/control (e.g. Telnet, interactive games)	Transactions (e.g. E-commerce, WWW browsing, Email access)	Messaging, Downloads (e.g. FTP, still image)	Background (e.g. Usenet)

T1213060-02

Table 3-1: Model for user-centric QoS categories

In short, the proposed service classification is as depicted in figure 3-**1**:

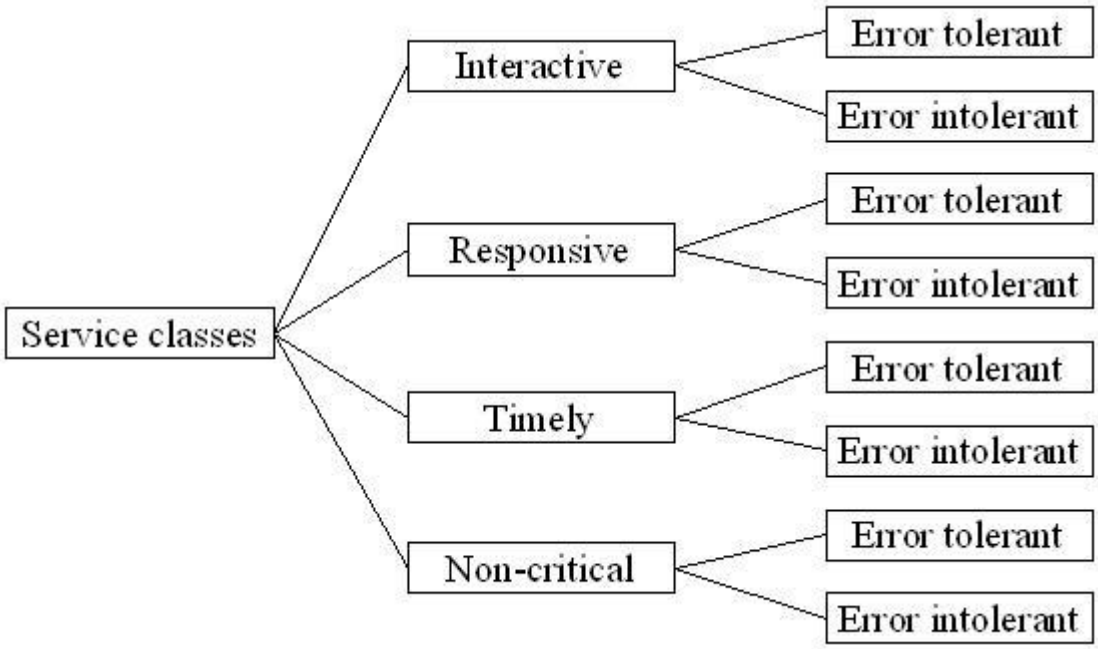


Figure 3-1: Proposed service classification

This classification of ITU-T G.1010 [QoS5] can be considered as similar to the one suggested by 3GPP [QoS7], except for some target performance parameters, since one applies to the mobile world ([QoS7]), while the other ([QoS5]) does not.

Within the MUSE project, the milestone MA2.5 discusses how many QoS classes are needed to support the identified services, see [QoS66]. The following text is extracted from there.

According to MA2.5, the natural way to group telecommunication services seems to be in function of the traffic profile and requirements that these services have. So, the first step to infer service classes could consist of identifying relevant traffic classes. This can be done in function of different attributes that can be ordered by their relative importance. For instance, the following ones can be considered (for simplicity, only two opposite levels are considered):

- elasticity level (elastic, inelastic),
- interactivity level (interactive, non-interactive),
- traffic symmetry (symmetric, asymmetric),
- service availability (standard, high),
- bandwidth (low or narrowband, high or broadband),
- traffic variability (CBR, VBR).

As such, a main traffic differentiator, which heavily depends on the nature of the traffic, is considered to be the elastic/inelastic characteristic. Elasticity level refers to the level up to which the traffic original shape can be modified. Not all services have the same elasticity level. Normally, communication services aspire to keep both the data and temporal integrity. In order to establish the elasticity level of a given service, it is useful to assess which of both integrities is more restrictive. So, elastic and inelastic services (or traffic generated by those services) can be distinguished in function of which of these both integrities is more relevant.

If data integrity is more relevant, we have elastic traffic, if temporal integrity is the point, we have inelastic traffic.

Interactivity level helps to emphasize (or not) the other not so relevant integrity. For instance, elastic traffic with high interactivity level would be generated by an service where data integrity occupies the first place, but where temporal integrity is also very relevant, e.g. for instance, e-commerce, web traffic, etc.

Availability is also considered as very important, and must of course be used as an attribute to identify the different traffic classes. Indeed, in core networks (which are not the object of MUSE) it is one of the most important considerations to take into account.

Other requirements can be, generally, adapted to the current (and evolving) technological and economical constraints. That is to say, further division or classification of traffic classes seems to be more artificial and dependent on the state of the art.

In the end, a traffic classes tree considering previous identified attributes has been identified, where some MUSE reference services, as well as service classes, have been mapped, see figure 3-2.

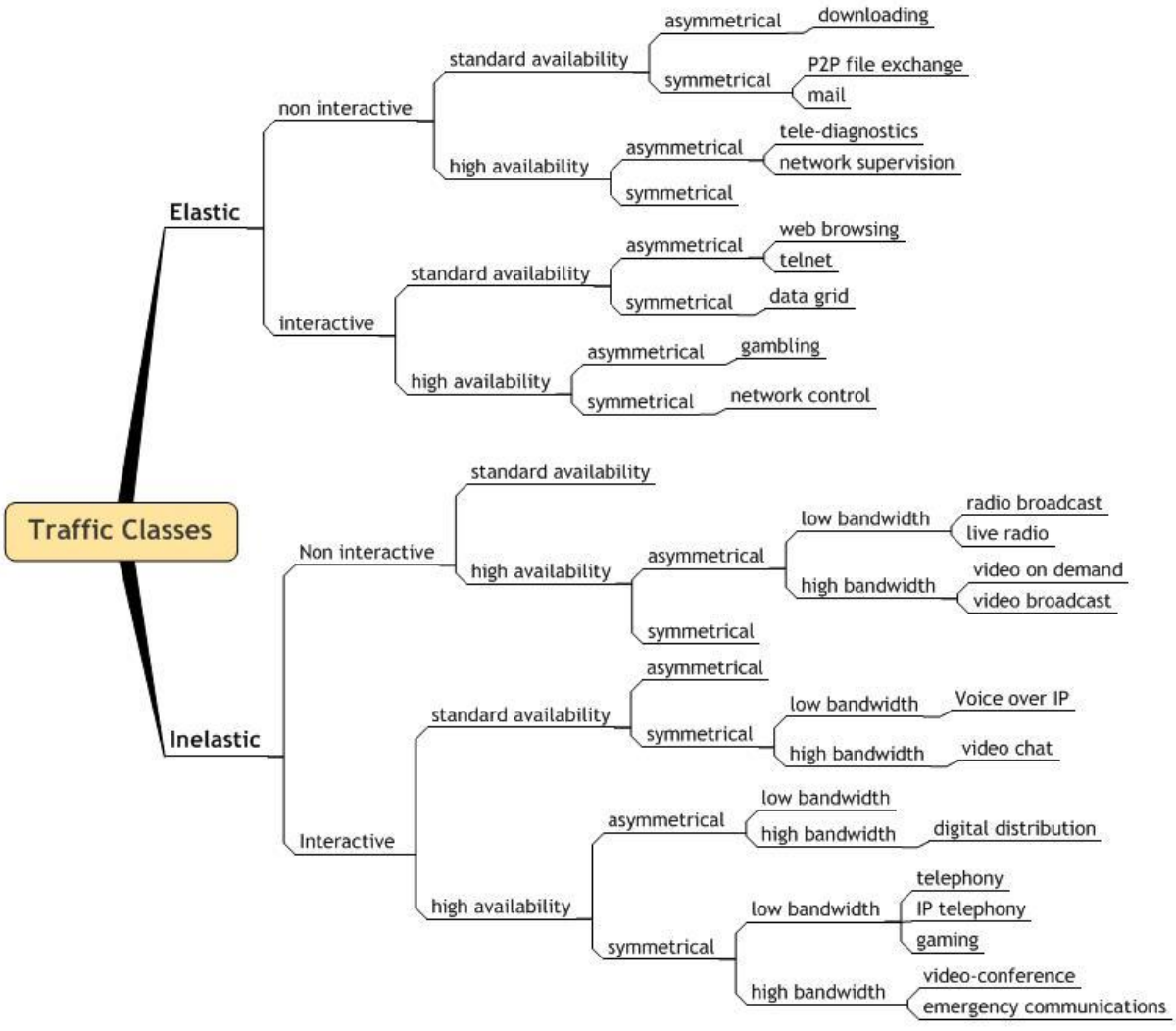


Figure 3-2: Traffic classes tree

This ordered tree makes it possible to get a flexible schema of service classes that allow easy interconnection and that a given operator can specialize (or not) in particular business. In this way, for QoS purposes, only inelastic class would be mandatory. Inelastic class would be associated to the idea of guaranteed QoS.

On its turn, elastic class may be recommended, as it could be associated with best effort services. The inelastic / elastic choice would therefore refer to stringent requirements vs less stringent requirements.

For purposes of compatibility with both ITU and 3GPP recommendations, it is be highly recommended that the following classes would be implemented:

- the **elastic and non-interactive** class may be called, for instance, **best effort**, and would match with the background class (3GPP) or the non-critical class (ITU),
- the **elastic and interactive** class may be called, for instance, **transactional**, and would match with the interactive class (3GPP) or the responsive class (ITU),
- the **inelastic and non-interactive** class may be called, for instance, **streaming**, and would match with the streaming class (3GPP) or the timely class (ITU),
- the **inelastic and interactive** class may be called, for instance, **real-time**, and would match with the conversational class (3GPP) or the interactive class (ITU).

Also, other approaches are advocating an architecture with no classes of service, that is, only a premium class would exist. This might be possible by combining admission control and fair queuing in what has been called a “cross-protect” router, see [QoS67]. This might be a very desirable result since even to manage two classes of service could be very complicated, see [QoS68]. However, currently these ideas for flow-aware networking are not implementable since routers don't yet allow per-flow admission control or scheduling.

MA2.5 concludes as follows: “*a flexible scheme of QoS classes where a very reduced number of QoS/CoS classes are mandatory is needed, there also being a more extensive set of optional/recommended classes (derived from the compulsory ones) in order to reflect all the market needs according to the different providers constraints. In addition, the proposed scheme should be totally compatible with the existing standardization bodies approaches (3GPP, ITU), and it should allow an easy network interconnection, specially with core networks, which possibly may not have so many QoS classes as the access has. So, although it seems very difficult to provide the right number of traffic classes, a flexible tree scheme might provide a wide range of classes and, in this way, each network operator could easily choose his “star” options, according to its business model and to the defined tree*.”

For the MUSE lab trails we will follow the above service based classification approach, which as already mentioned, complies with international standardization bodies such as ITU-T and 3GPP. In the following section we will select applications that are realisations of the service classes.

3.3 Classification of Network Domains

End-to-End connectivity testing means that one tests over multiple elements located in different parts of an interconnected network. This interconnected network is divided in the following Network domains according to who is owner and/or responsible for a given part of the network. The following domains are defined:

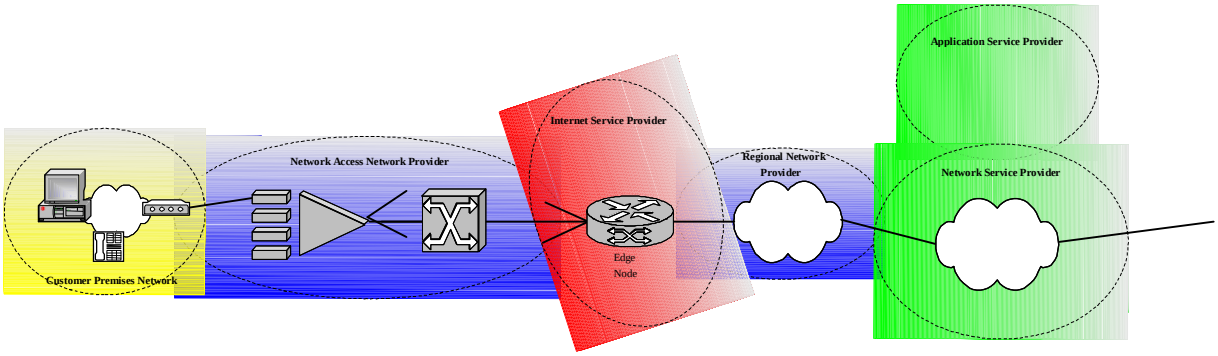


Figure 3-3: Relationship between Domains

- Customer Premises Network (CPN)

This is the network either located at the end-user his home (Home network) or the network located at a SOHO location. This network and the devices it comprises is owned and managed by the end-user

- Network Access Provider (NAP)

Typically the telecommunications carrier who delivers data and voice communication services to customers. The NAP owns/operates the DSLAM and the transport network.

- Regional Network Provider (RNP)

A regional network is a digital network that connects the DSLAM to a Service Provider's equipment

- Network Service Provider (NSP)

An NSP is a company that provides Internet access to ISPs. Sometimes called backbone providers, NSPs offer direct access to the Internet backbone and the network access points.

- Internet Service Provider (ISP)

A company that enables customers to access the Internet via dial-up telephone lines, dedicated lines or high-speed access (such as a digital subscriber line, or DSL).

- Application Service Provider (ASP)

Application Service Providers are third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data centre. In essence, ASPs are a way for companies to outsource some or almost all aspects of their information technology needs.

3.4 Classification of Connectivity

3.4.1 OSI Reference Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers and is the de facto reference model that is applied in the Telecommunications world. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

7	**Application Layer** This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
6	**Presentation Layer** This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.
5	**Session Layer** This layer establishes manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
4	**Transport Layer** This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
3	**Network Layer** This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
2	**Data Link Layer** At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
1	**Physical Layer** This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

REFERENCE: Text taken from Webopedia, www.webopedia.com

3.4.2 TCP/IP Reference Model

The OSI reference model is an almost pure theoretical model because in reality one has that one protocol specification (and implementation) is composed of one or more OSI layer functionalities. Hence a slightly different framework which is closer to the way Internet

(TCP/IP) applications/Services are build-up is used in this document. This is commonly referred to as the "TCP/IP reference model".

This reference model is composed of 5 layers as indicated below:

5	**(TCP/IP) Application Layer** In TCP/IP reference model the Application Layer also includes the OSI Presentation Layer and Session Layer. In this document an application is any process that occurs above the Transport Layer. This includes all of the processes that involve user interaction. The application determines the presentation of the data and controls the session. There are numerous application level protocols in TCP/IP, including Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) used for e-mail, Hyper Text Transfer Protocol (HTTP) used for the World-Wide-Web, and File Transfer Protocol (FTP). Most application level protocols are associated with one or more (transport layer) port number.
4	**Transport Layer** This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
3	**Network Layer** This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
2	**Data Link Layer** At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
1	**Physical Layer** This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

3.5 Classification of QoS

The term Quality of Service (QoS) is defined in ITU-T Rec. E.800 [Con90] as "The collective effect of service performance which determines the degree of satisfaction of a user of the service".

In fact, the term Quality of Service (QoS) can be used in many contexts. For a customer or end-user of a service, external QoS factors and technical quality aspects of a service can be distinguished. External QoS factors are for example marketing/sales aspects, installation issues, helpdesk availability and quality, etc. The technical QoS aspects are the availability of the service itself, the transmission quality, terminal quality, etc. In MUSE, QoS will be evaluated both at the perceived level and at the network level.

Hence in MUSE a distinction is made between two types of QoS:

- User-perceived QoS
  "Quality of a service or application as experienced by an end-user."

  A typical user is not concerned with how a particular service is implemented, e.g. the user is interested in comparing the same service offered by different providers in terms of universal, user-oriented performance parameters. This implies that performance should be expressed by parameters that:

  - Take into account all aspects of the service from the user's point of view;
  - Focus on user-perceivable effects, rather than their causes within the network;
  - Are independent of the specific network architecture or technology;
  - Can be objectively or subjectively measured at the service access point;
  - Can be easily related to network performance parameters

- Network QoS
  "Statement of the performance of a network in terms of delay, delay variation, packet loss, out-of-order delivery, bandwidth and techniques and protocols to implement it."

  Network Performance is a statement of the performance of a connection element or concatenation of connection elements employed to provide a service. It is defined and measured in terms of parameters (delay, jitter,...), which are meaningful to the network and to the service provider and are used for the purposes of system design, configuration, operation and maintenance. Network Performance is defined independently of terminal performance and user/customer actions. It is also service independent in that, it must be able to support all the services that the particular network level is required to transport.

  Related to the above mentioned "measurable" aspect of Network QoS we also have the technical aspect. With this we mean the techniques and protocols used by applications and supported by the network in order to guarantee a level of network performance that is required by an application.

This E2E connectivity testing chapter of this Test Suite will focus on the protocols that can be used by an application to request from the network a given end-to-end network performance. The more general QoS parameters and the verification/measurement/scoring of the user-perceived QoS are part of the QoS chapter of the this Test Suite document.

3.6 Classification of Management functions

The description of management functions can be organized in different ways, each with its own advantages and disadvantages. Two reference models have been described below, the TMN model (using the well-known FCAPS classification) and the e-TOM model. Since this chapter is only a summary of classifications, the choice between both models is discussed in a separate chapter, fully dedicated to management testing.

3.6.1 TMN model

ITU management model is named TMN (Telecommunications Management Network) and is defined in M.3010 Recommendation . TMN provides an overall architectural framework as following:

- Management Functions (vertical view).
- TMN layers (horizontal view)

In TMN model, management functions are grouped under the well known FCAPS classification:

- F : Fault management
- C: Configuration management
- P : Performance management
- A : Accounting management
- S : Security management

Regarding the horizontal splitting, TMN model distinguishes five layers as shown in the figure below. From these layers, only the upper 4 are related to management issues, being the bottom layer – Network Elements – exclusively added for contextualization.

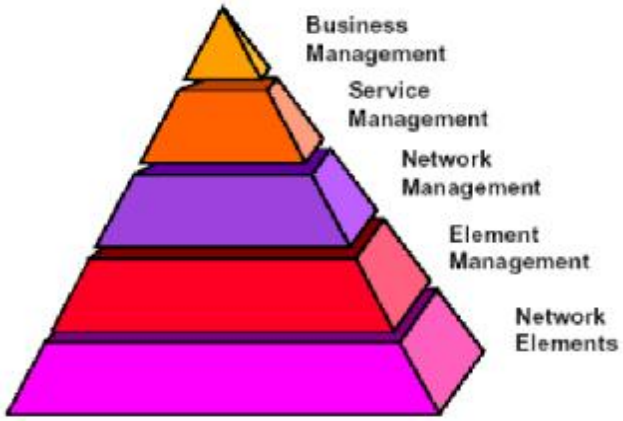


Figure 3-4: TMN Model

3.6.2 e-TOM model

The Enhanced Telecom Operations Map® (or eTOM for short), has been developed by the TeleManagement Forum (TMF) (see GB921 reference). It describes the enterprise processes required by a service provider and analyzes them to different levels of detail according to their significance and priority for the business. This business process approach has built on the concepts of Management Services and Functions in order to develop a framework for categorizing all the business activities.

The following table gives an overview of this approach. Those processes allow managing services and networks according to 3 levels: resources, services and interface with the customer. This approach is illustrated in the following table.

	Fulfilment grouping process	Insurance grouping process	Billing grouping process
Interface with the customer	Order capture	Customer complaint Information collect on customers services	Bill production
Services	Services provisioning	Network supervision and maintenance of network and equipment	Accounting information correlation related to equipment and customers features
Resources	Network equipment configuration needed to guarantee the required service	Network and equipment overview : alarms, performance counters, accounting information, Equipment tests and maintenance	Collect of accounting information related to equipment

Table 3-2: eTOM Model

4 INVENTORY OF SERVICE REQUIREMENTS

4.1 Introduction

Different services have different characteristics and requirements, and the access solution under test should cope with these characteristics and should meet these requirements to enable proper operation. The list of service characteristics and requirements can be indefinitely long, but some of them are simple to summarize.

As an introduction to full-service, end-to-end testing, this chapter provides an (incomplete) overview of basic characteristics of many well-known services, and is based on the results of [Srq1]. This list is not considered as complete, but should be regarded as a starting point for end-to-end testing. The requirement values obtained in the MUSE analysis in [Srq1] are only orientative and based on the current situation. As a matter of fact, the list of reference applications is based on existing and emerging applications/services. An access solution must at least be capable of coping with these characteristics, and fulfil this minimum set of requirements.

This chapter 4 starts with identifying several commonalities of various services, such as characteristics (*traffic attributes*) and basic requirements (*throughput, quality,..)*.

All these commonalities are provided for a whole range of services, but the number of services is too high to have them all tested in a lab environment. Therefore this chapter includes a section on what services should be chosen to enable “full service” testing in practice.

4.2 Basic Characteristics of Services

Services can be characterized by different properties. Traffic attributes are characteristics related to the dataflow generated by these services, and the following traffic attributes have been identified:

- **Responsiveness**:
  - ***RT: Real-time*** traffic means that the dataflow and the control dataflow will be transmitted in real-time for example VoD zapping based or Video conferencing.
  - ***NRT: Non Real Time*** is the opposite of real time

- **Interactivity**:
  - ***Interactive*** means there is some dialogue between end users/systems or between end user/system and the network. That applies for both bidirectional and unidirectional applications (e.g. VoD zapping based, EPG, Video telephony, Video conference), but an active return channel is always needed to enable the user to interact.
  - ***Non-Interactive*** is the opposite of Interactive.

- **Duplicity**:
  - ***Unidirectional*** means that the dataflow is transmitted only in one direction, from transmitter to receiver.
  - ***Bi-directional*** means that the dataflow is transmitted from transmitter to receiver and vice versa.

- **Symmetry in rate**:
  - ***Asymmetrical*** means that the dataflow in downstream direction is (usually) significantly higher than in upstream direction (including control data). In some cases the dataflow for upstream is higher than for downstream, such as for instance for Concast-applications.
  - ***Symmetrical*** means that the dataflow in downstream direction is similar (in size) to the flow in upstream direction (including control data).

- **Connection types**:
  - ***Unicast*****,** means 1:1 communication between terminals. The dataflow can be unidirectionally (such as Video on Demand and Data Downloading) or bidirectionally (e.g. video telephony).
  - ***Multicast/Broadcast***, means 1:n communication between one terminal and many terminals. The dataflow is unidirectional (e.g. broadcast TV)
  - ***Concast***, means m:1 communication between many terminal and one terminal. The dataflow is unidirectional (e.g. Tele-Working, Webcam, Data-Upload)
  - ***Anycast***, means m:n communication between many terminal and one terminal. The dataflow is multidirectional (e.g. Video conference, Gaming).

- **Nomadism**
  Nomadism is the ability, for a person who is in a moving situation, (but without moving of his terminal as in mobile world), to recover, whatever his access of connection to the network, his services environment.
  Some applications may require nomadic mechanisms. The possible values for this requirements are:
  - Yes (maybe Required)
  - No (maybe Not Required)
  - Not Applicable

Different services have different traffic attributes, They are summarized below, and sorted according to the type of terminal being used for the service.

Characteristics of residential applications						
	RT/ NRT	Inter/ Non-Inter	Uni/ Bidir	SYM/ ASYM	Unicast Multicast Broadcast Concast Anycast	**Nomadism** Yes/ No/ Not Applicable
Telephony Applications						
Legacy POTS, ISDN	RT	Int	Bidir	SYM	U	na
VoDSL	RT	Int	Bidir	SYM	U	y
VoIP	RT	Int	Bidir	SYM	U	y
Visiophony	RT	Int	Bidir	SYM	U M	y
Voice Messaging	NRT	Non Inter	Uni	ASYM	U M	y
News on Demand	NRT	Int	Uni	ASYM	U	y
TV Based Applications						
Broadcast TV	RT	Non Inter	Uni	ASYM	B	n
Broadcast Audio	RT	Non Inter	Uni	ASYM	B	n
EPG	RT, NRT	Non Inter	Uni	ASYM	B	n
PPV	RT	Non Inter	Uni	ASYM	B	n
VOD	RT	Inter	Bidir	ASYM	U	n
PVR	RT, NRT	Non Inter	Uni	ASYM	U M	n
On-screen navigator	NRT	Inter	Bidir	ASYM	U	n
PIP	RT	Non Inter	Uni	ASYM	B	n
Picture on browser	RT	Inter	Bidir	ASYM	B	n
I TV	RT, NRT	Inter	Bidir	ASYM	U M	n
Video Conf.	RT	Inter	Bidir	SYM	U M	n
PC based Applications						
H S I	RT, NRT	Inter	Bidir	ASYM	U M	n
P2P	RT, NRT	Inter	Bidir	SYM, ASYM	U M A	na
Community aps	RT, NRT	Inter	Bidir	ASYM	U M	y
e-mail	NRT	Non Inter	Uni	ASYM	U M C	y
Unified Messaging	NRT	Non Inter	Uni	ASYM	M	y
Facsimile over Internet	NRT	Non Inter	Uni	ASYM	U M C	y
Broadcast video	RT	Non Inter	Uni	ASYM	B	n
VOD	RT	Inter	Bidir	ASYM	U	n
NVOD	RT	Non Inter	Uni	ASYM	M B	n
MOD	RT	Inter	Bidir	ASYM	U	n
Near MOD	RT	Non Inter	Uni	ASYM	M B	n
Video conferencing	RT	Inter	Bidir	SYM	A M	n
Interactive games	RT	Inter	Bidir	ASYM	M U	y

Home working	RT, NRT	Inter	Bidir	SYM, ASYM	U C	y
Security aps	RT, NRT	Inter	Bidir	SYM, ASYM	U M	y
Tele-learning	RT, NRT	Inter	Bidir	SYM, ASYM	U M	y
Care and wellness aps	RT, NRT	Inter	Bidir	SYM, ASYM	U M	y
Console based Applications						
Live gaming	RT	Inter	Bidir	ASYM	M	y
Download gaming	NRT, RT	Non Inter/Inter	Uni Bidir	ASYM	M	y
H S I	RT, NRT	Inter	Bidir	ASYM	U	n
Domestic Applications	RT, NRT	Inter	Bidir	ASYM	U M	
Nomadism Applications	RT, NRT	Inter	Bidir	ASYM	M	
Content storage applications	NRT	Inter	Bidir	ASYM	U	
Content filtering applications						

Characteristics of business applications						
	RT/ NRT	Inter/ Non-Inter	Uni/ Bidir	SYM/ ASYM	U, M, B, A	nomadism
PC based Applications						
H S I	RT, NRT	Inter	Bidir	SYM ASYM	U	
P2P						
e-mail	NRT	Non Inter	Uni	ASYM	U M C	
Facsimile over Internet	NRT	Non Inter	Uni	ASYM	U M C	
Video Conf	RT	Inter	Bidir	SYM	A M	
Audio Conf with whiteboard	RT	Inter	Bidir	SYM	A M	
E-conf	RT, NRT	Non Inter	Bidir	ASYM	U M	
Tele training	RT, NRT	Non Inter	Bidir	ASYM	U M	
Security applications	RT, NRT	Inter	Bidir	SYM, ASYM	U M	
Home working / Tele-working	RT, NRT	Inter	Bidir	SYM, ASYM	U C	
Telephony Applications						
Legacy POTS, ISDN	RT	Int	Bidir	SYM	U	na
VoDSL	RT	Int	Bidir	SYM	U	y
VoIP	RT	Int	Bidir	SYM	U	y
Visiophony	RT	Int	Bidir	SYM	M U	y
Voice Messaging	NRT	Non Inter	Uni	ASYM	M U	y

News on Demand	NRT	Int	Uni	ASYM	U	y
TV Based Applications	RT	Inter	Uni	ASYM	U M	n
Content Storage applications – Storage area network	RT, NRT	Inter	Bidir	ASYM	U M	
Content filtering applications						
Nomadism applications					M	
Bearer applications						
Leased lines applications	RT	Inter	Bidir	SYM, ASYM	U	
VPN	RT	Inter	Bidir	SYM, ASYM	U M A	
Business service overview						

Table 4-1 - Basic characteristics of services

After this first classification, the list of services can be reduced, by grouping services with communalities, in the following one:

- *telephony*: this class of applications/services is characterized by its **interactivity**; in this class we have chosen:
  - *telephony*, and
  - *video conferencing*;

  the application/service video conferencing is an extension of the current telephony service in two dimensions:
  - multiparty instead of dual party,
  - exchange of video instead of only voice/audio;

- *broadcast TV/radio*: this class of applications/services is characterized by the **reception** by smaller and larger groups of recipients of **video and audio material**.

- *personalized TV/radio:*
  - *video/audio/application on demand*, and
  - *personal video recorder*;

  the application/service video/audio/application on demand is an extension of the current broadcast TV/radio in:
  - control, and
  - unicast or narrowcast;

  the application personal video recorder is a similar extension as the video/audio/application on demand service, but it adds:
  - personal (public/home) network based storage;

- *internet access*: this class of services is characterized by the presence of (**best-effort**) **IP connectivity;**
  in this class we have chosen:
  - *web browsing and downloading,*

- *e-mail,*
- *instant messaging and chatting,*
- *multiplayer gaming,*
- *peer-2-peer video/audio/file exchange, and*
- *server (web-, video-, file-) application;*

Beside the previous ones, *Security connectivity* application and *Nomadic* application can be considered as transversal functionalities/mechanisms that, when associated with the applications, provide them added value.

This set of applications is intended to cover the most important network aspects and will be considered as a reference list for the identification of Requirements in the following sections.

4.3 Basic Requirements to Enable Quality

A first group of requirements are demands to enable the quality of a service. The concept of quality of service is quite complex, is strongly dependent on human perception of that application, and is elaborated in great detail in succeeding chapters. However, a few technical parameters are simple to specify (and measure) and can be regarded as a minimum set of requirements. In this chapter the following parameters have been identified:

- **Blocking probability**: The failure of a network to establish a connection in order to provide a user service demand because of the lack of available resources. Given as a ratio between blocking cases between attempts ones.

- **Network Availability**: Requirement for uninterrupted service with acceptable quality, given as a ratio between time where the network is not available between total time.

- **Application set-up time**: Network time between the user application request and the response.

- **Connection set-up time**: Network time to set up a connection or a session between A-party and B-party. The time is counted from the first message the A-party sends until the network is ready to transmit user data and the B-party is ready to receive the data from the A-side. Given in msec.

- **Network robustness**: The degree to which a network or part of it can function correctly in the presence of invalid inputs or stressful environment conditions (such as congestion or network elements outage). Network robustness is achieved through resilience mechanisms, and mainly applied in the core network. Therefore, it is out of scope of MUSE.

- **Throughput**: The amount of data transferred from A-party to B-party or processed in a specified amount of time. Data transfer rates for networks are measured in terms of throughput. Typically, throughputs are measured in kbps, Mbps and Gbps. When characterising throughput it is necessary to consider minimum requirements, bursts sizes and other parameters. These bandwidth requirements are separately covered in the following subsection.

- **Delay**, from the point of view of application requirements, is an end-to-end parameter. It is the time it takes for application data units to be carried from one edge to the destination edge, including end application processing to the user. Delay can be

measured as absolute end-to-end delay or alternatively round-trip delay (easier to measure without need for accurate synchronization). Delay is more critical for bi-directional (conversational) services like VoIP and less for unidirectional services streaming-like (e.g. VoD). In other words, delay can be considered as the delay in one direction only (e.g. from service provider to end user), or as a "round-trip delay", which encompasses the delay in both directions (including latency of the edge when responding to received data). The latter is particularly important for full-duplex applications such as telephony.

- **Jitter** is the delay variation. While certain levels of jitter can be absorbed by the application through the use of buffering, excessive variation of end-to-end delay means that application data packets may reach the receiver too late to be useful.

- **Data loss** (BER or packet loss)
  - **Bit Error Rate (BER)** is a variable indicating the ratio between the total number of bits received to those that were errored during transmission.
  - **Packet Loss:** At the user-perception level, packet loss does not necessarily coincide with data packet loss at the network level. It might be data loss at the application level (for example, loss of signal fidelity due to encoding), or it might be completely user-specific. In this case, it is translated as a “user perceivable” loss of information that leads to user discomfort, lack of timely judgement and reaction needed to execute the task successfully, annoyance, disorientation, lack of interest, etc. Therefore, packet loss corresponds to the amount of information (visual content as the user sees it, loss of audio clarity, etc.) that a user perceives as missing. Note that this metric may have a subjective component as well. For example, a user might believe that something is wrong with a stream even in a lossless network environment. Also, more commonly, despite the fact that data are lost on the network, a user might not understand or perceive this (for example, if packet loss affected a non-audible, non-visible, or non-perceivable part of the transmitted information).

Different services have different characteristics, which can be regarded as a minimum set of requirements to enable a service of sufficient quality:

Representative application	Blocking probability	Network availability	Application set-up time	Connection set-up time	Delay	Jitter	Packet loss rate
legacy telephony	<1%	>99,99%	<2s	<100ms (time to get the tonality)	<100ms	<20ms	<5E-2
VoIP	<1%	>99%	<2s	<300ms	<200ms [1]	<20ms	<1E-3
video conferencing	<1%	>99%	<2s	<300ms	<200ms	<10ms	<1E-5
Broadcast TV/radio	<0,01%	>99,99%	<500ms	<3s	<400ms	N/A	<1E-5 (MPEG2) should be better for MPEG4
video/audio/application on demand	<0,01%	>99,99%	<500ms	<3s	<400 ms	N/A	<1E-5 (MPEG2) should be better for

[1] Delay for Legacy telephony service : 100 ms -> this value is normalized (ITU-T G114) and reflects the normal transport over copper line.
Delay for VoIP and videoconferance : 200ms -> not really a normalized value to-day, but an expected one (ETSI TR 101-329-2 (tiphon)). This also represents some value that FT has observed in experimentation fields.

Representative application	Blocking probability	Network availability	Application set-up time	Connection set-up time	Delay	Jitter	Packet loss rate
							MPEG4
personal video recorder	<0,1%	>99%	N/A	<3s	N/A	N/A	<1E-3
web browsing and downloading	<0,1%	>99%	<1s	<3s	N/A	N/A	N/A
e-mail	<0,1%	>99%	<1s	<3s	N/A	N/A	N/A
instant messaging and chatting	<0,1%	>99%	<1s	<3s	N/A	N/A	N/A
multiplayer gaming	<0,1%	>99%	<1s	<3s	<50ms	<1ms	<1E-3
peer-2-peer video/audio/file exchange	<0,1%	>99%	<1s	<3s	<200ms	N/A	N/A
server (web-, video-, file-) application	<0,1%	>99%	<1s	<3s	<200ms	N/A	Depends on
nomadic	<0,1%	>99%	<1s	<3s	<200ms	Depends on[2]	Depends on
secure connectivity	<0,1%	>99%	<1s	<3s	<200ms	Depends on	Depends on

Table 4-2 - Basic requirements to enable quality

Bandwidth is also considered as a QoS requirement. Within Bandwidth requirements there are several parameters, described and parametrised below:

- **Min Bandwidth**: The minimum bandwidth on the up- or downlink needed for the specific application.
- **Burstiness**: Range between min and Max Bandwidth required for the application. Given as a yes/no and a range in Mbit/s.
- **Max Number of simultaneous channels per user** : in other words for digital TV how many simultaneous channels per user must support the network. Fifty channels come up to the DSLAM, but we only allow a single living unit to watch only 3 channels at the same time (depending on the last mile technology). Note that 3 channels could go to different users in the same living unit.
- **Max Number of flows**: Max Number of concurrent flows to establish an application session. All these flows need to be synchronized at the end point (e.g. voice and video).
- **Bandwidth saving**: The bandwidth that might be saved in the network (core or access) when using special functions like IP or ATM broadcast, caching, etc. Given as Mbit/s and explaining what mechanism is used and where the bandwidth is saved. Storage and caching can also be a means to reduce the response time.

Representative Application	Min band-width up/down (bps)	Burstiness	Max number of simultaneous channels / user	Max number of concurrent flows required for single session[3]	Bandwidth or delay time improvements saving (multicast, storage, caching, etc.)
legacy telephony	64k	N	1	1	N
VoIP	10k	Y	4	3	N
video conferencing (depends on the architectures, MCU or peer2peer)	300k	Y	1 – up to the number of participants	1	Y multicast

[2] Depends on the application to be considered.
[3] Implementation dependent. An orientative value is given.

Representative Application	Min band-width up/down (bps)	Burstiness	Max number of simultaneous channels / user	Max number of concurrent flows required for single session[3]	Bandwidth or delay time improvements saving (multicast, storage, caching, etc.)
broadcast TV/radio	MPEG2 : SDTV : <6M HDTV : <20M MPEG4 : SDTV :<3M HDTV : <10M	Y (<500kbps)	3-4	3	Y multicast
video/audio/application on demand	MPEG2 : SDTV : <6M HDTV : <20M MPEG4 : SDTV :<3M HDTV : <10M	Y	3-4	2	Y multicast, storage
personal video recorder	MPEG2 : SDTV : <6M HDTV : <20M MPEG4 : SDTV :<3M HDTV : <10M	Y	1	2	Y multicast, storage
web browsing and downloading	<<5M/<<3M*	Y	4	1	N
e-mail	<<1M/<<500k*	Y	4	1	N
instant messaging and chatting	<<1M/<<500k*	Y	4		Y multicast
multiplayer gaming	<<2M/<<500k*	Y	1 – up to the number of participants		Y multicast, storage
peer-2-peer video/audio/file exchange	N/A	Y	4	1	Y multicast, storage
server (web-, video-, file-) application	<<2M/<<1M*	Y	4	1	N
nomadic application	<<2M/<<1M*	Y	1	2	Y Multicast
secure connectivity application	<<1M/<<500k*	Y	4	1	N

Table 4-3 - Basic BW requirements

* these applications will select low values for Min Bandwidth to minimise cost. For example Web browsing is possible with good quality with 100kb/s. Statistical multiplexing gain in the network gives at least a factor of 10, which means that the user gets an average bandwidth of 1Mb/s when he has selected a Min Bandwidth of 100kb/s.

4.4 Basic Requirements to Enable Security

There are many aspects of security that are to be considered in broadband access and related services / applications. In this section security threats are bundled into 4 different groups. For each of the groups a number of more specific threats are given. Then in each group a table is given where for all services/applications of the shortlist the need for protection against this threat is indicated.

In this section, the important applications / services are tabulated according to the following four broad categories of security issues:

1. Unauthorised reception/obtaining of information
2. Unauthorised usage of resources
3. Disturbing the proper functioning of services, networks, applications
4. Untraceable or repudiated sending of 'bad' information

For a more detailed description, see [Srq1].

4.4.1 Unauthorised reception/obtaining of information

This group of threats deals about confidentiality and privacy of information.

Representative application	Confidentiality of sent information (needed: yes/no?)	Confidentiality of identity of sender (needed: yes/no?)	Confidentiality of identity of receiver (needed: yes/no?)	Payment for content received (needed: yes/no?	Protection against modification of content of information	Protection against user identity theft	Other security requirements related to unauthorised reception/ obtaining of information
Legacy telephony	Yes	Yes (possibility of CLIP/ CLIR [4])	Yes (possibility of COLP/ COLR [5])	No (caller pays)	Yes	Yes	
Video conferencing	Yes	Yes (possibility of CLIP/ CLIR)	Yes (possibility of COLP/ COLR)	No (caller pays)	Yes	Yes	
BroadcastV/radio	Yes (for pay channels, anybody must intercept the signal)	No (public identity of service supplier)	Yes	Yes	Yes	Yes	
video/audio/application on demand	Yes (users that not paying for content)	No (public identity of service supplier)	Yes	Yes	Yes	Yes	
personal video recorder	Yes (users that not paying for content)	No (public identity of service supplier)	Yes	Yes	Yes	Yes	
web browsing and downloading	Yes (not free information) No (free information) is a load balancer in front of a server farm then illegal since it inspects the payload of Http traffic? Information should not be analysed, only HTTP header.	No (public identity of service supplier)	Yes	Yes (not free information) No (free information)	Yes	Yes	
e-mail	Yes	Yes	Yes	No	Yes	Yes	Payment for service (not free e-mail)
instant messaging and chatting	Yes One2one chat is private but what about in a chat room? A chat room can be private only	Yes The directory service has to be public (like the broadcast television) But identify of people to take part in a	Yes	No There may be any messaging application where people have to pay for received	Yes	Yes	

[4] The CLIP supplementary service provides the called party with the possibility of receiving identification of the calling party. The CLIR supplementary service enables the calling party to prevent presentation of its ISDN number to the called party.

[5] The COLP supplementary service provides the calling party with the possibility to receive identification of the connected party. The COLR supplementary service enables the connected party to prevent presentation of its ISDN number to the calling party.

Representative application	Confidentiality of sent information (needed: yes/no?)	Confidentiality of identity of sender (needed: yes/no?)	Confidentiality of identity of receiver (needed: yes/no?)	Payment for content received (needed: yes/no?	Protection against modification of content of information	Protection against user identity theft	Other security requirements related to unauthorised reception/ obtaining of information
	for authorized people. Use of access lists.	chat is private.		byte or for time			
multiplayer gaming	Yes	Yes How to join a network game? Same as chatting, identity of service supplier has to be public to be able to join a network game, but identity of people to take part in a game is private.	Yes	No	Yes	Yes	Payment for service or invocations
peer-2-peer video/audio/file exchange	Yes My requests can be forwarded by a node in the p2p network, will it be illegal?	Yes	Yes	No??? (it depends on application or service)	Yes	Yes	
server (web-, video-, file-) application	Yes	No (server)	Yes	Yes	Yes	Yes	
Nomadic application	Yes	Yes	Yes	Yes/no (it depends on application)	Yes	Yes	
secure connectivity application	Yes	Yes	Yes	Yes/no (it depends on application)	Yes	Yes	

Table 4-4 - Protection against unauthorised reception/obtaining of information

4.4.2 Unauthorised usage of resources

Resources usually cannot be used without authorisation. In many cases resources are also associated with payment by users.

The table below aims at identifying the security objectives for each of the reference application where the objectives are:

- payment of service use,
- payment for QoS use,
- payment for bandwidth, and
- prevention of masquerading/falsifying of identities.
- Thus, in this group of threats the main two threats are:

- o usage of resources (such as a service, QoS, bandwidth, etc.) without having paid for them;
- o usage of false identities (for e.g. buying/ordering things, etc.)

Representative application	Payment for service use (needed: yes/no?)	Payment for network QoS (needed: yes/no?)	Payment for bandwidth (needed: yes/no?)	Prevention of masquerading and usage of false identities (needed: yes/no?)
Voice	Yes	No (POTS) Yes(IP)	No (POTS) Yes(IP)	Yes
Broadcast TV/radio	Yes	No => yes	No	Yes
Video/audio on demand	Yes	No => yes	No	Yes
High Speed Internet	No (free information) Yes (not free information)	No	Yes (web browsing and downloading) No (e-mail)	Yes (when registration is needed)
Peer-2-Peer	No	Yes[6]	Yes	Yes
Gaming	Yes	Yes	Yes	Yes
Nomadism	No?	Yes	Yes	Yes

Table 4-5 - Protection against unauthorised usage of resources

4.4.3 Disturbing the proper functioning of services, networks, applications

Services, networks, and application should function properly. From the existence of phenomena such as denial of service attacks, viruses and worms, it appears that parties exist in the world whose only aim is to disturb the proper functioning of services, networks and applications.

The service objectives described in the table below therefore aim at protecting against various of this type of threats.

Representative application	Protection against denial of service attacks (needed: yes/no?)	Protection against attacks with malformed messages	Protection against attacks by sending unsolicited messages	Protection against viruses/ worms/ trojan horses (needed: yes/no?)	Protection against line mutilation (needed: yes/no?)
Voice	Yes	Yes	Yes	No(POTS) Yes (IP, Protecting the computers where the clients and the gatekeeper run, and any other software element which participates in the conference)	Yes
Broadcast TV/radio	No	No	No	No (TV/radio signal)	Yes
Video/audio on demand	Yes (requests to a server)	Yes	Yes	No (reliable information)	Yes
High Speed Internet	Yes	Yes	Yes	Yes	Yes
Instant messaging and chatting	Yes	Yes	Yes	No. No data is stored on the user side	Yes

[6] Ideal situation where user can pay for a more than best-effort peer-to-peer service

Representative application	Protection against denial of service attacks (needed: yes/no?)	Protection against attacks with malformed messages	Protection against attacks by sending unsolicited messages	Protection against viruses/ worms/ trojan horses (needed: yes/no?)	Protection against line mutilation (needed: yes/no?)
Peer-2-Peer	No (not server) Yes (server)	Yes	Yes	Yes	Yes
Gaming	Yes	Yes	Yes	Yes The EXE files should be reliable? Received information is not exe files, but user executes the local exe file (in the server) that should be reliable.	Yes
Nomadism	Yes (request to a server of work sessions)	Yes	Yes	Yes	Yes

Table 4-6 - Protection against disturbing of services, networks, and applications

4.4.4 Untraceable or repudiated sending of 'bad' information

However, sometimes sent information is not received well by the recipients or the sending of the information is considered 'bad' by third parties (such as governments). In addition to the sending of unwanted and/or 'bad' information, usually malicious senders also want to hide their identities or have to possibility to repudiate the fact that they were the sender. This gives rise to the following threats shown in the table below:

Representative application	Protection against sending of 'bad' information (needed: yes/no?)	Protection against hiding of identity of sender (needed: yes/no?)	Protection against repudiation of sending of information (needed: yes/no?)
Voice	No (audio and video, not data)	Yes	No
Broadcast TV/radio	No=>yes Can we censure pornographic or violence information if children use this service?	No	No
Video/audio on demand	No	No	No
High Speed Internet	Yes (e-mail) No (not e-mail)	Yes (e-mail) No (if not necessary identification)	Yes
instant messaging and chatting	No	Yes	No
Gaming	No	Yes (if subscription)	No
Peer-2-Peer	Yes	Yes	Yes
Nomadism	No	Yes	No

Table 4-7 - Protection against sending of 'bad' information

4.5 Basic Requirements to Enable Connectivity

Connectivity, from the application level point of view, is defined as the ability to interact (locally or remotely) between other “humans” or entities (e.g. servers, machines, sensors) to send or retrieve information. Connectivity will imply end-to-end interoperability. The sent/received information comprises any type of data including voice, messaging, email, video and other types of electronic content.

Each application imposes its own connectivity constraints that may impact on the network. According to the application purpose, it is possible to find out the following groups: 1:1, 1:N, N:1 and N:M applications. Network connectivity requirements will change depending on the number of flows, on the network technology and on the application under discussion.

Connectivity requirements are summarized in the table below:

Representative application	Type of access network connectivity	Number of flows	Flows synchronization	Flow segregation capacity
Telephony (legacy or IP based)	1:1	1	NA	NA
video conferencing	1:1 1:N N:1 N:M	≥1	Yes	Recommended
broadcast TV/radio	1:1 1:N	≥1	No	Recommended
video/audio/application on demand	1:1 N:1	≥1	Yes	NA
personal video recorder	1:1 N:1	≥1	No	NA
web browsing and downloading	1:1 N:1	≥1	No	NA
e-mail	1:1 1:N	≥1	No	Recommended
instant messaging and chatting	1:1 1:N N:1 N:M	≥1	No	Recommended
Multiplayer gaming	1:1 1:N N:1 N:M	≥1	Yes	Recommended
peer-2-peer video/audio/file exchange	1:1 N:1	≥1	No	NA
server (web-, video-, file-) application	1:1	1	NA	NA
nomadic application	Depends on	≥1	Depends on	Depends on
secure connectivity application	Depends on	≥1	Depends on	Depends on

Table 4-8 – Basic requirements to enable connectivity

4.6 Basic requirements on Naming and Numbering

Names and numbers serve to convey information necessary for the establishment, control and management of telecommunication services. The best starting point for the determination of the numbers needed in the MUSE network is therefore an analysis of the information requirements.

From the user perspective, the requirements for names are the most important. Addresses are of less interest, as they are typically invisible to the user. The MUSE network must be able to handle the names that users want to have.

Representative application	Phone numbers	Domain names	Aliases, nick names	Directory service
legacy telephony	Yes	Yes	Yes	Yes
video conferencing	Yes	Yes	Yes	Yes
broadcast TV/radio	No	No	No	Yes?
video/audio/application on demand	No	No	No	Yes?
personal video recorder	No	Yes?	No	Yes?
web browsing and downloading	No	No	No	No
e-mail	No	Yes	Yes	Yes
instant messaging and chatting	No	Yes	Yes	Yes
Multiplayer gaming	No	Yes?	Yes	Yes
peer-2-peer video/audio/file exchange	No	Yes	Yes	Yes?
server (web-, video-, file-) application	No	Yes	No	No
nomadic application	Yes	Yes	Yes	Yes
secure connectivity application	Yes	Yes	Yes	Yes

Table 4-9 – Naming and numbering network requirements from the user perspective

From the service provider perspective, MUSE network must be able to handle addresses and different kind of identifiers such as nomadism and charging ones.

Representative application	Addresses for (1) network internal routing and (2) interconnect routing	Identifiers for nomadism	Charging identifiers
legacy telephony	Internal: IPv6 (prefix), Ethernet MAC (depending on architecture) Interconnect: IPv6, IPv4, SS7 pointcodes	Yes. Candidates: IMSI? Something in WLANs?	• Every service will need its service identifier to distinguish it from other services in billing • Probably, every service will require all users to have a user identifier for proper billing • Depending on the wholesale billing model of a service, every operator involved may need to be identified by an operator ID. • Depending on the retail billing model, correlation identifiers may be needed for proper billing. In case of flat fee billing, there is no need for correlation identifiers.
video conferencing	Internal: IPv6 (prefix), Ethernet MAC (depending on architecture) Interconnect: IPv6, IPv4	Same	
broadcast TV/radio	Same	No	
video/audio/application on demand	Same	Yes. Candidates: IMSI? Something in WLANs?	
personal video recorder	Same	Same	
web browsing and downloading	Same	No	
e-mail	Same	Yes. Candidates: User name? IMSI? Something in WLANs?	
instant messaging and chatting	Same	Yes. User name?	
multiplayer gaming	Same	Same	
peer-2-peer video/audio/file exchange	Same	No?	
server (web-, video-, file-) application	Same	No	
nomadic application	Same	Yes	
secure connectivity application	Same	Yes. Candidates: User name? IMSI? Something in WLANs?	

Table 4-10 – Naming and numbering network requirements from the service provider perspective

A more general perspective includes requirements from telecommunication regulations and from general architectural considerations.

Representative application	Service portability	Service provider portability	Location portability
legacy telephony	Phone number: Maybe Domain name: Yes Nick names: No?	Phone number: Yes Nick names: No	Phone number: Maybe Domain name: Yes Nick names: Yes
video conferencing	Phone number: Maybe Domain name: Yes Nick names: No?	Yes Nick names: No	Phone number: Maybe Domain name: Yes Nick names: Yes
broadcast TV/radio	No	No	No
video/audio/application on demand	No	No	No

Representative application	Service portability	Service provider portability	Location portability
personal video recorder	No?	No?	Yes
web browsing and downloading	No	No	No
e-mail	Yes	Yes	Yes
instant messaging and chatting	No	No	Yes
multiplayer gaming	Domain name: Yes Nick names: No	Domain name: Yes Nick names: No	Yes
peer-2-peer video/audio/file exchange	Domain name: Yes Nick names: No	Domain name: Yes Nick names: No	Yes
server (web-, video-, file-) application	Yes	Yes	Yes
nomadic application	Phone number: Maybe Domain name: Yes Nick name: No	Phone number: Yes Domain name: Yes Nick name: No	Phone number: Maybe Domain name: Yes Nick name: Yes
secure connectivity application	Phone number: Maybe Domain name: Yes Nick name: No	Phone number: Yes Domain name: Yes Nick name: No	Phone number: Maybe Domain name: Yes Nick name: Yes

Table 4-11 – Naming and numbering network requirements from a general perspective

4.7 Basic Requirements on AAA

Authentication, Authorization and Accounting. Describes the system to control what resources users have access to and to keep track of the activity of users over a network.

The different applications in the reference list, will require different levels of AAA. The requirements regarding AAA are summarized in the following sections:

4.7.1 Authentication requirements

Reference Application	Authentication	User Prompting	Strong Authentication	Re-Authentication
Legacy Telephony (POTS)	No	No	No	No
VoIP	Yes	Yes	Maybe	Yes
Video Conferencing	Yes	Yes	Maybe	Yes
Broadcast TV/radio	No (public channels) Yes (private channels)	No (public channels) Yes (private channels)	No (public channels) Maybe (private channels)	No (public channels) Yes (private channels)
Video/Audio/Application on Demand	Yes	Yes	Maybe	Yes
Personal Recorder	Yes	Yes	Maybe	Yes
Web browsing & downloading	No Yes (private pages)	No Yes (private pages)	No	No Yes (private pages)
e-mail	Yes	Yes	Maybe	Yes
Instant Messaging & Chatting	Yes	Yes	Maybe	Yes
Multiplayer Gaming	Yes	Yes	No	Yes
P2P	No	No	No	No
Server Application	Yes	Yes	Maybe	Yes
Nomadic Application	Yes	Yes	Maybe	Yes
Secure Connectivity Application	Yes	Yes	Maybe	Yes

Table 4-12 – Authentication requirements

4.7.2 Authorization requirements

Reference Application	User Profile Check	Concurrent Logins Check	Network State	Requested Bandwidth	Failure Reason Reporting
Legacy Telephony (POTS)	Yes (phone	No	Yes	Yes	Yes

	number)				
VoIP	Yes	Yes	Yes	Yes	Yes
Tele Conferencing	Yes	Yes	Yes	Yes	Yes
Broadcast TV/radio	No (public channels) Yes (private channels)	No (public channels) Yes (private channels)	Yes	No (fixed)	Yes
Video/Audio/Application on Demand	Yes	Yes	Yes	Yes	Yes
Personal Video Recorder	Yes	Yes	Yes	Yes	Yes
Web Browsing & Downloading	No Yes (private pages)	No Yes (private pages)	No	No (best effort)	No Yes (private pages)
e-mail	Yes	Yes	No	No	Yes
Instant Messaging & Chatting	Yes	Yes	No	No	Yes
Multiplayer Gaming	Yes	Yes	Maybe	Maybe	Yes
P2P	No	No	No	No	Yes
Server Application	Yes	Yes	Maybe	Maybe	Yes
Nomadic Application	Yes	Yes	Yes	Yes	Yes
Secure Connectivity Application	Yes	Yes	No	No	Yes

Table 4-13 – Authorization requirements

4.7.3 Accounting requirements

Reference Application	Subscription	Service	Number of minutes	Number of bits	Number of invocations
Legacy Telephony (POTS)	Yes	Yes, A	Yes, B&A	No (switched circuit network)	Yes, A
VoIP	Yes	Yes, A	Yes, B&A	No (not relevant)	Yes, A
Video Conferencing	Yes	Yes, A	Yes, B&A	No (not relevant)	Yes, A
Broadcast TV/radio	No (public channels) Yes (private channels)	Yes, B&A	Yes, A	No	Yes, A
Video/Audio/Application on Demand	Yes	Yes, A	Yes, A	Yes, A	Yes, B&A
Personal Video Recorder	Yes	Yes, A	Yes, A	Yes, A	Yes, B&A
Web Browsing & Downloading	Yes (ISP or private pages subscription)	Yes, B&A	Yes, B&A	Yes, B&A	Yes, B&A
e-mail	Yes	Yes, B&A	No (not relevant)	Yes, A	Yes, A
Instant Messaging & Chatting	Yes	Yes, B&A	Yes,A	No	Yes, A
Multiplayer Gaming	Yes	Yes, A	Yes, B&A	No	Yes, B&A
P2P	Maybe (ISP subscription)	No	No (not relevant)	Yes, B&A	Yes, B&A
Server Application	Yes (registration on server)	Yes, B&A	Yes, A	Yes, B&A	Yes, A
Nomadic Application	Yes	Yes, B&A	Yes, B&A	No	Yes, B&A
Secure Connectivity Application	Maybe	Yes, B&A	Yes, A	No	Yes, B&A

Table 4-14 – Accounting requirements[7]

[7] Some parameters could be needed only for accounting, but not for billing, to keep a historical information. In that case, in the table it appears "A". When the information is needed for both billing and accounting, "B&A" is written.
Some services can be billed in different ways. In that case, it will appear billing&accounting in different cells for this service.
Some services could have a billing scheme resulting from the combination of some of the parameters in the table.

4.8 Other Basic Requirements

From the service provider point of view, other requirements imposed by the services should be considered, such as Provisioning and Fault&Performance management. These are general requirements, so that, no classification by service has been done. A brief description is given below:

- **Provisioning** is the process in which network elements are configured with the goal to offer the Customer his desired set of services with the proper QoS, Security, etc. Different Provisioning requirements can be identified per business role. The provisioning process depends on the distribution of business roles by market players.

- **Network performance** and **fault management** are important and challenging tasks in management of modern telecommunications networks. These tasks are grouped into the called **Supervision requirements.** In order to fulfill this requirements, a model for measuring and monitoring should be defined in the network.

4.9 High level requirements for advanced applications

Apart from the reference list of services (see section 4.2), advanced applications should be considered when thinking in a complete test-suite. As well as in the case of basic services, the list of advanced applications and their requirements could be indefinitely long. Hence, a list with the most significant ones has been selected [Srq3].

- Entertainment Applications
  - Peer-to-Peer Content Distribution
  - Content Management and Delivery
  - Gaming
    - Massively Multiplayer Online Games
  - Advanced Multimedia Delivery
    - HDTV and 3DTV on Demand
    - Intelligent TV-multicast
  - Entertainment application n

- Social applications
  - Medical applications
    - Remote Diagnosis
    - Remote Monitoring
    - Remote Nursing
  - Virtual Reality Video-Conferencing, VRVC

- Advanced networking applications
  - GRID
  - Thin Client Computing

- Fixed Mobile Convergence (FMC) and Nomadism

Basic requirements for these applications, such as QoS parameters, can be inferred from the basic services requirements (see sections 4.3 and following). That is the reason why, in the case of advanced applications, other higher level requirements are identified. These requirements will have some impact not only over an end-to-end testing scenario but also over the business model in a real deployment.

Now, the high-level requirements are specified and their possible implication in the access network, the information has been taken from the [Srq4], where much more detailed information can be found about these and other requirements imposed by the detailed applications. After the analysis of the requirements imposed by the applications, exposed in [Srq3] and [Srq4], it can be stated that these applications can work correctly in MUSE architecture.

High level requirements:

DRM

DRM is unlikely to have any significant impact on the network and therefore of little relevance to MUSE. DRM data (media description/decomposition plus REL for each component part) is small in comparison to the media data itself, and so does not increase bandwidth requirements.

MicroPayments

Micro Payments have little direct impact on the network other than acting as an enabler for people to buy services which otherwise they might not bother to buy. But they could be a significant network service if they can be abstracted away from their current web-based front ends.

Presence

The currently accepted form of “presence” is IM, however a better form is by showing a thumbnail video representation of the distant party. This is bandwidth hungry if a large picture is required, because an upload is required from each party being monitored and therefore requires more upstream capacity than downstream i.e. is asymmetric in the reverse direction to that provided by ADSL.

Trans-coding

It is expected that the trans-coding will be done in some kind of server. The source material could either reside on the server or be uploaded as and when required. If the latter, it is again a case of reverse asymmetry compared to the asymmetrical nature of ADSL i.e. more upstream capacity would be required than downstream.

Discovery

There are different implications on network bandwidth usage patterns depending on these two scenarios:

- Discovery could be compared to searching for a book in a library, where you need to know something about the book, but you can be reasonably sure that most books will be available or that they can be obtained after a short wait.
- Alternatively, a search could be likened to searching for a book in a bookshop, where you know that the stock will be popular best-sellers, and that the stock room has more of the same rather than breadth.

The difference between a library and a bookshop is that the former has a wider stock and a less commercially-oriented set of material. The stock in a bookshop will be smaller and is likely to be influenced by the availability and popularity of books stocked.

The library comparison is search-intensive (low bandwidth requirements) whilst the bookshop is likely to be more multimedia-based, and therefore consume more download bandwidth.

Remote Management

There are likely to be two modes:

- Normal Monitoring
- When something goes wrong and detailed information is required

In the latter case, the quantity of information flow changes and the symmetry of the connection is likely to reverse.

Remote Processing

As in the case of trans-coding noted above, the network requirements depend on whether uploading is necessary. It is possible that a lot of people might want remote processing e.g. uploading video clips of a local football match. Some form of remote processing of the material could then take place e.g. editing and different degrees of compression for later downloading by other fans. In this case, one person uploads and many download, so the net impact on the network is for data to flow in the downstream direction.

Remote storage

Two cases can be envisaged:

- Use as read/write storage (symmetrical, rather than asymmetrical)
- Archival of a safety copy (uploaded and possibly never downloaded) – reverse asymmetry. In the case of a safety copy, the location should be distant from the original material being backed-up.

Content distribution

For network efficiency, information is needed about the number and location of potential downloads so that replication capabilities can be made available in the network.

Overall the most significant conclusions are as follows (for more information read chapter 7 and 8 of [Srq4]):

- Demand for high bandwidth 50 -100 Mbit.
  We may have identified a true killer application or the main driver for high bandwidth

demand to be “file transfer in a reasonable time”. If one imagines that all end users in the private and as well as business sector, would outsource their daily storage and backup service as well as application demand to an external service provider, it would lead to a natural demand for high bandwidth and fast response time. Outsourcing of storage creates a kind of virtual intranet relation and the demand would be from 50 - 100 Mbit.

- Demand for symmetric bandwidth.
  The trend is towards more symmetric traffic. Outsourcing of storage, videoconference and P2P is by nature symmetric and in some cases correspond to more than 80 % of the traffic in the access network.
- Demand for low latency, 50 ms.
  Several Applications such as games, VOIP, Video conferences requires low latency.

- GRID and VRVC are the most demanding applications on Network Requirements (capacity, security, and dynamic QoS in particular) and in some circumstances would benefit from as much bandwidth as could be made available, 50- 100 Mbit bandwidth for business as well as residential users.

Summary of Network Requirements:

	Downstream Data Rate	Upstream Data Rate	QoS	Real time streamed data	Secure Data	Comment
ENTERTAINMENT APPLICATIONS						
Peer to peer Content Distribution						
File exchange	L	L	H	No	Yes	
Micro payments	L	L	H	No	Yes	Little impact on network
Discovery	L	L	M	No	No	
Content Management and Distribution						
Personal content	L	L	M	No	No	Images - audio, video, applications. Personal content streamed to appropriate device. None real time
Gaming						
Multiplayer on-line games	L	L	H	Yes	No	Large potential growth area. Low Latency Required
Advanced Multimedia delivery						
H Definition Television	H	L	H	Yes	No	10 - 20 Mbps data rate
Intelligent multicast	H	L	H	Yes	No	High bandwidth
Entertainment Applications: VOD, PVRs and beyond						

VOD service	H	L	H	Yes	No	
PVR service	M	L	H	No	No	
COD service	L	L	H	No	No	
SOCIAL APPLICATIONS						
Medical Applications						
Remote diagnosis	H	L	H	No	Yes	Image transfer & patient details
Remote monitoring	M/ H	H	H	Yes	Yes	Continuous real time data, video conferencing
Remote Nursing	M/ H	H	H	Yes	Yes	Continuous real time data, High quality video conferencing
VR Video conferencing						
Network requirements	M	M	H	Yes	Yes	Multicast video conferencing, audio, Low latency
ADVANCED NETWORKING APPLICATIONS						
GRID	M	L	H	No		500Kbps
Thin Client Computing	H	M	H	Yes	Yes	3Mbps for video
FIXED MOBILE CONVERGENCE AND NOMADISM						
	M	M	H	Yes	No	Move to an IP network
USER BEHAVIOURS						
Digital TV						Merging of television based broadband and PC based broadband is evident with video and audio downloads to PC to be watched on the television. TV screens are becoming flat panels and can be used for TV and PC content.
Internet						

4.10 "Full service" testing with a limited number of applications

4.10.1 E2E Service Requirements

So far we have described a service based classification. Obviously, for the MUSE lab trails only a limited number of applications from the identified service classes will be considered. In this subsection we will fix the set of applications that will be tested in MUSE.

In the following, along with the chosen service, the associated application(s) will be indicated, as well as the reason for taking it into account for the trails and demos. It is assumed that the global requirements of each service class are represented by the requirements of the corresponding selected application(s).

4.10.1.1 Interactive, error tolerant services

From this group we choose two applications: Voice-over-IP and Videoconference. Voice-over-IP is chosen because voice is a commodity application. Videoconference is chosen because it has the same strict delay requirements as Voice-over-IP and in addition it is a possible killer app for broadband networks.

Voice-over-IP

For Voice-over -IP a main issue is the delay caused by the network due to the limited performance of heavily loaded IP networks. The main requirements for this application are very low delay and jitter.

Videoconference

Obviously, the requirements of bandwidth for this application are higher than for VoIP and relate to the required quality of the video signal. Also, two-way interactivity of this application and their specific characteristics mean that latency requirements are very stringent (low delay and jitter), being also essential to keep them easily understandable. In addition the difference in delay between the audio and video signals (audio-video skew) must be very low.

4.10.1.2 Interactive, error intolerant services

From this group we choose interactive gaming. It is chosen because it has delay requirements comparable to Voice-over-IP and in addition many users already are playing interactive games over the Internet.

Interactive gaming

The main performance parameter for interactive gaming is delay, with requirements close to that of VoIP. It should be noted that sensitivity of the perceived quality on the delay also depends on the nature of the game, i.e., fast paced games (so-called “First Person Shooter” games) have the strictest requirements while strategy games have more relaxed requirements. Currently bandwidth requirements for interactive games are very modest but this might change when broadband penetration further increases.

4.10.1.3 Responsive, error intolerant services

From this group we choose web browsing. It is chosen because it is a commodity application.

Web browsing

In general, client-server commercial applications (e.g., Web services, video-surveillance with low-quality, information services) belong to this service class. These applications can be provided with guaranteed QoS or with the lower quality "best-effort". In general, the requirements of this type of application are low and will depend on the type of data to be transferred. The bandwidth, delay and packet loss are the main parameters that can affect the quality perceived by the users in these services, but the limits of these parameters are defined by the QoS required in every scenario.

4.10.1.4 Timely, error tolerant services

From this group we choose video streaming. It is chosen because it is a possible killer app for broadband networks. In addition this application might generate considerable amounts of traffic.

Video streaming

The requirements for this application depend on the required quality of the audio and video signal (MPEG, HDTV) so the bandwidth and packet-loss are the main parameters that can affect the quality of this application.

4.10.1.5 Timely, error tolerant services

From this group we choose downloads. It is chosen because it is a commodity service.

Downloads

This service, also referred to as bulk data, is strongly related to web browsing. The difference lies in the fact that delay requirements are relaxed. Because both web browsing and downloads will use TCP as transport protocol we will consider the two applications as one in the sequel.

4.10.2 E2E Network Requirements

The limits pointed out in the current Subsection for the network performance parameters, i.e., throughput, delay, packet loss and jitter, are all related to the end-to-end quality of each of the selected applications, according to what is defined in ITU-T Rec. G.1010 [QoS5], which has been the selected approach for the MUSE lab trials and demos, in what the QoS requirements is concerned. However, as the test labs of the MUSE project deal only with IP networks, those parameters should be translated to IP packet information transfer performance parameters, i.e. IP packet Transfer Delay, IP packet Delay Variation, IP packet Loss Ratio, and IP packet Error Ratio, as defined in ITU-T Rec. Y.1540 [QoS32].

Just in order to stand as a reference, the graphic presented below, which has been extracted from [QoS5], denotes a possible overall association between application and network parameters:

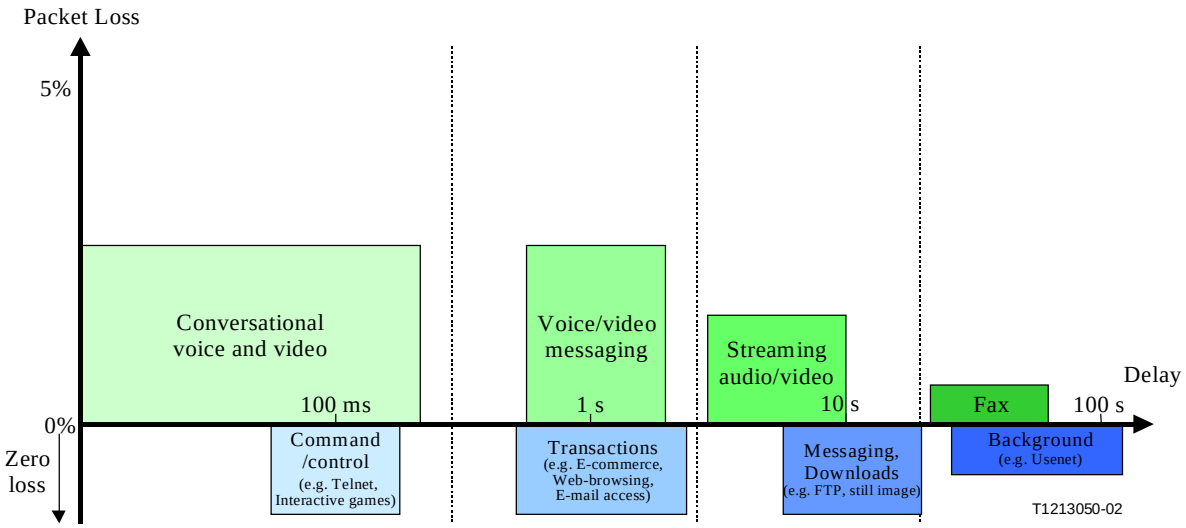


Figure 4.2 - Applications vs network parameters

The following tables contain the above mentioned end-to-end network requirements for the services and associated applications that will be considered within the MUSE lab trails, according to ITU-T Rec. G.1010 [QoS5], in what the QoS requirements is concerned.

Application	Degree of symmetry	Typical data rates	Key performance parameters and target values			
			One-way delay (note 1)	Delay variation	Information loss ratio (note 2)	Other
Voice-over-IP	Two-way	4-64 kbit/s	<150 ms	< 1 ms	< 1%	
NOTE 1 – Assumes adequate echo control. NOTE 2 – Impact of information loss depends both on the codec type and the use of Error Concealment techniques						

Table 4.15 - Performance requirements for conversational voice

Remark 1: The network delay variation can actually be larger than 1 ms mentioned in the above table but it will be removed by the operation of a jitter buffer. Jitter buffers remove jitter at the cost of additional delay. A commonly mentioned upper bound for the jitter is 30 ms, see [QoS58]. Earlier in this chapter an upper bound for jitter of 20 ms is mentioned.

Remark 2: Earlier in this chapter a BER/packet loss requirement of 10^{-7} is mentioned but this presumably refers to the BER.

Application	Degree of symmetry	Typical data rates	Key performance parameters and target values			
			One-way delay	Delay variation	Information loss (Note 1)	Other
Videoconference	Two-way	16-10000 kbit/s	< 150 ms	30 ms	< 1%	Lip-synch: < 80 ms
Streaming Video	One-way	16-10000 kbit/s	< 10 s	Note 2	< 1%	
NOTE 1 – Impact of information loss depends both on the codec type and the use of Error Concealment techniques						

Table 4.16 - Performance requirements for video services

For Videoconference the Section on Service Requirements gives upper bounds of 400 ms and 40 ms for one-way delay and jitter respectively. However, for one-way delay of 150 ms and up, the loss of interactivity becomes noticeably to customers. Therefore we stick to the upperbound of 150 ms.
For Streaming Video the Section on Service Requirements gives an upper bound of 500 ms for the delay. However, due to fact that this application is one-way, buffering at the receiving side allows delay up to a few seconds.

The bandwidth requirements relies on the used video format, see e.g. [QoS6]:

Video format	Typical bandwidth requirement
Uncompressed HDTV	1.5 Gbits/sec
HDTV, Interim format	360 Mbits/sec
Standard Definition TV (SDTV), SMPTE	270 Mbits/sec
Compressed MPEG-2 4:2:2	25–60 Mbits/sec
Broadcast quality HDTV (MPEG-2)	19.4 Mbits/sec
MPEG-2 Standard Definition TV (SDTV)	4-6 Mbits/sec
MPEG-1	1.5 Mbits/sec
MPEG-4	5 Kbits/sec–4 Mbits/sec
H.323 (H.263)	28 Kbits/sec–1 Mbits/sec

Table 4.17 - Typical bandwidth requirements for some commonly used video formats

Application	Degree of symmetry	Typical amount of data	Key performance parameters and target values		
			One-way delay (Note)	Delay variation	Information loss
Web-browsing	Primarily one-way	~10 KB	Preferred < 2 s /page	N.A.	Zero

– HTML			Acceptable < 4 s /page		
Bulk data transfer/retrieval	Primarily one-way	10 KB-10 MB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero

Table 4.18 - Performance requirements for data services

Remark 3: Note that the data services make use of TCP which is a reliable transport protocol, hence assuring zero information loss. However, packet loss might still occur because TCP uses packet loss to find its optimal sending rate. As such it is hard to give an optimal value for the packet loss.

Remark 4: Earlier in this chapter requirements for web browsing and downloads in terms of delay and jitter for packets are given.

Medium	Application	Degree of symmetry	Typical amount of data	Key performance parameters and target values		
				Response Time	Delay variation	Information loss
Data	Interactive games	Two-way	< 1 KB	< 200 ms	N.A.	Zero

Table 4.19 - Performance requirements for interactive gaming

Remark 5: Earlier in this chapter a delay of 200 ms i.e. a Response Time of 400 ms, is mentioned. According to Färber [QoS69], for First Person Shooter games a ping (= response time) below 50 ms is associated with excellent game play: a ping below 100 ms is good and above that, playability decreases noticeably. For Real Time Strategy games pings ranging from hundreds of milliseconds to seconds do not affect overall user performance, see [QoS72].

Remark 6: The impact of packet loss on interactive gaming quality is rarely discussed but Beigbeder et al [QoS73] suggest that users rarely notice packet losses as high as even 5% for the First Shooter Person game Unreal Tournament 2003 (UT). This might be due to the use of error concealment techniques by the designers UT. In fact, it is shown in [QoS95] that the First Person Shooter Quake IV is robust for packet loss as high as 40%!

The objectives in the above tables are all end-to-end. In order to translate them into objectives for the MUSE access network, assumptions will have to be made with respect to the core network and with respect to the terminal equipment, taking into account that the end-to-end path consists of the following chain:

terminal – access network – core network – access network – terminal.

Generic conditions with respect to network quality in the core network can be obtained from the NOBEL project.

5 QOS TESTING

5.1 Introduction

It is the aim of this chapter 5 to describe “what should be measured in the MUSE lab trails, with respect to QoS”.
First in section 5.2 we explain that the primary focus in the MUSE lab trails should be on the perceived quality of service. Next we discuss the quality factors that determine the perceived quality for the applications that will be considered in the MUSE lab trails: VoIP, Videoconference, Video streaming, web browsing/bulk data and Interactive Gaming.

Next in section 5.3 we explain the methods that are available to score the perceived quality of a given application: objective measurements, subjective measurements and the mapping from network quality to perceived quality. The preferred method of scoring is through objective measurements.

If objective or subjective methods are not available then we must fall back to network quality measurements. The network quality parameters that should be measured are discussed in section 5.4.

Finally in section 5.5 we summarize all tests that should be conducted.

5.2 Perceived service quality for end users

There are several perspectives with respect to QoS: perceived QoS, network quality, terminal quality and QoS mechanisms that are supported by the network entities, see Figure 5.1.

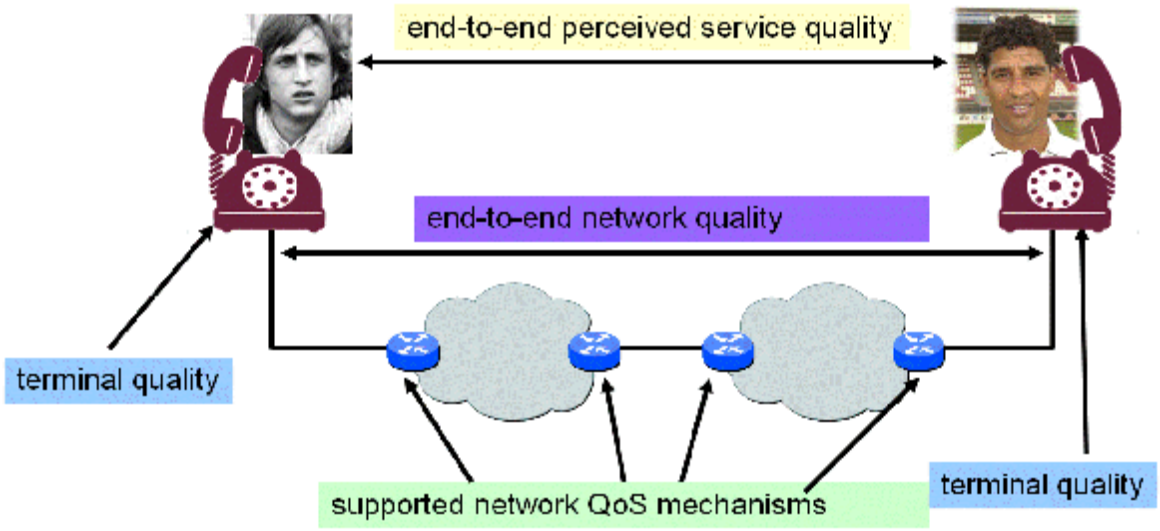


Figure 5.1: Four QoS perspectives

In our opinion the MUSE lab trails should have its primary focus on the perceived QoS because in the end customers have to be satisfied with the quality of the services that will be delivered over the MUSE network. Therefore each selected application will be analyzed in terms of these perceptual quality factors. A preliminary consideration has to be done about the set of definitions related to QoS and network performance that are defined in ITU-T E.800 [QoS1]. Regarding the user perceived service quality, e.g., for the voice service, examples of general key performance indicators (KPI) are:

- Call set-up time,
- Dial Tone Delay,
- Call Success Ratio,
- Dropped Call Rate (or alternatively Call Completion Rate),
- Billing correctness,
- End-to-end perceived transmission quality.

Throughout this document, only the last KPI, the perceived quality, will be discussed extensively in association to all transmission aspects during a live connection. The other KPIs mentioned above are considered of minor importance in this document. Another way of putting this is that in this chapter we only consider the perceived quality of the service while the service is being consumed by the user.
It should be mentioned here that within MUSE TF1.7 [QoS96] the validity of the ITU-T E.800 framework is questioned. In fact, according to [QoS96] the following issues need to be addressed when dealing with Quality of Experience (a term that recently became a fashionable substitute for perceived QoS):

- Easy first time service set-up
- Easy and fast service start and stop
- Available when needed
- Quality matching the expectations/ needs
- Responsiveness
- Consistency
- Security
- Cost Transparency
- Reliable and comprehensible Billing
- Easy de-installation of a service

5.2.1 Perceived quality factors for Voice over IP

The main perceptual factors influencing voice are quality clarity, delay and echo, see [QoS10]:

Clarity
Clarity can be defined as the clearness, or the fidelity, of voice as it is reproduced by a network and perceived by a listener.

Delay
The delay has an impact on the interactivity of a conversation. If the delay is too large, an interactive conversation becomes impossible, see e.g. [QoS11]. The delay also has a possible impact on the echo.

Echo
Echo is caused by delay that affects the speaker, but not the listener. It occurs when the voice of the speaker is leaking in to the receiving path, see e.g. [QoS29].

The overall perceived quality of a Voice over IP service is called conversational speech quality.

As such, it has to be considered that the conversational quality of a voice link is influenced by four parts:

- **Listening quality,** the quality of the speech received from the talker's voice at the other side, dominated by noise and speech distortion.
- **Talking quality,** the quality of the speech received from the talker's own voice, dominated by echo and side tone distortion.
- **Interaction quality,** the quality associated with the alternation of talking and listening, dominated by end-to-end delay and noise/speech switching.
- **Background noise transmission quality,** the quality of the transmission of background noises received from the other side. Note that Background noise transmission quality and Listening quality are not independent: the first may or may not have been included in the latter.

Therefore, for VoIP we get the following:

Test: For VoIP the following quality aspects need to be scored: *listening quality, talking quality, interaction quality, background noise transmission quality.*

Note that conversational quality is determined by the lowest quality of the results.

Remark. It was already mentioned in the previous section that other identified issues related to user perceived service quality, such as e.g. call set-up time, call success ratio etc., are considered of less importance than the factors mentioned above. Therefore, we do not further take these issues into account in this document.

5.2.2 Perceived quality factors for Streaming video

The perceived image quality of video depends on many factors. Visually the most important factors for the video quality are: viewing distance, display size, resolution, brightness, contrast, sharpness, colorfulness and naturalness, see [QoS13]. A distinction should be made between fidelity and quality, where fidelity stands for the closeness of the processed video to the original. For instance, for a low quality original, a high fidelity reproduction will still have low quality.

Visible distortions will most often lower the perceived quality. These may be introduced by lossy compression. The most widely used codecs use block-based Discrete-Cosine Transform (DCT) with motion compensation followed by quantisation of the coefficients as a compression scheme e.g. MPEG 2 [QoS14], ITU-T H.263 [QoS15]. The main distortion introduced by such codecs are, see [QoS13]: blockiness, blurring, color bleeding, ringing, DCT basis image effect (a single DCT component is dominant in a block), staircase effects on slanted lines, false edges, jagged motion, chrominance mismatch, mosquito noise, flickering and aliasing.

For video containing audio the synchronization between video and audio is also an important perceptual factor, see Steinmetz [QoS16].

An equally important source of errors is the transmission. The three most important sources of this in a packet-based network are packet loss, delay and delay variations (jitter). The visual effect of lost information is highly dependent on the codec and on which type of information that is lost. Some errors might be possible to hide using error concealment strategies, whereas others have severe effects.

Finally, also channel zapping time can be identified as an important factor.

Summarizing, for Streaming Video we need to assess audio quality, visual quality, synchronization quality and zapping quality. This yields the following test:

Test: For Streaming Video the following quality aspects need to be scored: *audio quality, visual quality, synchronization quality, zapping quality.*

Remark. A number of other factors influence the user perceived service quality for Streaming Video. Examples include easy and fast service start and stop, Electronic Programming Guide responsiveness and support of software updates. Again, these factors are assumed to be of less importance than the user perceived quality of the streamed video.

5.2.3 Perceived quality factors for Videoconference

The perceived quality factors that are listed for streaming video also hold for videoconference. In addition due to its interactive nature the same strict delay requirements as for Voice over IP hold, see e.g. [QoS6].

Therefore the following items need to be assessed:

Test: For Videoconference the following quality aspects need to be scored: *listening quality, talking quality, interaction quality, background noise transmission quality, visual quality, synchronization quality.*

5.2.4 Perceived quality factors for Web browsing and bulk data

Web browsing and bulk data services have two basic requirements (apart from issues like security, privacy, cost etc.), namely the data integrity and fast response and delivery of requested information and data services. The user perception is based on user expectation: the importance of the information to the user influences the willingness to wait longer.

The end-to-end perceived service quality of information and data services is mainly determined by:

- First response time,
- Total download time.

The first response time is the delay between a data request by a user and the first response of the application. For example, when clicking on a URL in a browser, it corresponds to the first visible response on the browser window.

The total download time is the delay between a data request by a user and the complete download. In the browsing example the requested page is now completely shown on the screen.

Test: For Web browsing and bulk data the following quality aspects need to be scored: *response time quality, total download time quality.*

5.2.5 Perceived quality factors for Interactive gaming

In current interactive games the main network related perceptual aspect is the response time, see e.g. [QoS69] and [QoS70]. It is defined by the time the system needs to detect a user-initiated input event, to process it, and to send the updated game state to the local output device. The nature of the game influences the dependency of the perceived quality on the response time. For instance, fast paced "First Person Shooter" games, such as Quake and Half-life are much more sensitive for a high delay than "Real Time Strategy" games, such as WarCraft III and Command & Conquer.

If voice and/or video are part of an interactive game then obviously the perceived aspects of these applications, and the synchronicity between voice, video and the gamers actions, also determine the overall perceived quality of the interactive game.

Test: For Interactive Gaming the following quality aspects need to be scored: *Interaction quality, visual quality, synchronization quality.*

Summarizing this subsection we come to the following:

Test: Obtain scores for the perceived quality of service for *VoIP, Streaming Video, Videoconference, web browsing/bulk data and interactive gaming*

5.3 Measuring perceived quality

When performing MUSE lab trails or demos, for the specific MUSE solution tested under varying conditions, it should become evident that the perceived QoS is sufficiently high for each considered service.

Having this in mind, it should be noted that, as mentioned before, the user perceived service quality depends both on the end-user perception, on the network performance, as well as on the performance of the terminal equipment, as indicated in ITU-T Rec. Y.1541 [QoS3], and ETSI TS 101 329-1 [QoS4].

In this subsection we will discuss the type of methods that are available to obtain perceived quality of a service.

5.3.1 Subjective measurements

Since network services are targeted to human users, it is necessary at some point, in a controlled way, to measure the reactions and experiences of users. It might seem impossible to measure a subjective experience, but there are scientifically developed psychological and psychophysical methods to do that. Some of these have been adapted to certain applications and then standardised, e.g. ITU-R Rec. BT 500-11 [QoS18] for quality of television pictures.

The repeatability and stability of subjective data are often questioned, since the response of a single user can vary if a particular experiment is repeated. However, the average of a users panel is stable. For instance, in the evaluation of video quality performed by Video Quality Expert Group (VQEG), the correlation between two different laboratories that ran the same experiment was 0.97, see [QoS19].

5.3.2 Objective measurements

Although there are well-tested procedures to perform subjective measurements, there are several problems with them, i.e., they require a lot of work, careful preparation and they take long time to perform, which also make them expensive. Furthermore, it is not possible, or at least is very difficult to use them for measuring in-service applications. It would, therefore, be useful to have objective measurement procedures, based on computer software programs, which could be used as an alternative.
The most important class of objective measurements is formed by the so-called black box method. A black box method is not focused on the specifics of the system under test. Therefore it does not require knowledge of the system under test but it does require extensive knowledge of human perception. For black box based objective quality measurements one needs the original signal (at least in reduced form) and the degraded signal in order to compute the perceived quality.

For speech the black box method for objective measurement of the listening quality has been standardized in 2001 and it is called PESQ (Perceptual Evaluation for Speech Quality), see [QoS23]. For the visual quality of video four black box methods were standardized in 2004, in ITU-T J.144, see [QoS25]. Of the four black box methods defined in [QoS25] we propose to use the overall best model, which is called VQM (Video Quality Metric), see also [QoS24].

5.3.3 Using network quality to predict user-perceived quality

For objective quality measurements such as PESQ (for voice) and VQM (for video) one needs the original signal (at least in reduced form) and the degraded signal in order to compute the perceived quality.

A completely different approach is to use a computational model that predicts the subjective quality of an application as based on transmission characteristics. Obviously such a computational model should be trained on datasets with subjective data.

For Voice, this approach is standardized and has led to the so-called E-model [QoS27]. The E-model relates network and terminal characteristics, such as delay, packet loss ratio, used codec, to perceived quality, as expressed in a MOS score.

For Video, the mapping between network performance and perceived quality is not understood as good as for Voice. Verscheure et al [QoS28] propose a mapping between the MOS score versus coding rate and packet loss for MPEG-2 video.

For Web browsing no mapping is known between user perceived quality and network quality. However, Khirman et al [QoS26] have established a relation between response times and the cancellation rate of web page requests.

In addition, and according to [QoS17] the most significant factor that determines the user perceived quality is the time to receive the data. With respect to response time limits, the following guidelines are stated:

- 0.1 s: user feels system reacts instantaneously
- 1 s: user's flow of thought stays uninterrupted
- 10s: limit for keeping user's attention focused

Additional guidelines can be found in [QoS17].

For Interactive Gaming no standard is available for mapping network quality to user perceived quality.

For the First Person Shooter game Xblast Schaefer et al [QoS70] suggest a mapping between response time and the MOS score. Recently Wattimena et al [QoS95] suggested a mapping between MOS for the First Person Shooter Quake IV and response time and jitter.

5.3.4 Hierarchy of test methods for perceived quality

In this subsection we discuss the hierarchy of test methods for obtaining the perceived quality of services:

- objective standardized, or in the process of being standardized, measurement methodologies will be given priority;

- if there are no objective measurement methodologies that cover all the aspects considered as relevant, or even if there are, but don't cover the entire desired set of aspects that are to be tested, existing subjective measurements standardized, or in the process of being standardized, must be used;

- if subjective measurements methodologies are non-existent, they must be invented or indicated as FFS. However, it should be noted that the subjective obtained score is highly dependent on the experimental context;

- whenever considered as relevant, tests to the network packet itself should be performed (e.g. video), and if considered as relevant, the relationship between network quality and perceived quality should also be investigated (e.g. interactive games);

- performance tests for terminal equipment are considered out of the scope of the present Section, and therefore will not be specified. However, their impact should be taken into account when evaluating the results.

The hierarchy introduced above is visualised in Figure 5.2.

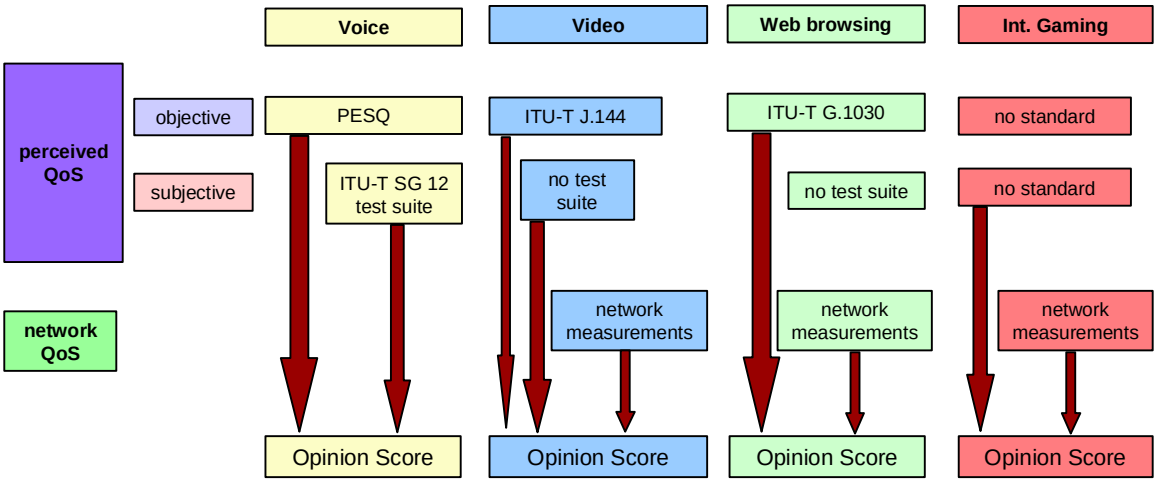


Figure 5.2: Hierachy of preferred test methods for perceived quality

ITU-T Rec. G.1030 [QoS 81] is a recommendation to the ITU-T Study Group 12 which is as yet prepublished.

5.3.5 Summary

In this subsection we have seen that there are three ways to score perceived quality for a given application: subjective measurements, objective measurements and by mapping network quality to perceived quality.

The preferred method is the use of standardized objective measurements. If objective measurements are not available then standardized subjective measurements need to be conducted, possible together with network quality measurements.

5.4 Measuring network quality

5.4.1 Network QoS parameters

We have seen that the preferred method to score perceived quality is by objective standardized methods. If objective methods are not available and subjective methods are not available either or too cumbersome to apply then we must rely on network QoS measurements. Network quality obviously gives an indication about the expected perceived quality.

The most important metrics that characterize the performance of a packet-switched network, which are the most significant factors that influence the end-to-end quality of an application, can be found in e.g. ITU-T Rec. Y.1540 [QoS32], ITU-T Rec. G.1010 [QoS5], Miras [QoS6], or Tanenbaum [QoS33]. In the following, a global definition is provided:

Bandwidth
This signifies the portion of the available capacity of an end-to-end network path that is accessible to the application or data flow.

Delay
Delay manifests itself in a number of ways, including the time taken to establish a particular service from the initial user request and the time to receive specific information once the service is established.

Delay variation
Delay variation is sometimes also denoted as jitter. Services that are highly intolerant of delay variation will usually take steps to remove (or at least significantly reduce) the delay variation by means of buffering.

Information loss
Information loss has a very direct effect on the quality of the information finally presented to the user, whether it be voice, image, video or data. In this context, information loss is not limited to the effects of bit errors or packet loss during transmission, but also includes the effects of any degradation introduced by media coding for more efficient transmission (e.g. the use of low bit-rate speech codecs for voice).

Loss pattern
The loss pattern or the loss period is often equally important, as it may offer valuable hints to the designers of codecs and applications. The most notable observation concerning loss patterns in today's Internet is that losses appear in bursts — usually short, but occasionally, at times of extreme congestion, more lengthy, see for instance Bolot [QoS34] and Yajnik et al [QoS35].

It is to be noted that, in this study we mainly focus on network performance for IP networks. The above network parameters within the context of IP networks are defined in ITU-T Rec. Y.1540 [QoS32]:

- IP packet Transfer Delay (IPTD)
- IP packet Delay Variation (IPDV)
- IP packet loss ratio (IPLR).

In addition to the IPLR, ITU-T Rec. Y.1540 [QoS32] also defines the IP packet Error Ratio (IPER), but because it is assumed that it is accounted for in the IPLR, the IPER is not considered in this document.

Moreover, the ITU-T Rec. Y.1540 [QoS32] also defines IP service availability, i.e., if the IPLR on and end-to-end basis is smaller than a given threshold (0.75, 0.9 or 0.99), then the service is called available. Because availability deals with very large time scales (as compared to packet-level time-scales) we will not take availability into account in this Section.

Upper values for IPTD, IPDV, IPLR and IPER are given in ITU-T Rec. Y.1541 [QoS3].

The IETF also developed a framework for IP performance metrics, see RFC 2330 [QoS36]. The main difference between the ITU and the IETF frameworks is the way they define delay variation. The ITU base the IPDV on a delay histogram whereas the IETF proposes to use a differential definition, see RFC 3393 [QoS37]. For a discussion on this matter, see [QoS38].

Although we restrict ourselves to IP network performance for completeness sake we also refer to two documents which state definitions of network performance parameters for Frame Relay, Frame Relay Forum 13 [QoS39], and for ATM, ITU-T Rec. I.371 [QoS40].

5.4.2 Measurement framework

A framework for measurement of network performance in the IP context is described in ITU-T Y-1540 [QoS32]. This framework is in line with the framework presented in IETF RFC 2330 [QoS36], except with respect to delay variation.

An important remark is that default measurements often characterise the network performance on a time scale much coarser than the time scale on which users perceive a service. For instance, SNMP by default records 5 minutes workload averages whereas for web browsing the relevant time scale is in the order of 100 ms, see also Sears et al [QoS17]. An example of measured network performance on different time scales can be found in Fraleigh et al [QoS44].

A theoretical treatment of network performance on different timescales can be found in Fraleigh2 et al [QoS45]. Both in [QoS44] and [QoS45], the emphasis is on bandwidth usage.

Prasad et al [QoS56] review the recent bandwidth estimation literature focusing on underlying techniques and methodologies as well as open source bandwidth measurement tools.

5.4.3 Proposed measurements for network quality per application

In this subsection we will list per service that will be considered in the MUSE lab trails what network quality parameters should be measured.

5.4.3.1 Voice over IP

Because for VoIP the objective and subjective methods for obtaining perceived QoS are standardized we do not have to measure the network quality for VoIP.

5.4.3.2 Videoconference and streaming video

Because for video applications objective and subjective methods for obtaining perceived QoS are not very mature we will have to conduct network quality measurements for both Videoconference and streaming video.

Test: for Videoconference and Streaming Video measure delay, jitter, packet loss and throughput

5.4.3.3 Web browsing and bulk data

The perceived quality of this service is directly coupled to the Response Time and the Total Download Time. Therefore these aspects should be measured in the network:

Test: for Web browsing and bulk data measure Response Time and Total Download Time

5.4.3.4 Interactive gaming

According to Färber [QoS69], for First Shooter Person games a ping (= response time) below 50 ms is associated with excellent game play. According to [QoS95] also the jitter plays an important role.
As noted before, for other type of games, such as Real Time Strategy games the delay requirement can be relaxed.

ITU-T Rec. G.1010 [QoS5] states that interactive gaming requires zero packet loss but this seems to be contradicted by some references, see e.g. [QoS73]. This point is left for further study.

The required bandwidth for currently played interactive games is very modest, even below 40 kbps, but this might change when broadband penetration further increases.

Test: for Interactive Gaming measure ping, jitter, packet loss and throughput

Remark: As already stated before, the user perceived service quality depends both on the network performance and on the performance of the terminal equipment, see also ITU-T Rec. Y.1541 [QoS3], and ETSI TS 101 329-1 [QoS4]. Performance tests for terminal equipment are considered out of the scope of the present Section, and therefore will not be specified. However, their impact should be taken into account when evaluating the results.

5.5 Summary

In this section we summarize the findings of this chapter with respect to what should be tested within the MUSE lab trails. The summary consists of service specific tables denoting what to test, either by scoring or by measuring.
It should be noted that for end-to-end testing both network and terminal performance have to be taken into account.

Service	Voice-over-IP
Scoring	Listening quality Speech quality Interaction quality Background noise transmission quality

Table 5.1: QoS testing for VoIP

Service	Streaming Video
Scoring	Audio quality Visual quality

	Synchronization quality Zapping quality
Measuring	Delay Jitter Packet loss Throughput

Table 5.2: QoS testing for Streaming Video

Service	Video Conference
Scoring	Audio quality Visual quality Interaction quality Background noise transmission Synchronization quality
Measuring	Delay Jitter Packet loss Throughput

Table 5.3: QoS testing for Videoconference

Service	Web browsing and bulk data
Scoring	Response Time quality Download Time quality
Measuring	Response Time Download Time

Table 5.4: QoS testing for Web browsing and bulk data

Service	Interactive Gaming
Scoring	Interaction quality Visual quality Synchronization quality
Measuring	Ping Jitter Packet loss Throughput

Table 5.5: QoS testing for Interactive Gaming

5.6 Inventory of Standards

With respect to QoS the two most important standardization bodies are the International Telecommunication Union (ITU) and the Internet Engineering Task Force (IETF). Traditionally, the Telecom-sector of ITU, the ITU-T, represents the old Telecom world of telephony and packet switched networks with QoS support (i.e. ATM). The IETF find its origin in the best effort IP networking world.

Of course, nowadays the activities of both bodies converge to the situation where multiple services can be employed over the Next Generation Network.

Other relevant standardization bodies and organisations include ETSI, 3GPP and DSLF. Also worth mentioning is VQEG (Video Quality Expertise Group). Although not a standardization body this independent organization evaluates video quality measurement algorithms.

5.6.1 ITU

Most of standards relevant for QoS belong to the ITU-T, which gives an overview of terms and definitions related to QoS and network performance in E.800. Methods for subjective assessment of quality of voice and video are given in P.800 and P.910 respectively. A method for measuring voice (listening) quality objectively is standardized in P.862. Similar methods for video are standardized in J.144.

G.1010 lists end-user multimedia categories. This includes target network requirements for a variety of applications.

G.107 describes a mapping between network and terminal characteristics and user perceived quality of voice. Some of these characteristics are given in more detail in G.113, G.114 and G.131.

A framework for IP network performance parameters is discussed in Y.1540 and Y.1541. This framework includes performance objectives for IP-based services.

There are relevant standards within in the ITU-R, especially for television e.g ITU-R BT.500-11

5.6.2 IETF

A framework for IP performance metrics is the subject of RFC 2330.

Generic approaches for the support of QoS in IP networks are discussed in RFC 1633 (IntServ), RFC 2475 (DiffServ) and RFC 3031 (MPLS).

Additional RFCs contain more information on specific aspects of IntServ, DiffServ and MPLS or combinations of the approaches.

5.6.3 Other standardization bodies

ETSI TS 101 also describes a framework for QoS and network performance for IP networks that carry a variety of applications. The emphasis is on voice, including signalling and control issues.

3GPP TS22.105 describes service and service capabilities comparable to ITU-T G.1010. Finally, the VQEG (Video Quality Experts Group) deals with the validation of objective models of video quality assessment. The standards are then formed by the ITU, based on the work by the VQEG as ITU-T J.144.

Work related to perceived QoS is also carried out within DSLF WT-126 which deals with "Triple-Play QoE Requirements". MUSE contributes to WT-126 through taskforce TF1.7.

5.7 References

[QoS1] ITU-T E.800, "Terms and definitions related to quality of service and network performance including dependability", 1994

[QoS2] ETSI, ETR 003, Network aspects (NA); "General aspects of Quality of Service (QoS) and Network Performance (NP)", 1994

[QoS3] ITU-T Y.1541, "Network performance objectives for IP-based services", 2001

[QoS4] ETSI TR 101 329-1 V3.1.2 (2002-01), (TIPHON) Release 3; "End-to-end Quality of Service in TIPHON systems; Part 1: General aspects of Quality of Service (QoS)"

[QoS5] ITU-T G.1010, "End-user multimedia QoS categories", November 2001

[QoS6] Dimitrios Miras, "A survey on Network QoS Needs of Advanced Internet Applications", University College London, 2002, http://qos.internet2.edu/wg/apps/fellowship/Docs/Internet2AppsQoSNeeds.pdf

[QoS7] 3GPP TS22.105, "UMTS: Service and service capabilities," October 2001

[QoS8] B. Buxton, "Integrating the periphery and context: A new taxonomy of telematics", 1995 http://www.dgp.toronto.edu/people/rroom/research/papers/bg fg/bg fg.html

[QoS9] Ahumada, A. J., Jr. and Null, C., "Image Quality: A Multidimensional Problem", in Digital Images and Human Vision", A. WatsonEd., MIT Press, Cambridge MA (1993)

[QoS10] J. Anderson, "Methods for Measuring Perceptual Speech Quality", White Paper of Agilent technologies, Network Systems Test Division, (2000)

[QoS11] ITU-T G.114, General characteristics of international telephone connections and international telephone circuits, 1998

[QoS12] ITU-T G.131, Control of talker echo, August 1996

[QoS13] Winkler, S., "Vision models and quality metrics for image processing applications", Ecole Polytechnique Fédérale de Lausanne, PhD, Thesis no 2313, (2000)

[QoS14] Moving Pictures Expert Group, "MPEG 2", ISO/IEC 13818, (2000)

[QoS15] ITU-T, "Video Coding for Low Bit Rate Communication", International Telecommunication Union, Telecommunication standardization sector, ITU-T Rec. H.263, (1998)

[QoS16] R. Steinmetz, "Human perception of jitter and media synchronization", IEEE Journal on Selected Areas in Communications, 14(1):61–72, January 1996

[QoS17] Sears, J. A. Jacko and M. S. Borella, “Internet Delay Effects: How Users Perceive Quality,Organization, and Ease of Use of Information,” http://www.acm.org/sigchi/chi97/proceedings/short-talk/als2.htm (1997, August)

[QoS18] ITU-R BT.500-11, "Methodology for the Subjective Assessment of the Quality of Television Pictures", International Telecommunication Union - Radiocommunication Sector, (2002)

[QoS19] VQEG, "Final Report From the Video Quality Experts Group on the Validation of Objective Models of Video Quality Assessment, Phase II", Video Quality Experts Group (VQEG), VQEG FInal Report of FR-TV Phase II Validation Test, (2003)

[QoS20] ITU-T Rec. P.800, "Methods for Subjective Determination of Transmission Quality", International Telecommunication Union, Telecommunication standardization sector, (1996)

[QoS21] ITU-T Rec. P.830, "Subjective Performance Assessment of Telephone-Band and Wideband Digital Codecs", International Telecommunication Union, Telecommunication standardization sector, (1996)

[QoS22] ITU-T Rec. P.910, "Subjective Video Quality Assessment Methods for Multimedia Applications", International Telecommunication Union, Telecommunication standardization sector, (1999)

[QoS23] ITU-T Rec. P.862, "Perceptual Evalutation of Speech Quality (PESQ): An Objective Method for End-to-End Speech Quality Assessment of Narrow-Band Telephone Networks and Speech Codecs", International Telecommunication Union, Telecommunication standardization sector, ITU-T Rec. P.862, (2001)

[QoS24] S. Wolf and M. Pinson, “Spatial-temporal distortion metrics for in-service quality monitoring of any digital video system” *in* “Proceedings of SPIE International Symposium on Voice, Video and Data Communications”, pages 175–184, Boston, USA, September 1999

[QoS25] ITU-T Rec. J.144, "Objective Perceptual Video Quality Measurement Techniques for Digital Cable Television in the Presence of Full Reference ", International Telecommunication Union, Telecommunication standardization sector, (2004)

[QoS26] Stas Khirman and Peter Henriksen, “Relationship Between Quality-of-Service and Quality-of-Experience for Public Internet Service”, PAM Workshop 2002, Colorado USA

[QoS27] ITU-T G.107, “The E-model, a computational tool for use in transmission planning”, March 2003 (revised version)

[QoS28] O. Verscheure, P. Frossard, and M. Hamdi “MPEG-2 video services over packet networks: Joint effect of encoding rate and data loss on user-oriented QoS”, *in* “Proceedings of NOSSDAV 98”, pages 257–264, Cambridge, July 1998

[QoS29] ITU-T G.113, “Transmission impairments due to speech processing”, February 2002

[QoS30] C. Perkins, O. Hodson, V. Hardman, “A Survey of Packet Loss Recovery techniques for Streaming Audio”, IEEE Network, September-October 1998, 40-48

[QoS31] W. Richard Stevens, “TCP/IP Illustrated, Volume 1: The Protocols”, Addison-Wesley 1994

[QoS32] ITU-T Y.1540, “Internet Protocol Data Communication Service: IP Packet Transfer and availability performance parameters”, 2001

[QoS33] A.S. Tanenbaum, “Computer networks”, 4th ed., New Jersey, prentice Hall PTR, 2003

[QoS34] J.C. Bolot, “End-to-end packet delay and loss behavior in the Internet”, Deepinder P. Sidhu, editor, in, “SIGCOMM Symposium on Communications Architectures and Protocols”, pages 289–298, San Francisco, California, September 1993, ACM

[QoS35] M. Yajnik, S. Moon, J. Kurose, and D. Towsley, “Measurement and modelling of the temporal dependence in packet loss”, *in* “Proceedings of the Conference on Computer Communications (IEEE Infocom)”, New York, March 1999

[QoS36] RFC-2330, “Framework for IP Performance Metrics”, V. Paxson, G. Almes, J. Mahdavi, M. Mathis, Internet Engineering Task Force (IETF), May 1998

[QoS37] RFC-3393, “IP packet delay variation metric for IP Performance Metrics”, C. Demichelis, P. Chimento, Internet Engineering Task Force (IETF), November 1999

[QoS38] Comments on draft-ietf-ippm-ipdv.05, www.advanced.org/IPPM/archive.3/0074.html

[QoS39] FRF.13, “Service Level Definitions Implementation Agreement”, Frame Relay Forum

[QoS40] ITU-T Rec. I.371, “Traffic control and congestion control in B-ISDN”

[QoS41] J. M. Boyce and R. D. Gaglianello, “Packet loss effects on mpeg video sent over the public internet”, *in* “ACM Multimedia 98”, Bristol, UK, September 1998

[QoS42] Paul Coverdale, “Multimedia QoS requirements from a user perspective”. Presentation to ITU-T Workshop on “QoS and user-perceived transmission quality in evolving networks”, October 2001. http://www.itu.int/itudoc/itu-t/workshop/qos/s2p1.html

[QoS43] UKERNA, “Report of QoS Think Tank”, ND/STG/QOS/DOC/010, version 1.0 release, The JNT Association, July 2001 http://www.ja.net/development/qos/qos tt report.pdf

[QoS44] Chuck Fraleigh , Sue Moon, Bryan Lyles, Chase Cotton, Mujahid Khan, Deb Moll, Rob Rockell, Ted Seely, Christophe Diot, “Packet-Level Traffic Measurements”, from the “Sprint IP Backbone”, IEEE Network, November/December 2003, 6-16

[QoS45] Chuck Fraleigh and Fouad Tobagi Christophe Diot, “Provisioning IP Backbone Networks to Support Latency Sensitive Traffic”, IEEE Infocom, 2003

[QoS46] R. S. Prasad, M. Murray, C. Dovrolis, K. Claffy, “Bandwidth estimation: metrics, measurement techniques, and tools”, IEEE Network, November/December 2003, 27- 38

[QoS47] RFC-1349, “Type of Service in the Internet Protocol Suite”, P. Almquist, July 1992

[QoS48] RFC-1633, “Integrated Services in the Internet Architecture: an Overview”, R. Braden, D. Clark, S. Shenker, June 1994

[QoS49] RFC-2205 “Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification”, R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, September 1997

[QoS50] RFC-2210, “The Use of RSVP with IETF Integrated Services”, J. Wroclawski, September 1997

[QoS51] RFC-2474, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, K. Nichols, S. Blake, F. Baker, D. Black, December 1998

[QoS52] RFC-2475, “An Architecture for Differentiated Service”, S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, December 1998

[QoS53] RFC-3031, “Multiprotocol Label Switching Architecture”, E. Rosen, A. Viswanathan, R. Callon, January 2001

[QoS54] RFC-3032, “MPLS Label Stack Encoding”, E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta, January 2001

[QoS55] J.G. Beerends, ITU-T Study Group 12, Contribution 55, “A subjective/objective test protocol for determining the conversational quality of a voice link”, July 2003

[QoS56] ETSI TS 101 329-3v212: "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); End to End Quality of Service in TIPHON Systems; Part3: Signalling and control of end-to-end Quality of Service (QoS)"

[QoS57] M.R.H. Mandjes, J.C. van der Wal, R.E. Kooij and H. Bastiaansen, “End-to-end delay analysis for interactive services on a large-scale IP network”, *in* “Seventh IFIP workshop on performance modelling and evaluation of ATM/IP networks” 28th - 30th June, Antwerp Belgium, 1999

[QoS58] Service Provider Quality of Service, http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/spqsd_wp.pdf

[QoS59] ITU-T P.920, "Interactive Test Methods for Audio-Visual Communications", 2000

[QoS60] Ennis, J. and Cermak, G., "Videoconferencing Quality as a Function of Bandwidth, Latency and Packet Loss", ITU-T Study Group 9 Question 21/9, Contribution to the meeting, Jan. 15, 2004, (1-15-2004)

[QoS61] RFC-791, “Internet Protocol”, September 1981

[QoS62] RFC-2478, “The COPS (Common Open Policy Service) Protocol”, D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, January 2000

[QoS63] RFC 2597 “Assured Forwarding PHB Group”, J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, June 1999

[QoS64] RFC 3209 “RSVP-TE: Extensions to RSVP for LSP Tunnels”, D. Awduche, L. Berger, D. Gan, T. Li ,V. Srinivasan ,G. Swallow, December 2001

[QoS65] MUSE Deliverable MA2.3 - "Network Architecture: high-level description for i ndividual architectural issues", June 2004

[QoS66] MUSE Deliverable MA2.5 - "Network Architecture and functional specifications for the multi-service access and edge", September 2004

[QoS67] J.W. Roberts, "Internet Traffic, QoS and Pricing", to appear in Proceedings of IEEE, 2004

[QoS68] Ben Teitelbaum, Stanislav Shalunov, “Why Premium IP Service Has Not Deployed (and Probably Never Will)”, Internet2 QoS Working Group Informational Document, May 3, 2002

[QoS69] Johannes Färber, “Network Game Traffic Modelling”, *in* “NetGames 2002”, Braunschweig, Germany, April 16-17, 2002

[QoS70] C. Schaefer, T. Enderes, H. Ritter, M. Zitterbart, “Subjective Quality-Assessment for Multiplayer Real-Time Games”, *in* “NetGames 2002”, Braunschweig, Germany, April 16-17, 2002

[QoS71] M. Oliveira, T. Henderson, “What Online Gamers Really Think of the Internet?”, *in* “NetGames’03”, Redwood City California, May 22-23, 2003

[QoS72] N. Sheldon, E. Girard, S. Borg, M. Claypool, E. Agu, “The Effect of Latency on User Performance in Warcraft III”®, *in* “NetGames’03”, Redwood City California, May 22-23, 2003

[QoS73] T. Beigbeder, R. Coughlan, C. Lusher, J. Plunkett, E. Agu, “The Effect of Loss and Latency on User Performance in Unreal Tournament 2003”®, *in* “SIGCOMM’04 Workshops”, Aug. 30 + Sept. 3, Portland, Oregon, U.S.A., 2004

[QoS74] ITU-T Rec. P.810, “Modulated Noice Reference Unit (MNRU)”, February 1996

[QoS75] ITU-T Rec. P.562, “Analysis and interpretation of INMD voice-service measurements,” May 2000

[QoS76] T. Jehaes, D.de Vleeschauwer, T. Coppens, B. van Doorselaer, E. Deckers, W. Naudts, K. Spruyt, R. Smets, Acces Network Delay in Networked Games, NetGames’03, Redwood City California, May 22-23, 2003.

[QoS77] T. Henderson, S. Bhatti, “Networked Games – a QoS-sensitive application for QoS-insensitive users?”, *in* “ACM SIGCOMM 2003 Workshops”, Aug. 25 & 27, Karlsruhe, Germany, 2003

[QoS78] Harald Øverby, Tønnes Brekne, Hans Almåsbakk, “Online Gaming: An Overview”, *in* “Q2S Friday Colloquium”, May 2004

[QoS79] Eurescom Report P1347, “Online Console Gaming – A whole new game?”, June 2004

[QoS80] MUSE Deliverable DTF4.1, “Test objectives”, Edited by R.F.M van den Brink and F.N. Krommendijk, December 2004.

[QoS81] ITU-T Rec. G.1030, “Estimating end-to-end performance in IP networks for data applications”, prepublished recommendation, November 2005.

[QoS82] ITU-R Rec. BS.1387, “Method for Objective Measurements of Perceived Audio Quality,” International Telecommunication Union, Geneva, Switzerland, 1998.

[QoS83] J.G. Beerends, J. M. van Vugt, R.E. Kooij, “An objective/subjective test protocol for determining the end-to-end perceived quality of streaming video”, ITU-T SG12 contribution C19, August 2005.

[QoS84] ITU-R Rec. BT.1683, “Objective perceptual video quality measurement techniques for standard definition digital broadcast television in the presence of a full reference”, International Telecommunication Union, Radiocommunication Sector, 2004.

[QoS85] Pinson, M. and Wolf, S., “In-Service Video Quality Metric (IVQM) User's Manual”, (NTIA Handbook HB-05-xxx), Institute of Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO, USA, 2005.

[QoS86] Pinson, M., Wolf, S., Austin, P. G., and Allhands, A., “Video Quality Measurement PC User's manual”, Institute of Telecommunication Sciences (ITS), National Telecommunication and Information Administration (NTIA), Boulder, CO, USA, 2002.

[QoS87] J. G. Beerends and F. E. de Caluwe, “The influence of Video Quality on Perceived Audio Quality and Vice Versa”. Journal of Audio Engineering Society, vol. 47, No, 5, May 1999, pp 355-362

[QoS88] D. S. Hands, “A basic Multimedia quality model”. IEEE Transactions on multimedia, Vol. 6, No. 6, December 2004, pp. 806-816

[QoS89] S. Rihs, “The Influence of Audio on Perceived Picture Quality and Subjective Audio-video Delay Tolerance”, in RACE MOSAIC deliverable no: R2111 80CESR007.B1, Chapter 13, June 1995.

[QoS90] ITU-R Rec. BT.1359-1: Relative timing of sound and vision for broadcasting

[QoS91] Hendrik Knoche, Hermann de Meer, David Kirsh, “Compensating for Low Frame Rates”, to appear in Proceedings of CHI 2005, 4-7 April 2005, Portland, Oregon.

[QoS92] Iperf Version 2.0.2, http://dast.nlanr.net/projects/Iperf/

[QoS93] J. Padhye, V. Firoiu, D. Towsley, J. Kurose, Modeling TCP throughput: A Simple Model and its Empirical Validation, IEEE/ACM Transactions on Networking, 8(2): 133-145 (April), 2000

[QoS94] V. Paxson, M. Allman, Computing TCP's Retransmission Timer, Internet Archives RFC 2988, November 2000

[QoS95] A.F. Wattimena, R.E. Kooij, J.M. van Vugt, O.K. Ahmed, "Predicting the perceived quality of a First Person Shooter: the Quake IV G-model", submitted for publication, August 2006.

[QoS96] MUSE TF1.7, Multimedia Enabled Access Solutions, October 2006.

6 SERVICE CONNECTIVITY TESTING

6.1 Introduction

This chapter 6 describes an E2E connectivity testing framework for MUSE. Since it is virtually impossible to describe all the elements that build up all the possible applications that run on a MUSE type of network it was chosen to have a two fold approach. In this approach one looks at the E2E connectivity from two perspectives: one from the service connectivity point of view and one from the network connectivity point of view.

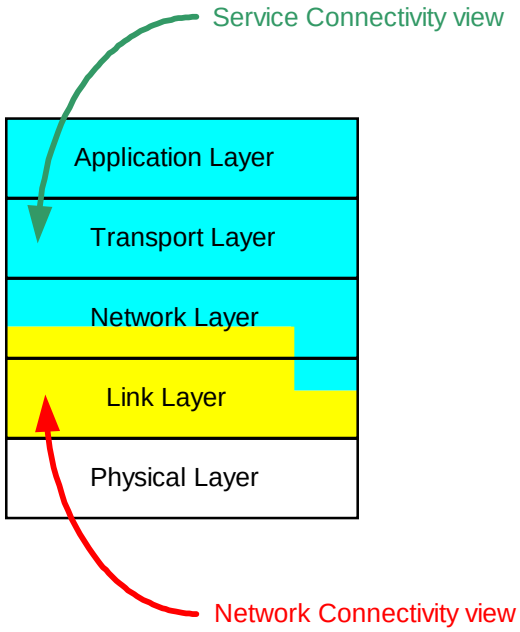


Figure 6-1: Split-view approach

- Service View

In the service connectivity point of view a top-down analysis of the E2E Connectivity capabilities that need to be verified is performed. This top-down analysis is typically done until the Network layer. Optionally this is extended to the link-layer if the service has special requirements. Since there exists a multitude of potential services to be deployed on a next-generation access network like MUSE it was chosen to limit the discussion to only a few applications/services that are characteristic for each of the service/traffic classes that have been identified in this document.

- Network View

In this a bottom-up approach is used where starting from the different proposed MUSE architectures a description is made of the functionality that needs to be offered and verified at the different layers upwards till the Network Layer is reached. In a sense this is the basis E2E connectivity that needs to be in place before one is able to offer the services that are described in the Services view. The physical layer is not looked at here, this because it is dealt with in the xDSL testing chapter of this document.

By having both views we are able to offer in this document a total view about E2E connectivity testing.

6.2 Test Objectives: Service VIEW

In the Service View we will use the Service classification and we will describe the testing objectives for one of the Services typical for the given classes.

- Elastic Applications (Best-Effort)

Within the class of the elastic applications one has the sub-classes interactive and non-interactive. In the context of E2E connectivity no distinction is made between interactive and non-interactive elastic applications (best-effort) because the interactivity constraints are such that they can easily be met with any high-speed access architecture. The limiting factor on the interactivity of a given application will be the way the application is designed and implemented rather than the network.

The most characteristic service for this type is in fact the ***High-speed Internet Access Service***. This service comprises numerous applications like HTTP, FTP, POP3, SMTP, etc.

- Non-interactive Inelastic Applications (Streaming)

For this class of services the ***Multicast Streaming Service*** was chosen. This is a service that delivers audio and video streams to multiple simultaneous receivers. This service is inelastic because it has strict requirements towards bandwidth and packet loss but the delay and jitter requirements are more relaxed.

- Interactive Inelastic Applications (Conversational)

For this type of applications the ***Voice over IP (VoIP) service*** was withheld, this because it represents one of the most challenging services to deploy on a network because of the strict bandwidth, loss, delay and jitter requirements.

The QoS testing chapter of this deliverable additionally discusses Video Conferencing and Interactive Gaming. But seen that video Conferencing is quite similar to VoIP from a network and protocols point of view it was decided to limit the discussion to testing objectives for the VoIP service. Similarly given that the network requirements for Interactive Gaming are quite similar to VoIP it was chosen to omit Interactive Gaming from the E2E connectivity testing chapter.

6.3 High-speed Internet Access Service

6.3.1 Description

The High-Speed Internet Access Service is the best-effort broadband Internet access as we currently know, with increased bandwidths through the use of advanced access technologies like the ones being developed in MUSE.

6.3.2 Limiting Presumptions

The High-speed Internet Access service supports numerous applications and protocols like (HTTP, FTP, POP3, SMTP, ..) but this document will not contain tests objectives for these specific applications but will be limited to the IP layer.

6.3.3 Application Layer protocols

The applications that are foreseen (HTTP, FTP, SMTP, POP3, SSH, ...) all have more or less the same requirements towards the network. Furthermore, since these applications are already widely used and understood by the whole network community, there is no immediate need to elaborate on these individual applications and associated application protocols.

6.3.4 Transport Protocols

The transport protocols employed by the applications in the High Speed Internet service are the typical IETF standards based TCP and UDP. One Quality aspect of the High Speed Internet Service — which is usually underestimated and overlooked — is ***the social behavior of individual applications*** in an environment, like the Internet. Applications that aggressively try to acquire as great a share of network resources as possible, in a network that does not impose any direct penalties for doing so, may seem to increase their own quality in comparison to applications that are more cautious (like those based on TCP transmission). While on a first look this does not seem to directly influence the quality or acceptability of an application, it may have undesirable implications for the health and well-being of the network and the HSI Service in general. Unresponsive and excessive use of resources by applications can lead to severe congestion conditions that will inevitably affect the irresponsible applications as well.

There is hence the requirement for an application to adapt to the state of the network. Since non adaptive applications can severely jeopardize the operational status of a network there is the requirement for network operators and designers to devise and deploy mechanisms in the network to help prevent such behavior (Traffic Shapers/Policers), the cooperation of the applications is also required.

6.3.5 Network Protocols

No special requirements here. General aspects are discussed in the Network connectivity View section of this document.

6.3.6 High-Speed Internet Tests

6.3.6.1 Application Layer

Since these application layer protocols are already widely used and understood by the whole network community, it is esteemed unnecessary to include in this document application layer specific tests.

6.3.6.2 Transport Layer

6.3.6.2.1 Conformance Tests

1. RFC 768 – "User Datagram Protocol", J. Postel, August 1980.
2. RFC 793 – "Transmission Control Protocol", DARPA, September 1981.
    - This is the mother of the TCP specification. Over the years there have been numerous updates/enhancements to this initial specification. The "A Roadmap for TCP Specification Documents" [Con97], gives a detailed overview of all TCP related RFCs that have been published up to June 2005.
3. **Traffic Shaping:** Verify that your network provides mechanisms to limit TCP unfriendly traffic. (i.e. Traffic shapers). See Network connectivity view.

6.3.6.2.2 Functional Tests

1. **Shaper test:** Ensure that unfriendly traffic is shaped. (See Network connectivity view)

6.3.6.2.3 Performance Tests

1. **Shaper performance:** Assess the performance of the traffic shaper/policer implementation under load. See Network connectivity view.

6.3.6.3 Network Layer

6.3.6.3.1 Conformance Tests

1. RFC 791 – "Internet Protocol", DARPA, September 1981. See also "Network connectivity view".

6.3.6.3.2 Functional Tests

1. **Auto-Configuration Test:** See Network connectivity view.
2. **Basic Connectivity Test:** See Network connectivity view.
3. **Advanced Connectivity Test:** See Network connectivity view.

6.3.6.3.3 Performance Tests

No specific tests. See also "Network connectivity View".

6.3.6.4 Link Layer

No specific tests. See also “Network connectivity View”.

6.4 Multicast Streaming Service

6.4.1 Description

In this part an analysis is made of the E2E connectivity requirements of a service that allows the end-user to watch broadcast style of programs. The individual streams of a given broadcast are delivered using the IP Multicast transmission technique. IP Multicast is a technology that allows the content provider (Broadcaster) to send out the stream only once and the network delivers the multi-media stream to the end-users who want to watch at that moment.

6.4.2 Limiting presumptions

The discussion is limited to three different deployment cases:

Case 1: The multimedia stream is injected into the access network at the edge or access node.
Case 2: The multimedia streams originate from within the Service Provider’s own network.
Case 3: The multimedia streams originate from somewhere on the Internet.

The different cases require different functionalities (multicast protocols) that need to be present in the network in order to be able to deliver the service end-to-end.

We further presume IETF standards/drafts based technologies and techniques. For video we presume that MPEG-4 AVC is used and MPEG-4 AAC for audio.

6.4.3 Application Layer Protocols

6.4.3.1 Real-time media streaming

6.4.3.1.1 RTP/RTCP

The Real-Time Transport Protocol (RTP) provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers.

All the technical details about RTP and RTCP can be found in RFC 3550 [Con12].

6.4.3.1.2 RTP Payload Format for MPEG-4 Audio/Visual Streams

[Con44] describes Real-Time Transport Protocol (RTP) payload formats for carrying each of MPEG-4 Audio and MPEG-4 Visual bitstreams without using MPEG-4 Systems. For the purpose of directly mapping MPEG-4 Audio/Visual bitstreams onto RTP packets, it provides specifications for the use of RTP header fields and also specifies fragmentation rules. It is beneficial to define the fragmentation rules of RTP packets for MPEG-4 Video streams so as to enhance error resiliency by utilizing the error resilience tools provided inside the MPEG-4 Video stream.

6.4.4 Transport Layer Protocols

6.4.4.1 NAT and Firewalls

The deployment of Network Translators (NATS) and firewalls can cause problems when one wants to deploy an end-to-end service based on IP Multicast.

In the case of NATs this is mainly because they typically do not process IGMP messages as to know what channels are requested by the internal clients so that when the IP multicast datagrams arrive they are not able to forward them. Equally Firewalls are typically configured in such a way that traversal of UDP packets is limited to only a few well-known UDP ports.

In some cases NAT and Firewall implementations are so restrictive that one has to fall back to a tunneling solution. Especially solutions that require no prior CPE configuration are the most interesting for wide deployment. Within the IETF there are currently two proposals namely "IPv4 Automatic Multicast without Explicit tunnels (AMT)" [Con91] and "CastGate: an auto-tunnelling architecture for IP Multicast." [Con92].

6.4.5 Network Layer Protocols

6.4.5.1 IPv4 and IPv6 Multicast

IP Multicast is a scalable mechanism to simultaneously deliver content to a large set of receivers. IP Multicast in IPv4 is an incremental feature in IPv6 on the other hand it is an integral part of the IPv6 specification. But although an integral part of IPv6 it uses the same protocols as in the IPv4 case to allow inter- and intra-domain delivery of IP Multicast datagrams.

6.4.5.2 IGMP/MLDv2

The Internet Group Management Protocol (IGMP) is used by hosts to inform the access router of their group membership information. Hosts inform routers by multicasting IGMP Host Membership Reports. The multicast enabled router listens for these reports, and uses this information to build up a distribution tree among the different multicast routers between the source and the receiver.

There exist three interoperable versions of IGMP:

IGMPv1 which is specified in RFC1112 [Con06] offers the following functionality:

- Hosts inform router of group membership
- Router queries at regular intervals for the membership status of the hosts

IGMPv2 (RFC2236) [Con17] adds the possibility for a host to explicitly indicate that it is no longer interested in a given group. IGMPv1 simply used a time-out mechanism for this.

IGMPv3 (RFC3376) [Con56] adds the possibility for a host to indicate in his group membership report also the sources from which he wants or doesn't want to receive multicast datagrams. Support of IGMPv3 is essential for the Single Source Multicast (SSM) delivery model (cfr. Later.)

In the presence of hosts with different IGMP versions all hosts and the router will fall back to the lowest IGMP version present on the network.

IPv6 Hosts and routers use the Multicast Listener Discovery protocol (MLD) detailed in RFC2710 [Con31]. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. One important difference to note is that MLD uses ICMPv6 (IP Protocol 58) message types, rather than IGMP (IP Protocol 2) message types.

MLDv2 (RFC3810) [Con71] is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses similar to IGMPv3.

6.4.5.3 Intra-domain Multicast Routing

IGMP and MLD are used by receivers to join existing multicast groups. The local router uses this process to determine where it should deliver multicast data. When a router acts in this manner, it is called the Last Hop Router (LHR) since it is located by the receivers and is at the end of the communications path. Conversely, the First Hop Router (FHR) is the nearest router to the source of the multicast traffic. An intelligent control plane mechanism is required so that the data can be efficiently delivered from the first hop router to all of the participating last hop routers. In short, a routing protocol is needed.

There are several different multicast routing protocols, and each one has its own unique technological solution. The Distance Vector Multicast Routing Protocol (DVMRP) [Con05] is the earliest protocol for multicast routing. A key concept introduced by DVMRP is the use of separate forwarding trees for each multicast group; this fundamental principle continues to be used in the newer multicast routing protocols. DVMRP, as the name implies, is analogous to RIP. It is a distance-vector protocol that provides very limited flexibility, functionality, and scalability. Nonetheless, the early Internet multicast experiments (known as the MBone) were based on DVMRP. DVMRP has largely been superseded by Protocol Independent Multicast.

6.4.5.3.1 Protocol Independent Multicast (PIM)

A new breed of multicast routing protocols was developed in the late 1990s. This family of protocols is collectively known as Protocol Independent Multicast (PIM). The name PIM is derived from the fact that these multicast forwarding protocols are not dependent upon any specific routing protocol. Instead, PIM will take advantage of the existing unicast routing tables, regardless of how they were constructed, in order to forward multicast data.

There are two different versions of PIM.

- **Protocol Independent Multicast – Dense Mode (PIM-DM):** As the name implies, this particular rendering of PIM is optimized for densely populated communities of users (optimally each Last Hop Router has at least one receiver for a given stream). PIM-DM is described in [Con81]. The philosophy of PIM-DM is to "push" multicast data toward the users. A router which deploys this protocol simply floods multicast traffic streams to all interfaces (this is similar to broadcast mechanisms). If the downstream routers are not attached to any users that require this particular multicast stream, they will send a "stop" message to the upstream router. This message is called a "prune" message since the upstream router will then prune its forwarding tree to eliminate that particular branch. PIM-DM routers forward all multicast traffic until a downstream router objects. Similar to DVMRP, PIM-DM constructs separate delivery trees for each multicast group. These trees are built with the source serving as the root of the trees, and the receivers are the leaves. The branches consist of all of the intermediate routers. Initially, reverse path trees are constructed, which simply means that the data is routed away from the source. (This is called "reverse" path because it directly contrasts traditional unicast forwarding mechanisms which route data towards the recipient.) Since the participating routers already have unicast forwarding tables, they use this information to determine which interface would be the correct interface for forwarding information to the source. The router will only forward data from that source if the information has been received on that one particular interface; this prevents loops, and results in a significant reduction in overhead. PIM-DM is typically only used in special deployments (i.e. Stock Exchanges) where the same multicast streams have to be delivered to all parts of the network almost all the time, never in, e.g., ISPs' networks.

- **Protocol Independent Multicast – Sparse Mode (PIM-SM):** The most commonly implemented form of Protocol Independent Multicast is PIM Sparse Mode (PIM-SM) [Con22]. This is a direct contrast to PIM-DM since it uses a "pull" instead of a "push" technique. This means that PIM-SM routers must specifically request a particular multicast stream before the data is forwarded to them. PIM-SM is well suited for the Internet since it reduces the overhead and bandwidth requirements for multicast data streams. PIM-SM is a protocol which exists exclusively between routers. Hosts (sources or receivers) do not participate in the protocol. PIM-SM shares many of the common characteristics of a routing protocol, such as discovery messages, topology information, and error detection and notification. PIM-SM also differs from traditional protocols since it does not participate in any kind of exchange of databases. PIM-SM routers periodically generate "Hello" messages to discover and maintain stateful sessions with neighbors. These messages are multicasted using a dedicated multicast address. After neighbors are discovered, PIM-SM routers can signal their intentions to join specific multicast groups. This is accomplished by having a downstream router send an explicit PIM-SM "join" message (not to be confused with IGMP or MLD "join" messages) to the upstream router. The "join" message will specify the group and the source (if applicable) that the router wants to join – this can be represented with a (*,G1) or (S1,G1) notation. The upstream routers can then forward multicast information to the downstream routers. PIM-SM, like most other multicast routing protocols, implements forwarding trees for each multicast group. These trees are called Rendezvous Point Trees (RPT) since they rely on a central router called a rendezvous point.

When talking about PIM-SM one has to make the distinction between two different IP Multicast models:

- **Any Source Multicast (ASM):** The traditional IP Multicast model described in RFC1112 allows having multiple senders onto the same channel. This has as major drawback that anyone is capable of injecting content onto an existing multicast channel. This is very useful in the context of multi-party videoconferencing but in the context of multimedia streaming it represents a serious hazard. This is one of the reasons that wide scale adoption of IP multicast for delivery of streaming media hasn't happened yet.

- **Single Source Multicast (SSM):** In response to the above mentioned problem and in response to issues at the level of inter domain multicast, some people came up with a new distribution model entitled Single Source Multicast (some times also called Source Specific Multicast). As the name implies it allows only one sender onto the distribution tree. For this operation mode to work on top of PIM-SM there is the requirement for some sort of out-of-band mechanism to let the Last Hop Router know the source address of the stream. The receiver signals this information to the Last Hop router via IGMPv3. This Last Hop Router will send PIM JOIN messages directly towards the indicated source rather that towards the rendezvous point as would be done in the case of ASM. The result is a Shortest Path Tree rooted at the source.

6.4.5.4 Inter-domain Multicast

Service providers do not want to rely on a competitor's Rendezvous Point (RP) in the case of PIM-SM for transmitting multicast traffic, but they must be able to get information from the multicast source to the receivers, regardless of where the source's RP is located. They also may need to place RPs someplace other than at a common interconnection point. The Multicast Source Discovery Protocol (MSDP) was developed to solve these problems, at least in the short term.

- **Multicast Source Discovery Protocol (MSDP):** Multicast Source Discovery Protocol (MSDP) [Con22] is a mechanism to connect multiple PIM-SM domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path. The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain's RP. MSDP depends heavily on M-BGP for inter-domain operation.

- **Multi-protocol extensions to BGP (M-BGP):** One AS's multicast network need not be congruent with that of the unicast network. These differences may be because of topology and/or policy constraints. Some of the routers in the network may not be multicast-enabled, for example, or there may be portions of the network that, because of policy decisions, reject multicast traffic. Therefore, in order to construct distribution trees, an exterior multicast routing protocol must not only know the path back to the

source, it must also be able to determine which parts of the infrastructure are available for multicasting. With the Multi-protocol extension to BGP [Con34] it is possible to populate a Multicast routing table in the different routers with reachability information for certain destination network ranges. This multicast routing table gets precedence over the unicast table when performing Reverse Path Checks.

6.4.5.5 Deployment scenarios

- Scenario 1: Access Node - Edge Node

In the case where the Audio and Video streams are injected in the Access network at the Access Node or at the Edge Node there is only a requirement to support IGMPvx and optionally some link-layer IGMP snooping mechanism (See Link Layer).

- Scenario 2: Intra-domain

In the case the content is sourced from within the ISP's own network (Same AS). Then it is sufficient to support IGMP and PIM-SM in the network. For this the ISP will need to install one or more Rendezvous Point (RP) routers.

- Scenario 3: Inter-domain

In the case the content can be sources from outside the ISP's own network (from some other AS) then there is the additional requirement to deploy MSDP between one or more RPs located in other ASs. Further if the unicast topology and multicast topologies are incongruent then one is forced to explicitly propagate multicast routes through MBGP.

6.4.5.6 Multicast QoS

No multicast specific technique will be used in MUSE. See Network connectivity view for details on the GSB QoS architecture.

6.4.6 Link-Layer Protocols

This section describes Link layer requirements and test objectives that are specific for this service. The general aspects are discussed in the " Network connectivity View" subsection.

6.4.6.1 IGMP Snooping

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

A layer-2 switch that supports IGMP snooping can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP Multicast Routers and IP Multicast hosts to learn the IP Multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures Ethernet multicast forwarding accordingly.

It should be noted given that one Ethernet Multicast MAC address corresponds to 32 consecutive IP Multicast addresses and that if the deployed Ethernet switches only

implement MAC Layer filtering they will not be able to filter out all IP Multicast traffic correctly. Hence MUSE advises operators to configure the streaming sources in such a way that this doesn't pose a problem. In the case Global IP multicast connectivity is provided through a GSB compliant MUSE access network it is advised to deploy Ethernet switches with MAC and IP Layer filtering.

IGMP snooping switches may implement "proxy-reporting" in which reports received from downstream hosts are summarized and used to build internal membership states. An IGMP proxy-reporting switch would then report its own state in response to upstream queriers. An IGMP proxy-reporting switch may act as Querier for the down stream hosts while proxy reporting to the 'real' upstream queriers.

Considerations for IGMP and MLD Snooping Switches are described in <draft-ietf-magma-snoop-11.txt>.

6.4.7 Multicast Streaming Tests

6.4.7.1 Application Layer

6.4.7.1.1 Conformance tests

1. **RTP/RTCP conformance:** Verify compliance with RFC 3550 [Con12] .

2. **A/V Profile Conformance:** It should be verified that the given RTP Audio Video profile is supported by the streaming servers and by the different playback devices one intends to use and that the implementation is standards compliant. (See Audio/Video Transport (avt) working group at http://www.ietf.org/html.charters/avt-charter.html)

3. **ISMA Conformance:** The Internet Streaming Media Alliance, Inc. (http://www.ISMA.tv) is a non-profit corporation formed to create specifications that define an interoperable implementation for streaming rich media -- video, audio and data -- over Internet Protocol (IP) networks.

   They define Internet Streaming Conformance Profiles

   Internet Streaming Conformance Profiles (ISCPs) provide the framework for the Conformance Program. There are five categories of ISCPs. The first category contains the program description and procedural documents. The remaining four categories define the functional areas of Internet Streaming Conformance, including test profiles and definitions of conformance for each product category.

   As such the following documents are esteemed relevant in the context of this document:

   ISCP-4201Streaming Client Document
   ISCP-3101File Streaming Server Document
   ISCP-3201Live Streaming Encoder Document

6.4.7.1.2 Functional Tests

1. **IP multicast reception:** Verify the reception of IP Multicast traffic originating from either the access network, ISP/ASP network or the Internet.
2. **Packet loss and out of order delivery test:** To verify the delivery of RTP in an end-to-end way one can inspect the packet loss and out-of-order packet delivery of an RTP stream.

6.4.7.1.3 Performance Tests

1. **IPv4 multicast benchmarking test:** Measure the delay, delay variation (jitter) and packet loss of an RTP stream under various conditions of load. See Network layer for the same test.

6.4.7.2 Transport Layer

6.4.7.2.1 Conformance Tests

1. **IP multicast through NAT/Firewall test:** When the architecture contains NATS verify that the NATS support the traversal of IP Multicast.

6.4.7.2.2 Functional Tests

1. **NAT/Firewall traversal test:** Do a functional test of the forwarding of IGMP and IP multicast datagrams through the NAT/Firewall.

6.4.7.2.3 Performance Tests

1. **NAT/Firewall Performance test:** Many SOHO NAT/Firewall devices do not have enough CPU power to process fragmented IP Packets. Measure the attainable throughput in case of fragmented IP multicast packets.

6.4.7.3 Network Layer

6.4.7.3.1 Conformance Tests

1. **IGMP:** It should be verified that the appropriate version of IGMP is available on all hosts and devices due to the fall-back mechanisms in IGMP. So for example if the multi-media stream is delivered using a Single Source Multicast stream then the requirement is that all hosts and devices within the CPN support the IGMPv3 protocol. If this is not the case all hosts will start to operate in the lowest IGMP version mode that is present on the network (broadcast domain) making the reception of the SSM stream impossible. cfr. RFC1112 [Con06], RFC 2236 [Con17], RFC 3376 [Con56].

2. **MLD:** In the case of IPv6 verify the standards compliance of the MLD implementation. See RFC 2710 [Con31] and RFC 3810 [Con71].

3. **PIM-SM:** When implementing intra-domain IP Multicast routing verify that the routers conform to PIM-SM Version 2. If your architecture requires SSM, verify that the border routers support SSM. See RFC 2362 [Con51].

4. **MSDP:** When implementing inter-domain ASM using PIM-SM verify the compliance and interoperability of the MSDP implementations. See RFC 3618 [Con65].

5. **M-BGP:** Verify compliance and interoperability of the multi-protocol BGP extension that allows the announcement of multicast specific routes. See RFC 2858 [Con34].

6.4.7.3.2 Functional Tests

1. **IP multicast reception**: See Application Layer functional test.
2. **IGMP version mix**: The presence of a CPN running in a lower version of IGMP should not affect the IGMP operation mode of other CPN connected to the same Service Provider. The same holds for the IPv6 case with MLD.

6.4.7.3.3 Performance Tests

1. **IPv4 multicast benchmarking test:** evaluate the performance of an IP multicast enabled device per RFC 3918, “Methodology for IP Multicast Benchmarking.” [Con72]. Measure multicast throughput, latency, delay of multicast group Joins or Leaves, and group capacity.
2. **Zapping time under load**: To evaluate the time taken for a CPE device to join/leave multicast streams while the access/edge node is fully loaded with incoming streams and subscribers.

6.4.7.4 Link Layer

6.4.7.4.1 Conformance Tests

1. **IGMP/MLD snooping:** Verify the presence of the correct IGMP/MLD snooping version(s) in all switches.
2. **IGMP/MLD conformance:** Verify the conformance of the IGMP/MLD snooping implementation. See draft-ietf-magma-snoop-*.txt.

6.4.7.4.2 Functional Tests

1. **IGMP/MLD snooping test:** Verify correct operation of the IGMP/MLDvx snooping functionality. Verify that IP Multicast traffic is only received on those ports for which there are hosts joining IP multicast groups. Assess that only IP Multicast traffic is received for joined IP Multicast groups. In the case VLANS are used, verify that IP Multicast is contained within the same VLAN and that Multicast is only forwarded to VLAN enabled ports with active receivers.

6.4.7.4.3 Performance Tests

1. **IGMP/VLAN scalability test:** Measure how large the Group/VLAN combination can grow: For each VLAN there is a separate IGMP/MLD snooping table. As the number of VLANs increase the number of snooping tables will increase. What is the upper limit?

6.5 Voice over IP Service

6.5.1 Description

Innovative communications technologies are developed because they offer some advantage over existing ones. One recent example is Voice Over Internet Protocol (VoIP) which is a term used for voice being transported via the internet Protocol regardless whether H.323, SIP or a proprietary standard is used. VoIP defines a way to carry voice calls over an IP network including the digitization and the packetisation of the voice streams. These VoIP services are typically delivered to customers through a MUSE Style broadband access network. The data network involved might be the Internet itself, or a corporate intranet, or managed networks used by local or long distance carriers and ISPs.

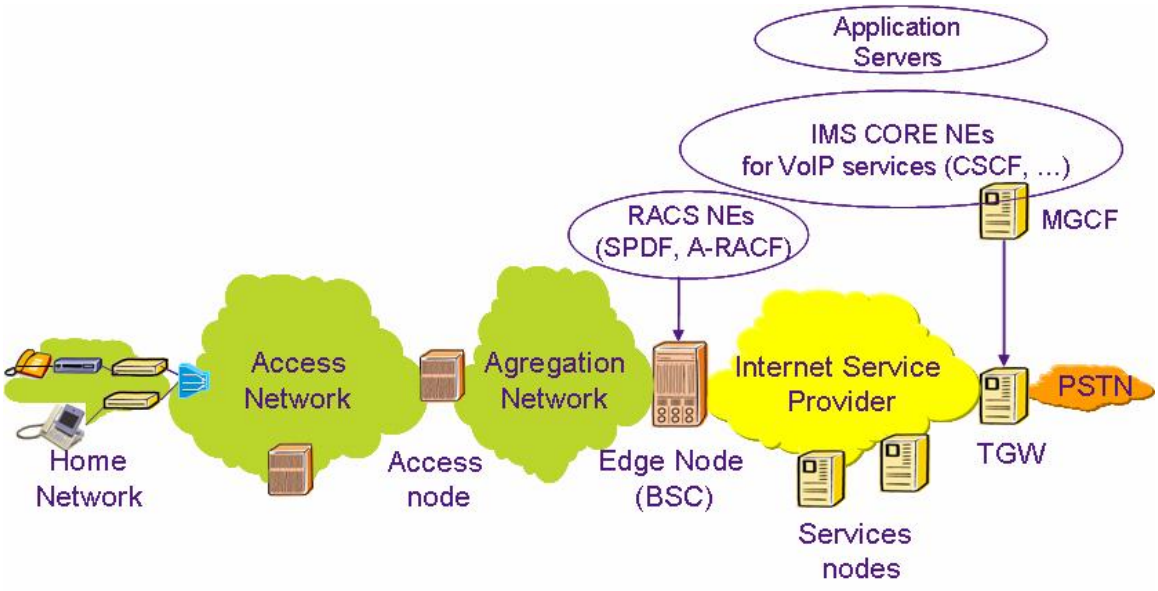


Figure 6-2: VoIP Architecture

In the MUSE context, the "edge node" functional entity (Figure 6-2) is a key component for the VoIP service roll-out. This entity indeed allows securing the traffic intended for the service platforms, to secure flows (NAPT function) intended for the customers of VoIP services. Moreover, it can interact with a control element to establish the session admission control within the framework of a tight QoS approach (booking/allocation of bandwidth by flow) and implements IP QoS mechanisms (flow marking, …).

However, along with the many advantages of VoIP technology, comes a new set of challenges (quality of service, security, NAT/Firewall traversal issues, interconnecting VoIP

protocols, interworking with other networks …). Voice traffic needs to be prioritized over data traffic to ensure real-time performance.

This chapter focuses on an IETF standards based VoIP architecture based around the Session Initiation Protocol (SIP).

6.5.2 Limiting Presumptions

A deployment of the VoIP service as depicted in Figure 6-2 is presumed.

6.5.3 Application Layer Protocols

6.5.3.1 Session Initiation Protocol (SIP)

Text based on reference [Con01].

SIP stands for Session Initiation Protocol. It is an application-layer control protocol that has been developed and designed within the IETF. The protocol has been designed with easy implementation, good scalability, and flexibility in mind. The specification is available in form of several RFCs. The most important one is RFC3261 [Con50], which contains the core protocol specification. The protocol is used for creating, modifying and terminating sessions with one or more participants. By sessions, we understand a set of senders and receivers that communicate and the state kept in those senders and receivers during the communication. Examples of a session can include Internet telephone calls, distribution of multimedia, multimedia conferences, distributed computer games, etc.

SIP is not the only protocol that the communicating devices will need. It is not meant to be a general purpose protocol. The purpose of SIP is just to make the communication possible. The communication itself must be achieved by other means (and possibly another protocol). Two protocols that are most often used along with SIP are RTP and SDP. The RTP protocol is used to carry the real-time multimedia data (including audio, video and text). The protocol makes it possible to encode and split the data into packets and transport these packets over the Internet. Another important protocol is SDP, Session Description Protocol, which is used to describe and encode capabilities of session participants. Such a description is then used to negotiate the characteristics of the session so that all of the devices can participate, including, for example, negotiation of codecs used to encode media so all the participants will be able to decode it, negotiation of transport protocol used and so on.

Although, in the simplest configuration, it is possible to use just two user agents that send SIP messages directly to each other, a typical SIP network will contain more than one type of SIP element.

Basic SIP elements are:

- **User agents**: Internet endpoints that use SIP to find each other and to negotiate a session's characteristics are called user agents. User agents usually, but not necessarily, reside on a user's computer in form of an application. This is currently the most widely-used approach, but user agents can be also cellular phones, PSTN gateways, PDAs, automated IVR systems and so on. User agents are often referred to as User Agent Server (UAS) and User Agent Client (UAC). UAS and UAC are logical entities and each user agent contains a UAC and UAS. UAC is the part of the

user agent that sends requests and receives responses. UAS is the part of the user agent that receives requests and sends responses. Because a user agent contains both UAC and UAS, user agents behave like a UAC or a UAS. For instance, a calling party's user agent behaves like UAC when it sends an INVITE request and receives responses to the request. A called party's user agent behaves like a UAS when it receives the INVITE and sends responses. But this situation changes when the called party decides to send a BYE and terminate the session. In this case the called party's user agent (sending BYE) behaves like UAC and the calling party's user agent behaves like UAS.

Figure 6-3 shows three user agents and one stateful forking proxy. Each user agent contains UAC and UAS. The part of the proxy that receives the INVITE from the calling party, in fact, acts as a UAS. When forwarding the request stateful, the proxy creates two UACs, each of them responsible for one branch.

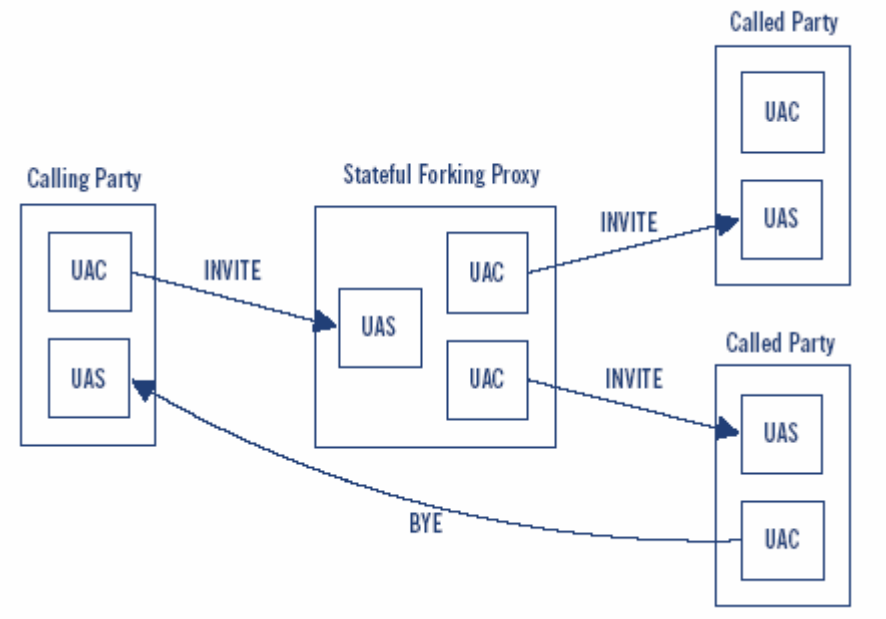


Figure 6-3: UAC and UAS

- **Proxy servers**: SIP allows the creation of an infrastructure of network hosts called proxy servers. User agents can send messages to a proxy server. Proxy servers are very important entities in the SIP infrastructure. They perform routing of a session invitations according to invitee's current location, authentication, accounting and many other important functions. The most important task of a proxy server is to route session invitations 'closer' to a called party. The session invitation will usually traverse a set of proxies until it finds one which knows the actual location of the called party. Such a proxy will forward the session invitation directly to the called party and the called party will then accept or decline the session invitation.
- **Registrar**: A Registrar is a service where the User Agent registers itself. The location of the User Agent is stored in a so called location database. The location database is then used by the user's proxy server to find the exact address to forward SIP calls to. For example, when a proxy receives an invitation for sip:bob@b.com it will search the location database. It finds sip:bob@1.2.3.4:5060 and will send the invitation there. A registrar is very often a logical entity only. Because of their tight coupling with proxies, registrars are usually co-located with proxy servers.

- **Redirect server**: The entity that receives a request and sends back a reply containing a list of the current location of a particular user is called redirect server. A redirect server receives requests and looks up the intended recipient of the request in the location database, created by a registrar. It then creates a list of current locations of the user and sends it to the request originator in a response within SIP 3xx redirection responses class. The originator of the request then extracts the list of destinations and sends another request directly to them.

More advanced SIP services are:

- **Call Admission Control (CAC)**: Responsible for the enforcement of network-wide admission policies.
- **Network Routing Engine (NRE):** Provides route information and translates a network address or logical address to an IP address.
- **Service Broker (SB):** Provides the CCE, upon request, the address of the appropriate as to treat the call.
- **User Profile Engine (UPE):** Contains user data, including registered devices, presence information and geographical location.
- **Call Control Element (CCE):** The Call Control Element (CCE) controls and manages the VoIP infrastructure and provides a single interface to application servers residing in the Applications Layer. Working with various BEs, the CCE creates and removes call legs and joins call legs to establish connectivity between end-points. The application servers residing in the Applications Layer provide the service logic capabilities to implement various types of services.
- **H.323 Gateway Border Element**: Implements gatekeeper-routed signaling for H.323 CPE gateways, from the access side. From the CCE, it acts as a SIP UA.
- **MEGACO/MGCP Gateway**: Implements Call Agent (or Media Gateway Controller) signaling for MEGACO/MGCP devices, from the access side. From the CCE, it functions as a SIP UA.
- **POTS Network Gateway Border Element:** Provides all required PSTN interface functions, including SS7 signaling and media conversion. The NG BE also operates as a gateway between circuit-switching and packet-switching networks. From the CCE, it acts as a SIP User Agent (UA).
- **CALEA Server**: Responsible for the interception of communications for law enforcement and other purposes.
- **E-911 Server:** Routes emergency calls to the appropriate Public Safety Answering Points, (PSAPs) based on the caller's location.
- **Media Server:** Handles and terminates media streams, providing functions such as announcement, DTMF, text-to-speech (TTS), automatic speech recognition (ASR), bridging and transcoding.

Note that the elements, as presented in this section, are often only logical entities. It is often profitable to co-locate them, for instance, to increase the speed of processing, but that depends on the particular implementation and configuration.

Note that the elements relative to the call control function, such as the Call Control Element defined above, are not handled in the context of MUSE and are considered as out of scope for this document.

6.5.3.2 RTP/RTCP

RTP and RTCP are the transport protocols used for IP Telephony media streams. Both of them were defined in RFC 3550 [Con12]: the former as a protocol to carry data that has real-time properties, the latter to monitor the quality of service and to convey information about the participants in ongoing session. The services provided by the RTP protocol are:

- identification of the carried information (audio and video codecs);
- checking packet in-order delivery and, if necessary, re-ordering the out-of-sequence blocks;
- transport of the coder/decoder synchronization information;
- Monitoring of the information delivery.

The RTP protocol uses the underlying User Datagram Protocol (UDP) to manage multiple connections between two entities and to check for data integrity (checksum). An important point to stress is that RTP neither provides any means to have a guaranteed QoS nor assumes the underlying network delivers ordered packets. The RTCP protocol uses the same protocols as RTP to periodically send control packets to all session participants. Every RTP channel using port number N has its own RTCP protocol channel with port number equal to N+1. The services provided by the RTCP are:

- giving a feedback on the data quality distribution, feedback used to keep control of the active codecs;
- transporting a constant identifier for the RTP source (CNAME), used by the video data;
- advertising the number of session participants which is used to adjust the RTP data transmission rate;
- Carrying session control information used to identify the session participants.

6.5.4 Network Layer

The VoIP service has no specific requirements towards the Network layer except for the stringent QoS requirements. The QoS mechanisms are implemented in a generic – service independent – way and will be dealt with in the Network connectivity view section of this document.

6.5.5 Voice over IP Tests

6.5.5.1 Application layer

6.5.5.1.1 Conformance Test

- **SIP conformance:** Verify the correct operation of the SIP implementations of the applications/devices (RFC3261 [Con50], RFC2327 [Con20], RFC2916 [Con39], RFC2976 [Con41], RFC3262 [Con51], RFC3263 [Con52], RFC3311 [Con53], …). Verify if the SIP messages are according to the SIP syntax.
- **SDP conformance:** Verify if the SDP bodies are according to the SDP syntax defined in RFC2327 [Con20].

- **Audio/Video Profile Conformance:** It should be verified that the given RTP Audio Video profile is supported by the SIP endpoints (SIP phones, Media Servers …) and that the implementation is standards compliant
- **RTP/RTCP conformance:** Verify the correct operation of the RTP/RTCP implementations of the applications/devices

6.5.5.1.2 Functional Test

- **SIP registration test:** Verify that a SIP endpoint can registered to the service node through the edge node
- **SIP functional test:** Verify that a SIP endpoint or a SIP UA can initiate, maintain and tear down a session when calling another UA SIP
- **SIP interworking test:** Verify that a SIP endpoint or a SIP UA can initiate, maintain and tear down a session when calling another client in a different access network
- **SIP supplementary services test:** Verify the correct operation of a SIP endpoint or SIP UA in terms of supplementary services implementation (Call forward, calling line identification, …) through the edge node
- **DTMF code transmission test:** Verify the correct transmission of DTMF code between two SIP endpoints or SIP UA through the edge node. The DTMF code can be transmitted according to two methods, the first one in-band and the second out-of-band (signalling). When DTMF signals are transmitted in band, the DTMF are encoded, packetized, reassembled and decoded in the same way as the voice flow
- **RTP delivery test:** To verify the delivery of RTP in an end-to-end way one can inspect the packet loss and out-of-order packet delivery of an RTP stream.

6.5.5.1.3 Performance Test

- **Torture test:** Assess the robustness and the security level of a SIP implementation. See the following internet draft "draft-ietf-sipping-torture-tests-04" which gives examples of Session Initiation Protocol (SIP) test messages designed to exercise and "torture" SIP implementations.
- **Delivery Characteristics test:** Measure the delay, jitter (delay variation) and packet loss of a RTP stream under various conditions of traffic load. See also Network connectivity view.
- **Session Setup performance test:** Measure the number of VoIP sessions per second at the edge node level under various conditions of traffic load
- **Session Setup scalability test:** Measure the number of simultaneous VoIP sessions at the edge node level under various conditions of traffic load
- **Call Setup Time test:** Measure the setup time to establish a session between 2 endpoints or SIP UA under various conditions of traffic load
- **Registration Performance test:** Measure the number of registration per second and the number of simultaneous registrations at the service node level under various conditions of traffic load
- **Service availability test:** check the failover behavior of the VoIP implementation when a network element goes down.

6.5.5.2 Transport Layer

6.5.5.2.1 Conformance Test

- **SIP conformance:** Verify the correct operation of the SIP implementations relative to the transport layer protocols (UDP, TCP)
- **SIP signaling test:** Verify that the SIP signaling flows use the 5060 port number.

6.5.5.2.2 Functional Test

- No specific tests. See also “Network View” for more information.

6.5.5.2.3 Performance Test

- No specific tests. See also “Network View” for more information.

6.5.5.3 Network Layer

6.5.5.3.1 Conformance Test

- **Packet Loss conformance:** Verify the packet loss in the transfer plane in an end-to-end configuration. As general rule, the packet loss rate should be less than 5% and preferably less than 1%.
- **SIP message fragmentation test:** Verify that SIP messages transported over more than one IP packet is well supported (i.e. SIP messages bigger than the MTU)
- **IP version tests:** check if the network supports both IPv4 and IPv6 traffic. See also " Network connectivity View" section for more information.

6.5.5.3.2 Functional Test

- **VoIP flows through NAT/PAT - Firewall test:** When the architecture contains NAT/PAT features, verify that the NAT/PAT supports the traversal of VoIP flows (Home Network and edge node level)
- **Flows prioritization test:** To check if the edge node or access network/home network can prioritize voice flows with regard to the data flows.
- **Flows marking test:** check if the access/edge node or Home Network can mark voice flows differently from the data flows.

6.5.5.3.3 Performance Test

- **Delivery performance test:** Measure the number of VoIP sessions established per second and the number of simultaneous sessions established at the edge node level
- **NAT/Firewall Performance test:** Many Soho NAT/Firewall devices do not have enough CPU power to process fragmented IP Packets. Measure the attainable throughput in case of fragmented IP multicast packets.

6.6 Inventory of standards

With respect to E2E connectivity testing the two most important standardization bodies are the ITU-T and the IETF. Traditionally the ITU-T represents the old Telecom world of telephony and packet switched. The IETF, the Internet Engineering Task Force, find its origin in the best effort IP networking world. Of course, nowadays the activities of both bodies converge to the situation where multiple services can be employed over the Next Generation Network.

6.6.1 ITU-T

The ITU-T gives an overview of terms and definitions related to QoS and network performance in E.800.

A framework for IP network performance parameters is discussed in Y.1540 and Y.1541. This framework includes performance objectives for IP-based services.

6.6.2 IETF

Since all applications that are described here are IETF standards or Internet drafts based it is clear that the IETF is the authorative source for standards documents. See reference list for an overview of relevant IETF documents.

6.6.3 Other standardization bodies

6.6.3.1 SIPForum

The SIP Forum's mission is to advance the adoption of products and services based on the Session Initiation Protocol - SIP. The Forum provides information on the benefits and capabilities of SIP, highlights successful applications and deployments, and directs activities aimed at achieving high levels of product interoperability.

6.6.3.2 Internet Streaming Media Alliance

The Internet Streaming Media Alliance, Inc. (http://www.ISMA.tv) is a non-profit corporation formed to create specifications that define an interoperable implementation for streaming rich media -- video, audio and data -- over Internet Protocol (IP) networks.

6.6.3.3 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. It is a co-operation between ETSI (Europe), ARIB/TTC (Japan), CCSA (China), ATIS (North America) and TTA (South Korea).

The scope of 3GPP is to make a globally applicable third generation (3G) mobile phone system specification within the scope of the ITU's IMT-2000 project. 3GPP specifications are based on evolved GSM specifications. 3GPP standardisation encompasses Radio, Core Network and Service architecture.

The standards that are currently worked upon are focusing on decreasing latency, QoS and improvements to real-time applications like VoIP. This specification will also focus on HSPA+ (High Speed Packet Access Evolution), SIM high-speed protocol and contactless front-end interface (Near Field Communication enabling operators to deliver contactless services like Mobile Payments), EDGE Evolution.

6.6.3.4 References

[Con01] "IP Telephony Cookbook (TERENA Report)", ISBN 90-7759-08-6, March 2004.
[Con02] RFC 768, “User Datagram Protocol”, J. Postel, August 1980.
[Con03] RFC 791, “Internet Protocol”, DARPA, September 1981.
[Con04] RFC 793, “Transmission Control Protocol”, DARPA, September 1981.
[Con05] RFC1075, "Distance Vector Multicast Routing Protocol", Waitzman, November 1988.
[Con06] RFC 1112, "Host extensions for IP multicasting", S. Deering, August 1989.
[Con07] RFC 1242, “Benchmarking Terminology for Network Interconnection Devices”, S. Bradner, July 1991.
[Con08] RFC 1242, “Benchmarking Terminology for Network Interconnection Devices”, S. Bradner, July 1991.
[Con09] RFC 1332, “The PPP Internet Protocol Control Protocol (IPCP)”, G. McGregor, May 1992.
[Con10] RFC 1334, “PPP Authentication Protocols”, B. Lloyd et al., October 1992.
[Con11] RFC 1661, “The Point-to-Point Protocol (PPP)”, W. Simpson, July 1994.
[Con12] RFC 3550, "RTP: A Transport Protocol for Real-Time Applications", Schulzrinne H. et al., IETF, July 2003.
[Con13] RFC 1962, “The PPP Compression Control Protocol (CCP)”, D. Rand, June 1996.
[Con14] RFC 1968, “The PPP Encryption Control Protocol (ECP)”, G. Meyer, June 1996.
[Con15] RFC 1994, “PPP Challenge Handshake Authentication Protocol (CHAP)”, W. Simpson, August 1996.
[Con16] RFC 2131, “Dynamic Host Configuration Protocol”, R. Droms, March 1997.
[Con17] RFC2236, "Internet Group Management Protocol, Version 2", W. Fenner, IETF, November 1997.
[Con18] RFC2283, "Multiprotocol Extensions for BGP-4", T. Bates, R. Chandra, D. Katz, Y. Rekhter, IETF, February 1998.
[Con19] RFC 2285, “Benchmarking Terminology for LAN Switching Devices”, R. Mandeville, February 1998.
[Con20] RFC 2327, “SDP: Session Description Protocol”, M. Handley et al., April 1998.
[Con21] RFC 2330, “Framework for IP Performance Metrics”, V. Paxson, May 1998.
[Con22] RFC 2362, “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification”, D. Estrin et al., June 1998.
[Con23] RFC2432, "Terminology for IP Multicast Benchmarking", K. Dubray, October 1998.
[Con24] RFC 2516, “A Method for Transmitting PPP Over Ethernet (PPPoE)”, L. Mamakos et al., February 1999.
[Con25] RFC 2544, “Benchmarking Methodology for Network Interconnect Devices”, S. Bradner et al., March 1999.
[Con26] RFC 2563, “DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients“,R. Troll, May 1999.
[Con27] RFC 2678, “IPPM Metrics for Measuring Connectivity”, J. Mahdavi et al., September 1999.
[Con28] RFC 2679, “A One-way Delay Metric for IPPM”, G. Almes, September 1999.
[Con29] RFC 2680, “A One-way Packet Loss Metric for IPPM”, G. Almes, September 1999.
[Con30] RFC 2681, “A Round-trip Delay Metric for IPPM”, G. Almes, September 1999.

[Con31] RFC 2710, "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman, IETF, October 1999.
[Con32] RFC 2715, "Interoperability Rules for Multicast Routing Protocols", D. Thaler, IETF, October 1999.
[Con33] RFC 2716, “PPP EAP TLS Authentication Protocol”, B. Aboba et al., October 1999.
[Con34] RFC 2858, “Multiprotocol Extensions for BGP-4”, T. Bates et al., June 2000.
[Con35] RFC 2865, “Remote Authentication Dial In User Service (RADIUS)”, C. Rigney, June 2000.
[Con36] RFC 2866, “RADIUS Accounting”, C. Rigney, June 2000.
[Con37] RFC 2868, “RADIUS Attributes for Tunnel Protocol Support”, G. Zorn et al., June 2000.
[Con38] RFC 2869, “RADIUS Extensions”, C. Rigney et al., June 2000.
[Con39] RFC 2916, “E.164 number and DNS”, P. Faltstrom, September 2000.
[Con40] RFC 2937, “The Name Service Search Option for DHCP”, C. Smith, September 2000.
[Con41] RFC 2976, “The SIP INFO Method”, S. Donovan, October 2000.
[Con42] RFC 3004, “The User Class Option for DHCP”, G. Stump, November 2000.
[Con43] RFC 3011, “The IPv4 Subnet Selection Option for DHCP”, G. Waters, November 2000.
[Con44] RFC 3016, "RTP Payload Format for MPEG-4 Audio/Visual Streams", Y. Kikuchi et al. , November 2000.
[Con45] RFC 3046, “DHCP Relay Agent Information Option”, M. Patrick, January 2001.
[Con46] RFC 3074, “DHC Load Balancing Algorithm”, B. Volz et al., February 2001.
[Con47] RFC 3118, “Authentication for DHCP Messages”, R. Droms et al., June 2001.
[Con48] RFC 3148, “A Framework for Defining Empirical Bulk Transfer Capacity Metrics”, M. Mathis et al., July 2001.
[Con49] RFC 3203, “DHCP reconfigure extension”, Y. T'Joens et al., December 2001.
[Con50] RFC 3261, “SIP: Session Initiation Protocol”, J. Rosenberg et al., June 2002.
[Con51] RFC 3262, “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, J. Rosenberg et al., June 2002.
[Con52] RFC 3263, “Session Initiation Protocol (SIP): Locating SIP Servers”, J. Rosenberg et al., June 2002.
[Con53] RFC 3311, “The Session Initiation Protocol (SIP) UPDATE Method”, J. Rosenberg, September 2002.
[Con54] RFC 3315, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, R. Droms et al., July 2003.
[Con55] RFC 3357, “One-way Loss Pattern Sample Metrics”, R. Koodli et al., August 2002.
[Con56] RFC 3376, "Internet Group Management Protocol, Version 3", B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, IETF, September 2002.
[Con57] RFC 3393, “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, C. Demichelis et al., November 2002.
[Con58] RFC 3396, “Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)”, T. Lemon et al., November 2002.
[Con59] RFC 3432, “Network performance measurement with periodic streams”, V. Raisanen et al., November 2002.
[Con60] RFC 3442, The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4”, T. Lemon et al., December 2002.
[Con61] RFC 3446, "Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP).", D. Kim, D. Meyer, H. Kilmer, D. Farinacci, IETF, January 2003.

[Con62] RFC 3527, “Link Selection sub-option for the Relay Agent Information Option for DHCPv4”, K. Kinnear et al., April 2003.
[Con63] RFC 3588, “Diameter Base Protocol”, P. Calhoun et al., September 2003.
[Con64] RFC 3589, “Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5”, J. Loughney, September 2003.
[Con65] RFC3618, "Multicast Source Discovery Protocol (MSDP)", IETF, September 2004.
[Con66] RFC 3633, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6”, O. Troan et al., December 2003.
[Con67] RFC 3646, “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, R. Droms et al., December 2003.
[Con68] RFC 3736, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”, R. Droms, April 2004.
[Con69] RFC 3748, “Extensible Authentication Protocol (EAP)”, B. Aboba et al., June 2004.
[Con70] RFC 3763, “One-way Active Measurement Protocol (OWAMP) Requirements”, S. Shalunov et al., April 2004.
[Con71] RFC 3810, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", R. Vida, L. Costa, IETF, June 2004.
[Con72] RFC 3918 ,"Methodology for IP Multicast Benchmarking", D. Stopp et al., October 2004.
[Con73] RFC 3925, “Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)”, J. Littlefield, October 2004.
[Con74] RFC 3942, “Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options”, B. Volz, November 2004.
[Con75] RFC 3993, “Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option”, R. Johnson et al., March 2005.
[Con76] RFC 4014, “Remote Authentication Dial-In User Service (RADIUS): Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option”, R. Droms et al., February 2005.
[Con77] RFC 4030, “The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option”, M. Stapp et al., March 2005.
[Con78] RFC 4039, “Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)”, S. Park et al., March 2005.
[Con79] RFC 4148, “IP Performance Metrics (IPPM) Metrics Registry”, E. Stephan, August 2005.
[Con80] ISO/IEC JTC1/SC29/WG11N3233 , "Report on Transmission of MPEG-4 Audio over RTP", IETF, March 2000.
[Con81] draft-ietf-pim-dm-new-v2-*.txt, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", A. Adams, J. Nicholas, W. Siadack, IETF, June 2004.
[Con82] draft-ietf-pim-sm-v2-new-*.txt, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, IETF, October 2004.
[Con83] ISCP-4201, "Internet Streaming Conformance Profile: Streaming Client Document", ISMA, September 2004.
[Con84] ISCP-3101, "Internet Streaming Conformance Profile: File Streaming Server Document", ISMA, September 2004.
[Con85] ISCP-3201, "Internet Streaming Conformance Profile: Live Steaming Encoder Document", ISMA, September 2004.
[Con86] draft-ietf-sipping-torture-tests-*.txt, "Session Initiation Protocol Torture Test Messages."

[Con87] draft-ietf-sipping-pstn-call-flows-*.txt, "Session Initiation Protocol PSTN Call Flows", A. Johnston, S. Donovan, IETF, April 2003.
[Con88] draft-ietf-sipping-basic-call-flows-*.txt, "Session Initiation Protocol Basic Call Flow Examples", A. Johnston, IETF, April 2003.
[Con89] draft-ietf-sipping-service-examples-*.txt, "Session Initiation Protocol Service Examples", A. Johnston, S. Donovan, IETF, March 2003.
[Con90] ITU-T Recommendation E.800, Quality of service and dependability vocabulary, August 1994.
[Con91] draft-ietf-mboned-auto-multicast-*.txt, "IPv4 Automatic Multicast Without Explicit Tunnels (AMT)", D. Thaler et al., October 2004.
[Con92] draft-liefooghe-castgate-*.txt, "CastGate: an auto-tunneling architecture for IP Multicast", P. Liefooghe, October 2004.
[Con93] 3GPP TS 23.228 V6.6.0 (2004-06), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)
[Con94] 3GPP TS 23.060 V6.5.0 (2004-06), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 6)
[Con95] 3GPP TS 29.207 V6.1.0 (2004-09), 3rd Generation Partnership Project; Technical Specification Group Core Network; Policy control over Go interface (Release 6)
[Con96] 3GPP TS 29.209 V1.0.0 (2004-5), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network; Policy control over Gq interface (Release 6)
[Con97] draft-ietf-tcpm-tcp-roadmap-*.txt, “A Roadmap for TCP Specification Documents”, M. Duke et al., IETF, June 2005.
[Con98] TR-69: “CPE WAN Management Protocol” (May 2004).
[Con99] TR-64: “LAN-Side DSL CPE Configuration” (May 2004).
[Con100] TR-98 DSLHome™ Internet Gateway Device Version 1.1 Data Model for TR-069
[Con101] TR-104 DSLHome™ Provisioning Parameters for VoIP CPE
[Con102] TR-106 DSLHome™ Data Model Template for TR-069 Enabled Devices
[Con103] TR-110 DSLHome™ Reference Models for VoIP Configurations
[Con104] TR-133 DSLHome™ TR-064 Extensions for Service Differentiation
[Con105] TR-67v2, “ADSL Interoperability Test Plan”, Testing & Interoperability Working Group, December 2004.
[Con106] WT-123v1, “TR-069 Validation Testing Architecture”

7 NETWORK CONNECTIVITY TESTING

7.1 MUSE Architectures

MUSE describes two Network models, one model for Ethernet transport and one model for IP transport.

Network model 1: "Ethernet-based architecture" is based on the use of Ethernet technology for connectivity between CPN and edge nodes and relies on L2 and/or L3 QoS capabilities. All nodes must be able to base the forwarding handling on information of the Ethernet frames.

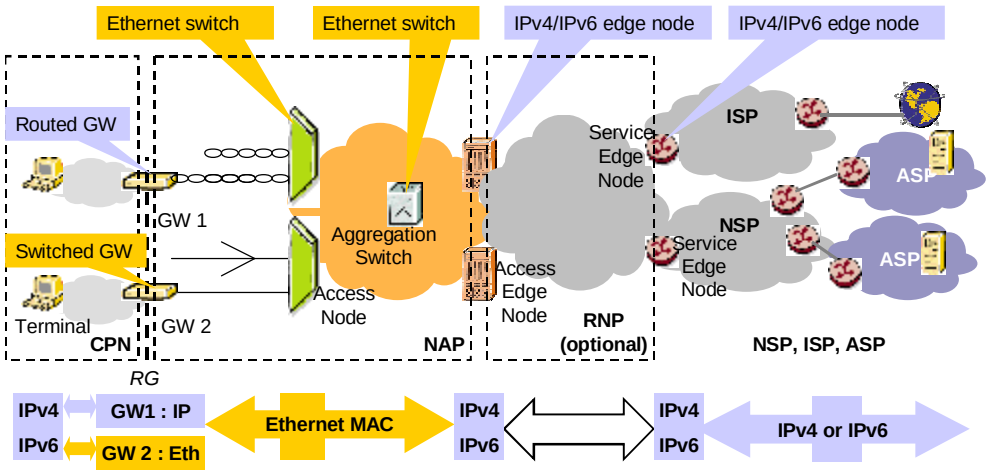


Figure 7-1: Network model 1, Ethernet based architecture.

The Ethernet based architecture requires end-to-end Ethernet connectivity between the CPN and the Edge Node. This implies that all nodes between the CPN and the Edge Node must be Ethernet aware.

Network model 2: "IP-based architecture" is one in which the forwarding for connectivity and QoS management in the access multiplexer and aggregation network are entirely based on IP information at L3. Some IP edge functionality will be moved to the access multiplexer, which possibly allows for an optimization of the distribution of functions and cost.

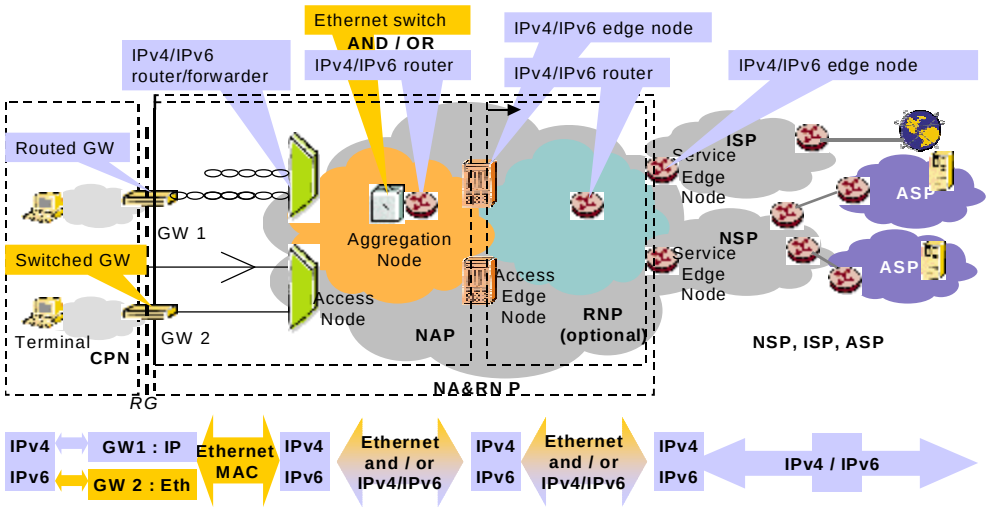


Figure 7-2: Network model 2, IP based architecture.

The main characteristic at the data plane of the IPv4/IPv6 network model is the separation of access and aggregation part at Layer 2 by the Access Node, which now acts as a Layer 3 node.
There are two degrees of IP awareness that can be brought closer to the end-user by introducing aggregation nodes; in a light degree these nodes act as IP forwarders (terminating layer 2, using IP knowledge for internal forwarding, but not acting as an IP node), and in the full degree these nodes act as routers (terminating layer 2, routing at IP, using routing protocols on its interfaces).

7.2 The MUSE reference model

The MUSE reference model in Figure 7-3 contains those functional elements that provide the end-to-end service connection from the customer domain to the application server, i.e. terminal, customer premise gateway (CPG)[8], access node (AN), aggregation node(s), access edge node (AEN), regional router(s), service edge node (SEN) and application server. In end user to end user applications, e.g. VoIP then the service edge node will be interconnected across an IP core network to another service edge node and subsequent access and aggregation network. For this document we will only consider the customer to application server part.

[8] The term Customer Premise Gateway is intended to cover any group of functions that allow connection of customer premise equipment to the access network. In much of MUSE the focus has been on the Residential Gateway which is a particular example of a CPG. Business premises may well have a different gateway.

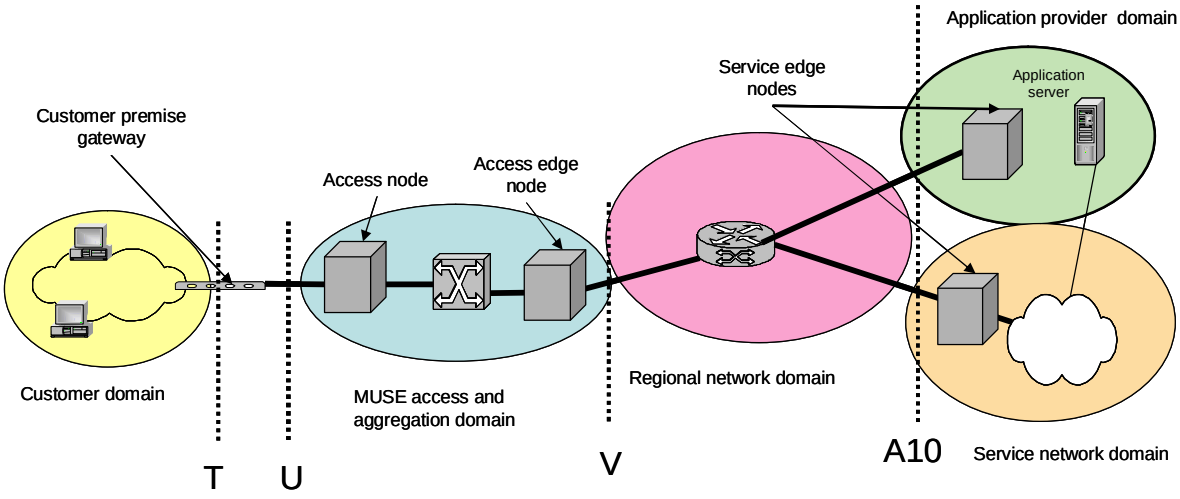


Figure 7-3: MUSE reference model and reference points.

The reference points of interest in this model are labeled T, U, V and A10. This terminology is taken from the reference architecture described by the DSL Forum. V and A10 may be coincident in some realizations where the service and access edge nodes are combined.

Using the reference points defined in Figure 7-3 the following interfaces can be defined:

- Network Termination 1 to Network Termination 2 Interface (T)
- Access Edge Node to CPG Interface (U)
- Access Edge Node to Regional Network Interface (V) or Regional Network to Service Edge Node (A10)

7.3 The MUSE Data Plane

The forwarding or data plane handles only the per-flow or per-packet forwarding as calculated by a control plane. It also performs policing and scheduling as well as services such as protection and load sharing. The forwarding plane is often said to perform "forwarding" or "switching".

To understand the data plane protocols that operate across the above defined interfaces it is useful to look at the protocol stacks that are implemented in each of the nodes. Figure 7-4 shows the generalized protocol stacks used at each of the nodes and the CPG for the case of an Ethernet aggregation network. As we will see below there are elements of these protocol stacks that are not required for different deployment scenarios.

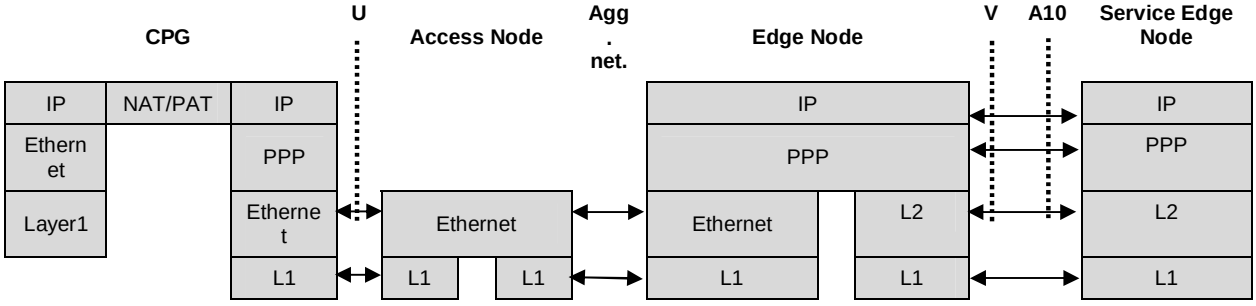


Figure 7-4: Generalized Protocol Stacks for Ethernet MUSE Data Plane

7.3.1 Interfaces

7.3.1.1 T-Interface

The Network Termination 1 to Network Termination 2 Interface (T) reference point in the MUSE architecture is usually assumed to be within the CPG. As such it does not make sense to define tests at the T reference point.

7.3.1.2 U-Interface

The Access Edge Node to CPG Interface (U) reference point is the point at which CPGs, which may well be obtained by the customer from one of many suppliers, are connected to the Access Provider's Network and so an open interface at this point is essential. The data plane interface is defined at L1 and L2, there being a number of options for each layer described in the MUSE architecture.

- L1 U Interfaces
  The L1 and physical characteristics of this interface are strongly media dependent, e.g. DSL, fibre, radio. We refer the reader to the appropriate chapters in this document (xDSL testing, …) for details about L1 specific tests.

- L2 U Interfaces
  These L1 standards often include definition of the L2, e.g. ATM over DSL. However, the MUSE architecture focuses on Ethernet as the L2 protocol of choice for this interface.

It should be noted that given there may be a long term convergence towards an end-to-end Ethernet L2 in the access and aggregation network a variety of L2 protocols will coexist for a number of years. In this document however we will focus for the U-interface on an Ethernet L2 solution.

There are three options for the Ethernet U interface defined in MUSE related to the way Ethernet is used in the AN:

- **Intelligent bridging** (residential users): the connectivity in the AN is based on the MAC addresses, as in an ordinary Ethernet switch but the AN has additional intelligence for security, traffic management and accounting.
- **Cross-connecting** (residential users): the connectivity at the AN is based on VLAN-IDs, namely by associating one individual VLAN-ID to every end-user (i.e. to every line aggregated in the AN). The AN then behaves as a cross-connect, switching ports via the VLAN-IDs for connectivity in the downstream direction, and switching upstream traffic to the uplink. (cfr. IEEE 802.1Q)
- **S-VLANs** (business users): These users will generate 802.1Q-tagged Ethernet frames, and expect them to be transported transparently across the network to one or multiple other business locations (L2 VPN). In the ANs, the upstream frames are transparently sent and tagged with the corresponding S-VLAN (based on the line), and the downstream frames are transparently sent (after stripping the S-VLAN tag) to the line corresponding to the S-VID. This approach can be combined with the bridged model and with the cross-connect model. In both cases some S-VLANs must be reserved in the network for business users only. Cfr. IEEE 802.1ad.

In the first two options there is no difference in the Ethernet across the U-interface. For the business user case, however, the frames are S-VLAN tagged.

7.3.1.3 V and A10-Interface

There are a number of options for the Access Edge Node to Regional Network Interface (V) or Regional Network to Service Edge Node (A10) interface depending on the business model being used. DA2.2 Section 2.3 defines a number of business models which from the point of view of different interfaces gives rise to three particular variants of the reference model in Figure 7-3.

7.3.1.3.1 PPP Wholesale Model

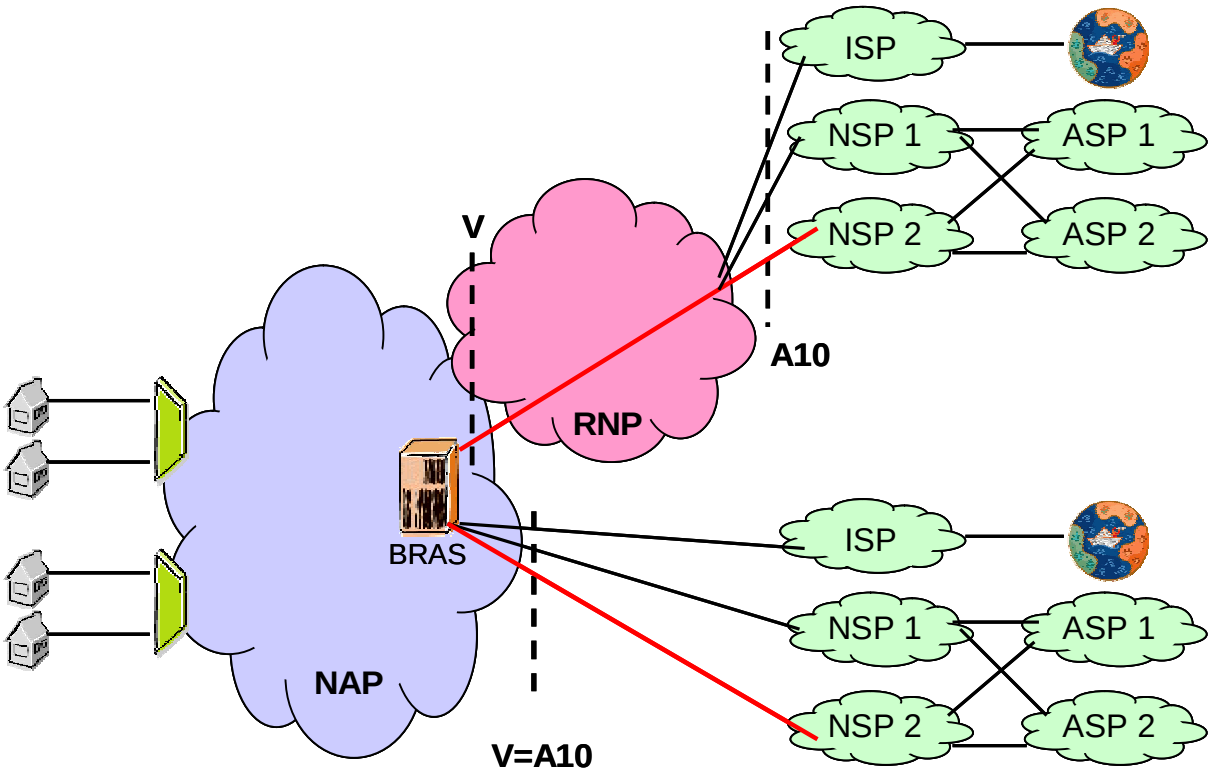


Figure 7-5: PPP Wholesale Model.

The first variant is shown in Figure 7-5. The edge node (for instance a BRAS) of the Access and Aggregation network offers PPP wholesale to NSPs and ISPs either directly or through a Regional Network. The L2 and above interfaces at V or A10 are both IPoPPPoE. The L1 interface at V and A10 may be different, but at L2 and above V and A10 are identical.

7.3.1.3.2 IP Wholesale Model

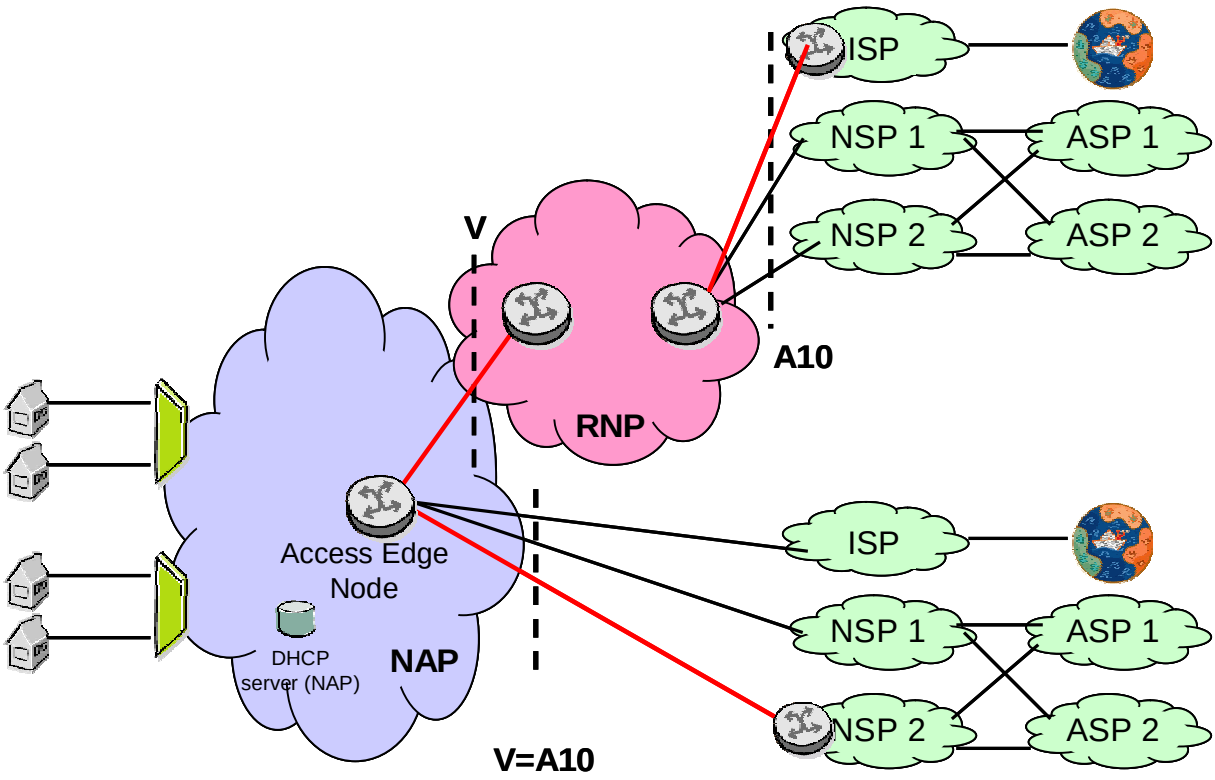


Figure 7-6: IP Wholesale Model.

The second variant is shown in Figure 7-6. A router of the NSP network interfaces to an access edge node of the Access and Aggregation network (A10=V), or a router of the regional network (A10 interface) to transport IPoE traffic. The L2 and above interfaces at V or A10 are both IPoE and DHCP is provided by the NAP. Under the assumption that if the regional network uses MPLS it is confined to the regional network and does not extended into the access or service network domains then the V and V10 interfaces are identical. In this model PPP is removed from the protocol stacks in Figure 7-5.

7.3.1.3.3 L2 Wholesale Model

The third variant is shown in Figure 7-7. An access edge node of the Access and Aggregation network interfaces to a network element of the NSP/ISP either directly or through a L2 regional network in order to provide Ethernet service connectivity or MEF types of services (L2 VPN and Ethernet virtual lines). The V and A10 interfaces are up to L2. A L2 V and A10 are identical but at L1 may be different. In this model PPP and IP are removed from the protocol stack for the edge node in Figure 7-3.

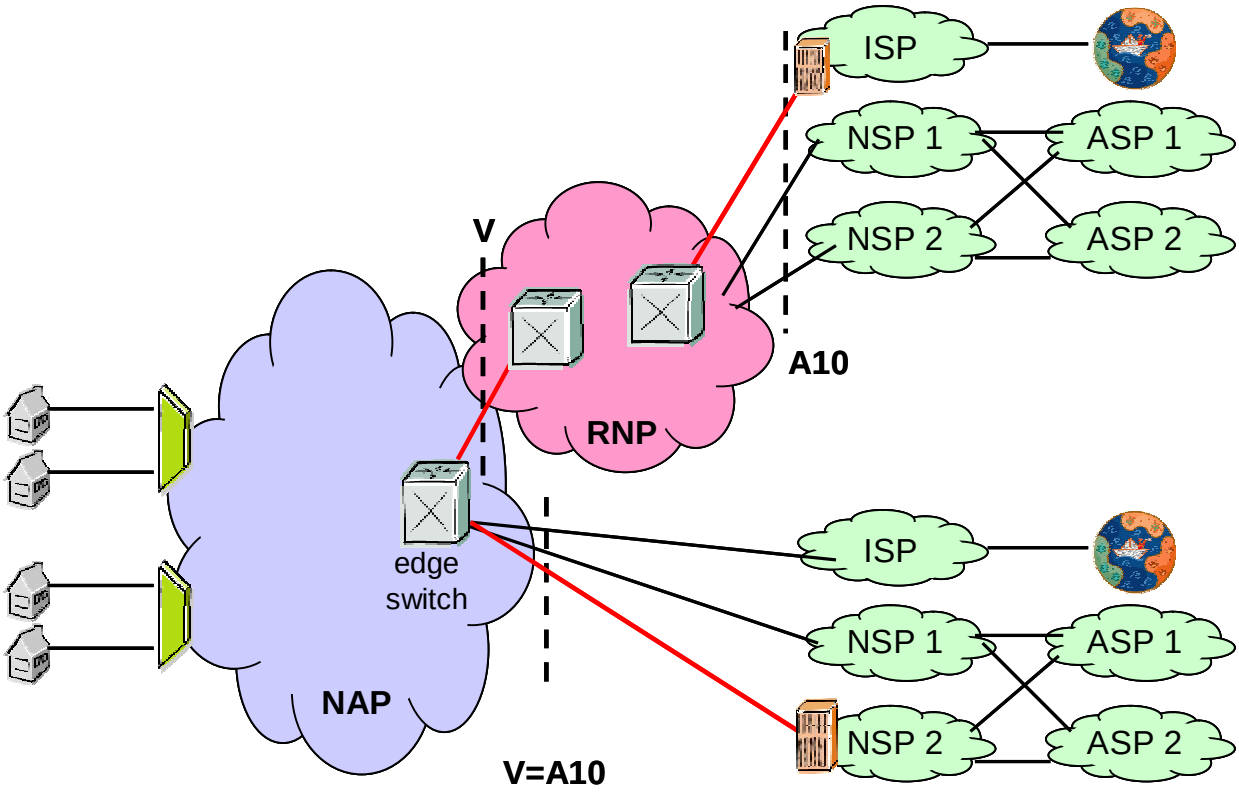


Figure 7-7: L2 Wholesale Model

7.3.2 Data Plane TESTS

7.3.2.1 Link Layer

Considering the MUSE Architectures, Link Layer tests are indicated for the Ethernet network model essentially in the context of end-to-end connectivity. The Ethernet model assumes a transparent Ethernet (Link Layer) connection between RGW and Edge Node but in contrast to this Ethernet approach the IP network model requires a Link Layer termination within each IP node on the path. That means basically Network Layer tests are needed for the IP network model to evaluate end-to-end connectivity with the exception of an optional implementation of Ethernet transport functionalities for IPoPPPoE support.

Following topics need to be considered for the Ethernet network model in terms of end-to-end Link Layer connectivity tests:

- Support of standardized Ethernet traffic
  - (unicast, multicast, broadcast)
- Customer and Service separation
- Connectivity characteristics (including Multicast support)
  - P-to-P (including Peer-to-Peer), P-to-MP and MP-to-MP
- Link layer Redundancy aspects
- Topology aspects (star, tree, ring or mesh topology)

Note: QoS, Security, Auto-configuration, OAM and IGMP aspects are out of scope of this section.

7.3.2.1.1 Conformance Tests

7.3.2.1.1.1 Support of standardized Ethernet traffic:

- Verify that forwarding of standardized Ethernet frames specified by IEEE-802.3 with unicast, multicast and broadcast MAC addresses are supported.
- Intelligent bridging option
  - Check that forwarding is based on Ethernet MAC switching in combination with VLAN tagging
- Cross-connecting option
  - Check that forwarding is based on static VLAN connections without Ethernet MAC leaning

7.3.2.1.1.2 Customer and Service separation:

- Verify that VLAN tagging specified by IEEE 802.1D and IEEE 802.1ad (Provider Bridges) is supported in order to separate customers and services.
- In case of MPLS in the aggregation network to solve the VLAN scalability restriction, verify that the MPLS mechanisms are conform to IETF specifications.

7.3.2.1.1.3 Link layer Redundancy aspects

- Verify if Link layer protection is supported and that it is conform to:
  - § Link Aggregation Control Protocol
  - § Spanning Tree Protocols
    - Spanning Tree Protocol (native)
    - Rapid spanning tree protocol
    - Multiple spanning tree
  - § Resilience Packet Ring (RPR)
  - § Ethernet Automatic Protection Switching
  - § MPLS

7.3.2.1.1.4 Topology aspects

- § Verify if Spanning Tree (native), Rapid spanning tree, Multiple spanning tree Protocol conform to the IEEE specifications can be used to enable star, tree, ring or mesh topologies without packet loops in the network

7.3.2.1.2 Functional Tests

7.3.2.1.2.1 Customer and Service separation:

- Verify that traffic and services of different customers are strictly separated.

7.3.2.1.2.2 Connectivity characteristics (including Multicast support)

- Verify that Ethernet P-to-P connections are supported between CPN and EN
- Verify if Ethernet P-to-MP connections are supported between CPN and EN (e.g. using one or multiple Multicast Service VLANs)
- Connectivity services option
  - § Peer-to-Peer: Check if Layer-2 Peer-to-Peer connections are supported between two customers
  - § Verify if Ethernet MP-to-MP connections are supported between multiple locations of one customer or between several customers

7.3.2.1.2.3 Link layer Redundancy aspects

- Verify if reconfiguration is performed in case of link layer failure.
- Check that a Spanning Tree Protocol BPDU (Bridge Protocol Data Unit) generated by the CPN does not start a reconfiguration process in the Access network

7.3.2.1.2.4 Topology aspects

- Verify if star, tree, ring or mesh topologies are supported in the Network without packet loops (e.g. using Spanning Tree Protocol)

7.3.2.1.3 Performance Tests

7.3.2.1.3.1 Connectivity characteristics (including Multicast support)

- One-to-One Ethernet performance tests between CPN and EN
  - § Verify the Ethernet throughput
  - § Verify the Ethernet Frame delay
  - § Verify the Ethernet Frame loss rate
  - § Verify the Ethernet Frame delay variation
- Many-to-One/ One-to-Many Ethernet performance tests between multiple CPN and EN
  - § Throughput, Frame delay, Frame loss rate, Frame delay variation
- Ethernet performance tests between two or multiple CPNs (One-to-One, Many-to-One/ One-to-Many and Many-to-Many)
  - § Throughput, Frame delay, Frame loss rate, Frame delay variation

7.3.2.1.3.2 Link layer Redundancy aspects

- Verify the reconfiguration time in case of link layer failure

7.3.2.2 Network Layer

7.3.2.2.1.1 Conformance Tests

The network layer should conform to the following standards:

1. RFC 791 – "INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981".
2. RFC 792 – "INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981".

7.3.2.2.1.2 Functional Tests

- **Basic connectivity test:** Use ICMP ECHO request and Reply to see if the network layer is operational.
- **Advanced Connectivity Test:** Use a web browser to verify network operation.

7.3.2.2.1.3 Performance Tests

- **Throughput, Frame Loss, E2E Delay, E2E Jitter (Delay Variation), Packet sequence** from host to Access Edge Node and to ISP/NSP/ASP border router.

  The measurement of the abovementioned characteristics should be performed in compliance with the following IETF recommendations.

  - RFC 2330: "Framework for IP Performance Metrics", V. Paxson, G. Almes, J. Mahdavi, M. Mathis, May 1998
  - RFC 3432: "Network performance measurement with periodic streams", V. Raisanen, G. Grotefeld, A. Morton, November 2002
  - RFC 4148: "IP Performance Metrics (IPPM) Metrics Registry", E. Stephan, August 2005
  - RFC 2678: "IPPM Metrics for Measuring Connectivity", J. Mahdavi, V. Paxson, September 1999
  - RFC 2679: "A One-way Delay Metric for IPPM", G. Almes, S. Kalidindi, M. Zekauskas, September 1999
  - RFC 2680: "A One-way Packet Loss Metric for IPPM", G. Almes, S. Kalidindi, M. Zekauskas, September 1999
  - RFC 2681: "A Round-trip Delay Metric for IPPM", G. Almes, S. Kalidindi, M. Zekauskas, September 1999
  - RFC 3148: "A Framework for Defining Empirical Bulk Transfer Capacity Metrics", M. Mathis, M. Allman, July 2001
  - RFC 3357: "One-way Loss Pattern Sample Metrics", R. Koodli, R. Ravikanth, August 2002
  - RFC 3393: "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", C. Demichelis, P. Chimento, November 2002
  - RFC 3763: "One-way Active Measurement Protocol (OWAMP) Requirements", S. Shalunov, B. Teitelbaum, April 2004.

7.4 The MUSE Control Plane

The control plane oversees the operation of the data plane, allocating resources, providing information, and handling errors to allow data plane operations to be continuous and efficient.

In the context of the MUSE control Plane we will discuss in the next subsections the aspects of Authentication, Auto-configuration and that of Quality of Service.

7.4.1 Authentication

Two authentication types are considered for access networks: implicit authentication and explicit authentication. Both implicit authentication and explicit authentication may be used independently as network level access authentication mechanism, notwithstanding the fact that implicit authentication may be a consequence of explicit authentication, e.g., the implicit line authentication used together with an explicit method such as PPP in xDSL access.

Depending on the access network configuration, especially for wired broadband access networks, the implicit access authentication may rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer. A CPE can directly access the access network without an explicit authentication procedure. Which implicit authentication applies depends on the operator policies.

The following are examples of implicit authentication mechanism that can be applied:

- Line authentication based on the activation of the L2 connection between the CNG and the access network,
- Port authentication,
- MAC address authentication, and
- VLAN/PVC authentication.

On the other hand, explicit authentication is an authentication process that relies on an explicit authentication signaling between the CPE and the NASS. In this case, an identity must be used for access authentication, which may depend on the authentication mechanism applied, and on the access network to which the CPE is connected to:

- User identity and credentials provided by the user, and
- CPE identity.

The following are examples of explicit authentication mechanisms:

- PPP-based authentication,
- DHCP Option 90,
- IEEE 802.1X-based authentication,
- PANA-based authentication, and
- WEB-based authentication.

In the context of this document we will limit the discussion to the explicit authentication mechanisms: PPPoE, DHCP Option 90, IEEE 802.1X and PANA.

7.4.1.1 PPPoE

PPPoE, point-to-point protocol over Ethernet (RFC 2516 [Con24]), is a network protocol for encapsulating PPP frames in Ethernet frames. It offers standard PPP (RFC 1661 [Con11]) features such as authentication, encryption, and compression.

The PPP protocol consists of two separate protocols:

- **Link Configuration Protocol (LCP):** is in charge of setting up and maintaining PPP links. LCP invokes an authentication protocol when PPP is configured to use authentication.

- **Network Control Protocol (NCP)**: After an LCP link has been opened; PPP invokes one or more Network Control Protocols for the layer three protocols being carried on the link. These perform any network-layer-specific configuration needed before the link can carry that particular network layer protocol.

PPP as defined in RFC 1661 specifies no specific authentication protocol. The most commonly used protocols are the **Password Authentication Protocol (PAP)** (RFC 1334 [Con01]) and the **Challenge Handshake Authentication Protocol (CHAP)** (RFC 1994 [Con15]).

The **Extensible Authentication Protocol (EAP)** defined in RFC3748 [Con69] is a general authentication protocol which supports multiple authentication methods, including traditional passwords, token cards, Kerberos, Digital Certificates and public-key authentication.

The EAP authentication method dictates the format and content of the EAP messages. Some of the well-known EAP schemes are:

- *Certificate based schemes:* EAP-TLS (RFC 2716 [Con33]), EAP-TTLS (draft-ietfpppext-eap-ttls-03.txt), PEAP (draft-josefsson-pppext-eap-tls-eap-08.txt).
- *Symmetric key based schemes:* EAP-SIM (draft-haverinen-pppext-eap-sim-16), EAP-AKA (draft-arkko-pppext-eap-aka-15), EAP-SKE (draft-salgarellipppext-eap-ske-01.txt)
- *Password based schemes:* such as EAP-SRP, EAP-MD5, etc

NOTE: The EAP authentication can also be run over IEEE 802 wired networks (IEEE-802.1X), and IEEE 802.11 wireless LANs (IEEE-802.11i).

7.4.1.2 DHCP Option 90

The RFC 3118 [Con47] defines a solution for the authentication of the DHCP messages. This solution provides both entity authentication (i.e. (mutual) authentication between DHCP client/server) and message authentication (i.e. authentication of the messages exchanged between the DHCP client and server).

The solution (RFC 3118) is based on the authentication option (the code of this option is 90). The authentication option includes replay detection data and authentication information in the DHCP message. The authentication information is dependent of the protocol that is used.

Two such protocols are specified in RFC 3118:

- **Configuration token**: in this case authentication information contains un-encoded token known to both client and server. The token is simply compared at the receiving side with the known value of it in order to authenticate the sender of the information. This protocol provides only weak entity authentication and no message authentication.
- **Delayed authentication**: in this case the authentication is based on the message authentication code. A Message Authentication Code (MAC) is issued to verify the authenticity (and at the same time to protect the integrity) of the DHCP message. A MAC provides message authentication provided that there exists mutual trust – in the case of the DHCP the trust (DHCP security association) is expressed in a way that the secret key is shared between DHCP client and DHCP server. The particular algorithm used to calculate the MAC as specified in RFC 3118 is keyed HMAC-MD5. The authentication information also contains a secret ID that is a unique identifier for the key used to calculate the HMAC-MD5 value. The delayed authentication protocol allows both message authentication and entity verification.

7.4.1.3 IEEE 802.1x

The IEEE 802.1x standard provides an architectural framework on top of which different **Extensible Authentication Protocol (EAP)** based authentication methods can be applied. These authentication methods could be, for example, certificate-based authentication, one-time passwords, smartcards, etc.

The standard describes port-based access control for different network technologies, such as Token Ring, FDDI, 802.3 and IEEE 802.11 networks. It specifies usage of EAPOL (EAP Over LAN) protocol between the peer and authenticator to perform user authentication.

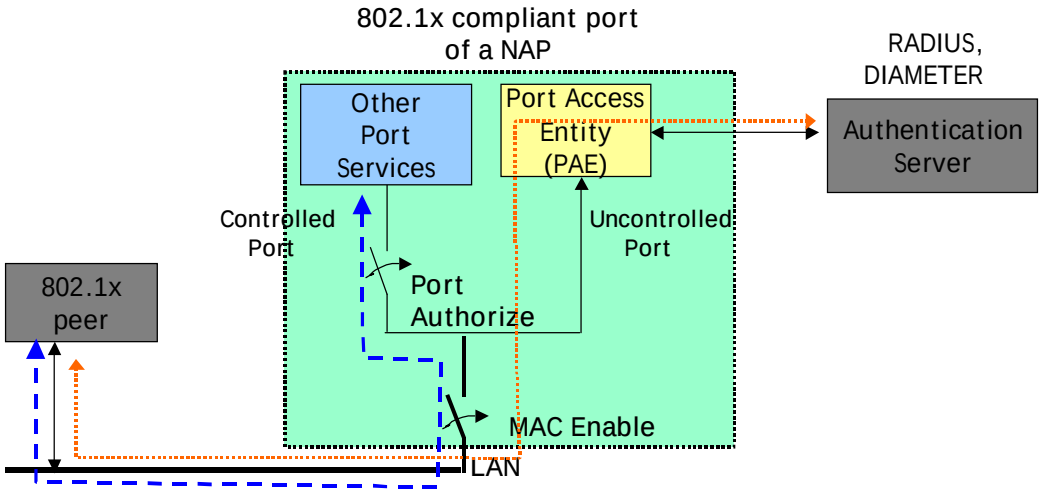


Figure 7-8: 802.1x Protocol entities

The authenticator has two ports: an uncontrolled port that allows only EAPOL packets in unencrypted format, and a controlled port that allows regular packets to pass only after the EAP authentication exchange through the uncontrolled port was successful. The authenticator communicates with an AAA authentication server using EAP-over-RADIUS (in future EAP-over-DIAMETER) to complete the EAP authentication protocol.

By enabling pass-through, authenticators can support any method implemented on the peer and server, not just locally implemented methods. This allows the authenticator to avoid implementing code for each EAP method required by peers.

7.4.1.4 PANA

PANA (Protocol for carrying Authentication for Network Access) is a link-layer agnostic network access authentication protocol that runs between a node that wants to gain access to the network and a server on the network side . It is defined as a network-layer transport for EAP. This is the main difference to 802.1x, which is designed to transport EAP by IEEE 802 link layers.

With the help of PANA transporting EAP authentication a basic authentication and authorization of the user or the RGW takes place. Thereby a security authorization is created, which is used to secure the DHCP protocol between user/RGW and a DHCP server in the network.

The following figure shows the elements and protocols of the PANA architecture.

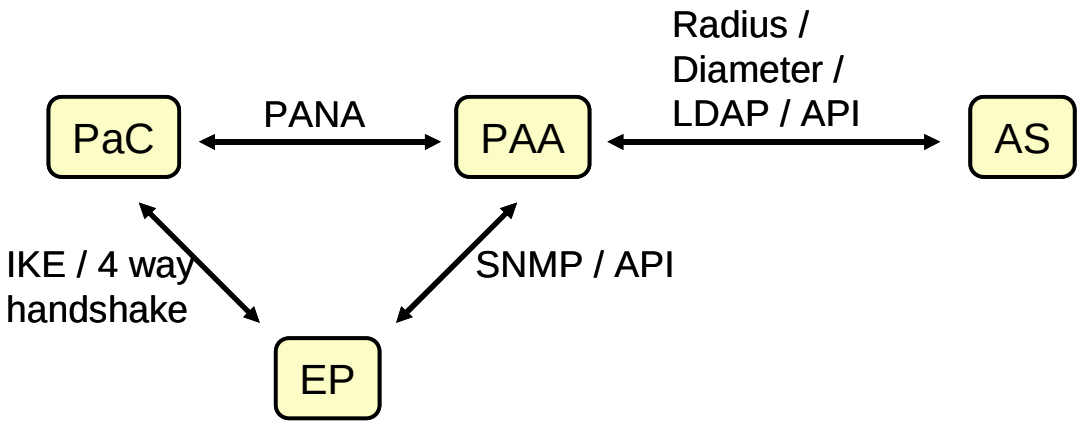


Figure 7-9: Components and protocols of PANA architecture

- PANA client (PaC)
- PANA authentication agent (PAA)
- Authentication server (AS)
- Enforcement point (EP)

Before starting the PANA authentication an IP connection must exist between the PaC and the PAA. So the PaC must get an initial IP address, which is only used for the PANA/EAP authentication. After being authenticated the user/RGW gets a new IP address from a DHCP server. This IP address is also used for further PANA communication (e.g. refresh). The initial IP address can be provided by several mechanisms (e.g. zero-conf or DHCP) and should allow a connection to the PAA with a lease reasonably long to complete PANA authentication.

During the authentication phase an EAP request is carried by PANA from the PaC to the PAA. The PAA contacts the Authentication Server (AS) to get the authentication decision. The interface between PAA and AS can be a protocol like Radius, Diameter or LDAP. The

PAA and AS can also be located on the same node. Then the communication between PAA and AS can be implemented by an API.

The successful PANA authentication creates cryptographic keys, which the PAA sends to the DHCP client (running on same node as PaC) and a DHCP server/relay. So a security association for requesting and providing the "final" IP address using DHCP option 90 (see 7.4.1.2) is established.

7.4.2 Auto-configuration

Broadband access technologies allow bundling of several services on the same physical access. And often, different service providers offer these services. So, one of the main problems in a broadband access rollout scenario is the service provisioning, especially CPE configuration.

Complexity of the problem that carriers have to face up will be increased in a multi-service and multi-provider environment. CPE configuration depends on which services signed up the user and the same user can sign up different services with different service providers.

In a multi-service and multi-provider environment carrier and each service provider has to access to the CPE in order to configure its own service parameters. In the case of an xDSL access:

1. First of all, access carrier or NAP (Network Access Provider) has to configure the CPE: VCCs (VPIs/VCIs), ATM transfer capabilities, bit-rates, …
2. NSP has to provide some parameters like IP address and netmask, IP filters, routes and routing protocols and QoS capabilities.
3. In case of services, like VoIP/ToIP, TVoIP, … other providers can take part in the CPE configuration process.
4. The same will happen for other ASPs, video over IP providers, gaming providers, ...

Definition of auto-configuration:

Auto-configuration is the process by which the CPE obtains autonomously configuration information from the network and its service providers.

7.4.2.1 Protocols for auto-configuration of the L2 Network Services

NONE

7.4.2.2 Protocols for auto-configuration of the L3 Network Services

There are a number of possible auto-configuration options depending on the business model being used as indicated in 7.3.1.3.

- ***PPP Wholesale Model:*** In this model the auto-configuration protocol used will be PPP over Ethernet. PPP over Ethernet (RFC 2516 [Con24]) is an encapsulation specification on how to carry RFC 1661 Point-to-Point Protocol frames over Ethernet.
- ***IP Wholesale Model:*** In the IP Wholesale model the hosts are configured through the Dynamic Host Configuration Protocol (DHCP) as described in RFC 2131 [Con16].

- ***L2 Wholesale Model:*** Given that the L2 Wholesale model only does L2 pass-through there are no special auto-configuration mechanisms.

7.4.2.3 Protocols for auto-configuration of the Application Services

- DSL Forum standards.
    - o TR-69: “CPE WAN Management Protocol” (May 2004).
    - o TR-64: “LAN-Side DSL CPE Configuration” (May 2004).
    - o TR-98 DSLHome™ Internet Gateway Device Version 1.1 Data Model for TR-069
    - o TR-104 DSLHome™ Provisioning Parameters for VoIP CPE
    - o TR-106 DSLHome™ Data Model Template for TR-069 Enabled Devices
    - o TR-110 DSLHome™ Reference Models for VoIP Configurations
    - o TR-133 DSLHome™ TR-064 Extensions for Service Differentiation

The figure below depicts the different auto-configuration protocols defined by the DSL Forum and their relation.

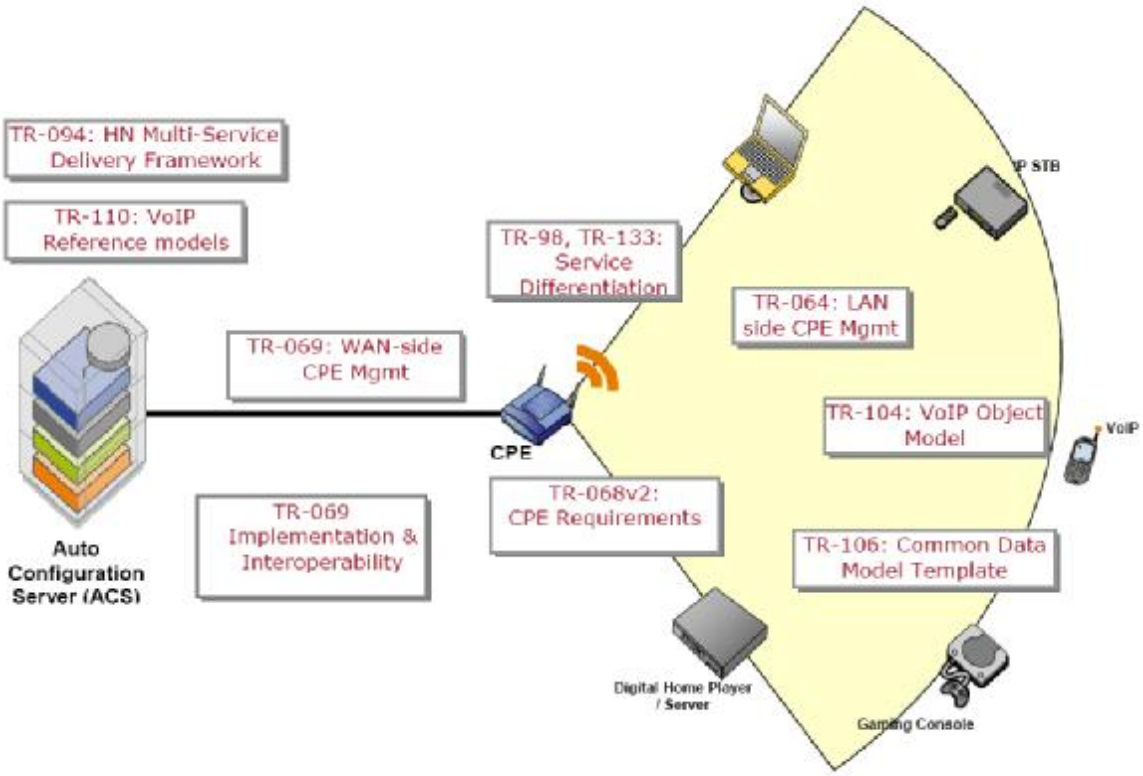


Figure 7-10: DSL Forum auto-configuration standards and their relation

- IETF standards.
    - o RFC 2865: “Remote Authentication Dial In User Service (RADIUS)” (June 2000).
    - o RFC 2866: “RADIUS Accounting” (June 2000).
    - o RFC 2868: “RADIUS Attributes for Tunnel Protocol Support” (June 2000).

- RFC 2869: “RADIUS Extensions” (June 2000).
- RFC 3588: “Diameter Base Protocol” (September 2003).
- RFC 3589: “Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5” (September 2003).

7.4.3 MUSE QoS Architecture

MUSE describes following three QoS approaches:

1. Tight QoS approach
   - **Philosophy:**
     - Central QoS control mechanism using Network Resource Management and Call Admission Control
   - **Basis:**
     - IMS/TISPAN QoS architecture specifications
   - **Advantages:**
     - Guaranteed end-to-end QoS on the basis of Resource Management
   - **Disadvantages:**
     - Scalability problems are expected for large networks with many QoS requests

2. Loose QoS approach
   - **Philosophy:**
     - Essentially decentralized QoS control mechanisms
     - Complex QoS mechanisms mainly at the edges (Very Intelligent Policing Access Node - VIP-AN),
     - Resources are not reserved end-to-end but only in network parts with congestion risk (e.g. first mile)
   - **Basis:**
     - Bandwidth broker functionality and Call Admission control processed by Residential Gateway and/or Access Node in order to reserve resources on the first mile link
     - Edges realise QoS with predefined Policing profiles autonomously
     - In case of congestion an additional central unit instructs to use more restrict Policing profiles
     - QoS in the Aggregation network is realized on the basis of over-provisioning in combination with Class of Service (CoS) that requires a careful traffic engineering
   - **Advantages**
     - Scalability for residential user networks
   - **Disadvantages:**
     - Only soft QoS, no guaranteed end-to-end QoS

3. Mixed QoS approach (GSB QoS architecture)
   - **Philosophy:**
     - Combine the advantages of Tight and Loose approach and solve the disadvantages
   - **Basis:**
     - Mixed approach integrates Tight and Loose QoS mechanisms

§ Loose control for the majority (mainly residential users) and Tight control for services with guaranteed end-to-end QoS requirements (mainly business users).

MUSE recommends a Mixed QoS approach for the GSB QoS architecture.

7.4.3.1 Tight QoS Control

The MUSE QoS approach developed so far is documented in M A2.7 D A2.2 and MA2.10. It is based on the 3GPP IMS and ETSI TISPAN models for QoS control. The main starting points for the guaranteed QoS approach, which is the one that is currently being developed by TISPAN are:

- A central view is kept of all network resources in the access network.
- A central view is kept of all resources that are currently in use.
- Requests for network resources are accepted or denied individually and on request. Requests are only accepted if the network resources available at the time of the request are sufficient to meet the requested QoS.
- Requests for network resources can be made by end users and by application service providers.
- Resources are reserved after a request has been accepted and released after the session has finished.
- Requests, acceptance and reservation of network resources can be handled independently for the upstream and downstream directions. For example, the upstream and downstream directions can have different delays and packet loss.

The IMS/TISPAN approach can be considered as a “tight” approach, as:

- The resource reservation is performed at the finest level of aggregation: the individual IP flow.
- The control for a given access network is concentrated in a small number of centralized resource control entities.

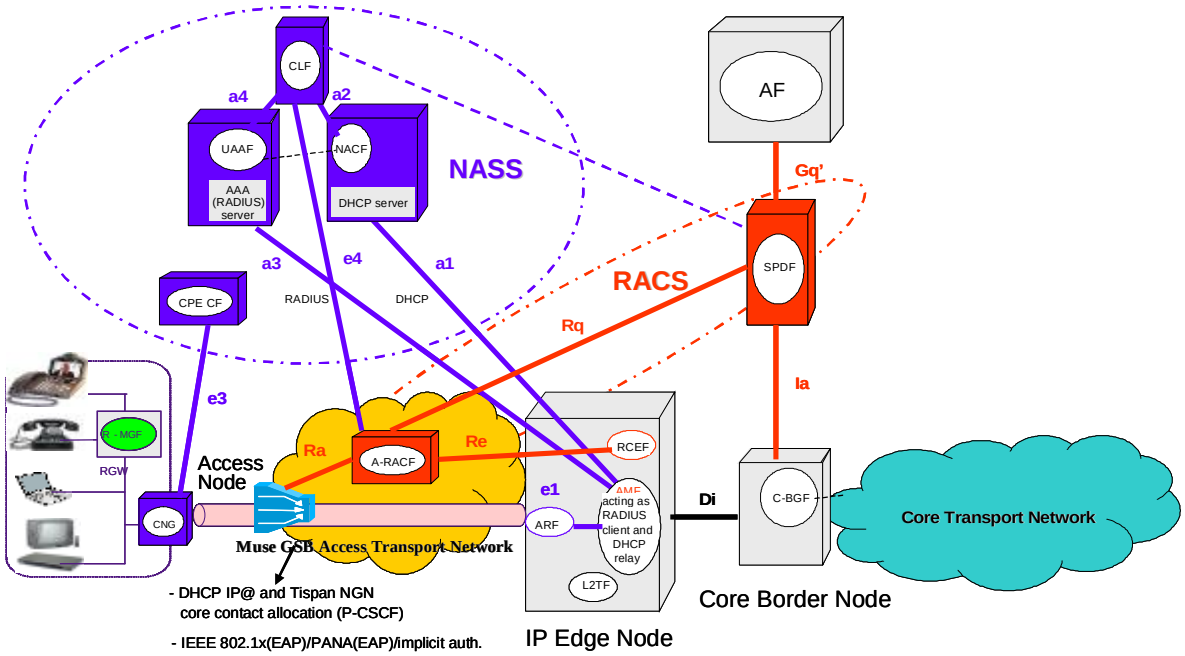


Figure 7-11: Proposal for interconnecting MUSE GSB and TISPAN

7.4.3.2 Loose QoS Control

In a well-traffic-engineered access network, the actions and effort needed to achieve the desired QoS can remain limited and local during most of the time. Under normal traffic conditions, call admission control in the residential gateway and/or the access node based on pre-provisioned user profiles and subscriptions are sufficient. The dimensioning of the network should be such that the majority of traffic situations fall in the category “normal traffic conditions”. Thus, adequate traffic engineering is crucial. The QoS control under normal conditions can be characterized as a “loose” mechanism.

7.4.3.3 Bottom-up solution for QoS

MUSE (MA2.10) describes a bottom-up solution that should evolve to a recommended MUSE implementation for QoS support. It describes a minimum functional set which must be supported by any MUSE conformant node and RGW. Additional features may be supported. The recommended MUSE implementation for QoS describes all elements which are needed in a node for QoS support; in particular switch cores, schedulers, shapers and policing circuits.

The MUSE QoS implementation proposal is based on the general concept that a MUSE node consists of a **standard Ethernet switch in the core with additional (MUSE) functionality realized at the ports**. This concept is described in D TF1.5 and D C1.4.

MUSE QoS implementation relies on **Ethernet switches with 4 queues per (output) port** with **strict priority according to IEEE 802.1pq** Ethernet QoS, defined as 8 classes with strict priority. Congestion within the core is avoided by appropriate means such as over-dimensioning, backpressure or dynamic bandwidth allocation etc. Therefore the main queuing points are the output ports. Traffic classification and policing is implemented at the input ports.

Scheduler of bottom-up solution

To realize a hierarchically layered network a strict priority scheduler must be implemented at each queuing point in the network. The Packet Classifier sorts the incoming packets according to their priorities into 4 queues. These are served by the strict priority multiplexer in such a way that after each packet transfer the strict priority multiplexer starts scanning for occupied queues from highest to lowest. This means that as long as there are packets available in the highest priority queue this queue is served and packets in lower priority queues have to wait. The lowest priority queue is only served if all other queues are empty. Depending on the load of the higher priority queues it could have to wait forever. This is called starvation. The idea of the bottom-up solution is that the upper 3 queues never take 100% of the bandwidth.

QoS classes
The bottom-up approach defines following 4 QoS classes.

QoS class	Node Mechanism of bottom-up approach
Low Latency	Separate queue with preferential (first priority) servicing, traffic grooming with limited load
Real Time	Separate queue with second priority servicing, traffic grooming with limited load, *no drop priority*
Elastic	Separate, long queue with third priority servicing, drop priority, guaranteed throughput for high priority, fair throughput share for low priority traffic
Best Effort	Separate queue, lowest priority

Table 7-1: QoS classes of bottom-up approach

For each QoS class the parameters max. burst size, max. jitter and max. Packet loss rate per node are defined (Table 7-1)

QoS class	Max. burst size	Max. jitter target per node	Max. Packet loss rate per node	DiffServ code point
Low latency	200 byte	1 ms	10^{-10}	101 010
Real time	1500 byte	30 ms	10^{-10}	101 110 (EF)
Elastic	9000 byte	900 ms	10^{-10}	100 010 (AF low drop precedence)
			-	100 110 (AF high drop precedence)
Best effort	-	-	-	000 000

Table 7-2 Proposed GSB traffic classes

Notes:

- When a connection is set up the rate must be specified, except for Best Effort.
- For simplicity and to align to Ethernet it is proposed to specify rates in multiples of 100kb/s.
- In order to fulfill the challenging Low Latency class over low rate links the 200byte limit on the packet size has been introduced. It is well suited for VoIP and MPEG2.

Low rate link restrictions

The high end QoS classes over low rate links are difficult to achieve. Rates for each class are limited and also the number of independent flows sharing a class. Hence a deterministic view is needed. Statistical effects can be exploited only partially.
1st mile rates up to 10Mb/s have to be considered as low rate. The most critical part is the low rate uplink for ADSL. A careful analysis which has been carried out in the document "QoS_1stMile_update.doc" which can be found on the MUSE server:
https://www.ist-MUSE.org/ftpdir/TF2/QoS_1stMile_update.doc .
Some results of the study are summarised in Table 7-3.

Rate	Low latency class		Real Time class		Elastic class	
	Restriction	Queue size	Restriction	Queue size	Restriction	Queue size
0.5M	1 flow only	200 byte	1 flow only	1500 byte	3 flows max.	27 kbyte
1M	1 flow only	200 byte	3 flows max.	4500 byte	6 flows max.	54 kbyte
2M	1 flow only	400 byte	5 flows max.	7500 byte	10 flows max.	90 kbyte
5M	3 flows max.	1000 byte	25% load max.	15000 byte	58% load max.	225 kbyte
10M	10 flows max.	2000 byte	50% load max.	33750 byte	77% load max.	450 kbyte

Table 7-3: Parameters for low rate links

Backhaul link restriction

Table 7-4 lists the maximum possible load values for the 3 non-best-effort QoS classes for some typical backhaul link types. It shows that on the backhaul links the load restrictions are minimal.

Line rate	Maximum load Low Latency class	Maximum load Real Time class	Maximum load Elastic class
Jitter value	1ms	30ms	900ms
Packet size	200byte	1500byte	9000byte
100 Mb/s	57%	92%	98%
150 Mb/s	72%	95%	98%
600 Mb/s	93%	98%	98%
1 Gb/s	95%	98%	98%

Table 7-4: Maximum load values for typical backhaul links

For all values in Table 7-4 it is assumed that there is no other traffic on the link. For example on a 100Mb/s link the maximum Real Time class load is 92% assuming that Low Latency and Elastic class load is zero. If for example Low Latency class traffic takes away 57% of the bandwidth the remaining bandwidth for Real Time class will be lower.

7.4.3.4 Traffic Shaping and Policing

Shaping and Policing are important in packet networks because they limit the amount of traffic a customer can generate. The MUSE QoS approaches are based on Admission control that performs policing. The Admission control has to consider the link restrictions described in 7.4.3.3.

Prioritized access to bandwidth on congested access links is increasingly managed by a set of dedicated traffic shaping devices or features in the RGW, access and edge nodes. The critical success criterion for these devices is to enforce policies at the application level, and, increasingly, at Layer 7. This allows network performance to be ensured for the high-revenue services (i.e. VoiP and TVoiP) while pacing network access for recreational services and sessions (i.e. Internet access). Mapping each type of traffic to a specific bandwidth allocation policy ensures that each traffic type receives appropriate bandwidth and that malicious activity is easily limited or blocked.

Many of these traffic shaping systems offer features to specify bandwidth minimums and/or maximums for a seemingly infinite number of applications, sessions, users, IP addresses, port numbers, and other traffic subsets. This level of discrete control is essential. Using web traffic as an example, simply managing it by HTTP protocol and port number is no longer sufficient. Instead, intelligent L7 payload inspection functionality allows the Network Operator to devise traffic prioritization and access control policies based on the destination of the HTTP GET request.

7.4.4 Control Plane TESTS

7.4.4.1 PPP Wholesale Model Specific

7.4.4.1.1.1 Conformance Tests

- An implementation should be conformant to the following standards:
    - Method for Transmitting PPP Over Ethernet (RFC 2516 [Con24])
    - Point-to-Point Protocol (PPP) (RFC 1661 [Con11])
    - PPP Internet Protocol Control Protocol (IPCP) (RFC 1332 [Con09])
    - PPP Authentication Protocols (RFC 1334 [Con10])
    - PPP Encryption Control Protocol (ECP) (RFC 1968 [Con14])
    - PPP Compression Control Protocol (CCP) (RFC 1962 [Con13])
- And may optionally implement the following specifications correctly:
    - PPP Challenge Handshake Authentication Protocol (CHAP) (RFC 1994 [Con15])
    - Extensible Authentication Protocol (EAP) (RFC3748 [Con69])

7.4.4.1.1.2 Functional Tests

- **Network Layer Configuration**: Verify that after start-up you obtain the correct IP address, subnet mask, router IP address and DNS settings. Optionally verify correct exchange of additional parameters (WINS, …).

- **Connectivity with background noise**: verify that you have connectivity (e.g. using ping, http, …) with different levels of background noise. See DSLForum TR-067v2 "9.3 PPPoE End-to-End Connectivity Test" section for details.

7.4.4.1.1.3 Performance Tests

- **Duration**: Measure the time it takes before a host obtains all the configuration parameters. This should be performed under different loads.
- **Scalability**: Measure how many simultaneous PPPoE requests can be processed at once.
- **Failure testing**: Verify that clients re-obtain valid network layer configuration when the main PPPoE server goes down and a secondary server takes over.

7.4.4.2 IP Wholesale Model Specific

7.4.4.2.1.1 Conformance Tests

- An L3 auto-configuration implementation should be conform the following standard:
    - Dynamic Host Configuration Protocol (RFC 2131 [Con16])
    - Authentication for DHCP Messages (RFC 3118 [Con47])
- Depending on the specific use cases different DHCP options/functionalities will be required as specified in the following standards.
    - DHCP Options and BOOTP Vendor Extensions (RFC 2132 [Con16])
    - DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients (RFC 2563 [Con26])
    - The Name Service Search Option for DHCP (RFC 2937 [Con40])
    - The User Class Option for DHCP (RFC 3004 [Con42])
    - The Subnet Selection Option for DHCP (RFC 3011 [Con43])
    - DHCP Relay Agent Information Option (RFC 3046 [Con45])
    - DHCP load balancing algorithm (RFC 3074 [Con46])
    - DHCP reconfigure extension (RFC 3203 [Con49])
    - Encoding Long Options in DHCPv4 (RFC 3396 [Con58])
    - The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4 (RFC 3442 [Con60])
    - Link Selection sub-option for the Relay Agent Information Option for DHCPv4 (RFC 3527 [Con62])
    - Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (RFC 3315 [Con54])
    - DNS Configuration Options for DHCPv6 (RFC 3646 [Con67])
    - IPv6 Prefix Options for DHCPv6 (RFC 3633 [Con66])
    - Stateless DHCP Service for IPv6 (RFC 3736 [Con68])
    - Vendor-Identifying Vendor Options for DHCPv4 (RFC 3925 [Con73])
    - Reclassifying DHCPv4 Options (RFC 3942 [Con74])
    - RADIUS Attributes Sub-option for the DHCP Relay Agent Information Option (RFC 4014 [Con76])
    - DHCP Subscriber ID Suboption for the DHCP Relay Agent Option (RFC 3993 [Con75])
    - The Authentication Suboption for the DHCP Relay Agent Option (RFC 4030 [Con77])

- Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4) (RFC 4039 [Con78])

7.4.4.2.1.2 Functional Tests

- **Network Layer auto-configuration**: Verify that after start-up you obtain the correct IP address, subnet mask, router IP address and DNS settings. Optionally verify correct exchange of additional parameters (WINS, …).
- **Connectivity with background noise**: verify that you have connectivity (e.g. using ping, http, …) with different levels of background noise. See DSLForum TR-067v2 "9.3 PPPoE End-to-End Connectivity Test" section for details, but adapted to the DHCP auto-configuration scenario.

7.4.4.2.1.3 Performance Tests

- **Duration**: Measure the time it takes before a host obtains all the configuration parameters. This should be performed under different loads.
- **Scalability**: Measure how many simultaneous DHCP requests can be processed at once.
- **Failure testing**: Verify that clients continue to obtain valid network layer configuration when the main DHCP server goes down and a backup server takes over.

7.4.4.3 L2 Wholesale Model Specific

Since the L2 Wholesale model offers LAN-to-LAN connectivity the access network is agnostic to the network layer protocols.

7.4.4.4 Wholesale Model Independent

7.4.4.4.1.1 Conformance Tests

- DSL Forum.
  - **Technical Report TR-64** [Con99]**: "LAN-Side DSL CPE Configuration"** (May 2004).
  - **Technical Report TR-69** [Con98]**: "CPE WAN Management Protocol"** (May 2004).
  - DSL Forum Working Text WT-098v1 [Con100]: "Parameter Model Extensions for Service Differentiation" (December 2003).
  - ***Working text WT-123v1*** [Con106]***: "TR-069 Validation Testing Architecture"*** (February 2005) : This document outlines architecture and a set of test requirements for TR-069 compliance and interoperability testing. TR-69 "CPE WAN Management Protocol" (CWMP) specifies a messaging protocol between a CPE and an Auto-Configuration Server (ACS) for the purposes of auto-configuration and dynamic service provisioning, software/firmware image management, status and performance monitoring, and diagnostics. CWMP compliance comprehends a number of different areas, including appropriate implementation of its underlying protocols,

appropriate implementation of the TR-069 specified RPC-based messaging and object hierarchy, and functional correctness. The document outlines the three major parts of TR-069 test architecture:
  - § Validation of CPE compliance
  - § Validation of ACS compliance
  - § Validation of interoperability between a CPE and an ACS.
- IETF.
  - o **RFC 2865: "Remote Authentication Dial In User Service (RADIUS)"** (June 2000).
  - o **RFC 2866: "RADIUS Accounting"** (June 2000).
  - o **RFC 2868: "RADIUS Attributes for Tunnel Protocol Support"** (June 2000).
  - o **RFC 2869: "RADIUS Extensions"** (June 2000).
  - o **RFC 3588: "Diameter Base Protocol"** (September 2003).
  - o **RFC 3589: "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5"** (September 2003).

7.4.4.4.1.2 Functional Tests

- **Application Layer Configuration**: Verify that after start-up the CPE device is configured with all the appropriate application layer parameters.

7.4.4.4.1.3 Performance Tests

- **Auto-configuration Duration**: Measure the time it takes a CPE device to obtain all the configuration parameters (L1/L2,L3,L3+ parameters). The impact of the load on the Access Network should be assessed.

- **Traffic Shaping/Policing test**

  - o **Baseline Throughput test:** Establish a baseline throughput measurement of stateful traffic through the SUT without enabling any traffic prioritization policies.
  - o **Bandwidth policing test**: Test traffic-shaping functionality and performance of the SUT based on different values defined in the HTTP payload. Each flow has a corresponding policy defining the maximum bandwidth.
  - o **Prioritization policing test:** Test traffic-shaping functionality and performance of the SUT based on different values defined in the HTTP payload. Each payload value has a corresponding policy defining the traffic's priority versus other traffic running through the SUT.
  - o **Mixed traffic policing test:** Test the traffic-shaping performance of the SUT when a mixture of stateful and stateless is flowing through the SUT. The Stateful traffic can be generic background traffic (e.g., IMIX) or Denial of Service (DOS) attack traffic (e.g. ping flood or sync flood).

7.4.4.5 QoS verification

7.4.4.5.1.1 Conformance Tests

- Verify that QoS control is supported on the basis of the MUSE Tight- or Loose- or Mixed- QoS approach (GSB QoS architecture)

- Verify that at least 4 QoS classes are supported conform to the MUSE bottom-up approach for QoS
- Verify that at least strict priority queuing is supported conform to the MUSE bottom-up approach for QoS

7.4.4.5.1.2 Functional Tests

- Verify that the system is able to reserve resources end-to-end using Tight QoS control
- Verify that the system is able to reserve resources on links with congestion risk (First Mile) using Loose QoS control
- Verify the system behavior using Loose QoS control in case of congestion
    - An additional central QoS control unit should instruct to use more restrict policing profiles
- Verify if a switching from Loose to Tight QoS control is supported
- Verify Bandwidth broker and Call Admission control functionalities considering the link restrictions described in 7.4.3.3, for example:
    - Low rate link with 1 Mbit/s: only 1 Low latency class flow, 3 Real Time class flows, 6 Elastic class flows
- Verify the queuing behavior of the system under test considering all supported queuing mechanisms but at least strict priority queuing

7.4.4.5.1.3 Performance Tests

Note:

QoS is not needed when resources are not limited. From this it follows that additional background traffic is needed to stress a system under test in order to verify the QoS performance of that system. This background traffic approach is the basis of following described QoS test.

7.4.4.5.1.3.1 Low latency QoS class stream with full link capacity background traffic

- Verify the end-to-end Throughput
- Verify the end-to-end delay
- Verify the end-to-end Packet loss rate
- Verify the end-to-end Jitter
- Verify the Packet sequence

7.4.4.5.1.3.2 Real time QoS class stream with full link capacity background traffic

- Verify the end-to-end Throughput
- Verify the end-to-end delay
- Verify the end-to-end Packet loss rate
- Verify the end-to-end Jitter
- Verify the Packet sequence

7.4.4.5.1.3.3 Elastic QoS class stream with full link capacity background traffic

- Verify the end-to-end Throughput
- Verify the end-to-end delay
- Verify the end-to-end Packet loss rate
- Verify the end-to-end Jitter
- Verify the Packet sequence

7.4.4.5.1.3.4 Max. burst size per QoS class

- Verify the Max. burst size of the Low latency QoS class
- Verify the Max. burst size of the Real time QoS class
- Verify the Max. burst size of the Elastic QoS class

7.5 References

[Con01] "IP Telephony Cookbook (TERENA Report)", ISBN 90-7759-08-6, March 2004.
[Con02] RFC 768, “User Datagram Protocol”, J. Postel, August 1980.
[Con03] RFC 791, “Internet Protocol”, DARPA, September 1981.
[Con04] RFC 793, “Transmission Control Protocol”, DARPA, September 1981.
[Con05] RFC1075, "Distance Vector Multicast Routing Protocol", Waitzman, November 1988.
[Con06] RFC 1112, "Host extensions for IP multicasting", S. Deering, August 1989.
[Con07] RFC 1242, “Benchmarking Terminology for Network Interconnection Devices”, S. Bradner, July 1991.
[Con08] RFC 1242, “Benchmarking Terminology for Network Interconnection Devices”, S. Bradner, July 1991.
[Con09] RFC 1332, “The PPP Internet Protocol Control Protocol (IPCP)”, G. McGregor, May 1992.
[Con10] RFC 1334, “PPP Authentication Protocols”, B. Lloyd et al., October 1992.
[Con11] RFC 1661, “The Point-to-Point Protocol (PPP)”, W. Simpson, July 1994.
[Con12] RFC 3550, "RTP: A Transport Protocol for Real-Time Applications", Schulzrinne H. et al., IETF, July 2003.
[Con13] RFC 1962, “The PPP Compression Control Protocol (CCP)”, D. Rand, June 1996.
[Con14] RFC 1968, “The PPP Encryption Control Protocol (ECP)”, G. Meyer, June 1996.
[Con15] RFC 1994, “PPP Challenge Handshake Authentication Protocol (CHAP)”, W. Simpson, August 1996.
[Con16] RFC 2131, “Dynamic Host Configuration Protocol”, R. Droms, March 1997.
[Con17] RFC2236, "Internet Group Management Protocol, Version 2", W. Fenner, IETF, November 1997.
[Con18] RFC2283, "Multiprotocol Extensions for BGP-4", T. Bates, R. Chandra, D. Katz, Y. Rekhter, IETF, February 1998.
[Con19] RFC 2285, “Benchmarking Terminology for LAN Switching Devices”, R. Mandeville, February 1998.
[Con20] RFC 2327, “SDP: Session Description Protocol”, M. Handley et al., April 1998.
[Con21] RFC 2330, “Framework for IP Performance Metrics”, V. Paxson, May 1998.

[Con22] RFC 2362, “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification”, D. Estrin et al., June 1998.
[Con23] RFC2432, "Terminology for IP Multicast Benchmarking", K. Dubray, October 1998.
[Con24] RFC 2516, “A Method for Transmitting PPP Over Ethernet (PPPoE)”, L. Mamakos et al., February 1999.
[Con25] RFC 2544, “Benchmarking Methodology for Network Interconnect Devices”, S. Bradner et al., March 1999.
[Con26] RFC 2563, “DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients“,R. Troll, May 1999.
[Con27] RFC 2678, “IPPM Metrics for Measuring Connectivity”, J. Mahdavi et al., September 1999.
[Con28] RFC 2679, “A One-way Delay Metric for IPPM”, G. Almes, September 1999.
[Con29] RFC 2680, “A One-way Packet Loss Metric for IPPM”, G. Almes, September 1999.
[Con30] RFC 2681, “A Round-trip Delay Metric for IPPM”, G. Almes, September 1999.
[Con31] RFC 2710, "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman, IETF, October 1999.
[Con32] RFC 2715, "Interoperability Rules for Multicast Routing Protocols", D. Thaler, IETF, October 1999.
[Con33] RFC 2716, “PPP EAP TLS Authentication Protocol”, B. Aboba et al., October 1999.
[Con34] RFC 2858, “Multiprotocol Extensions for BGP-4”, T. Bates et al., June 2000.
[Con35] RFC 2865, “Remote Authentication Dial In User Service (RADIUS)”, C. Rigney, June 2000.
[Con36] RFC 2866, “RADIUS Accounting”, C. Rigney, June 2000.
[Con37] RFC 2868, “RADIUS Attributes for Tunnel Protocol Support”, G. Zorn et al., June 2000.
[Con38] RFC 2869, “RADIUS Extensions”, C. Rigney et al., June 2000.
[Con39] RFC 2916, “E.164 number and DNS”, P. Faltstrom, September 2000.
[Con40] RFC 2937, “The Name Service Search Option for DHCP”, C. Smith, September 2000.
[Con41] RFC 2976, “The SIP INFO Method”, S. Donovan, October 2000.
[Con42] RFC 3004, “The User Class Option for DHCP”, G. Stump, November 2000.
[Con43] RFC 3011, “The IPv4 Subnet Selection Option for DHCP”, G. Waters, November 2000.
[Con44] RFC 3016, "RTP Payload Format for MPEG-4 Audio/Visual Streams", Y. Kikuchi et al. , November 2000.
[Con45] RFC 3046, “DHCP Relay Agent Information Option”, M. Patrick, January 2001.
[Con46] RFC 3074, “DHC Load Balancing Algorithm”, B. Volz et al., February 2001.
[Con47] RFC 3118, “Authentication for DHCP Messages”, R. Droms et al., June 2001.
[Con48] RFC 3148, “A Framework for Defining Empirical Bulk Transfer Capacity Metrics”, M. Mathis et al., July 2001.
[Con49] RFC 3203, “DHCP reconfigure extension”, Y. T'Joens et al., December 2001.
[Con50] RFC 3261, “SIP: Session Initiation Protocol”, J. Rosenberg et al., June 2002.
[Con51] RFC 3262, “Reliability of Provisional Responses in the Session Initiation Protocol (SIP)”, J. Rosenberg et al., June 2002.
[Con52] RFC 3263, “Session Initiation Protocol (SIP): Locating SIP Servers”, J. Rosenberg et al., June 2002.
[Con53] RFC 3311, “The Session Initiation Protocol (SIP) UPDATE Method”, J. Rosenberg, September 2002.
[Con54] RFC 3315, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, R. Droms et al., July 2003.

[Con55] RFC 3357, “One-way Loss Pattern Sample Metrics”, R. Koodli et al., August 2002.
[Con56] RFC 3376, "Internet Group Management Protocol, Version 3", B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, IETF, September 2002.
[Con57] RFC 3393, “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)”, C. Demichelis et al., November 2002.
[Con58] RFC 3396, “Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)”, T. Lemon et al., November 2002.
[Con59] RFC 3432, “Network performance measurement with periodic streams”, V. Raisanen et al., November 2002.
[Con60] RFC 3442, The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4”, T. Lemon et al., December 2002.
[Con61] RFC 3446, "Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP).", D. Kim, D. Meyer, H. Kilmer, D. Farinacci, IETF, January 2003.
[Con62] RFC 3527, “Link Selection sub-option for the Relay Agent Information Option for DHCPv4”, K. Kinnear et al., April 2003.
[Con63] RFC 3588, “Diameter Base Protocol”, P. Calhoun et al., September 2003.
[Con64] RFC 3589, “Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5”, J. Loughney, September 2003.
[Con65] RFC3618, "Multicast Source Discovery Protocol (MSDP)", IETF, September 2004.
[Con66] RFC 3633, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6”, O. Troan et al., December 2003.
[Con67] RFC 3646, “DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, R. Droms et al., December 2003.
[Con68] RFC 3736, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”, R. Droms, April 2004.
[Con69] RFC 3748, “Extensible Authentication Protocol (EAP)”, B. Aboba et al., June 2004.
[Con70] RFC 3763, “One-way Active Measurement Protocol (OWAMP) Requirements”, S. Shalunov et al., April 2004.
[Con71] RFC 3810, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", R. Vida, L. Costa, IETF, June 2004.
[Con72] RFC 3918 ,"Methodology for IP Multicast Benchmarking", D. Stopp et al., October 2004.
[Con73] RFC 3925, “Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)”, J. Littlefield, October 2004.
[Con74] RFC 3942, “Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options”, B. Volz, November 2004.
[Con75] RFC 3993, “Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option”, R. Johnson et al., March 2005.
[Con76] RFC 4014, “Remote Authentication Dial-In User Service (RADIUS): Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option”, R. Droms et al., February 2005.
[Con77] RFC 4030, “The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option”, M. Stapp et al., March 2005.
[Con78] RFC 4039, “Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)”, S. Park et al., March 2005.
[Con79] RFC 4148, “IP Performance Metrics (IPPM) Metrics Registry”, E. Stephan, August 2005.
[Con80] ISO/IEC JTC1/SC29/WG11N3233 , "Report on Transmission of MPEG-4 Audio over RTP", IETF, March 2000.

[Con81] draft-ietf-pim-dm-new-v2-*.txt, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", A. Adams, J. Nicholas, W. Siadack, IETF, June 2004.
[Con82] draft-ietf-pim-sm-v2-new-*.txt, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, IETF, October 2004.
[Con83] ISCP-4201, "Internet Streaming Conformance Profile: Streaming Client Document", ISMA, September 2004.
[Con84] ISCP-3101, "Internet Streaming Conformance Profile: File Streaming Server Document", ISMA, September 2004.
[Con85] ISCP-3201, "Internet Streaming Conformance Profile: Live Steaming Encoder Document", ISMA, September 2004.
[Con86] draft-ietf-sipping-torture-tests-*.txt, "Session Initiation Protocol Torture Test Messages."
[Con87] draft-ietf-sipping-pstn-call-flows-*.txt, "Session Initiation Protocol PSTN Call Flows", A. Johnston, S. Donovan, IETF, April 2003.
[Con88] draft-ietf-sipping-basic-call-flows-*.txt, "Session Initiation Protocol Basic Call Flow Examples", A. Johnston, IETF, April 2003.
[Con89] draft-ietf-sipping-service-examples-*.txt, "Session Initiation Protocol Service Examples", A. Johnston, S. Donovan, IETF, March 2003.
[Con90] ITU-T Recommendation E.800, Quality of service and dependability vocabulary, August 1994.
[Con91] draft-ietf-mboned-auto-multicast-*.txt, "IPv4 Automatic Multicast Without Explicit Tunnels (AMT)", D. Thaler et al., October 2004.
[Con92] draft-liefooghe-castgate-*.txt, "CastGate: an auto-tunneling architecture for IP Multicast", P. Liefooghe, October 2004.
[Con93] 3GPP TS 23.228 V6.6.0 (2004-06), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)
[Con94] 3GPP TS 23.060 V6.5.0 (2004-06), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 6)
[Con95] 3GPP TS 29.207 V6.1.0 (2004-09), 3rd Generation Partnership Project; Technical Specification Group Core Network; Policy control over Go interface (Release 6)
[Con96] 3GPP TS 29.209 V1.0.0 (2004-5), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network; Policy control over Gq interface (Release 6)
[Con97] draft-ietf-tcpm-tcp-roadmap-*.txt, “A Roadmap for TCP Specification Documents”, M. Duke et al., IETF, June 2005.
[Con98] TR-69: “CPE WAN Management Protocol” (May 2004).
[Con99] TR-64: “LAN-Side DSL CPE Configuration” (May 2004).
[Con100] TR-98 DSLHome™ Internet Gateway Device Version 1.1 Data Model for TR-069
[Con101] TR-104 DSLHome™ Provisioning Parameters for VoIP CPE
[Con102] TR-106 DSLHome™ Data Model Template for TR-069 Enabled Devices
[Con103] TR-110 DSLHome™ Reference Models for VoIP Configurations
[Con104] TR-133 DSLHome™ TR-064 Extensions for Service Differentiation
[Con105] TR-67v2, “ADSL Interoperability Test Plan”, Testing & Interoperability Working Group, December 2004.
[Con106] WT-123v1, “TR-069 Validation Testing Architecture”

8 CONNECTIVITY TESTING OF RESIDENTIAL GATEWAYS

This chapter will describe a test suite for testing the higher layers (not physical layer) of residential gateways. A lot of standard organisations are listing requirements for RGs, but a test suite for those requirements is not yet defined. On top of that, the listing of requirements does sometimes introduce a lot of complex tests. E.g. a requirement 'An RG must support IGMPv3' needs a lot of tests for complete compliance. This chapter will define the needed detailed test objectives following from the different requirements. The following sources/standards were used for getting the requirements.

- **Requirements from DSLforum TR-101**
  - Migration to ethernet-based DSL aggregation
  - Focused on access node and broadband network gateway
  - Some RGW requirements for multicast, OAM, VLAN
- **Requirements from DSLforum WT-124**
  - Residential gateway requirements (WAN+LAN)
  - Focused on RGW
  - TR-68v2 'Base Requirements for an ADSL Modem with Routing' must be supported: physical + L2 req. (PPPoE, ATM PVCs, ...) + some firewall req.
  - Extra IPTV req. (from WT-101) -> multicast/IGMP
  - LAN wireless req., DHCP options, security (802.1x), TR-69 stuff
- **Requirements from RFC 2236 and RFC 3376**
  - Specification of IGMPv2 and IGMPv3 Protocol
  - Split up into Multicast Socket API, Packet Formats, Protocol for Group Members and Protocol for Multicast Routers
- **Requirements from draft-ietf-magma-igmp-proxy-06.txt**
  - Describes without going into great detail the functionality of igmp proxy
  - References IGMP specifications
- **Muse TF 3 document**
  - Physical LAN/WAN
  - Data plane
  - Control plane (DHCP, PPP, IGMP, SIP, EAP)
  - Management (LAN: UPnP, TR64, WAN: ILMI, TR69, telnet, ATM/eth OAM), OSGi
  - Security (DoS, firewall, wlan)
  - IPv6 (autoconfiguration, DHCPv6)

Out of these documents, the requirements were gathered and categorized for defining the 'RG test objectives'. These are focussed on the U interface (interface between access node and RG), but e.g. also the RG as DHCP server is tested.

The following categories are envisioned to be tested (random order):

- VLAN
- Forwarding
- Ethernet aggregation & STP
- Multicasting
- QoS

- Inter-working Function (IWF)
- DHCP Processing
- PPP
- Security
- Operation and Maintenance (OAM)

Most effort has been put into multicast and dhcp test objectives and requirements. As it is best to work both on the test objectives and test methods together, this chapter contains for now only full description of the multicast and dhcp test objectives.
The test methods document mentions cross reference tables between test objectives and test methods (mostly a single test does test more test objectives, and some test objectives are tested in multiple test methods).
The test objectives are described as requirements which must or should be tested/met. Compliance is then defined if the 'must' requirements are passed.

8.1 Multicast test objectives

8.1.1 IGMPv3 Requirements

8.1.1.1 Packet Requirements

8.1.1.1.1 IGMPv3 Packet Requirements

I 1 Every IGMPv3 message is sent with IP Time-to-Live of 1.

I 2 IGMPv3 are sent with IP Precedence of Internetwork Control (Type of Service 0xC0)

I 3 IGMPv3 messages carry an IP Router Alert option it its IP header.

I 4 General Queries are sent with an IP Destination Address of the All-Systems Multicast Address (224.0.0.1).

I 5 IGMPv3 reports are sent with IP Destination of 224.0.0.22.

I 6 IGMPv3 Group-Specific and Group-and-Source-Specific Queries are sent with an IP Destination Address equal to the multicast address of interest.

I 7 An IGMPv3 implementation must not include additional octets after the source address field in a query or after the group fields in report messages, but it must include these bytes in its checksum verification.

I 8 The checksum field in Query and Report messages MUST be verified before processing a message.

I 9 If the set of Group Records required in a Report does not fit within the size limit of a single Report message (as determined by the MTU of the network on which it will be sent), the Group Records are sent in as many Report messages as needed to repot the entire set. If the record type is MODE_IS_EXCLUDE or CHANGE_TO_EXCLUDE, a record is sent containing as many source addresses as can fit and the remaining source addresses are not reported; it is preferable to report the same set of sources in each subsequent report.

I 10 Unrecognized Record Type values MUST be silently ignored.

8.1.1.1.2 IGMPv2 Packet Requirements

I 11 Every IGMPv2 message is sent with IP Time-to-Live of 1.

I 12 IGMPv2 messages carry an IP Router Alert option it its IP header.

I 13 IGMPv2 reports are sent to the multicast group specified in the Group Address field of the Report.

I 14 IGMPv2 Leave messages are sent with an IP Destination Address set to 224.0.0.2.

8.1.1.1.3 IGMPv1 Packet Requirements

I 15 Every IGMPv1 message is sent with IP Time-to-Live of 1.

I 16 IGMPv1 reports are sent to the multicast group specified in the Group Address field of the Report.

I 17 An IGMPv1 router sends General Queries with Max Resp Code set to 0. This MUST be interpreted as a value of 100 (10 seconds).

8.1.1.2 Group Member Requirements

8.1.1.2.1 Pure IGMPv3 networks

I 18 A system must maintain a multicast reception state for each of its interfaces, that state consists of a set of records of the form:

(multicast-address, filter-mode, source-list)

IGMPv3 protocol actions on an interface are only triggered if the interface reception state changes or a query was received.

I 19 A change of interface state causes the system to immediately transmit a State-Change Report from that interface. The type and contents of the Group Record(s) in that Report are determined by comparing the filter mode and source list for the affected multicast address before and after the change.

Old State	New State	State-Change Record Sent
INCLUDE(A)	INCLUDE(B)	ALLOW(B-A), BLOCK(A-B)
EXCLUDE(A)	EXCLUDE(B)	ALLOW(A-B), BLOCK(B-A)
INCLUDE(A)	EXCLUDE(B)	TO_EX(B)
EXCLUDE(A)	INCLUDE(B)	TO_IN(B)

If no “old state” existed for that multicast address it is considered to have a filter mode of INCLUDE and an empty source list.

I 20 If the computed source list for either an ALLOW or a BLOCK State-Change Record is empty, that record is omitted from the Report message.

I 21 To cover the possibility of the State-Change Report being missed by one or more multicast routers, it is retransmitted [Robustness Variable] – 1 more times, at intervals chosen at random from the range (0, [Unsolicited Report Interval]).
Default value: Robustness Variable = 2
Unsolicited Report Interval = 1 sec

I 22 If the interface state changes before all retransmissions of a previous State-Change Report have been transmitted, the content of a new report is calculated by applying

the rules in I 19 and merging this difference report with the content of the pending report:

- Each time a source is included in the difference report, its state must be retransmitted [Robustness Variable] times.
- If the difference report holds a Filter-Mode Record, then the next [Robustness Variable] State-Change Reports will include a Filter-Mode-Change Record.

These merging rules are summarized in the tables below.

Old State	New State	Actions
INCLUDE(A)	INCLUDE(B)	X = (B-A) + (X*A) [B-A] = RV Y = (A-B) + (Y-B)
EXCLUDE(A)	EXCLUDE(B)	X = (A-B)+(X-B) [A-B] = RV Y = (B-A) + (Y*B) [B-A] = RV
INCLUDE(A)	EXCLUDE(B)	X = (Y-B) + (X-B) [Y-B] = RV Y = A*B + Y*B [A*B] = RV SendFilterModeChange = RV
EXCLUDE(A)	INCLUDE(B)	X = (A*B) + (X*B) [A*B] = RV Y = (X-B) + (Y-B) [X-B] = RV SendFilterModeChange = RV

Current State	SendFilterModeChange	State-Change Record Sent
INCLUDE(A)	> 0	TO_IN(A)
INCLUDE(A)	0	ALLOW(X), BLOCK(Y)
EXCLUDE(A)	> 0	TO_EX(A)
EXCLUDE(A)	0	ALLOW(X), BLOCK(Y)

I 23 When a system receives a Query, it does not respond immediately. Instead, it delays its response by a random amount of time, bounded by the Max Resp Time value derived from the Max Resp Code in the received Query Message.

I 24 Before scheduling a response to a Query, the system must first consider previously scheduled pending responses and in many cases schedule a combined response. When a new Query arrives on an interface, a delay for a response is randomly selected in the range (0, [Max Resp Time]). The following rules are then used to determine what kind of Report has to be scheduled.

1. If there is a pending response to a previous General Query scheduled sooner than the selected delay, no additional response needs to be scheduled.
2. If the received Query is a General Query, the interface timer is used to schedule a response to the General Query after the selected delay. Any previously pending response to a General Query is canceled.

3. If the received Query is a Group-Specific Query or a Group-and-Source-Specific Query and there is no pending response to a previous Query for this group, then the group timer is used to schedule a report. If the received query is a Group-and-Source-Specific Query, the list of queried sources is recorded to be used when generating a response.
4. If there already is a pending response to a previous Query scheduled for this group, and either the new Query is a Group-Specific Query or the recorded source-list associated with the group is empty, then the group source-list is cleared an a single response is scheduled using the group timer. The new response is scheduled to be sent at the earliest of the remaining time for the pending report and the selected delay.
5. If the received Query is a Group-and-Source-Specific Query and there is a pending response for this group with a non-empty source-list, then the group source list is augmented to contain the list of sources in the new Query and a single response is scheduled using the group timer. The new response is scheduled to be sent at the earliest of the remaining time for the pending report and the selected delay.

When a timer expires the system transmits on the associated interface one or more Report messages as follows:

1. If the expired timer is the interface timer then one Current-State Record is sent fore each multicast address for which the specified interface has reception state.
2. If the expired timer is a group timer and the list of recorded sources for that group is empty, then if and only if the interface has reception state for that group address, a single Current-State Record is sent or that address.
3. If the expired timer is a group timer and the list of recorded sources is non-empty, then if and only if the interface has reception state for that group address, the contents of the responding Current-State Records is specified in the following table:

Interface State	Set of recorded sources	Current-State Record
INCLUDE(A)	B	IS_IN(A*B)
EXCLUDE(A)	B	IS_IN(B-A)

I 25 A system MUST accept and process any query whose IP Destination Address contains *any* of the addresses (unicast or multicast) assigned to the interface on which the Query arrives.

8.1.1.2.2 Interoperation with older version of IGMP

I 26 IGMPv3 hosts MUST keep state per local interface regarding the compatibility mode of each attached network. The compatibility variable is based on whether an older version General Query was heard in the last [Older Version Querier Present Timeout] second. When a host receives a query it updates its Querier Present Timers and if needed its compatibility mode.

Host Compatibility Mode	Timer State
IGMPv3 (default)	IGMPv2 Querier Present not running and IGMPv1 Querier Present not running
IGMPv2	IGMPv2 Querier Present running and IGMPv1 Querier Present not running
IGMPv1	IGMPv1 Querier Present running

I 27 The version of IGMP a host uses MUST be equal to its Compatibility Mode.

I 28 An IGMPv3 host may be placed on a network where there are hosts that have not yet been upgraded to IGMPv3. The IGMPv3 host will respond to queries as normal and the not upgraded hosts will respond according to the IGMP version they are using.

I 29 An IGMPv3 host MAY allow its IGMPv3 Membership Report to be suppressed by either a Version 1 or a Version 2 Membership Report.

I 30 An IGMPv1 router will send General Queries with Max Resp Code set to 0. This MUST be interpreted as a value of 100 (10 seconds).

I 31 An IGMPv2 router will send General Queries with the Max Resp Code set to the desired Max Resp Time, e.g., the full range of this field is linear and the exponential algorithm is not used.

8.1.1.3 Multicast Router Requirements

8.1.1.3.1 Pure IGMPv3 networks

I 32 A Multicast Router that is also a group member performs both parts of IGMPv3, receiving an responding to its own IGMP message transmissions as well as those of its neighbors.

I 33 No IGMP messages are ever sent regarding the all-systems multicast address (224.0.0.1).

I 34 A Multicast Router MUST perform the group membership part of IGMPv3 for the multicast address 224.0.0.22.

I 35 Multicast Routers send General Queries periodically to request group membership information from an attached network.

I 36 Routers MUST accept a report with source address of 0.0.0.0, this source address may be used by systems that haven't acquired an ip address yet.

I 37 Multicast Routers keep state per group per attached network. This group state conceptually consists of a set of records of the form:

(multicast address, group timer, filter-mode, (source records)

Each source record is of the form:
(source address, source timer)

1. A source record with a running timer with a router filter-mode for the group of INCLUDE means that there is currently one or more systems which desire to receive that source. If a source timer expires with a router filter-mode for the group of INCLUDE, the router concludes that traffic from this particular source is no longer desired on the attached network, and deletes the associated source record.
2. The group timer is only used when a group is in EXCLUDE mode and it represents the time for the *filter-mode* of the group to expire and switch to INCLUDE mode. If there are any source records with source timers greater than zero a router switches to filter-mode of INCLUDE using those source records. Source records whose timers are zero are deleted.

3. Source Timers are treated differently when a router filter-mode for a group is EXCLUDE. If a source record has a running timer with a router filter-mode for the group of EXCLUDE, it means that at least one system desires the source. It should therefore be forwarded by a router on that network.

I 38 The following table describes the forwarding rules for traffic originating from a source destined to a group. It also summarizes the actions taken upon the expiration of a source timer based on the router filter-mode of the group.

Group Filter-Mode	Source Timer Value	Actions/Comments
INCLUDE	Timer > 0	Suggest to forward traffic from source.
INCLUDE	Timer = 0	Suggest to stop forwarding traffic from source and remove source record. If there are no more source records in the group, delete the group record.
INCLUDE	No source elements	Suggest not to forward source
EXCLUDE	Timer > 0	Suggest to forward traffic from source.
EXCLUDE	Timer = 0	Suggest to not forward traffic from source (DO NOT remove record)
EXCLUDE	No Source elements	Suggest to forward traffic from source

I 39 When receiving Current-State Records, a router updates both its group and source timers. The table below describes the actions, with respect to state and timers that occur to a router's state upon reception of Current-State Records.

Router State	Report Received	New Router State	Actions
INCLUDE(A)	IS_IN(B)	INCLUDE(A+B)	(B)=GMI
INCLUDE(A)	IS_EX(B)	EXCLUDE(A*B,B-A)	(B-A)=0 Delete (A-B) Group Timer=GMI
EXCLUDE(X,Y)	IS_IN(A)	EXCLUDE(X+A,Y-A)	(A)=GMI
EXCLUDE(X,Y)	IS_EX(A)	EXCLUDE(A-Y,Y*A)	(A-X-Y)=GMI Delete (X-A) Delete (Y-A) Group Timer=GMI

I 40 The following table describes the changes in group state and the action(s) taken when receiving either Filter-Mode-Change or Source-List-Change Records.

Router State	Report Received	New Router State	Actions
INCLUDE(A)	ALLOW(B)	INCLUDE(A+B)	(B)=GMI
INCLUDE(A)	BLOCK(B)	INCLUDE(A)	Send Q(G,A*B)
INCLUDE(A)	TO_EX(B)	EXCLUDE(A*B,B-A)	(B-A)=0 Delete (A-B) Send Q(G,A*B) Group Timer=GMI
INCLUDE(A)	TO_IN(B)	INCLUDE(A+B)	(B)=GMI Send Q(G,A-B)
EXCLUDE(X,Y)	ALLOW(A)	EXCLUDE(X+A,Y-A)	(A)=GMI
EXCLUDE(X,Y)	BLOCK(A)	EXCLUDE(X+(A-Y),Y)	(A-X-Y)=Group Timer

			Send Q(G, A-Y)
EXCLUDE(X,Y)	TO_EX(A)	EXCLUDE(A-Y,Y*A)	(A-X-Y)=Group Timer Delete (X-A) Delete (Y-A) Send Q(G, A-Y) Group Timer=GMI
EXCLUDE(X,Y)	TO_IN(A)	EXCLUDE(X+A,Y-A)	(A)=GMI Send Q(G,X-A) Send Q(G)

- When a table action “Send Q(G)” is encountered the group timer must be set to LMQT. The router must then immediately send a group specific query, if the group timer was larger then LMQT, the “Suppress Router-Side Processing” bit is set. The router must also schedule [Last Member Query Count – 1] query retransmissions to be sent every [Las Member Query Interval] over [Last Member Query Timer].
- When a table action “Send Q(G, X)” is encountered the source timer for each of the sources in X of group G with source timer larger then LMQT is lowered to LMQT and [Last Member Query Count] retransmissions for this source are scheduled.
  The router must then immediately send a group and source specific query as well as schedule [Last Member Query Count - 1] query retransmissions to be sent every [Last Member Query Interval] over [Last Member Query Time].

I 41 When building a group and source specific query for a group G, two separate query messages are sent for the group. The first one has the "Suppress Router-Side Processing" bit set and contains all the sources with retransmission state and timers greater than LMQT. The second has the "Suppress Router-Side Processing" bit clear and contains all the sources with retransmission state and timers lower or equal to LMQT. If either of the two calculated messages does not contain any sources, then its transmission is suppressed.

I 42 If a group specific query is scheduled to be transmitted at the same time as a group and source specific query for the same group, then transmission of the group and source specific message with the "Suppress Router-Side Processing" bit set may be suppressed.

I 43 When a router sends or receives a query with a clear Suppress Router-Side Processing flag, it must update its timers to reflect the correct timeout values for the group or sources being queried.

Query	Action
Q(G, A)	Source Timer for sources in A are lowered to LMQT
Q(G)	Group Timer is lowered to LMQT

When a router sends or receives a query with the Suppress Router-Side Processing flag set, it will not update its timers.

I 44 When a router receives a query with a lower IP address, it sets the Other-Querier-Present timer to Other Querier Present Interval and ceases to send queries on the network if it was the previously elected querier. After its Other-Querier Present timer expires, it becomes the elected querier and begins sending General Queries again.

8.1.1.3.2 Interoperation with older versions of IGMP

I 45 If an IGMPv3 router is placed in a network where at least one router has not yet been upgraded to IGMPv3, the IGMPv3 router must be configured to use the lowest version of IGMP present on the network. If a router is not explicitly configured to use IGMPv1 or IGMPv2 and hears an IGMPv1 Query or IGMPv2 General Query it should log a warning.

I 46 When in IGMPv1 mode, routers MUST send Periodic Queries with a Max Resp Code of 0 and truncated at the Group Address field. They must ignore Leave Group Messages.

I 47 When in IGMPv2 mode, routers MUST send Periodic Queries truncated at the Group Address Field.

I 48 In order to be compatible with older version hosts, IGMPv3 routers MUST operate in version 1 and version 2 compatibility modes. IGMPv3 routers keep a compatibility mode per group record. If an older Membership Report is received the group compatibility mode is changed to the version of the received report. In order to switch gracefully between versions of IGMP, routers keep an IGMPv1 Host Present timer and an IGMPv2 Host Present Timer per group record. When a timer expires, a router switches back to the appropriate IGMP version.

Group Compatibility Mode	Timer State
IGMPv3 (default)	IGMPv2 Host Present not running and IGMPv1 Host Present not running
IGMPv2	IGMPv2 Host Present running and IGMPv1 Host Present not running
IGMPv1	IGMPv1 Host Present running

I 49 When Group Compatibility Mode is IGMPv2, a router internally translates the following IGMPv2 messages for that group to their IGMPv3 equivalents:

IGMPv2 Message	IGMPv3 Equivalent
Report	IS_EX({})
Leave	TO_IN({})

IGMPv3 BLOCK messages are ignored, as are source-lists in TO_EX() messages(i.e., any TO_EX() message is treated as TO_EX({})).

I 50 When a Group Compatibility Mode is IGMPv1, a router internally translates the following IGMPv1 and IGMPv2 messages for that group to their IGMPv3 equivalents:

IGMP Message	IGMPv3 Equivalent
v1 Report	IS_EX({})
v2 Report	IS_EX({})

In addition to ignoring IGMPv3 BLOCK messages and source lists in TO_EX() messages as in IGMPv2 Group Compatibility Mode, IGMPv2 Leave messages and IGMPv3 TO_IN() messages are also ignored.

8.1.2 IGMPv3-Proxy Requirements

IP 1 An igmp proxy device has a single upstream and one or more downstream interfaces. These designations are explicitly configured.

IP 2 An igmp proxy device performs the router portion of the IGMP protocol on its downstream interfaces and the host portion of IGMP on its upstream interfaces.

IP 3 The igmp proxy device MUST NOT perform the router portion of IGMP on its upstream interface.

IP 4 The proxy device maintains a set of subscriptions on each downstream interface. The subscriptions on each downstream interface are merged into the membership database. If some subscriptions are IGMPv1 or IGMPv2 subscriptions, these subscriptions are converted to IGMPv3 subscriptions.

IP 5 The merging of subscriptions is performed using the same rules for merging socket states to interface states. For every multicast address a list is build of all records holding state information for this multicast address.

- If *any* such record has a filter mode of EXCLUDE, then the filter mode of the interface record is the intersection of the source lists of all socket records in EXCLUDE mode, minus the source addresses that appear in any socket record in INCLUDE mode.
- If *all* such records have a filter mode of INCLUDE, then the filter mode of the interface record is INCLUDE, and the source list of the interface record is the union of the source lists of all the socket records.

IP 6 When a proxy device receives a packet destined for a multicast group, it uses a list consisting of the upstream interface and any downstream which has a subscription pertaining to this packet and on which it is the IGMP Querier. It removes the interface on which this packet arrived from the list and forwards the packet to the remaining interfaces.

IP 7 If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will perform IGMPv1 or IGMPv2 on the upstream interface accordingly.

8.1.3 DSLForum Multicast RGW Requirements

8.1.3.1 General requirements

RG 1 The RG MUST support IGMP version 3 as per RFC 3376. [WT-101 R-191] [WT-101 R-191]

RG 2 The RG MUST support IGMP forwarding with local NAT and firewall features including establishing any pin-holes in the firewall for the multicast streams received (after join). [WT-101 R-193] [WT-124 R-44]

RG 3 All LAN ports and interfaces MUST be capable of supporting IGMP hosts. [WT-124 R-39]

RG 4 The RG MUST be capable of supporting LAN to LAN multicast on the same LAN interface and across multiple different LAN interfaces. [WT-124 R-55]

RG 5 The RG MUST be configurable as to how many simultaneous multicast streams are allowed from WAN to LAN. [WT-124 R-56]

RG 6 The RG MUST support a minimum of 32 multicast groups. [WT-124 R-47]

RG 7 The RG SHOULD support a minimum of 64 multicast groups. [WT-124 R-48]

RG 8 The RG MUST support a minimum of 64 devices per multicast group. This requirement is consistent with specification of the “source-list” for a “multicast-address” in IETF RFC 3376 defining IGMPv3. [WT-124 R-49]

8.1.3.2 Immediate Leave

RG 9 The RG MUST support IGMP immediate leave with explicit host tracking. [WT-101 R-200] [WT-124 R-46] [WT-124 R-50]

RG 10 The RG MUST have a join and leave latency less than 20 ms. [WT-124 R-45]

8.1.3.3 Upstream interfaces without an IP address

RG 11 It MUST be possible to configure an RG WAN-facing IP interface with an IPoE encapsulation and no IP address visible by the access network. [WT-101 R-233]

RG 12 The RG MUST be able to receive downstream multicast traffic on the interface described in RG 11, independent of whether upstream IGMP is sent on this interface or not. [WT-101 R-234]

RG 13 The RG IGMP Proxy-Routing function MUST be able to send upstream IGMP traffic on the interface described in RG 11, using a null (0.0.0.0) IP source address. [WT-101 R-235]

8.1.3.4 Multiple upstream interfaces

RG 14 When the RG is configured with multiple WAN-facing IP interfaces (e.g. PPP or IPoE), the IGMP Proxy-Routing function MUST be able to multicast upstream IGMP messages to all or a configured subset of those WAN interfaces. [WT-101 R-194]

RG 15 The default behavior MUST be to forward messages to all provisioned interfaces. [WT-101 R-195]

RG 16 When the RG receives an IGMP membership query on a given WAN-facing IP interface, the IGMP Proxy-Routing function MUST only send a corresponding membership report on this specific interface. [WT-101 R-196]

RG 17 The RG **MUST** use the same Ethernet MAC address for all interfaces over the same AAL5/ATM/DSL connection. [WT-124 R-38]

8.1.3.5 Filtering

RG 18 The RG SHOULD be able to classify IGMP requests according to source IP/MAC address or incoming LAN physical port on the RG to distinguish between multicast services (e.g. IPTV and some other Best Effort (BE) Internet IGMP application). [WT-101 R-197]

RG 19 The RG SHOULD be able to configure which ports are allowed to have IGMP hosts. [WT-101 R-199] [WT-124 R-40] [WT-124 R-41]

RG 20 The RG MUST have a way of suppressing the flooding of multicast on selected ports, either through dedicated ports connecting to IGMP hosts or IGMP Proxy-Routing. [WT-101 R-198]

8.1.3.6 Forwarding

RG 21 The RG MUST NOT forward UPNP multicast messages to its WAN interface. [WT-101 R-201]

RG 22 The RG **MUST** be configurable to prevent sending IGMP messages to the WAN interfaces for specified multicast groups or ranges (such as 239.0.0.0 through

239.255.255.255, which are limited scope or administratively scoped addresses). [WT-124 R-42]

RG 23 The RG **MUST** default to not sending IGMP messages for 239.0.0.0 through 239.255.255.255 to the WAN interfaces. [WT-124 R-43]

8.2 DHCP test objectives

8.2.1 Sources

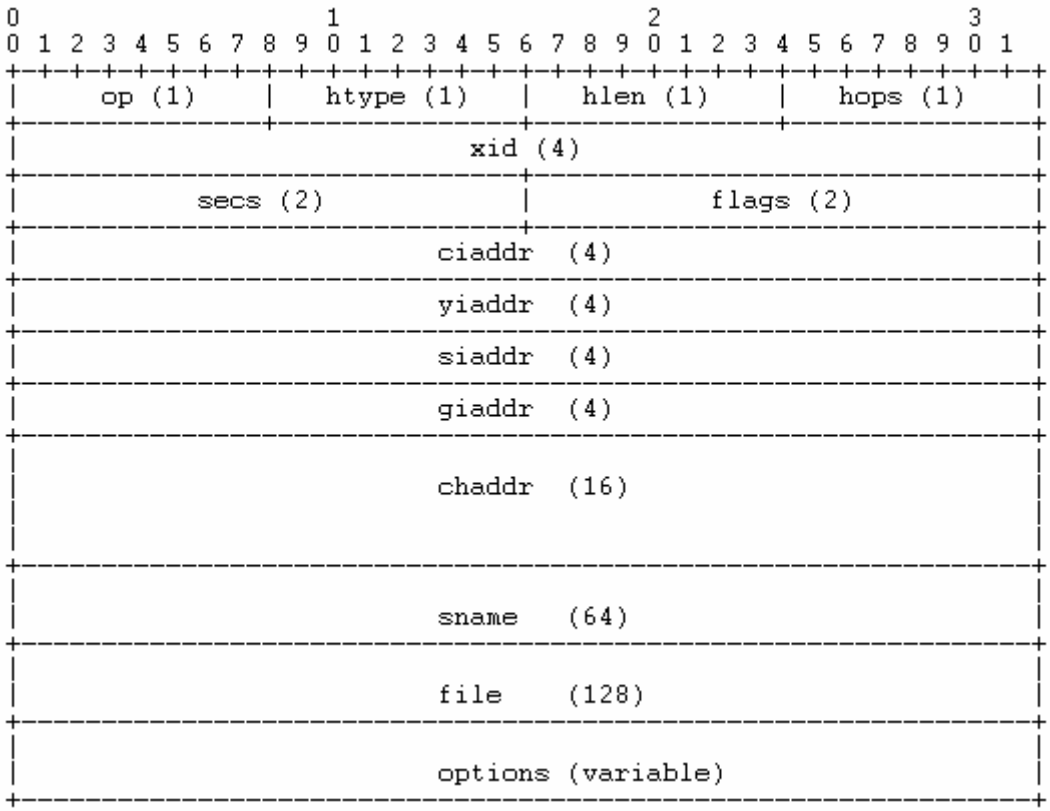
RFC 1532	Clarification and Extensions for the Bootstrap Protocol
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DHCP Options and BOOTP Vendor Extensions
Draft-ietf-dhc-emplementation-02	Implementation Issues with RFC 2131
RFC 3046	DHCP Relay Agent Information Option
RFC 3442	The Classless Static Route Option for DHCPv4

The following assumptions were made in this document:

1. The DHCP server is listening for DHCP messages on only one interface and serves one subnet.

8.2.2 Message requirements

8.2.2.1 DHCP Header



8.2.2.2 DHCP Header Requirements

R 1 DHCP uses UDP as its transport protocol. DHCP messages from a client to a server are sent to the 'DHCP server' port (67), and DHCP messages from a server to a client

are sent to the 'DHCP client' port (68). If 'giaddr' is non-zero DHCP messages from the server are sent to the DHCP relay agent on port 67.

R 2 NEW: The minimum size of a DHCP frame is 300 octets.

R 3 DHCP messages broadcasted by a client prior to that client obtaining its IP address MUST have the source address field in the IP header set to 0.0.0.0.

R 4 The length of 'chaddr' SHOULD be exactly specified by 'hlen', which SHOULD match the address length for 'htype'.

R 5 NEW: An htype of zero SHOULD be used to mean that 'chaddr' is an identifier unrelated to a specific link-level medium.

R 6 If the 'giaddr' field in a DHCP message from a client is non-zero, the server sends any return message to the 'DHCP server' port on the BOOTP relay agent whose address appears in 'giaddr'.

R 7 If the 'giaddr' field is zero and the 'ciaddr' field is nonzero, then the server unicasts return messages to the address in 'ciaddr'.

R 8 If 'giaddr' is zero and 'ciaddr' is zero, and the broadcast bit is set, then the server broadcasts return messages to 255.255.255.255.

R 9 If 'giaddr' is zero and 'ciaddr' is zero, and the broadcast bit is not set, then the server unicasts return messages to the client's hardware address and 'yiaddr' address.

R 10 The 'op' field of each DHCP message sent from client to server contains the value 1 (BOOTREQUEST). Value 2 (BOOTREPLY) is used for DHCP messages sent from server to client.

R 11 The 'DHCP message type' option MUST be included in every DHCP message.

8.2.2.3 Options field

R 12 The first four octets of the 'options' field of the DHCP message contain the (decimal) values 99, 130, 83, 99.

R 13 The 'options' field is variable in length. A DHCP client MUST be prepared to receive messages with an 'options' field of at least 312 octets. DHCP clients MAY negotiate the use of larger DHCP messages through the 'maximum DHCP message size' option.

R 14 The last option MUST always be the 'end' option and MAY contain one or more 'pad' options to fill the options field.

R 15 The values to be passed in an 'option' tag may be too long to fit in the 255 octets available to a single option. Unless otherwise specified, options may appear only once. The client concatenates the values of multiple instances of the same option into a single parameter list for configuration.

Option overloading

R 16 When an 'option overload' option is present in the 'options' field, the options in the 'options' field MUST still be terminated by an 'end' option and MAY contain one or more 'pad' options to fill the options field.

R 17 If there is not enough room in the 'options' field the client may use the 'sname' and 'file' fields to store more options. The client MUST then insert an 'option overload' option in the 'options' field, indication which additions fields are being used ('file', 'sname' or both).

R 18 If the 'option overload' option is present in the 'options' field, the options in the 'options' field MUST be terminated by an 'end' option, and MAY contain one or more 'pad' options to fill the options field.

R 19 The options in the 'sname' and 'file' fields (if present) MUST begin with the first octet of the field, MUST be terminated by an 'end' option, and MUST be followed by 'pad' options to fill the remainder of the field.

R 20 Any individual option in the 'options', 'sname' and 'file' fields MUST be entirely contained in that field.

R 21 The options in the 'options' field MUST be interpreted first, so that any 'option overload' option may be interpreted. The 'file' field MUST be interpreted next (if present), followed by the 'sname' field.

8.2.2.4 DHCP Message Types

8.2.2.4.1 DHCPDISCOVER message

This message is sent by the client to locate available DHCP servers.

Header Requirements:

R 22 DHCPDISCOVER messages are broadcasted to the 255.255.255.255 IP broadcast address.

R 23 DHCPDISCOVER messages MUST have the source address field in the IP header set to 0.0.0.0.

R 24 The value of the 'secs' field is set to the number of seconds passed since the DHCP process started.

R 25 The value of the 'ciaddr' , 'yiaddr' and 'siaddr' fields in the DHCP header MUST be zero.

R 26 A non-zero 'giaddr' field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 27 The client MUST include its hardware address in the 'chaddr' field of the DHCP header.

R 28 The client inserts a random transaction identifier into the 'xid' field.

Option Requirements:

R 29 The DHCPDISCOVER message MUST include a 'DHCP message type' option with value 1.

R 30 The client MAY suggest a network address and/or lease time by including the 'requested IP address' and 'IP address lease time' options.

R 31 A DHCPDISCOVER message MAY include a 'Client identifier' option.

R 32 A DHCPDISCOVER message MAY include a ‘Vendor class identifier’ option.

R 33 A DHCPDISCOVER message MUST NOT include a ‘Server identifier’ option.

R 34 The client MAY request specific parameters by including the ‘parameter request list’ option.

R 35 A DHCPDISCOVER message MAY include a ‘Maximum message size’ option.

R 36 A DHCPDISCOVER message SHOULD NOT include a ‘Message’ option.

R 37 Other options representing “hints” at configuration parameters are allowed.

8.2.2.4.2 DHCPOFFER message

Each server may respond to a DHCPDISCOVER message with a DHCPOFFER message that includes an available network address and other configuration parameters.

Header Requirements:

R 38 If the ‘giaddr’ field in the DHCPDISCOVER message from a client is non-zero, the server sends the DHCPOFFER message to the ‘DHCP server’ port on the BOOTP relay agent whose address appears in ‘giaddr’.

R 39 If the ‘giaddr’ field is zero and the ‘ciaddr’ field is nonzero, then the server unicasts DHCPOFFER messages to the address in ‘ciaddr’ (PROBLEM: is this possible ?).

R 40 If ‘giaddr’ is zero and ‘ciaddr’ is zero, and the broadcast bit is set, then the server broadcasts DHCPOFFER messages to 255.255.255.255.

R 41 If ‘giaddr’ is zero and ‘ciaddr’ is zero, and the broadcast bit is not set, then the server unicasts DHCPOFFER messages to the client’s hardware address and ‘yiaddr’ address.

R 42 The transaction identifier must be set into the ‘xid’ field of the DHCP header and MUST match the ‘xid’ of the most recent DHCPDISCOVER message.

R 43 The DHCPOFFER message includes an available network address in the ‘yiaddr’ field, other configuration parameters are set in the option field.

R 44 The value of the ‘siaddr’ must be the IP address of the next server to be used in the bootprocess.

R 45 The value of the ‘secs’ and ‘ciaddr’ fields in the DHCP header MUST be zero.

R 46 The server copies the values of the ‘flags’, ‘giaddr’, and ‘chaddr’ fields from the DHCPDISCOVER messages and includes them in the DHCPOFFER message.

Option Requirements:

R 47 A DHCPOFFER message MUST include a ‘DHCP message type’ option with value 2.

R 48 A DHCPOFFER message MUST NOT include a ‘Requested IP address’ option.

R 49 A DHCPOFFER message MUST include an ‘IP address lease time’ option.

R 50 A DHCPOFFER message MUST NOT include a ‘Parameter request list’ option.

R 51 A DHCPOFFER message SHOULD include a ‘Message’ option.

R 52 A DHCPOFFER message MUST NOT include a ‘Client identifier’ option. (NEW: change to MAY)

R 53 A DHCPOFFER message MAY include a ‘Vendor class identifier’ option.

R 54 A DHCPOFFER message MUST include a ‘Server identifier’ option.

R 55 A DHCPOFFER message MUST NOT include a ‘Maximum message size’ option.

R 56 A DHCPOFFER message MAY include other options.

Problem: does broadcasting to IP address 255.255.255.255 mean that the hardware address must be ff:ff:ff:ff:ff:ff (linux DHCP server uses hardware address of client)

8.2.2.4.3 DHCPREQUEST message

8.2.2.4.3.1 DHCPREQUEST generated during SELECING state

DHCPREQUEST message from a client in response to a DHCPOFFER message from a server.

Header Requirements:

R 57 DHCPREQUEST messages are broadcasted using the 255.255.55.255 IP broadcast address.

R 58 DHCP messages broadcast by a client prior to that client obtaining its IP address must have the source address field in the IP header set to 0.

R 59 The transaction identifier must be set into the ‘xid’ field of the DHCP header and MUST match the ‘xid’ of the DHCPOFFER message.

R 60 The value of the ‘secs’ field is set to the number of seconds passed since the DHCP process started. To help relay agents, the DHCPREQUEST message MUST use the same value in the DHCP message header’s ‘secs’ field as the original DHCPDISCOVER message.

R 61 The Broadcast flag MUST be set if the client requires a broadcasted reply.

R 62 The value of the ‘ciaddr’, ‘yiaddr’ and ‘siaddr’ fields in the DHCP header MUST be zero.

R 63 A non-zero ‘giaddr’ field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 64 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header. The value MUST NOT change from DHCPDISCOVER to DHCPREQUEST.

Option Requirements:

R 65 The DHCPREQUEST message MUST include a ‘DHCP message type’ option with value 3.

R 66 The DHCPREQUEST message MUST include the ‘server identifier’ option to indicate which server it has selected.

R 67 The DHCPREQUEST message MUST include the ‘requested IP address’ option, it MUST be set to the value of ‘yiaddr’ in the DHCPOFFER message from the server.

R 68 The DHCPREQUEST message MAY include the ‘IP address lease time’ options.

R 69 The DHCPREQUEST message MUST include the ‘Client identifier’ option if it was previously included in the DHCPDISCOVER message.

R 70 The DHCPREQUEST message MAY include the ‘Vendor class identifier’ option.

R 71 If the client includes a list of parameters in a DHCPDISCOVER message, it MUST include that list in any subsequent DHCPREQUEST message.

R 72 The DHCPREQUEST message MAY include the ‘Maximum message size’ option.

R 73 The DHCPREQUEST message SHOULD NOT include the ‘Message’ option.

Note: The DHCP protocol doesn’t require the client to copy values of the options received in the DHCPOFFER message. It isn’t clear if the client MAY change values to indicate values it prefers.

8.2.2.4.3.2 DHCPREQUEST generated during INIT-REBOOT state

DHCPREQUEST message from a client verifying a previously allocated IP address.

Header Requirements:

R 74 The clients broadcasts this message using the 255.255.255.255 IP broadcast address.

R 75 The value of the ‘ciaddr’, ‘yiaddr’ and ‘siaddr’ fields in the DHCP header MUST be zero.

R 76 A non-zero ‘giaddr’ field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 77 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

R 78 The client inserts a random transaction identifier into the ‘xid’ field.

R 79 The value of the ‘secs’ field is set to the number of seconds passed since the DHCP process started.

Option Requirements:

R 80 The DHCPREQUEST message MUST include a ‘DHCP message type’ option with value 3.

R 81 If the client used a ‘client identifier’ to obtain its address, the client MUST use the same ‘client identifier’ in the DHCPREQUEST message.

R 82 The ‘server identifier’ option MUST NOT be filled in.

R 83 The ‘requested IP address’ option MUST be filed in with client’s notion of its previously assigned address.

R 84 The client MAY request specific configuration parameters by including the ‘parameter request list’ option.

R 85 The DHCPREQUEST message MAY include a ‘Vendor class identifier’ option.

R 86 The DHCPREQUEST message MAY include a ‘Maximum message size’ option.

R 87 The DHCPREQUEST message SHOULD NOT include a ‘Message’ option.

R 88 Other options representing “hints” at configuration parameters are allowed.

8.2.2.4.3.3 DHCPREQUEST generated during RENEWING state

The client tries to extend the lease on a network address by contacting the server that originally issued the client’s network address.

Header Requirements:

R 89 This DHCPREQUEST message is unicasted, therefore the ‘giaddr’ field is not filled in.

R 90 The ‘flags’ field MUST be zero.

R 91 The ‘ciaddr’ field of the DHCP header MUST be filled in with the client’s IP address.

R 92 The value of the ‘yiaddr’, ‘siaddr’ and ‘giaddr’ fields in the DHCP header MUST be zero.

R 93 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

Option Requirements:

R 94 The DHCPREQUEST message MUST include a ‘DHCP message type’ option with value 3.

R 95 The ‘server identifier’ option MUST NOT be filled in.

R 96 The ‘requested IP address’ option MUST NOT be filled in.

R 97 This type of DHCPREQUEST message MUST include the ‘Client identifier’ option if it was previously included in the DHCPDISCOVER message.

R 98 If the client includes a list of parameters in a DHCPDISCOVER message, it MUST include that list in any subsequent DHCPREQUEST message.

R 99 This type of DHCPREQUEST message SHOULD NOT include a ‘Message’ option.

8.2.2.4.3.4 DHCPREQUEST generated during REBINDING state

The client attempts to extend the lease on a network address by contacting any DHCP server.

Header Requirements:

R 100 This DHCPREQUEST message is broadcasted to the 255.255.255.255 IP broadcast address.

R 101 The ‘ciaddr’ field of the DHCP header MUST be filled in with the client’s IP address.

R 102 The value of the ‘yiaddr’ and‘siaddr’ fields in the DHCP header MUST be zero.

R 103 A non-zero ‘giaddr’ field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 104 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

Option Requirements:

R 105 The DHCPREQUEST message MUST include a ‘DHCP message type’ option with value 3.

R 106 The ‘server identifier’ option MUST NOT be filled in.

R 107 The ‘requested IP address’ option MUST NOT be filled in.

R 108 The DHCPREQUEST message MUST include the ‘Client identifier’ option if it was previously included in the DHCPDISCOVER message.

R 109 If the client includes a list of parameters in a DHCPDISCOVER message, it MUST include that list in any subsequent DHCPREQUEST message.

8.2.2.4.4 DHCPACK message

8.2.2.4.4.1 DHCPACK generated in response to a DHCPREQUEST message

The server responds with a DHCPACK message when it commits the binding for the client to its database.

Header Requirements:

R 110 If the ‘giaddr’ field in a DHCPREQUEST message from a client is non-zero, the server sends the DHCPACK message to the ‘DHCP server’ port on the BOOTP relay agent whose address appears in ‘giaddr’.

R 111 If the ‘giaddr’ field is zero and the ‘ciaddr’ field is nonzero, then the server unicasts DHCPOFFER messages to the address in ‘ciaddr’.

R 112 If ‘giaddr’ is zero and ‘ciaddr’ is zero, and the broadcast bit is set, then the server broadcasts DHCPACK messages to 255.255.255.255.

R 113 If ‘giaddr’ is zero and ‘ciaddr’ is zero, and the broadcast bit is not set, then the server unicasts DHCPOFFER messages to the client’s hardware address and ‘yiaddr’ address.

R 114 The transaction identifier must be set into the ‘xid’ field of the DHCP header and MUST match the ‘xid’ of the DHCPREQUEST message it is responding to.

R 115 The value of the ‘secs’ field MUST be filled with zero’s.

R 116 The value of ‘siaddr’ must be the IP address of the next server to be used in the bootprocess.

R 117 The ‘yiaddr’ field in the DHCPACK message is filled in with the selected network address.

R 118 The value of the ‘ciaddr’, ‘flags’, ‘giaddr’ and ‘chaddr’ fields must be copied from the DHCPREQUEST message.

Option Requirements:

R 119 The DHCPACK message MUST include a ‘DHCP message type’ option with value 5.

R 120 The DHCPACK message MUST NOT include a ‘Requested IP address’ option.

R 121 The DHCPACK message MUST include a ‘IP address lease time’ option.

R 122 The DHCPACK message MUST NOT include a ‘Parameter request list’ option.

R 123 The DHCPACK message SHOULD include a ‘Message’ option.

R 124 The DHCPACK message MUST NOT include a ‘Client identifier’ option. (NEW: change to MAY)

R 125 The DHCPACK message MAY include a ‘Vendor class identifier’ option.

R 126 The DHCPACK message MUST include a ‘Server identifier’ option.

R 127 The DHCPACK message MUST NOT include a ‘Maximum message size’ option.

R 128 The DHCPACK message MAY include other options.

R 129 Any configuration parameters in the DHCPACK message SHOULD NOT conflict with those in the earlier DHCPOFFER message to which the client is responding.

8.2.2.4.4.2 DHCPACK generated in response to a DHCPINFORM message

Header Requirements:

R 130 If the ‘giaddr’ field in a DHCPINFORM message from a client is non-zero, the server sends the DHCPACK message to the ‘DHCP server’ port on the BOOTP relay agent whose address appears in ‘giaddr’.

R 131 If the ‘giaddr’ field is zero and the ‘ciaddr’ field is nonzero, then the server unicasts DHCPOFFER messages to the address in ‘ciaddr’.

R 132 The server SHOULD NOT fill in ‘yiaddr’.

R 133 The transaction identifier must be set into the ‘xid’ field of the DHCP header and MUST match the ‘xid’ of the DHCPINFORM message it is responding to.

R 134 NOT SURE: The value of the ‘secs’ field MUST be filled with zero’s.

R 135 NOT SURE: The value of the ‘ciaddr’, ‘flags’ and ‘chaddr’ fields must be copied from the DHCPINFORM message.

Option Requirements:
(except for the next requirement the option requirements are the same: copy R 119 - R 129)

R 136 The server MUST NOT send a lease expiration time to the client.

8.2.2.4.5 DHCPNAK message

Header Requirements:

R 137 If the 'giaddr' field in a DHCPREQUEST message from a client is non-zero, the server sends the DHCPNAK message to the 'DHCP server' port on the BOOTP relay agent whose address appears in 'giaddr' and it MUST set the broadcast flag so that the relay agent will broadcast the DHCPNAK message to the client.

R 138 In all cases, when 'giaddr' is zero, the server MUST broadcast the DHCPNAK message to the 255.255.255.255 broadcast address because the client may not have a correct network address or subnet mask.

R 139 The transaction identifier must be set into the 'xid' field of the DHCP header and MUST match the 'xid' of the DHCPREQUEST message it is responding to.

R 140 The value of the 'secs', 'ciaddr', 'yiaddr' and 'siaddr' fields must be filled with zero's.

R 141 The value of the 'flags', 'giaddr' and 'chaddr' fields must be copied from the DHCPREQUEST message.

Option Requirements:

R 142 A DHCPNAK message MUST include a 'DHCP message type' option with value 6.

R 143 A DHCPNAK message MUST NOT include a 'Requested IP address' option.

R 144 A DHCPNAK message MUST NOT include an 'IP address lease time' option.

R 145 A DHCPNAK message MUST NOT include a 'Parameter request list' option.

R 146 A DHCPNAK message SHOULD include a 'Message' option.

R 147 A DHCPNAK message MAY include a 'Client Identifier' option.

R 148 A DHCPNAK message MAY include a 'Vendor class identifier' option.

R 149 A DHCPNAK message MUST include a 'Server identifier' option.

R 150 A DHCPNAK message MUST NOT include a 'Maximum message size' option.

R 151 A DHCPNAK message MUST NOT include any other option.

8.2.2.4.6 DHCPDECLINE message

The client sends a DHCPDECLINE message when the client discovered that the suggested network address is already in use.

Header Requirements:

R 152 The DHCPDECLINE message is broadcasted to the 255.255.255.255 IP broadcast address.

R 153 The client inserts a random transaction identifier into the 'xid' field.

R 154 The 'secs', 'flags', 'ciaddr', 'yiaddr' and 'siaddr' fields are filled with zeros.

R 155 A non-zero 'giaddr' field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 156 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

Option Requirements:

R 157 A DHCPDECLINE message MUST include a ‘DHCP message type’ option with value 4.

R 158 A DHCPDECLINE message MUST include a ‘Requested IP address” options, the value for this option MUST be set to the IP address being declined.

R 159 A DHCPDECLINE message MUST NOT include a ‘IP address lease time’ option.

R 160 A DHCPDECLINE message MUST include the ‘Client identifier’ option if it was previously included in the DHCPDISCOVER message.

R 161 A DHCPDECLINE message MUST NOT include a ‘Vendor class identifier’ option.

R 162 A DHCPDECLINE message MUST include a ‘Server Identifier’ option.

R 163 A DHCPDECLINE message MUST NOT include a ‘Parameter request list’ option.

R 164 A DHCPDECLINE message MUST NOT include a ‘Maximum message size’ option.

R 165 A DHCPDECLINE message SHOULD include a ‘Message’ option.

R 166 A DHCPDECLINE message MUST NOT include any other option.

8.2.2.4.7 DHCPRELEASE message

The client may relinquish its lease on a network address by sending a DHCPRELEASE message to the server.

Header Requirements:

R 167 The client identifies the lease to be released with its ‘client identifier’, or ‘chaddr’ and network address in the DHCPRELEASE message. If the client used a ‘client identifier’ when it obtained the lease, it MUST use the same ‘client identifier’ in the DCHPRELEASE message.

R 168 The client inserts a random transaction identifier into the ‘xid’ field (NEW: could change to “xid from server DHCPACK message”).

R 169 The ‘secs’, ‘flags’, ‘yiaddr’, ‘siaddr’ and ‘giaddr’ fields are filled with zeros.

R 170 The client’s network address is included in the ‘ciaddr’ field of the DHCPRELEASE message.

R 171 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

Option Requirements:

R 172 A DHCPRELEASE message MUST include a ‘DHCP message type’ option with value 7.

R 173 A DHCPRELEASE message MUST NOT include a ‘Requested IP address’ option.

R 174 A DHCPRELEASE message MUST NOT include an ‘IP address lease time’ option.

R 175 A DHCPRELEASE message MAY include a ‘Client identifier’ option. (NEW: could change to MUST be the client identifier used in the DHCPDISCOVER message)

R 176 A DHCPRELEASE message MUST NOT include a ‘Vendor class identifier’ option.

R 177 A DHCPRELEASE message MUST include a ‘Server Identifier’ option.

R 178 A DHCPRELEASE message MUST NOT include a ‘Parameter request list’ option.

R 179 A DHCPRELEASE message MUST NOT include a ‘Maximum message size’ option.

R 180 A DHCPRELEASE message SHOULD include a ‘Message’ option.

R 181 A DHCPRELEASE message MUST NOT include a ‘Site-specific’ option.

R 182 A DHCPRELEASE message MUST NOT include any other option.

Note: We assume that DHCPRELEASE messages are not intended to be broadcasted, just as the client unicasts a DHCPREQUEST message to the server when the client tries to renew its lease. (+ read section 4.4.6; they write that the server sends a DHCPRELEASE message to the server)

8.2.2.4.8 DHCPINFORM message

If a client obtained a network address through some other means, the client may use a DHCPINFORM request message to obtain other local configuration parameters.

Header Requirements:

R 183 The client unicasts the DHCPINFORM message if it knows the server’s address, otherwise it broadcasts the message to the 255.255.255.255 broadcast address.

R 184 DHCPINFORM messages MUST be directed to the ‘DHCP server’ UDP port.

R 185 The client inserts a random transaction identifier into the ‘xid’ field.

R 186 The Broadcast flag MUST be set if the client requires a broadcasted reply.

R 187 The value of the ‘ciaddr’ fields contains the client’s network address.

R 188 The ‘yiaddr’ and ‘siaddr’ fields are filled with zeros.

R 189 A non-zero ‘giaddr’ field indicates that a DHCP Relay Agent is present, only the relay agent is allowed to insert a value in this field. A DHCP Client must set it to zero.

R 190 The client MUST include its hardware address in the ‘chaddr’ field of the DHCP header.

Option Requirements:

R 191 A DHCPINFORM message MUST include a ‘DHCP message type’ option with value 8.

R 192 A DHCPINFORM message MUST NOT include a ‘Requested IP address’ option.

R 193 A DHCPINFORM message MUST NOT include an ‘IP address lease time’ option.

R 194 A DHCPINFORM message MAY include a ‘Client Identifier’ option.

R 195 A DHCPINFORM message MAY include a ‘Vendor class identifier’ option.

R 196 A DHCPINFORM message MUST NOT include a ‘Server identifier’ option.

R 197 A DHCPINFORM message MAY include a ‘Parameter request list’ option.

R 198 A DHCPINFORM message MAY include a ‘Maximum message size’ option.

R 199 A DHCPINFORM message SHOULD NOT include a ‘Message’ option.

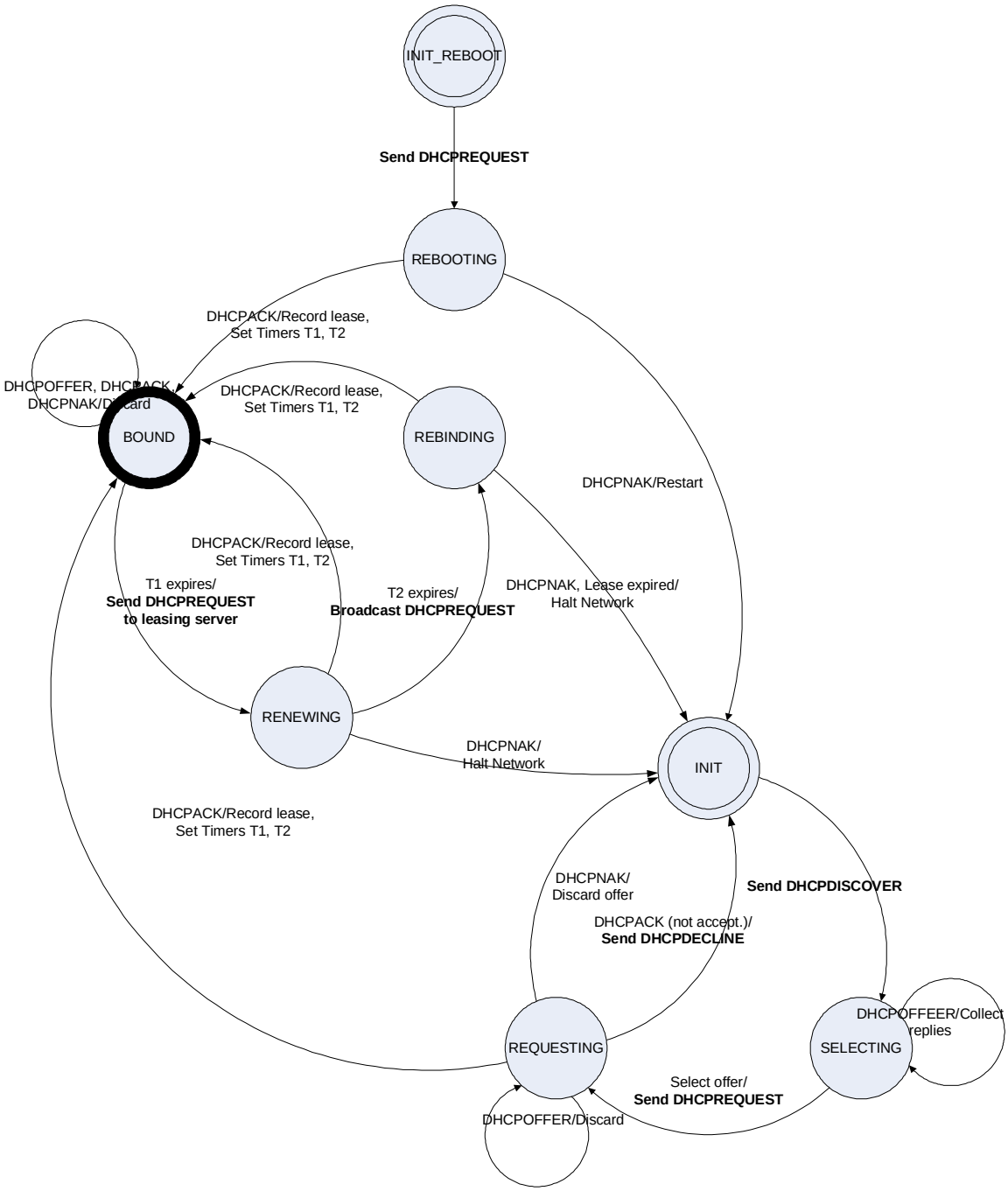
R 200 A DHCPINFORM message MAY include a ‘Site-specific’ option.

R 201 A DHCPINFORM message MAY include other options.

8.2.3 Client Requirements

8.2.3.1 State-transition diagram for DHCP clients

A DHCP client can start in the INIT state or in the INIT_REBOOT state depending on whether it is trying to acquire an address or is trying to verify a previously allocated address.



8.2.3.2 Reduction of DHCP Client parameters

R 202 Most of the parameters have default values defined in the Host Requirements RFCs; if the client receives no parameters from the server that override the defaults, a client uses the default values.

R 203 In its initial DHCPDISCOVER or DHCPREQUEST message, a client may provide the server with a list of parameters the client is interested in.

8.2.3.3 Message Retransmission (responsibility of the client)

R 204 The client MUST adopt a retransmission strategy that incorporates a randomized exponential back off algorithm to determine the delay between retransmissions.

R 205 A client MAY choose to reuse the same 'xid' or select a new 'xid' for each retransmitted message.

Example for a 10Mb/s Ethernet network

- The delay for the first retransmission SHOULD be 4 seconds randomized by the value of a uniform random number chosen from the range -1 to +1.
- The delay before the next retransmission SHOULD be 8 seconds again randomized by the value of a uniform random number chosen from the range -1 to +1.
- The retransmission delay SHOULD be doubled with subsequent retransmissions up to a maximum of 64 seconds.

8.2.3.4 Allocation of network address

The client begins in the INIT state.

8.2.3.4.1 Actions in the INIT state

R 206 The client SHOULD wait a random time between one and ten seconds to desynchronize the use of DHCP at startup. (e.g. at a power failure)

R 207 The client generates and records a random transaction identifier and inserts that identifier into the 'xid' field.

R 208 The client records its own local time for later use in computing the lease expiration.

R 209 The client forms and sends a DHCPDISCOVER message as specified in 8.2.2.4.1.

8.2.3.4.2 Actions in the SELECTING state

R 210 The DHCP client MAY wait for multiple responses (DHCPOFFER) and choose one server from which to request configuration parameters. The time over which the client collects messages and the mechanism used to select one DHCPOFFER message are implementation specific.

R 211 If the 'xid' of the arriving DHCPOFFER message does not match the 'xid' of the most recent DHCPDISCOVER message, the DHCPOFFER message MUST be silently discarded.

R 212 The client extracts the server address from the 'server identifier' option in the selected DHCPOFFER message.

R 213 Any arriving DHCPACK message MUST be silently discarded.

R 214 The client broadcasts a DHCPREQUEST message as specified in 8.2.2.4.3.1 (DHCPREQUEST generated in SELECTING state).

8.2.3.4.3 Actions in the REQUESTING state

R 215 The client waits for a DCHPACK or DHCPNAK message from the server before proceeding.

R 216 The client SHOULD use the parameters in the DHCPACK message for configuration.

R 217 The client times out and retransmits the DHCPREQUEST message if the client receives neither a DCHPACK or a DHCPNAK message. The client retransmits according to the algorithm described in 8.2.3.3. If the client receives neither a DHCPACK or a DHCPNAK message after employing the retransmission algorithm, the client reverts to INIT state and restarts the initialization process.

R 218 If the client receives a DHCPNAK message, the client restarts the configuration process and jumps to the INIT state.

R 219 The client records the lease expiration time as the sum of the time at which the original request was sent and the duration of the lease from the DHCPACK message (after DCHPACK ?).

R 220 The client SHOULD perform a check on the suggested address (and other parameters if needed) to ensure that the address is not already in use (after DCHPACK ?) (NEW: could change to MUST).

R 221 If the network supports ARP, the client may issue an ARP request to check if the address is not already in use. The client MUST fill in its own hardware address as the sender's hardware address and 0.0.0.0 as the sender's IP address.

R 222 If the network address appears to be in use, the client MUST send a DHCPDECLINE message. The client SHOULD wait a minimum of 10 seconds before restarting the configuration process and jumping to the INIT state to avoid excessive network traffic in case of looping.

R 223 The client SHOULD broadcast an ARP reply to announce the client's new IP address and clear any outdated ARP cache entries in hosts on the client's subnet.

8.2.3.5 Initializing with known network address

The client begins in the INIT-REBOOT state.

8.2.3.5.1 Actions in the INIT_REBOOT state

R 224 The client SHOULD wait a random time between one and ten seconds to desynchronize the use of DHCP at startup. (e.g. at a power failure)

R 225 The client records its own local time for later use in computing the lease time.

R 226 The client generates and records a random transaction identifier to be inserted in the 'xid' field.

R 227 The client sends a DHCPREQUEST message as specified in 8.2.2.4.3.2 (DHCPREQUEST generated during INIT-REBOOT state).

8.2.3.5.2 Actions in the REBOOTING state

R 228 The client waits for a DHCPACK message with a 'xid' field matching that the recorded value.

R 229 The client performs a final check on the parameters and notes the duration of the lease specified in the DHCPACK message as in 8.2.3.4.3 and send a DHCPDECLINE message if needed.

Problem: what should it check?

R 230 The client SHOULD use the parameters in the DHCPACK message for configuration.

R 231 The client records the lease expiration time as the sum of the time at which the DHCPREQUEST message was sent and the duration of the lease from the DHCPACK message.

R 232 If the client receives a DHCPNAK message, it cannot reuse its remembered network address. It must instead request a new address by restarting the configuration process, this time using the procedure described in 8.2.3.2 (procedure starting in the INIT state).

R 233 The client times out and retransmits the DHCPREQUEST message if the client receives neither a DHCPACK nor a DHCPNAK message. The client retransmits according to the algorithm described in 8.2.3.3. If the client receives neither a DHCPACK nor a DHCPNAK message after employing the retransmission algorithm, the client MAY choose to use the previously allocated network address and configuration parameters for the remainder of the unexpired lease.

8.2.3.6 Reacquisition and expiration

R 234 T1 is the time at which the client enters the RENEWING state and attempts to contact the server that originally issued the client's network address.

R 235 T2 is the time at which the client enters the REBINDING state and attempts to contact any server.

R 236 T1 MUST be earlier T2, which, in turn, MUST be earlier than the time at which the client's lease will expire.

R 237 Times T1 and T2 are configurable by the server through options. T1 defaults to (0.5 * duration_of_lease). T2 defaults to (0.875 * duration_of_lease).

R 238 Times T1 and T2 SHOULD be chosen with some random "fuzz" around a fixed value, to avoid synchronization of client reacquisition.

8.2.3.6.1 Actions in the BOUND state

R 239 At T1 the client moves to RENEWING state.

R 240 A client MAY choose to renew or extend its lease prior to T1.

8.2.3.6.2 Actions in the RENEWING state

R 241 The client sends (via unicast) a DHCPREQUEST message to the server to extend its lease. (8.2.2.4.3.3)

R 242 The client records the local time at which the DHCPREQUEST message is sent for computation of he lease expiration time.

R 243 A DHCPACK message that arrives with a 'xid' that does not match the 'xid' of the client's DHCPREQUEST message are silently discarded.

R 244 When the client receives a DHCPACK from the server, the client computes the lease expiration time as the sum of the time at which the client sent the DHCPREQUEST message and the duration of the lease in the DHCPACK message. The client has

successfully reacquired its network address, return to BOUND state and may continue network processing.

R 245 If the client receives no response to its DHCPREQUEST message, the client SHOULD wait one-half of the remaining time until T2 down to a minimum of 60 seconds, before retransmitting the DHCPREQUEST message.

R 246 If no DHCPACK arrives before time T2, the client moves to REBINDING state.

Note: Although nothing was written about generating a new random 'xid' in the rfc, we assume it is best to do so.

8.2.3.6.3 Actions in the REBINDING state

R 247 The client sends (via broadcast) a DHCPREQUEST to extend its lease. (8.2.2.4.3.4)

(copy requirements R 242, R 243 and R 244 from the RENEWING state)

R 248 If the client receives no response to its DHCPREQUEST message, the client SHOULD wait one-half of the remaining lease time, down to a minimum of 60 seconds, before retransmitting the DHCPREQUEST message.

R 249 If the lease expires before the client receives a DHCPACK, the client moves to INIT state, MUST immediately stop any other network processing and request network initialization parameters as if the client were uninitialized. If the client then receives a DHCPACK allocating that client its previous network address, the client SHOULD continue network processing. If the client is given a new network address, it MUST NOT continue using the previous network address and SHOULD notify the local users of the problem.

8.2.3.7 Releasing an acquired lease

R 250 If the client no longer requires use of its assigned network address the client sends a DHCPRELEASE message to the server.

R 251 The correct operation of DHCP does not depend on the retransmission of DHCPRELEASE messages

8.2.3.8 Initializing with an externally assigned network address

R 252 The client sends a DHCPINFORM message.

R 253 The client unicasts the DHCPINFORM message if it knows the server's address, otherwise it broadcasts the message to the 255.255.255.255 broadcast address.

R 254 The client generates and records a random transaction identifier to be inserted in the 'xid' field.

R 255 The client places its own network address in the 'ciaddr' field.

R 256 Once a DHCPACK message with a 'xid' field matching that in the client's DHCPINFORM message arrives from any server, the client is initialized.

R 257 If the client does not receive a DHCPACK within a reasonable period or time (60 seconds or 4 tries if retransmission is used), then it SHOULD display a message informing the user of the problem, and then SHOULD begin network processing using suitable defaults as per Appendix A (RFC 2131).

8.2.4 Server Requirements

A DHCP server can receive the following messages from a client:

- DHCPDISCOVER
- DHCPREQUEST
- DHCPDECLINE
- DHCPRELEASE
- DHCPINFORM

R 258 When a client has requested the use of an address for some period of time, the allocation mechanism (the collection of DHCP servers) guarantees not to reallocate that address within the requested time to another client.

R 259 The allocation mechanism attempts to return the same network address each time the client requests an address.

R 260 When the available addresses have been exhausted the allocation mechanism will reuse those addresses whose lease has expired.

R 261 To compensate for drift between the clocks of the server and the client, the server may return a shorter lease duration to the client than the server commits to its local database of client information.

R 262 If the client does not provide a 'client identifier' option, the server MUST use the contents of the 'chaddr' field to identify the client.

8.2.4.1 DHCPDISCOVER message

R 263 When a server receives a DHCPDISCOVER message from a client, the server chooses a network address, a lease expiration time and the configuration parameters for the requesting client. The server constructs a DHCPOFFER message with the offered configuration and sends it to the client.

R 264 When allocating a new address, servers SHOULD check that the offered network address is not already in user; e.g. the server may probe the offered address with an ICMP Echo Request (NEW: could change to MAY).

R 265 Servers SHOULD be implemented so that network administrators may choose to disable probes of newly allocated addresses.

R 266 The server MAY choose to return the 'vendor class identifier' used to determine the parameters in the DHCPOFFER message to assist he client in selecting which DHCPOFFER to accept.

R 267 NEW: Servers MAY deliver a full configuration in a DHCPOFFER, but are NOT required to do so. The DHCPDISCOVER MUST contain an IP address and a lease time, and MAY contain other information.

R 268 NEW: The server SHOULD be permitted to return the 'parameter request list' including the option codes for each option it is prepared to deliver in the a DHCPACK message.

8.2.4.1.1 Network address

The new address SHOULD be chosen as follows:

R 269 The client's current address as recorded in the client's current binding.

R 270 The client's previous address as recorded in the client's (now expired or released) binding, if that address is in the server's pool of available address and not already allocated.

R 271 The address requested in the 'Requested IP Address' option, if that address is valid and not already allocated.

R 272 A new address allocated from the server's pool of available addresses; the address is selected based on the subnet from which the message was received (if 'giaddr' is 0.0.0.0) or on the address of the relay agent that forwarded the message ('giaddr' when not 0.0.0.0).

Notes:

R 273 A server MAY, for administrative reasons, assign an address other than the one requested, or may refuse to allocate an address to a particular client even though free addresses addresses are available.

R 274 In some network architectures it may be the case that the DHCP client should be assigned an address from a different subnet than the address recorded in 'giaddr'. DHCP does not require that the client be assigned an address from the subnet in 'giaddr'.

R 275 Servers need not reserve the offered network address, although the protocol will work more efficiently if the server avoids allocating the offered network address to another client. Servers SHOULD NOT reuse offered address and may use an implementation-specific timeout mechanism to decide when to reuse an offered address.

8.2.4.1.2 Leases duration

The server chooses an expiration time for the lease as follows:

R 276 If the client has not requested a specific lease in the DHCPDISCOVER message and the client already has an assigned network address, the server returns the lease expiration time previously assigned to that address.

R 277 If the client has not requested a specific lease in the DHCPDISCOVER message and the client does not have an assigned network address, the server assigns a locally configured default lease time

R 278 If the client has requested a specific lease in the DHCPDISCOVER message (regardless of whether the client has an assigned network address), the server may choose either to return the requested lease (if the lease is acceptable to local policy) or select another lease.

8.2.4.1.3 Other configuration parameters

The configuration parameters MUST be selected by applying the following rules in the order below:

R 279 If the server has been explicitly configured with a default value for the parameter, the server MUST include that value for the parameter, the server MUST include that value in an appropriate option in the 'option' field.

R 280 If the server recognizes the parameter as a parameter defined in the Host Requirements Document, the server MUST include the default value for that parameter as given in the Host Requirements Document in an appropriate option in the 'option' field.

R 281 The server MUST supply as many of the requested parameters as possible and MUST omit any parameters it cannot provide. The server MUST include each requested parameter only once unless explicitly allowed.

R 282 Any parameters from the existing binding that differ from the Host Requirements Document defaults.

R 283 Any parameters specific to this client as configured by the network administrator.

R 284 Any parameters specific to this client's class (ad identified by the 'vendor class identifier' option) as configured by the network administrator.

R 285 Parameters with non-default values on the client's subnet.

8.2.4.2 DHCPREQUEST message

A DHCPREQUEST message may come from a client responding to a DHCPOFFER message from a server, from a client verifying a previously allocated IP address or from a client extending the lease on a network address.

If the DHCPREQUEST message contains a 'server identifier' option, the message is in response to a DHCPOFFER message. Otherwise, the message is a request to verify or extend an existing lease.

R 286 Servers with knowledge of the client's configuration parameters respond with a DHCPACK message to the client.

R 287 If the client's request is invalid (e.g., the client has moved to a new subnet), servers SHOULD respond with a DHCPNAK message to the client. Servers SHOULD NOT respond if their information is not guaranteed to be accurate.

R 288 Servers SHOULD NOT check that the client's network is already in use; the client may be responding to ICMP Echo Request messages at this point.

8.2.4.2.1 DCHPREQUEST in response to a DHCPOFFER message (SELECTING state)

R 289 Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer.

R 290 If the server sends a DHCPACK message, the lease time offered MUST be at least as long as that in the DHCPOFFER message. The IP address MUST be the same.

R 291 The options delivered in a DHCPACK message MAY differ from those in a DHCPOFFER message.

R 292 NEW: RFC2131 appears to permit a long list of options to be sent partly in the DHCPOFFER message and partly in the DHCPACK message. (Problem: shouldn't the client use configuration in DHCPACK message?)

8.2.4.2.2 DHCPREQUEST generated during INIT-REBOOT state

R 293 The client is seeking to verify a previously allocated, cashed configuration. The ‘server identifier’ MUST NOT be filled in, ‘requested IP address’ option MUST be filled in with the client’s notion of its previously assigned address and ‘ciaddr’ MUST be zero.

R 294 The server SHOULD send a DHCPNAK message to the client if the ‘requested IP address’ is incorrect, or is on the wrong network.

R 295 Determining whether a client is on the correct network is done by examining the content s of ‘giaddr’, the ‘requested IP address’ option, and a database lookup. If the DHCP server detects that the client is on the wrong net (i.e., the result of applying the local subnet mask or remote subnet mask (if 'giaddr' is not zero) to 'requested IP address' option value doesn't match reality), then the server SHOULD send a DHCPNAK message to the client.

R 296 If the network is correct, then the DHCP server should check if the client's notion of its IP address is correct. If not, then the server SHOULD send a DHCPNAK message to the client.

R 297 If the DHCP server has no record of this client, then it MUST remain silent, and MAY output a warning to the network administrator. This behavior is necessary for peaceful coexistence of non-communicating DHCP servers on the same wire.

8.2.4.2.3 DHCPREQUEST generated during RENEWING state

R 298 The client is completely configured and is trying to extend its lease. The message will be unicast so no relay agents will be involved. The server will trust the value in ‘ciaddr’ and use it when replying to the client.

R 299 A client MAY choose to renew or extend its lease prior to T1. The server MAY choose not to extend the lease (as a policy decision by the network administrator), but should return a DHCPACK message regardless.

8.2.4.2.4 DHCPREQUEST generated during REBINDING state

R 300 The client is completely configured and is trying to extend its lease. The DHCPREQUEST from a REBINDING client is intended to accommodate sites that have multiple DHCP servers and a mechanism for maintaining consistency among leases managed by multiple servers.

R 301 A DHCP server MAY extend a client’s lease only if it has local administrative authority to do so.

R 302 The DHCP server SHOULD check ‘ciaddr’ for correctness before replying to the DHCPREQUEST.

8.2.4.3 DHCPDECLINE message

R 303 Upon receipt of a DHCPDECLINE message, the server MUST mark the network address as not available and SHOULD notify the local system administrator of a possible configuration problem.

8.2.4.4 DHCPRELEASE message

R 304 Upon receipt of a DHCPRELEASE message, the server marks the address as not allocated. The server SHOULD retain a record of the client's initialization parameters for possible reuse in response to subsequent requests from the client.

8.2.4.5 DHCPINFORM message

R 305 The DHCP server responds to a DHCPINFORM message by sending a DHCPACK message directly to the address given in the 'ciaddr' field of the DHCPINFORM message.

R 306 Servers construct a DHCPACK message with any local configuration parameters appropriate for the client without: allocating a new address, checking for an existing binding, filling in 'yiaddr' or including lease time parameters.

R 307 The server SHOULD check the network address in a DHCPINFORM message for consistency.

R 308 The server includes other parameters in the DHCPACK message as defined in 8.2.4.1.3.

8.2.5 DHCP Options

DHCP Option	
Pad Option	CRITICAL
End Option	CRITICAL
Subnet Mask	IMPORTANT
Time Offset	
Router Option	IMPORTANT
Time Server Option	
Name Server Option	?
Domain Name Server Option	IMPORTANT
Log Server Option	
Cooke Server Option	
LPR Server Option	
Impress Server Option	
Resource Server Option	
Host Name Option	IMPORTANT
Boot File Size Option	
Merit Dump File	
Domain Name	IMPORTANT
Swap Server	
Root Path	
Extension Path	
IP Forwarding Enable/Disable Option	
Non-Local Source Routing Enable/Disable Option	
Policy Filter Option	
Maximum Datagram Reassembly Size	
Default IP Time-to-live	
Path MTU Aging Timout Option	
Path MTU Plateau Table Option	

Interface MTU Option	
All Subnets are Local Option	
Broadcast Address Option	IMPORTANT
Perform Mask Discovery Option	
Mask Supplier Option	
Perform Router Discovery Option	
Router Solicitation Address Option	
Static Route Option	OBSOLETE
Trail Encapsulation Option	
ARP Cache Timeout Option	
Ethernet Encapsulation Option	
TCP Default TTL Option	
TCP Keepalive Interval Option	
TCP Keepalive Garbage Option	
Network Information Service Domain Option	
Network Information Servers Option	
Network Time Protocol Servers Option	?
Vendor Specific Information	IMPORTANT
NetBIOS over TCP/IP Name Server Option	
NetBIOS over TCP/IP Datagram Distribution Server Option	
NetBIOS over TCP/IP Node Type Option	
NetBIOS over TCP/IP Scope Option	
X Window System Font Server Option	
X Window System Display Manager Option	
Network Information Service+ Domain Option	
Network Information Service+ Server Option	
Mobile IP Home Agent Option	
Simple Mail Transport Protocol (SMTP) Server Option	?
Post Office Protocol (POP3) Server Option	?
Network News Transport Protocol (NNTP) Server Option	?
Default World Wide Web (WWW) Server Option	
Default Finger Server Option	
Default Internet Relay Chat (IRC) Server Option	
StreetTalk Server Option	
StreetTalk Directory Assistance (STDA) Server Option	
Requested IP Address	CRITICAL
IP Address Lease Time	CRITICIAL
Option Overload	CRITICIAL
TFTP server name	?
Bootfile name	?
DHCP Message Type	CRITICAL
Server Identifier	CRITICAL

Parameter Request List	CRITICAL
Message	IMPORTANT
Maximum DHCP Message Size	CRITICAL ?
Renewal (T1) Time Value	CRITICAL
Rebinding (T2) Time Value	CRITICIAL
Vendor class identifier	IMPORTANT
Client Identifier	CRITICAL
Relay Agent Information	IMPORTANT
Classless Static Route	IMPORTANT

8.2.5.1 Subnet Mask option

The subnet mask option specifies the client's subnet mask as per RFC 950.

R 309 If both subnet mask and router option are specified in a DHCP reply, the subnet mask option MUST be first.

8.2.5.2 Router option

The router option specifies a list of IP addresses for routers on the client's subnet.

8.2.5.3 Domain Name Server option

The domain name server option specifies a list of Domain Name System name servers available to the client.

8.2.5.4 Host Name option

This option specifies the name of the client. The name may or may not be qualified with the local domain name.

8.2.5.5 Domain Name option

This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.

8.2.5.6 Broadcast Address option

This option specifies the broadcast address in use on the client's subnet.

8.2.5.7 Static Route option (obsolete)

This option specifies a list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specifies, they are listed in descending order of priority.

Note: default route (0.0.0.0) is illegal

8.2.5.8 Vendor Specific Information option

Future work

8.2.5.9 Requested IP Address option

This option is used in a client request to allow the client to request that a particular IP address be assigned.

8.2.5.10 IP Address Lease Time option

This option is used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.

8.2.5.11 Option Overload option

This option is used to indicate that the DHCP ‘sname’ or ‘file’ fields are being overloaded by using them to carry DHCP options.

8.2.5.12 DHCP Message Type option

This option is used to convey the type of the DHCP message.

8.2.5.13 Server Identifier option

DHCP servers include this option in the DHCPOFFER in order to allow the client to distinguish between lease offers.

8.2.5.14 Parameter Request List option

This option is used by a DHCP client to request values for specified configuration parameters. The client MAY list the options in order of preference.

8.2.5.15 Message option

This option is used to provide an error message in the event of failure.

8.2.5.16 Maximum DHCP Message Size option

This option specifies the maximum length DHCP message that the client is willing to accept.

R 310 The minimum legal value is 576 octets.

8.2.5.17 Renewal (T1) Time Value option

This option specifies the time interval from address assignment until the client transitions to the RENEWING state.

8.2.5.18 Rebinding (T2) Time Value option

This option specifies the time interval from address assignment until the client transitions to the REBINDING state.

8.2.5.19 Vendor class identifier option

This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.

8.2.5.20 Client Identifier option

This option is used by DHCP clients to specify their unique identifier to the server. This value is an opaque key, not to be interpreted by the server, expected to be unique for all clients in an administrative domain.

R 311 The 'client identifier' chosen by a DHCP client MUST be unique to that client within the subnet to which the client is attached.

R 312 If the client uses a ‘client identifier’ in one message, it MUST use that same identifier in all subsequent messages, to ensure that all servers correctly identify the client.

R 313 The client identifier MAY consist of type-value pairs similar to the 'htype'/'chaddr' fields. For instance, it MAY consist of a hardware type and harware address. In this case the type field SHOULD be one of the ARP hardware types defined in STD2 (RFC 1700).

R 314 A hardware type of 0 (zero) SHOULD be used when the value field contains an identifier other than a hardware address (e.g. a fully qualified domain name).

8.2.5.21 Relay Agent Information option

The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies.

R 315 DHCP servers claiming to support the Relay Agent Information option SHALL echo the entire contents of the Relay Agent Information option in all replies. Servers SHOULD copy the Relay Agent Information option as the last DHCP option in the response.

R 316 Servers SHALL NOT place the echoed Relay Agent Information option in the overloaded sname or file fields. If a server is unable to copy a full Relay Agent Information field into a response, it SHALL send the response without the Relay Information Field, and SHOULD increment an error counter for the situation.

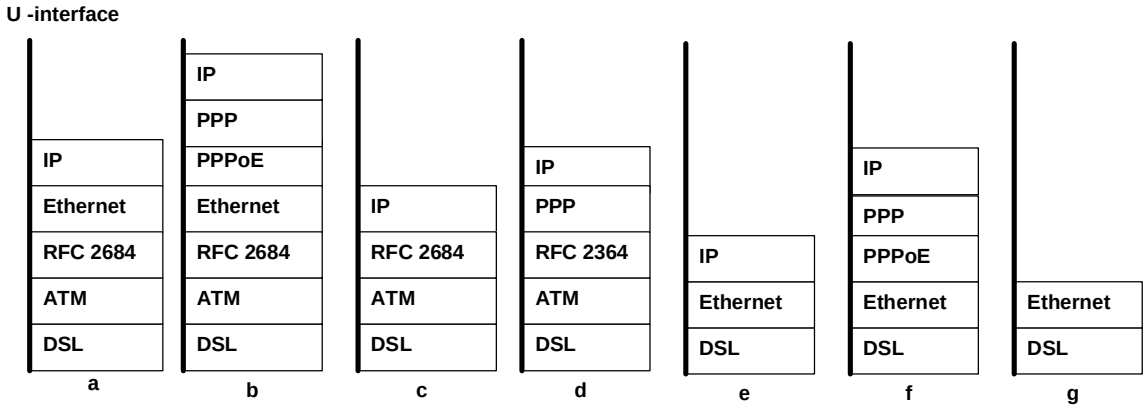
R 317 Servers SHOULD be prepared to handle relay agent options in unicast messages, but MUST NOT expect them to always be there.

8.2.5.22 Classless Static Route Option

The Static Routes option (option 33) does not provide a subnet mask for each route - it is assumed that the subnet mask is implicit in whatever network number is specified in each route entry. The Classless Static Routes option does provide a subnet mask for each entry, so that the subnet mask can be other than what would be determined using the algorithm specified in STD 5.

8.3 VLAN

VL 1 The RGW SHOULD support untagged frames, setting priority-tagged frames and setting VLAN-tagged Ethernet frames in the upstream direction for stacks a, b, e, f and g in the figure below. [TR-101 R-01]



VL 2 The RGW SHOULD support setting the priority tag and VLAN ID values. [TR-101 R-02]

VL 3 The RGW SHOULD support receiving untagged and VLAN tagged Ethernet frames in the downstream direction, and it SHOULD be able to strip the VLAN tagging from the ones received tagged. [TR-101 R-03]

VL 4 [TR-068 I-120] The device SHOULD allow for the selection of which traffic to forward over which connection (in the case of multiple PVCs, multiple PPPoE sessions, etc…) according to any one or more of the following pieces of information:
(1) IEEE 802.1Q VLAN identification, and
(2) packet length.

VL 5 TR-068 I-163] The device SHOULD support classification of WAN directed LAN traffic and placement into appropriate queues based on any one or more of the following pieces of information:
(1) IEEE 802.1Q VLAN identification, and
(2) packet length.

9 MANAGEMENT TESTING

Chapter 9 covers the motivations behind the selection of a reference model for MUSE Management Tests, and goes deeply inside TMN Model (rec. ITU-T M.3400), in order to obtain an exhaustive list of all Management Tests Objectives.

9.1 Selecting a reference model for MUSE Management Tests

Before describing management functionalities to be verified, we need to define the management architecture provided in MUSE phase I framework. After that, we should start from the TMN management Functions described in ITU-T M.3400, in order to obtain an exhaustive list of all TMN management requirements, and hence define the test objectives that are implicit on each requirement evaluation, using references as links to be used in the further work regarding to test methodologies.

The MUSE management model arose towards a comparison and relationship between TMN and eTOM models. This study is detailed described in Deliverable TF1.3 (AM and NSM chain automation for multi-domain/ multi-provider access networks).

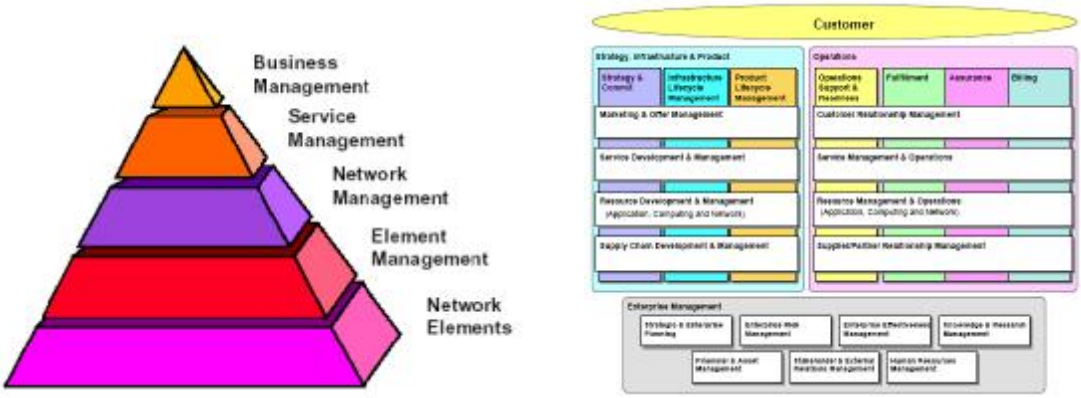


Figure 9-1: TMN and eTOM Models

As mentioned on MUSE_DTF1.3 [1], ITU-T has recently integrated eTOM in the TMN standards. This is done in M.3050 recommendation [3].

One main differentiator was noticed:

- TMN model is built on the requirements to manage network equipment and networks (bottom-up approach)
- eTOM model is built on the need to support processes of the entire service provider enterprise (top-down approach).

As it is written in M.3050 [3], both approaches can be used to identify generic and specialized management function sets to support management activities as defined in M.3400 [2]. TMN captures a technology and resource oriented view of the management domain, and the eTOM framework provides an additional business-oriented viewpoint. So,

the first approach (TMN) is relevant when considering the structure and organization of a management solution and the second (eTOM) is important when considering the business requirements of a service provider, as the user of a management solution.

At the horizontal levels, the following relationship exists between the 2 models:

- eTOM Service Management & Operations (SM&O) = TMN Service Management layer
- eTOM Resource Management & Operations (RM&O) = TMN Network Management Layer + Element Management Layer

TMN and eTOM are complementary:

- M.3400 [10] provides a detailed, functional view on the element, network, and service management layers
- eTOM provides business view for those layers.

Following these aspects, it was found interesting to build the MUSE management requirements based on the eTOM framework (FAB grouping processes), however, for the cases for which TMN can provide more details than eTOM (e.g.: management functions at SM&O and RM&O levels), then TMN recommendations (M.3400) were used as references in addition to eTOM documents.

Generically, MUSE management model is based on eTOM model for the upper management levels (service and network management levels) and on M3400 model for the lower management levels (element management level and NE management level), in a complementary basis. This way, being FCAPS the traditional way to describe Element Management functions, TMN model looks the most suitable to be used on MUSE's Management Tests.

The TMN management model provides an overall architectural framework for Management Functions (vertical view) and TMN layers (horizontal view), as shown in Figure 9-2.

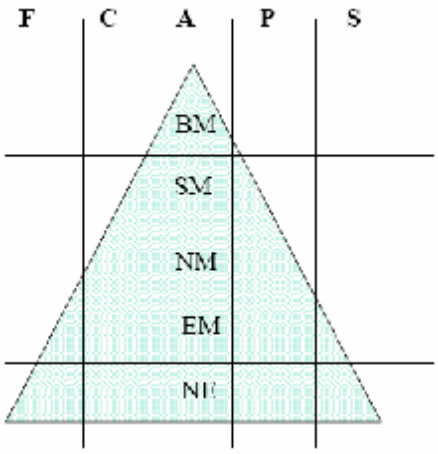


Figure 9-2: The FCAPS model defined by the TMN standard

Indeed, FCAPS management functions are currently used by the vendors of managers (EM managers especially) in the definition of their products.

9.1.1 Fault management

Fault Management is a set of functions which enables the detection, isolation and correction of abnormal operation of the telecommunication network and its environment. It provides facilities for the performance of the maintenance phases from ITU-T M.20. The quality assurance measurements for Fault Management include component measurements for Reliability, Availability and Survivability (RAS).
Fault Management includes the following function set groups:

- RAS Quality Assurance.
- Alarm Surveillance.
- Fault Localization.
- Fault Correction.
- Testing.
- Trouble Administration.

9.1.2 Configuration Management

Configuration Management provides functions to exercise control over, identify, collect data from and provide data to NEs. Configuration Management supports the following function set groups:

- Network Planning and Engineering.
- Installation.
- Service Planning and Negotiation.
- Provisioning.
- Status and Control.

9.1.3 Accounting Management

Accounting Management enables the measurement of the use of network services and the determination of costs to the service provider and charges to the customer for such use. It also supports the determination of prices for services. Accounting Management includes the following function set groups:

- Usage Measurement.
- Tariffing/Pricing.
- Collections and Finance.
- Enterprise Control.

9.1.4 Performance Management

Performance Management provides functions to evaluate and report upon the behaviour of telecommunication equipment and the effectiveness of the network or network element. Its role is to gather and analyse statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, NEs or other equipment and to aid in planning, provisioning, maintenance and the measurement of quality. As such, it is carrying out the performance measurement phase of ITU-T M.20.

A TMN collects Quality of Service (QoS) data from NEs and supports improvements in QoS. The TMN may request QoS data reports to be sent from the NE, or such a report may be sent automatically on a scheduled or exception basis. At any time, the TMN may modify the current schedule and/or exception thresholds. Reports from the NE on QoS data may consist of raw data (data gathered in the course of providing telecommunication services) that is

then analysed externally to the NE, or the NE may be capable of carrying out part of the analysis of the data before the report is sent.

Quality of Service includes monitoring and recording of parameters relating to:

a) Connection establishment (e.g. call set-up delays, successful and failed call requests).
b) Connection retention.
c) Connection quality.
d) Billing integrity.
e) Keeping and examining of logs of system state histories.
f) Cooperation with fault (or maintenance) management to establish possible failure of a resource and with configuration management to change routing and load control parameters/limits for links, etc.
g) Initiation of test calls to monitor QoS parameters.

Performance Management includes the following function set groups:

- Performance Quality Assurance.
- Performance Monitoring.
- Performance Control.
- Performance Analysis.

9.1.5 Security Management

Security Management provides for the management of security. In addition, security of management is required for all Management Functional Areas and for all TMN transactions. Security of management appears as part of the Security Function in ITU-T M.3010.

Security of Management functionality includes Security services for communications and Security event detection and reporting:

a) Security services for communications provides the services defined in ITU-T X.800 for authentication, access control, data confidentiality, data integrity, and non-repudiation that may be exercised in the course of any communications between systems, between customers and systems, and between internal users and systems. In addition, a set of pervasive security mechanisms are defined that are applicable to any communication (such as event detection, security audit trail management, and security recovery).
b) Security event detection and reporting reports to higher layers of security any activity that may be construed as a security violation (e.g. unauthorized user, physical tampering with equipment, etc.).

Security Management includes the following function set groups:

- Prevention.
- Detection.
- Containment and recovery.
- Security administration.

9.2 Management Tests Objectives

The current chapter describes the Tests Objectives for all the TMN management functions. Next figure illustrates the followed methodology.

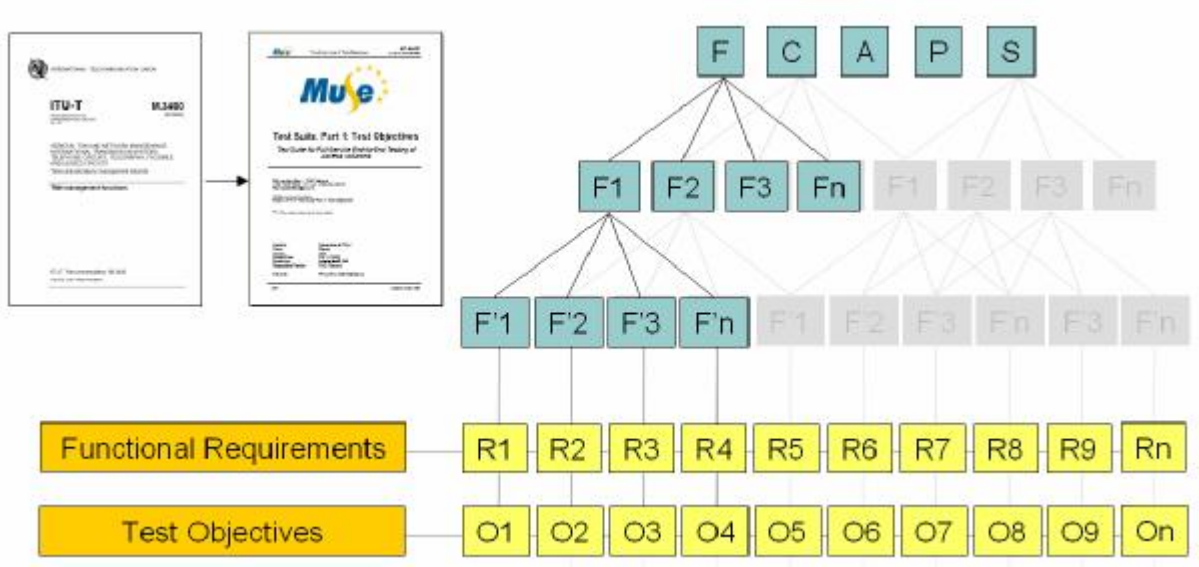


Figure 9-3: Defining Management Tests Objectives

Starting from the TMN Management Functions described in ITU-T M.3400, it was obtained an exhaustive list comprising all the TMN Management Requirements, herein mapped into Test Objectives that will implicitly assure all requirements fulfilment.

Each Test has its own ID (e.g. FM.01.01), which is going to be useful in further cross referencing purposes (FM stands for Fault Management, and the 2nd and 3rd fields – 01.01, on the previous example – stands for the sub-sections within the Fault Management main section, as it is also presented in ITU-T M.3400).

9.2.1 Testing Fault Management

FM.01.01: Requirement Name: Network RAS goal setting function set
Requirement Description: ITU-T M.3400 – Section 6.1.1
Test Objectives: Assure the support of access to quantitative goals that are set for the frequency and duration of network outages over a specified period of time.

FM.01.02: Requirement Name: Service availability goal setting function set
Requirement Description: ITU-T M.3400 – Section 6.1.2
Test Objectives: Assure the support of access quantitative goals that are set for the frequency and duration of network outages over a specified period of time.

FM.01.03: Requirement Name: RAS assessment function set
Requirement Description: ITU-T M.3400 – Section 6.1.3
Test Objectives: Assure that the RAS assessment function set is in accordance with the following TMN management functions:

1. Report network outage – Agent reports network outage to manager.
2. Report service outage – Agent reports service outage to manager.

3. Request network outage summary report – Manager requests agent to send network outage summary reports. Agent responds with the requested information.
4. Request service outage summary report – Manager requests agent to send service outage summary reports. Agent responds with the requested information.

FM.01.04: Requirement Name: Service outage reporting function set
Requirement Description: ITU-T M.3400 – Section 6.1.4
Test Objectives: Assure the support of access to a database of outage reports concerning an outage of services to multiple customers. The report may include the type of services affected, the number of customers affected, and the start and end times of the outage. Such reports include statistics concerning service outages by designated areas and over designated periods of time.

FM.01.05: Requirement Name: Network outage reporting function set
Requirement Description: ITU-T M.3400 – Section 6.1.5
Test Objectives: Assure the support of access to a database of outage reports concerning an outage of a network, or a major part of a network. Such reports include statistics concerning both NE outages and network outages by designated areas and over designated periods of time.

FM.01.06: Requirement Name: NE(s) outage reporting function set
Requirement Description: ITU-T M.3400 – Section 6.1.6
Test Objectives: Assure the support of access to a database of outage reports concerning an NE, or a major part of an NE, or a group of NEs. This type of report is created after outage has occurred and may be updated during and after the outage has been corrected. The final report should include the identification and location of the NE, the type of NE, the start time of the outage, the end time of the outage and the reason for the outage if known. Such reports are not made for protected faults.

FM.02.01: Requirement Name: Alarm Surveillance includes Alarm policy function set
Requirement Description: ITU-T M.3400 – Section 6.2.1
Test Objectives: Assure the support for creating and updating tables assigning domains of alarm reporting (in terms of coverage of lists of NEs, as individuals or by location) to surveillance centres and systems. It also supports network-level tables defining under what conditions an alarm is to be inhibited and the level of severity to be assigned to specific alarm conditions.

FM.02.02: Requirement Name: Alarm Surveillance includes Network fault event analysis, including correlation and filtering function set
Requirement Description: ITU-T M.3400 – Section 6.2.2
Test Objectives: Assure the support of access to a summary of non-redundant alarms at the network level, which allows further reduction of redundancy beyond what can be accomplished by correlation and filtering alarms in the context of an NE or group of NEs. This function set also supports notifications of new filtered, correlated alarms, or changes in the status of a previously reported alarm: for example, notification that an alarm has been cleared.

FM.02.03: Requirement Name: Alarm Surveillance includes Alarm status

modification function set
Requirement Description: ITU-T M.3400 – Section 6.2.3
Test Objectives: Assure the support for a user to administer rules for the revision of the alarm status (major, minor, etc.) as received from an NE before it is displayed or processed further. The rules reflect alarm policy, which in turn reflects field experience.

FM.02.04: Requirement Name: Alarm Surveillance includes Alarm reporting function set
Requirement Description: ITU-T M.3400 – Section 6.2.4
Test Objectives: Certify the "ACTIVE-REPORTABLE" alarm status, by causing alarms that do not persist long enough to qualify as no transient conditions. This way, it is necessary to assure that the Alarm Reporting function set is in accordance with TMN management functions:

1. Report Alarm – Agent notifies manager of alarm information upon the occurrence of an alarm.
2. Route Alarm Report – Manager specifies to the agent the destination address(es) for a specified set of alarm reports.
3. Request Alarm Report Route – Manager requests agent to send the current assignment of the destination address(es) for a specified set of alarm reports; agent responds with the current assignment of destination address(es).
4. Condition Alarm

FM.02.05: Requirement Name: Alarm Surveillance includes Alarm summary function set
Requirement Description: ITU-T M.3400 – Section 6.2.5
Test Objectives: Assure that the Alarm Summary function set is in accordance with the following TMN management functions:

1. Report current alarm summary – Agent provides manager (based on a predefined schedule) with a current alarm summary.
2. Route current alarm summary – Manager specifies to the agent the destination address(es) for a specified set of current alarm summaries.
3. Request current alarm summary route – Manager requests agent to send the current assignment of the destination address(es) for a specified set of current alarm summaries; agent responds with the current assignment of destination address(es).
4. Schedule current alarm summary – Manager specifies a schedule for the agent to establish for the reporting of current alarm summaries. The schedule information specifies what should be reported as well as when it should be reported.
5. Request current alarm summary schedule – Manager requests agent to send the current schedule information for Current Alarm Summary reporting; agent responds with the schedule information.
6. Allow/inhibit current alarm summary – Manager instructs the agent to allow/inhibit reporting of the scheduled current alarm summaries.
7. Request current alarm summary – Manager requests the agent to send a current alarm summary; agent responds with the summary. This function allows an agent to report alarm conditions of specified resources (severity, status, cause, etc.).

FM.02.06: Requirement Name: Alarm Surveillance includes Alarm event criteria

function set
Requirement Description: ITU-T M.3400 – Section 6.2.6
Test Objectives: Assure that the Alarm Event Criteria function set is in accordance with the following TMN management functions:

1. Condition alarm event criteria – Manager instructs the agent to assign specified alarm attributes (e.g. thresholds, etc.) used by resources accessed through the agent to determine if an event is to be considered an alarm.
2. Request alarm event criteria – Manager requests agent to report the current assignments of specified attributes (e.g. thresholds, etc.) used by the resources to determine if an event is to be considered an alarm; agent responds with the current assignment of the requested attributes, modes or thresholds.

FM.02.07: Requirement Name: Alarm Surveillance includes Alarm indication management function set
Requirement Description: ITU-T M.3400 – Section 6.2.7
Test Objectives: Assure that the Alarm Indication Management function set is in accordance with the following TMN management functions:

1. Inhibit/allow audible/visual alarm indications – Manager instructs the agent to inhibit/allow the operation of specified alarm indication/recording devices such as lamps, speakers, printers, etc. In the inhibit mode, new alarms will not trigger audible/visual alarm indicators.
2. Reset audible alarms – Manager instructs the agent to reset specified audible alarm indicator(s). This function momentarily removes any alarm indications, but allows further alarms to trigger audible/visual indicators.

FM.02.08: Requirement Name: Alarm Surveillance includes Log control function set
Requirement Description: ITU-T M.3400 – Section 6.2.8
Test Objectives: Assure that the Log Control function set is in accordance with the following TMN management functions:

1. Allow/inhibit logging – Manager instructs the agent to allow/inhibit logging of log records.
2. Condition logging – Manager instructs the agent to assign log attributes as specified by the manager.
3. Request log condition – Manager requests agent to send the current assignment of specified log attributes; agent responds with the current assignment of the specified attributes.

FM.02.09: Requirement Name: Alarm Surveillance includes Alarm correlation and filtering function set
Requirement Description: ITU-T M.3400 – Section 6.2.9
Test Objectives: Assure that the Alarm Correlation and Filtering function set is in accordance with the following TMN management functions:

1. Determine identity of event – Agent provides manager with event's unique identity.
2. Filter events – Manager requests agent to select specific event(s) from a general stream of events.

3. Suppress transient events – Manager requests agent to suppress events which only occur on a rare and intermittent basis which are not of consequence to the network services.
4. Suppress redundant events – Manager requests agent to suppress redundant events, but count those events.
5. Suppress implied events – Manager request agent to suppress all events which are implied by root cause event, but enhance information in root cause event.
6. Maintain event inter-dependencies – Manager requests agent to evaluate significance of event based on one or more other events which are generated and delivered independently.
7. Handle event arriving out of order – Manager handles events received from agent, which due to different network transient delays or clock skew in the device and manager systems, arrive in a different order than their creation time order.
8. Handle environmental conditions – Manager requests agent to correlate events based on environmental conditions such as business rules, time of day, configuration values, affecting event significance.
9. Access external data sources – Manager requests agent to correlate events based on information stored externally.
10. Trigger automatic action – Manager requests agent to initiate an action to be taken based on event information.
11. Take action that is based on non-arrival of an event – Manager requests agent to wait for the receipt of an event, and in turn initiates an action based on the non-arrival of the event within a specified period of time.
12. Receive raw data – Manager receives alarm and other events from agent.
13. Root cause message – Manager receives root cause notification from agent.
14. Forward alarms – Manager receives analysed, filtered alarms and other events from agent.

FM.02.10: Requirement Name: Alarm Surveillance includes Failure event detection and reporting function set
Requirement Description: ITU-T M.3400 – Section 6.2.10
Test Objectives: Assure the access availability to the results of hardware and software checks that are made in the course of carrying out telecommunications functionality, on schedule and as background processing.

FM.03.01: Requirement Name: Fault localization policy function set
Requirement Description: ITU-T M.3400 – Section 6.3.1
Test Objectives: Assure the access availability to tables assigning domains of fault localization (in terms of coverage of lists of circuits, paths, facilities and NEs, as individuals or by location) to fault localization centres and systems. Also assure the access availability to parameters of the procedures for escalation if a trouble is not resolved in an allowed time period.

FM.03.02: Requirement Name: Verification of parameters and connectivity function set
Requirement Description: ITU-T M.3400 – Section 6.3.2

Test Objectives: Assure the support of requests for verification and accesses of databases in other functions to verify that cross-connections and parameters of termination points are consistent with service features.

FM.03.03: Requirement Name: Network fault localization function set
Requirement Description: ITU-T M.3400 – Section 6.3.3
Test Objectives: Assure the support of requests for notifications that a root cause of a fault has been found. A trouble ticket may be created in databases of other functions. Also assure that the Network Fault Localization function set is in accordance with the following TMN management functions:

1. Alarm – Agent sends the alarm to manager.
2. Customer message – Agent sends the message to manager.
3. Network carriers status report– Agent reports the real-time status to manager.
4. Vendors status report – Agent sends the vendors status to manager.
5. Test result – Manager directs agent to report the result of automatic or manual testing routines.
6. System open/close tickets – Manager directs agent to open/close trouble ticket.
7. Consolidation of related tickets – Manager directs agent to consolidate with tickets related.
8. Cancel/clear trouble tickets – Manager directs agent to cancel/clear trouble ticket.
9. Trouble status updated – Manager directs agent to update trouble status.
10. Create historical record – Manager directs agent to create historical record.
11. Send trouble ticket – Manager directs agent to send trouble ticket to proper vendors.
12. Choose proper procedure – Manager directs agent to choose the proper procedure for determination process.
13. Select alternative – Manager directs agent to select procedure alternative.
14. Institute back-up procedure – Manager directs agent to perform back-up procedure.
15. Breakdown diagnostic – Manager directs to agent to breakdown diagnostic process.
16. Selected problem – Manager directs agent to select problem for diagnostic process based on priorities.
17. Help required – Manager directs agent to suspend diagnostic due to priorities.
18. Suspended diagnosis – Manager directs agent to suspend diagnostic due to priorities.
19. Went away – Manager directs agent to stop diagnostic since the problem has disappeared, and no further diagnosis is required.
20. Timer control – Manager directs agent to set up timer for monitoring whether a diagnostic process completes in an assigned time.
21. Review the trouble database – Manager directs agent to review trouble database.
22. Develop hypothesis – Manager directs agent to develop hypothesis in a special condition.
23. Provision of detail information – Manager directs agent to provide detailed information for further analysis.

24. Loop test – Manager directs agent to perform a loop test.
25. Send message – Manager directs agent to send message to customer about outage.
26. Initiate remote test – Manager directs agent to initiate a remote test.

FM.03.04: Requirement Name: NE(s) fault localization function set
Requirement Description: ITU-T M.3400 – Section 6.3.4
Test Objectives: Assure that the NE(s) Fault Localization function set is in accordance with the following TMN management functions:

1. Request diagnostic data – Manager requests agent to send the results of a diagnostic sequence.
2. Stop diagnosis in progress – Manager directs the agent to stop a particular diagnostic procedure in progress.
3. Diagnostic report – Agent reports the results of a diagnostic sequence to the manager. It may be used in conjunction with the request and stop functions and has applications where it may be necessary or desirable to repeat diagnostic tests for a period of time to “catch” a failure.
4. Schedule diagnosis – Manager directs agent to establish a routine schedule for the initiation of a diagnosis.
5. Request diagnostic schedule – Manager requests agent to report the current schedule of diagnosis.
6. Diagnostic schedule report – Agent sends the current schedule of diagnosis.
7. Request exercise report – Manager requests agent to send the results of a particular exercise.
8. Exercise report – Agent sends the results of an exercise to manager.
9. Stop exercise – Manager directs agent to stop a particular exercise in progress.
10. Exercise schedule – Manager directs agent to establish a routine schedule for the initiation of an exercise.
11. Request exercise report schedule – Manager directs agent to send the current schedule of an exercise. Agent responds with the schedule.
12. Operate/release loopback – Manager directs agent to establish or release a specific loopback. It may be activated either remotely by manager or by local action.
13. Test internal access path – Manager directs agent to connect a termination on agent to another termination by a specified path within agent, then test the path.
14. Hold network path – Manager directs agent to hold a particular network path.
15. Start/stop program traps – Manager directs agent to start or stop a specific program trap.
16. Program trap report – Agent automatically reports to manager the occurrence of a program trap.
17. Start/stop program trace – Manager directs agent to start or stop a specific trace.
18. Program trace report – Agent automatically reports to manager the results of a trace.
19. Start/stop audit – Manager directs agent to start or stop an audit.
20. Audit report – Agent automatically reports to manager the results of an audit.

21. Audit schedule – Manager directs agent to establish a specified schedule for a given audit.
22. Request audit schedule – Manager requests agent to send the current audit schedule. Agent responds with the test schedule.
23. Schedule loop insulation test – Manager directs agent to schedule a loop insulation test.
24. Start/stop loop insulation test – Manager directs agent to start or stop a loop insulation test.
25. Request loop insulation rest schedule – Manager requests agent to send a current loop insulation test schedule. Agent responds with the schedule.
26. Schedule routine tests.
27. Start/stop routine tests.
28. Report routine test schedule.

FM.03.05: Requirement Name: Running of diagnostic function set
Requirement Description: ITU-T M.3400 – Section 6.3.5
Test Objectives: Assure the support of reports related to the result of a diagnostic (a test of hardware or and audit or other check of software within an NE) and provides the ability to request a diagnostic. It may be necessary to remove a unit from service in order to run a diagnostic.

FM.04.01: Requirement Name: Management of repair process function set
Requirement Description: ITU-T M.3400 – Section 6.4.1
Test Objectives: Assure the support of database management, related to the repair process, including staffing levels, work units, costs, meantime-to-repair, scheduling effectiveness and efficiency, namely by supporting the following TMN management functions:

1. Set administrative domain – Manager directs agent to establish or change the administrative domain of a work centre or system.
2. Request administrative domain – Manager directs agent to send an administrative domain. Agent responds with the requested information.
3. Set training rules – Manager directs agent to establish or change the training requirements for classes of repair activities.
4. Request training rules – Manager directs agent to send training requirements for classes of repair activities. Agent responds with the requested information.
5. Request work force report – Manager requests agent to send report of work force information for current or previous interval. Agent responds with the requested information.
6. Request work report – Manager requests agent to send report of work flow for current or previous interval. Agent responds with the requested information.
7. Request scheduling report – Manager requests agent to send report of scheduling statistics for current or previous interval. Agent responds with the requested information.
8. Request materials report – Manager requests agent to send report of consumption of material resources (spare circuit packs, vehicle mileage, etc.) for current or previous interval. Agent responds with the requested information.

FM.04.02: Requirement Name: Arrangement of repair with customer function set
Requirement Description: ITU-T M.3400 – Section 6.4.2

Test Objectives: Assure the processes to support customer contact, in order to schedule dispatch to customer premises.

FM.04.03: Requirement Name: Scheduling and dispatch administration of repair forces function set
Requirement Description: ITU-T M.3400 – Section 6.4.3
Test Objectives: Assure the processes to support the creation of a work order, which may support repair, network growth or service activation.

FM.04.04: Requirement Name: NE(s) fault correction function set
Requirement Description: ITU-T M.3400 – Section 6.4.4
Test Objectives: Assure that the NE(s) Fault Correction function set is in accordance with the following TMN management functions:

1. Automatic restoration report – Agent reports to manager that it has switched a specified line, service, system or equipment as part of its protection procedures. Such procedures may or may not have been initiated by the manager.
2. Hot standby procedure – Manager requests agent to initiate or terminate hot-standby procedures for a service or a single system whereby a redundant unit can take over with the minimum disruption to traffic.
3. Reload procedure – Manager requests agent to reconstruct a service or a single system (main or standby) from a specified dump record.
4. Reload report – Agent reports to manager that it has reloaded a service or a single system (main or standby) from a dump.

FM.04.05: Requirement Name: Automatic restoration function set
Requirement Description: ITU-T M.3400 – Section 6.4.5
Test Objectives: Assure the support of notifications whenever a unit containing a fault has been removed from service, after a fault has been detected and the smallest protected unit containing the fault has been identified. Also assure the inhibition and override of automatic restoration functionality.

FM.05.01: Requirement Name: Test point policy function set
Requirement Description: ITU-T M.3400 – Section 6.5.1
Test Objectives: Assure the support of administers tables that define the conditions for providing test access at various points along a circuit.

FM.05.02: Requirement Name: Service test function set
Requirement Description: ITU-T M.3400 – Section 6.5.2
Test Objectives: Assure that the NE(s) Service Test function set is in accordance with the following TMN management functions:

1. Initiate service test – Manager requests agent to test a service to ensure that it is available for operation.
2. Report service test result – Agent reports to manager the results of testing the operational state of a service.

FM.05.03: Requirement Name: Circuit selection, test correlation and fault location function set
Requirement Description: ITU-T M.3400 – Section 6.5.3
Test Objectives: Assure the support of requests for tests of an end-to-end circuit and supports the return of test results.

FM.05.04: Requirement Name: Selection of test suite function set
Requirement Description: ITU-T M.3400 – Section 6.5.4
Test Objectives: Assure the support of requests for a specific part of a circuit to be tested and also supports the return of results.

FM.05.05: Requirement Name: Test access network control and recovery function set
Requirement Description: ITU-T M.3400 – Section 6.5.5
Test Objectives: Assure that the Test Access Network Control and Recovery function set is in accordance with the following TMN management functions:

1. Report test system initialization – Agent reports initialization of test system to manager.
2. Report test access system initialization – Agent reports initialization of test access system to manager.
3. Initialize and restore access system – Manager directs agent to release all existing test access connections in agent, and restore all TAPs involved to an idle state.

FM.05.06: Requirement Name: Test access configuration function set
Requirement Description: ITU-T M.3400 – Section 6.5.6
Test Objectives: Assure that the Test Access Configuration function set is in accordance with the following TMN management functions:

1. Connect test access – Analogue, voiceband data, subrate digital data, and DS1, E1 or T1: manager directs agent to provide test access for the circuit specified in agreement with the lead-pair assignment and configuration codes if applicable.
2. Change access mode – For analogue, voiceband data, subrate digital data, and DS1, manager directs agent to provide different access modes, such as split the specified pair or pairs at the metallic or digital access point in a designated direction, or to clear all test conditions and restore the circuit to a monitor state. For DS1, E1 or T1 either the monitor or split mode may be requested.
3. Release test access – Analogue, voiceband data, subrate digital data, and DS1, E1 or T1: manager directs agent to drop access to the circuit under test and return the circuit to its normal state.

FM.05.06: Requirement Name: Test access configuration function set
Requirement Description: ITU-T M.3400 – Section 6.5.6
Test Objectives: Assure that the Test Access Configuration function set is in accordance with the following TMN management functions:

1. Connect test access – Analogue, voiceband data, subrate digital data, and DS1, E1 or T1: manager directs agent to provide test access for the circuit specified in agreement with the lead-pair assignment and configuration codes if applicable.
2. Change access mode – For analogue, voiceband data, subrate digital data, and DS1, manager directs agent to provide different access modes, such as split the specified pair or pairs at the metallic or digital access point in a designated direction, or to clear all test conditions and restore the circuit to a monitor state. For DS1, E1 or T1 either the monitor or split mode may be requested.
3. Release test access – Analogue, voiceband data, subrate digital data, and DS1, E1 or T1: manager directs agent to drop access to the circuit under test and return the circuit to its normal state.

FM.05.07: Requirement Name: Test circuit configuration function set
Requirement Description: ITU-T M.3400 – Section 6.5.7
Test Objectives: Assure that the Test Circuit Configuration function set is in accordance with the following TMN management functions:

1. Interexchange pairs – Manager directs agent to execute reversal of specified transmission pairs for 4- and 6-wire metallic circuits, or the interchange of the A and B transmission pairs of a DS1, E1 or T1 on either the Equipment or Transmission Facility side of the test port.
2. Change leads – Manager directs agent to execute reversal of tip and ring leads of metallic transmission pair(s) on the circuit under test.
3. Change Terminate test and Leave (T&L) status – Manager directs agent to change T&L status of the circuit under test and report the resulting T&L state to the manager.
4. Request Terminate test and Leave (T&L) status – Manager directs agent to report the T&L status of the circuit under test.
5. Configure multipoint junction unit branches (select, restore, and block) – Manager directs agent to perform various control functions such as block, select, unselect, and release, on the Multipoint Junction Unit in the circuit.
6. Operate and release loopback equipment – Manager directs agent to split the circuit under test and change the operator release functions of digital network element latching loopback devices. Alternately, the manager directs the agent to change the activate, deactivate, and release functions of DS1/El loopback devices provided at network points and customer interfaces.

FM.05.08: Requirement Name: NE(s) test control function set
Requirement Description: ITU-T M.3400 – Section 6.5.8
Test Objectives: Assure that the NE(s) Test Control function set is in accordance with the following TMN management functions:

1. Control analogue test signal – Manager directs agent to connect a test signal generator, and to change or remove a test signal on the circuit under test.
2. Analogue transmission measurements – Manager directs agent to measure analogue transmission characteristics including: tone, noise, impulse noise, intermodular distortion, phase jitter, transients, and peak-to-average ratios.
3. Multimeter measurements – Manager directs agent to measure multimeter characteristics including: alternating and direct current voltage, resistance, alternating and direct current, and capacitance.
4. Signalling and supervision measurements – Manager directs the agent to perform and report supervision in both directions for alternating and direct current signalling.
5. Connect and disconnect monitor/talk line – Manager directs agent to establish talk and listen paths, or to remove any monitor or talk conditions between the circuit under test and the monitor/talk line.
6. Bridged monitor and listen – Manager listens selectively to the circuit under test and monitors any transmission pair in either direction.
7. Change monitor/talk level – Manager directs agent to change the level of the monitor connection.
8. Change monitor/talk filter – Manager directs agent to remove or insert the single frequency notch filter placed in the monitor connection.

9. Monitor digital data signals – Manager establishes digital data monitor test access and determines the presence of network control codes or customer data.
10. Test digital loopbacks – Manager directs agent to provide a loopback on the circuit under test and perform a digital loopback test.
11. Primary and secondary channel tests – Manager directs agent to split the circuit under test and perform primary and secondary channel uses on specified equipment, such as multipoint junction units and channel service units.
12. Digital tests – Manager directs agent to split the circuit under test and connect the required test modules that sends and receives test data to perform a test using both transmitter and receiver, or either transmitter or receiver.
13. Insert errors – Manager requests agent to insert a controlled number of logical bit errors, cyclic redundancy check errors and line code violations into the digital bit stream in one or both directions of the circuit under tests.
14. Simulated test – Manager requests agent to simulate a specified failure and mark ensuing actions as dummies.
15. Control DS1, E1 or T1 test signal – Manager requests agent to change the test signal to the DS1, E1 or T1 under tests.
16. Measure DS1, E1 or T1 signals – Manager directs agent to measure the line signals on the DS1, E1 or T1 under test. These measurements may be made with the circuit in either the monitor mode or split mode.
17. Terminate test measurement – Manager directs agent to terminate continuous or repeating type measurements. This includes the reporting of results in the response format of the command being terminated, stopping the measurement, and returning the circuit under test to a specified state. Examples include stopping a straightaway test, or DS1, E1 or T1 signal measurement.

FM.05.09: Requirement Name: Results and status reporting function set
Requirement Description: ITU-T M.3400 – Section 6.5.9
Test Objectives: Assure that Results and Status Reporting function set is in accordance with the following TMN management functions:

1. Request Test Results – Manager requests agent to report intermediate or final results from a measurement.
2. Test Results Reporting – Agent sends the results of a test to the manager.
3. Request Transmission Facility Status – Manager directs agent to send the state of the facility carrying the circuit under test.
4. Test Transmission Facility Reporting – Agent sends the state of the facility carrying a specified circuit.

FM.05.10: Requirement Name: Test access path management function set
Requirement Description: ITU-T M.3400 – Section 6.5.10
Test Objectives: Assure that the Test Access Path Management function set is in accordance with the following TMN management functions:

1. Establish loop around access – Manager directs agent to establish a test access to a metallic circuit by reserving the access point, selecting or providing a TAP and applying a loop around on the selected TAP.
2. TAP loopback test – The integrity of the metallic TAP provided by the "Establish" function is tested and calibrated from the test system.

3. Remove TAP from service – Manager directs agent to remove a TAP(s) from service.
4. Restore TAP in service – Manager directs agent to restore a TAP(s) into service.
5. Connect and disconnect loop around – Manager directs agent to apply or remove a loop around to the TAP(s) under test.

FM.05.11: Requirement Name: Test access function set
Requirement Description: ITU-T M.3400 – Section 6.5.11
Test Objectives: Assure the support of requests for test access to a path or circuit supported by an NE. Test access may involve removing the path or circuit from service.

FM.06.01: Requirement Name: Trouble report policy function set
Requirement Description: ITU-T M.3400 – Section 6.6.1
Test Objectives: Assure the access availability to rules for verification and testing and for assigning a trouble to a dispatch administration agent. Parameters of a trouble report policy include timing for internal escalation of the resources applied to an outstanding trouble and conditions under which network configuration changes (as opposed to automatic restoration or protection switching) may be used to restore service.

FM.06.02: Requirement Name: Trouble reporting function set
Requirement Description: ITU-T M.3400 – Section 6.6.2
Test Objectives: Assure that the Trouble Reporting function set is in accordance with the following TMN management functions:

1. Enter trouble report – A customer may request that a customer trouble report be created with the appropriate information.
2. Add trouble information – A customer may provide additional descriptive text for an open trouble report. This additional information will be appended to the description provided when the trouble was originally entered.
3. Cancel trouble report – A customer may attempt to close out a trouble report. Typically, the customer has resolved the trouble and wants to abort the trouble report.
4. Modify trouble information – A service customer may request that information in an existing trouble report be modified.
5. Enroll trouble report format definition – A notification of a new trouble report format is sent to a service customer.
6. Deenroll trouble report format definition – A notification of the deletion of a trouble report format is sent to a service customer.
7. Modify trouble report format definition – A notification that a trouble report format has been modified is sent to a service customer.

FM.06.03: Requirement Name: Trouble report status change notification function set
Requirement Description: ITU-T M.3400 – Section 6.6.3
Test Objectives: Assure that the Trouble Report Status Change Notification function set is in accordance with the following TMN management function:

1. Trouble report status update – A customer may be notified of changes or proposed changes in the trouble status.

FM.06.04: Requirement Name: Trouble information query function set

Requirement Description: ITU-T M.3400 – Section 6.6.4
Test Objectives: Assure that the Trouble Information Query function set is in accordance with the following TMN management functions:

2. Request trouble status – A customer may request status information on an open or closed customer trouble report.
3. Review trouble history – A customer may request information about past troubles reported for a particular service or circuit.
4. Request trouble report format – A customer may request information on what conditional package of attributes apply to trouble reports for a particular circuit or service.

FM.06.05: Requirement Name: Trouble ticket creation notification function set
Requirement Description: ITU-T M.3400 – Section 6.6.5
Test Objectives: Assure that the Trouble Ticket Creation Notification function set is in accordance with the following TMN management functions:

1. Enroll trouble report – Notifies a TMN that would normally originate a trouble report that a trouble report has been created, either as the result of a request or as a result of an internal action by the notifying TMN.
2. Deenroll trouble report – Notifies a TMN that would normally delete a trouble report that a trouble report has been deleted, either as the result of a request or as a result of an internal action by the notifying TMN.

FM.06.06: Requirement Name: Trouble ticket administration function set
Requirement Description: ITU-T M.3400 – Section 6.6.6
Test Objectives: Assure the access availability to all trouble tickets, whether created in response to trouble reports by service customers, internal staff, or analysis of alarms or performance monitoring exceptions (trouble tickets, as opposed to trouble reports, reflect the results of analysis). Tracking reports are provided of the progress of fault correction and the clearing of trouble reports and trouble tickets.

FM.06.07: Requirement Name: Management of trouble by service customer function set (new function set)
Requirement Description: ITU-T M.3400 – Section 6.6.7
Test Objectives: Assure that the Management of Trouble by Service Customer function set (new function set) is in accordance with the following TMN management functions:

1. Respond to request for outgoing trouble record – Agent (the S-OSF that supports this function set) provides access to manager to read records of outgoing trouble reports.
2. Update outgoing trouble record – Agent (the S-OSF that supports this function set) provides access to manager to update outgoing trouble records.

9.2.2 Testing Configuration Management

CM.01.01: Requirement Name: Product line budget function set
Requirement Description: ITU-T M.3400 – Section 7.1.1

Test Objectives: Assure the access availability to data concerning capital and expenses allocated to provide funding for new resources and expansion of existing capacity for a specific set of services and supporting network capabilities.

CM.01.02: Requirement Name: Supplier and technology policy function set
Requirement Description: ITU-T M.3400 – Section 7.1.2
Test Objectives: Assure the access availability to data concerning guidelines for selecting technologies and associated hardware and software to be deployed in the network based on customer demand, positioning for competitive advantage, modernization of existing plant, etc. Generally, the guidelines consist of rules for definition of specifications and restrictions such as maximum capacity of a unit. It also provides access to data concerning guidelines for qualified suppliers based on product offering, price, features, capability limits of products, operations support, availability, etc.

CM.01.03: Requirement Name: Area boundary definition function set
Requirement Description: ITU-T M.3400 – Section 7.1.3
Test Objectives: Assure that the Area Boundary Definition function set is in accordance with the following TMN management functions:

1. Request area boundary definition – Manager requests agent to send area boundary definition. Agent responds with requested information.
2. Request area identification – Manager requests agent to identify the area of a specified location point or item. Agent responds with requested information.

CM.01.04: Requirement Name: Infrastructure planning function set
Requirement Description: ITU-T M.3400 – Section 7.1.4
Test Objectives: Assure the access availability to information about status, changes, additions, or removal of property, buildings, other structures, parking facilities, electric power, heating, ventilating and air conditioning equipment, etc.

CM.01.05: Requirement Name: Management of planning and engineering process function set
Requirement Description: ITU-T M.3400 – Section 7.1.5
Test Objectives: Assure the access availability to information about planning tools, and development of planning and engineering methods and procedures. It also provides access to information about the status, costs and schedules of planning and engineering jobs in progress.

CM.01.06: Requirement Name: Demand forecasting function set
Requirement Description: ITU-T M.3400 – Section 7.1.6
Test Objectives: Assure that the Demand Forecasting function set is in accordance with the following TMN management functions:

1. Request demand forecast – Manager requests agent to send a demand forecast for specified services. Agent responds with requested information.
2. Request demand statistics – Manager requests agent to report statistical demand information on services of service customers. Agent responds with the requested information.

3. Request specific demand – Manager requests agent to report demand information concerning a specific (large) service customer. Agent responds with requested information.
4. Request configuration demand – Manager requests agent to report statistical demand information concerning service features. Agent responds with requested information.

CM.01.07: Requirement Name: Network infrastructure design function set
Requirement Description: ITU-T M.3400 – Section 7.1.7
Test Objectives: Assure the support of requests to design the network infrastructure capacity to meet the forecast demand based on demand forecasts, traffic loads, and planned service offerings so that resource capacity will be available when service is required. It supports actions to carry out the design.

CM.01.08: Requirement Name: Access infrastructure design function set
Requirement Description: ITU-T M.3400 – Section 7.1.8
Test Objectives: Assure the support of requests to design access circuits, based on customer location, and the requested service features and route. It supports actions to carry out the design.

CM.01.09: Requirement Name: Facility infrastructure design function set
Requirement Description: ITU-T M.3400 – Section 7.1.9
Test Objectives: Assure the support of requests to design facilities based on the location of nodes, product line budget, requested service features, route, and demand forecasts. It should also support actions to carry out the design.

CM.01.10: Requirement Name: Routing design function set
Requirement Description: ITU-T M.3400 – Section 7.1.10
Test Objectives: Assure the support of requests to determine the most efficient routing based on generic criteria for routing, such as traversing the least number of nodes, and customer specific criteria, such as alternate path routing. It supports responses that contain the proposed route.

CM.01.11: Requirement Name: NE(s) design function set
Requirement Description: ITU-T M.3400 – Section 7.1.11
Test Objectives: Assure the support of requests to design new or revised version of the software or hardware of NEs to meet the strategic demand for introduction of new technologies, new features or growth. It should provide access to guidelines for technology policy, supplier policy and product line budget. It should support actions to carry out the design. It should provide access to information about the NE design. This set should support requests to design a group of NE(s), including their transmission media interconnections.

CM.02.01: Requirement Name: Procurement function set
Requirement Description: ITU-T M.3400 – Section 7.2.1
Test Objectives: Assure the support of requests for procurement and provides access to information on the status of the procurement of equipment, tools, and supplies and negotiating for price and delivery date to meet corporate needs. It should use guidelines from Supplier policy, technology policy, etc.

CM.02.02: Requirement Name: Management of installation function set

Requirement Description: ITU-T M.3400 – Section 7.2.2
Test Objectives: Assure the support of access to information that can be used to monitor the installation process and the deliver of materials and coordinate contractors.

CM.02.03: Requirement Name: Contracting function set
Requirement Description: ITU-T M.3400 – Section 7.2.3
Test Objectives: Assure the support of requests for and provides access to status and other information concerning contracting services for installation. It should support management of the bidding process, contractor(s) selection, negotiation of job schedule and any special circumstances such as environmental concerns, job access restrictions, etc.

CM.02.04: Requirement Name: Real estate management function set
Requirement Description: ITU-T M.3400 – Section 7.2.4
Test Objectives: Assure the support of access to information about status, changes, additions or removal of property, buildings, other structures, parking facilities, etc. It should provide access to information concerning the usage of space in buildings. It should also provide access to information about maintenance associated with the real estate.

CM.02.05: Requirement Name: Arrangement of installation with customer function set
Requirement Description: ITU-T M.3400 – Section 7.2.5
Test Objectives: Assure the support of requests for an agreed schedule for service down time, equipment installation, customer premises access, and pre-service testing as required for service installation. It should also support responses with the agreed schedule.

CM.02.06: Requirement Name: Network installation administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.6
Test Objectives: Assure the support of access to information about the coordination of hardware and software for new installations, upgrades, and maintenance changes across the network.

CM.02.07: Requirement Name: Material management function set
Requirement Description: ITU-T M.3400 – Section 7.2.7
Test Objectives: Assure the support of access to information for the management of the ordering, shipping, and receipt of material both hardware and software for the installation of resources and activation of services. It should support the electronic ordering, shipping and receipt of software.

CM.02.08: Requirement Name: Scheduling and dispatch administration of installation force function set
Requirement Description: ITU-T M.3400 – Section 7.2.8
Test Objectives: Assure the support of requests for the installation force to provide installation and pre-service testing support at the appropriate times with regard to equipment and customer access availability. It should support actions to dispatch the installation force. It should provide access to the schedule and status of the work. It supports jeopardy reports.

CM.02.09: Requirement Name: Installation completion reporting function set
Requirement Description: ITU-T M.3400 – Section 7.2.9

Test Objectives: Assure the support of access to information about job status and supports notification of completion after acceptance testing as required. It should also support notification of failure to meet successful completion criteria, with the reason for unsuccessful completion. It should also support summary and exception reports for the management of installation jobs.

CM.02.10: Requirement Name: Software administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.10
Test Objectives: Assure the support for the acceptance of generic programs from suppliers (generic programs include applications, operating systems or middleware). It should also support administration of the versions of generic programs.

CM.02.11: Requirement Name: NE installation administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.11
Test Objectives: Assure the support of access to information about the coordination of hardware and software for new installation, upgrades, and maintenance changes for individual NEs or a collection of NEs.

CM.02.12: Requirement Name: Loading software into NEs function set
Requirement Description: ITU-T M.3400 – Section 7.2.12
Test Objectives: Assure the support for download of software to be stored in an NE. Loading includes initialization and testing that the load is successful and back-out of the software if the load is not successfully completed.

CM.03.01: Requirement Name: Service planning function set
Requirement Description: ITU-T M.3400 – Section 7.3.1
Test Objectives: Assure the support of access to a plan for service offerings on a generic basis for a wide range of customers. It also allows for the ongoing administration of those service offerings.

CM.03.02: Requirement Name: Service feature definition function set
Requirement Description: ITU-T M.3400 – Section 7.3.2
Test Objectives: Assure the support of access to descriptions of features that are used to characterize a particular service offering on a generic basis for a wide range of customers. It should also allow for the ongoing administration of those service offerings.

CM.03.03: Requirement Name: Marketing function set
Requirement Description: ITU-T M.3400 – Section 7.3.3
Test Objectives: Assure the support of access to information about marketing methods, procedures and trained personnel to contact customers about service offerings to meet their business needs. It should support requests to gather and summarize information indicating existent, latent or potential needs of new or enhanced telecommunication services. It should also support reports on such topics.

CM.03.04: Requirement Name: Management of sales process function set
Requirement Description: ITU-T M.3400 – Section 7.3.4
Test Objectives: Assure the support of access to information about sales skills, methods, procedures, trained personnel and automated tools to facilitate the selling of services to customers. It should provide access to information about individual sales activities and campaigns including individual

customer information, market segment, appointment schedule, mailings, telemarketing, advertising responsible sales personnel, service presentation materials, etc.

CM.03.05: Requirement Name: External relations (legal, stockholders, regulators, public relations) function set
Requirement Description: ITU-T M.3400 – Section 7.3.5
Test Objectives: Assure the support of information about the status of negotiations and other interactions with stock holders, general public, regulators and other government agencies. It should support activities needed to raise awareness about telecommunications issues that directly or indirectly affect the public, maintaining and improving company image, and working with governmental and regulatory bodies to improve telecommunications.

CM.03.06: Requirement Name: Customer identification function set
Requirement Description: ITU-T M.3400 – Section 7.3.6
Test Objectives: Assure the support of interactions with the customer to determine the customer's name, address, and any distinguishing characteristics about the customer such as current services, line of business, and past usage. It should support updates of the customer database as appropriate.

CM.03.07: Requirement Name: Customer need identification function set
Requirement Description: ITU-T M.3400 – Section 7.3.7
Test Objectives: Assure the support of interactions with the customer to determine specific service requirements that will meet the customer's service needs and that align with the customer's willingness to pay for those services.

CM.03.08: Requirement Name: Customer service planning function set
Requirement Description: ITU-T M.3400 – Section 7.3.8
Test Objectives: Assure the support of access to a plan for specific service offerings and creation of services for a customer based on specific customer needs, marketing input and customer-specific demand forecasts. It allows for the ongoing administration of those service offerings.

CM.03.09: Requirement Name: Customer service feature definition function set
Requirement Description: ITU-T M.3400 – Section 7.3.9
Test Objectives: Assure that the Customer Service Feature Definition function set is in accordance with the following TMN management functions:

1. Event reporting control – Customer's OSF selects and controls the flow of notifications from the provider's OSF.
2. Customize configuration – Customer's OSF requests the provider's OSF to customize the configuration of service resources provided to customer.
3. Log control – Customer's OSF selects and controls the information the provider's OSF should log.

CM.03.10: Requirement Name: Solution proposal function set
Requirement Description: ITU-T M.3400 – Section 7.3.10
Test Objectives: Assure the support of access to information to develop a proposal to meet a particular customer's business need based on the resources that will be available when the customer needs them and at a fair market price. Service feature conflicts should be identified and resolved during

the development of the solution proposal. It shall support interactions with the customer to present the proposal.

CM.04.01: Requirement Name: Provisioning policy function set
Requirement Description: ITU-T M.3400 – Section 7.4.1
Test Objectives: Assure that the Provisioning Policy function set is in accordance with the following TMN management functions:

1. Request route determination guidelines – Manager requests agent to send route determination guidelines (determination of economic route, route redundancy, etc.). Agent responds with requested information.
2. Request equipment design guidelines – Manager requests agent to send equipment design guidelines (equip partially or fully, variable vs. fixed bandwidth line card, etc.). Agent responds with the requested information.

CM.04.02: Requirement Name: Material management policy function set
Requirement Description: ITU-T M.3400 – Section 7.4.2
Test Objectives: Assure the support of access to guidelines for the selection and use of materials.

CM.04.03: Requirement Name: Access route determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.3
Test Objectives: Assure the support of requests for an access route for a specific service type. It should support responses that state an economic route from the customer point of presence to an appropriate transport network or switch.

CM.04.04: Requirement Name: Directory address determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.4
Test Objectives: Assure the support of requests for a directory address. It should support responses that state a telephone number or other network address.

CM.04.05: Requirement Name: Leased circuit route determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.5
Test Objectives: Assure that the Leased Circuit Route Determination function set is in accordance with the following TMN management function:

1. Set automatic switch to alternate routing on failure – Manager requests agent to specify back-ups for connection.

CM.04.06: Requirement Name: Request for service function set
Requirement Description: ITU-T M.3400 – Section 7.4.6
Test Objectives: Assure that the Request for Service function set is in accordance with the following TMN management functions:

1. Request creation of a telecommunications service – Manager requests the creation of a telecommunications service by an agent.
2. Request deletion of a telecommunications service – Manager requests the deletion of a telecommunications service by an agent.
3. Request modification of a telecommunications service – Manager requests the modification of a telecommunications service by an agent.
4. Cancel a telecommunications service request – Manager requests the cancellation of a previous telecommunications service request by an agent.

CM.04.07: Requirement Name: Service status administration function set
Requirement Description: ITU-T M.3400 – Section 7.4.7
Test Objectives: Assure that the Service Status Administration function set is in accordance with the following TMN management functions:

1. Report creation of service resource to service customer – When a service resource is created, an indication of creation is sent to the manager by the agent.
2. Report deletion of service resources to service customer – When a service resource is deleted, an indication of deletion is sent to the manager by the agent.
3. Report configuration change of service resource to service customer – When the configuration of a service resource is changed, an indication of configuration change is sent to the manager by the agent.
4. Report service state change of service resource to service customer – When the service state of service resource is changed, an indication of the service state change is sent to the manager by the agent.
5. Request of information about service resource by service customer – Manager requests agent to transmit information about a service resource to the manager.
6. Change administrative state of a service customer resource – Manager requests agent to change the administrative state of a service resource.
7. Report progress of a telecommunications service customer request – Agent reports progress of a telecommunications service request to a manager.
8. Retrieve progress of a telecommunications service customer request – Manager retrieves progress of a telecommunications service request from an agent.

CM.04.08: Requirement Name: Network resource selection and assignment function set
Requirement Description: ITU-T M.3400 – Section 7.4.8
Test Objectives: Assure the support of requests for network resources and responds with selected resources and the associated service features. It should provide access to a network resource database. It should support requests for selection and assignment of resources and service features that meet any designated selection criteria.

CM.04.09: Requirement Name: Interexchange circuit design function set
Requirement Description: ITU-T M.3400 – Section 7.4.9
Test Objectives: Assure the support of requests for the selection of an appropriate path for circuits that cross exchange boundaries (e.g. message trunks) based on routing design, facility design and demand forecast. It should support responses stating the selected resources.

CM.04.10: Requirement Name: Access circuit design function set
Requirement Description: ITU-T M.3400 – Section 7.4.10
Test Objectives: Assure the support of requests for access circuit design. It should support responses that state the access points from the customer to the network.

CM.04.11: Requirement Name: Leased circuit design function set

Requirement Description: ITU-T M.3400 – Section 7.4.11
Test Objectives: Assure that the Leased Circuit Design function set is in accordance with the following TMN management functions:

1. Dynamic link configuration – Manager requests agent to configure dynamic links.
2. Dynamic link reconfiguration – Manager requests agent to reconfigure dynamic links.
3. Dynamic link endpoint configuration – Manager requests agent to configure dynamic link endpoints.
4. Connection configuration – Manager requests agent to configure connections.
5. Connection reconfiguration – Manager requests agent to reconfigure connections.
6. Connection endpoint configuration – Manager requests agent to configure connection endpoints.

CM.04.12: Requirement Name: Facility design function set
Requirement Description: ITU-T M.3400 – Section 7.4.12
Test Objectives: Assure the support of requests for facility design, along a specified route. It should support responses that state the selected resources.

CM.04.13: Requirement Name: Manage pending network changes function set
Requirement Description: ITU-T M.3400 – Section 7.4.13
Test Objectives: Assure the support of requests for a coordinated set of changes in the connectivity and parameters of an end-to-end circuit at a specific future time. It should support actions to carry out the change. It should support confirmation and jeopardy reports. It should support confirmation of requests when all requested actions have been confirmed. It should support jeopardy reports as appropriate.

CM.04.14: Requirement Name: Network connection management function set
Requirement Description: ITU-T M.3400 – Section 7.4.14
Test Objectives: Assure the support of requests for a particular set of cross-connections required for implementation of a circuit design. It should support actions to request the cross-connections to be established in NEs or groups of NEs.

CM.04.15: Requirement Name: Circuit inventory notification function set
Requirement Description: ITU-T M.3400 – Section 7.4.15
Test Objectives: Assure that the Circuit Inventory Notification function set is in accordance with the following TMN management functions:

1. Report creation of circuit resource – When a circuit resource is created, an indication of creation is sent to manager from agent.
2. Report deletion of circuit resource – When a circuit resource is deleted, an indication of deletion is sent to manager from agent.
3. Report configuration change of circuit resource – When the configuration of a circuit resource is changed, an indication of configuration change is sent to manager from agent.
4. Report service state change of circuit resource – When the service state of circuit resource is changed, an indication of the service state change is sent to manager from agent.

CM.04.16: Requirement Name: Circuit inventory query function set

Requirement Description: ITU-T M.3400 – Section 7.4.16
Test Objectives: Assure that the Circuit Inventory Query function set is in accordance with the following TMN management function:

1. Request information of circuit resource for customer – Manager requests agent to transmit the information of network resource.

CM.04.17: Requirement Name: NE(s) configuration function set
Requirement Description: ITU-T M.3400 – Section 7.4.17
Test Objectives: Assure that the Circuit Inventory Notification function set is in accordance with the following TMN management functions:

1. Request configuration – Manager requests that the agent report the current configuration of each entity.
2. Configuration report – For each entity, agent reports status, capacity of the entity, optional parameters, type of entity (in sufficient detail for manager identification) and the version and revision of the version.
3. Grow – Manager notifies agent of the presence of a newly installed entity.
4. Prune – Manager notifies agent of the disconnection of an entity.
5. Restore – Manager notifies agent to begin monitoring the newly installed entity.
6. Assign – Manager notifies agent that a previously unequipped entity is now equipped.
7. Delete – Manager notifies agent that a previously equipped entity is no longer equipped.
8. Set service state – Manager directs agent to place the specified entity in one of the following states: in-service (available for use), out-of-service (unavailable for use), standby (not faulty but not performing normal function), reserved.
9. Request assignments – Manager requests that agent report the identity of each assigned entity. The request may be for a specified entity or for all equipped entities.
10. Assignment reports – Agent reports the identity of each assigned channel for each equipped entity or for a specified entity.
11. Set parameters – Manager directs agent to set parameters associated with a specified entity.
12. Set service thresholds – Manager directs agent to set performance thresholds for the specified channel.
13. Add/drop – Manager directs agent to insert or remove a channel from the complement of through-channels.
14. Cross-connect – Manager directs agent to interconnect two specified channels operating at the same rate.
15. Disconnect – Manager directs agent to remove the interconnection between two specified channels.
16. Start transmission test – Manager directs agent to begin a transmission test on a given circuit.
17. Balance – Manager directs agent to perform a balance test/adjustment.
18. Start transponder test – Manager directs agent to look for a transponder signal on the given circuit.
19. Set report periods – The manager directs agent to set or change report periods.
20. Request report periods – The manager requests agent to send the current periods to the manager.

21. Restart request – Manager requests agent to restart an equipment, service or the system. The restart may be soft or hard.
22. Restart report – Agent reports to manager that it has undertaken a soft or hard restart as part of its recover procedures. Such procedures may or may not have been initiated by the manager.

CM.04.18: Requirement Name: NE(s) administration function set
Requirement Description: ITU-T M.3400 – Section 7.4.18
Test Objectives: Assure that the NE(s) Administration Function function set is in accordance with the following TMN management functions:

1. Set clock – Manager directs agent to set agent system clock to current calendar, date and time.
2. Backup copy – Manager directs agent to make a backup copy of the designated agent database file for purposes of archiving for future restoration.
3. Terminate procedure – Manager directs the agent to terminate a process between a manager and a agent.
4. Route messages – Manager directs agent to route automatic messages generated by agent to one or multiple communications channels.
5. Set service controls – Manager directs agent to assign user access and functional capability.

CM.04.19: Requirement Name: NE(s) database management function set
Requirement Description: ITU-T M.3400 – Section 7.4.19
Test Objectives: Assure that the NE(s) Database Management function set is in accordance with the following TMN management functions:

1. Initialize – Manager configures a new database that is related to an agent. This may or may not be downloaded to the agent. This may also include loading a new program related to the agent.
2. Reinitialize – Manager reconfigures the database within a agent while it is in service.
3. Update – Manager adds, changes or deletes one or more records in the database of an agent. This can be done in a delayed activation mode or upon command entry. It may also be able to enter database updates on a test basis prior to permanent entry.
4. Query – Manager reads agent for all or part of its database contents.
5. Backup – Manager keeps a copy of all or part of the database of a agent. In case of memory failure in the agent, the manager downloads the backup copy to the agent.

CM.04.20: Requirement Name: Assignable inventory management function set
Requirement Description: ITU-T M.3400 – Section 7.4.20
Test Objectives: Assure the support of access to information concerning NE resources that are assigned to services or that are currently available for assignment. It should monitor utilization levels of resources and sends notifications when utilization exceeds thresholds. It should respond to requests for utilization information.

CM.04.21: Requirement Name: NE(s) resource selection and assignment function set
Requirement Description: ITU-T M.3400 – Section 7.4.21

Test Objectives: Assure the support of requests for availability status of resources, requests for the selection and assignment of those resources, requests for the resources to change service state, and reports the assignments, as appropriate. These resources may be NEs, a group of NEs, or logical resources such as bandwidth or service logic programs.

CM.04.22: Requirement Name: NE(s) path design function set
Requirement Description: ITU-T M.3400 – Section 7.4.22
Test Objectives: Assure the support of requests for a path through an NE or a group of NEs that will allow for connection with other NEs or network interfaces to establish an end-to-end circuit connection. It should Select and bind resources to form the required connection.

CM.04.23: Requirement Name: Loading program for service feature(s) function set
Requirement Description: ITU-T M.3400 – Section 7.4.23
Test Objectives: Assure the support of software loading to activate service-specific features in NE components such as the downloading of software features to line cards at the time of activation of service. Loading should include support of reporting the results of testing that the load is successful and of back-out of the software features if the load is not successfully completed.

CM.04.24: Requirement Name: NE(s) inventory notification function set
Requirement Description: ITU-T M.3400 – Section 7.4.24
Test Objectives: Assure the support of notifications from an NE about changes in the features that the NE supports.

CM.04.25: Requirement Name: NE(s) inventory query function set
Requirement Description: ITU-T M.3400 – Section 7.4.25
Test Objectives: Assure the support of access to information, as held in equipment that manages an NE, about the current resources of an NE and the features that an NE supports.

CM.04.26: Requirement Name: Manage pending changes in NE(s) function set
Requirement Description: ITU-T M.3400 – Section 7.4.26
Test Objectives: Assure the support of access to information about the management of individual NE connections and the removal of NE connections if end-to-end connections cannot be completed. It should support notification of changes that result from differences between assigned and installed NE configurations.

CM.04.27: Requirement Name: Storage of parameters and cross-connects function set
Requirement Description: ITU-T M.3400 – Section 7.4.27
Test Objectives: Assure the support of access to NE information about its parameters and cross-connects.

CM.04.28: Requirement Name: Storage and execution of service features
Requirement Description: ITU-T M.3400 – Section 7.4.28
Test Objectives: Assure the support of access to NE information about its service feature settings and the capabilities defined by those settings.

CM.04.29: Requirement Name: Self-inventory function set

Requirement Description: ITU-T M.3400 – Section 7.4.29
Test Objectives: Assure the support of requests of information from an NE about its equipment configuration.

CM.05.01: Requirement Name: Priority service policy function set
Requirement Description: ITU-T M.3400 – Section 7.5.1
Test Objectives: Assure the support of guidelines for determining which services have priority for restoration in the event of a catastrophic failure. For example, hospitals, police and emergency service would be designated as priority services for automatic restoration.

CM.05.02: Requirement Name: Priority service restoration function set
Requirement Description: ITU-T M.3400 – Section 7.5.2
Test Objectives: Assure the support of notifications of an out-of-service status of services that are designated to have priority service features. It should support actions for restoration of such services, where such actions may usurp resources from lower priority services, based on designated priority service features. For example, an emergency service would be designated as a priority service. It should support access to data concerning priority levels.

CM.05.03: Requirement Name: Message handling systems network status function set
Requirement Description: ITU-T M.3400 – Section 7.5.3
Test Objectives: Assure that the Message Handling Systems Network Status function set is in accordance with the following TMN management functions:

1. Request message storage status data – Manager requests agent to transmit the message storage status data of store-and-forward communication to manager.
2. Message storage status data report – Agent sends the status data to manager.

CM.05.04: Requirement Name: Leased circuit network status function set
Requirement Description: ITU-T M.3400 – Section 7.5.4
Test Objectives: Assure that the Leased Circuit Network Status function set is in accordance with the following TMN management functions:

1. Request status of dynamic provisioning of leased circuit network – Manager requests agent to transmit the status of dynamic provisioning to manager.
2. Status report of dynamic provisioning of leased circuit networks – Agent sends the current status to manager.

CM.05.05: Requirement Name: Transport network status function set
Requirement Description: ITU-T M.3400 – Section 7.5.5
Test Objectives: Assure that the Leased Circuit Network Status function set is in accordance with the following TMN management functions:

1. Request status of automatic transmission restoration – Manager requests agent to transmit the switching activities and current status of automatic transmission restoration.
2. Status report of automatic transmission restoration – Agent sends the current status of the switching operations to manager.

CM.05.06: Requirement Name: NE(s) status and control function set
Requirement Description: ITU-T M.3400 – Section 7.5.6

Test Objectives: Assure that the NE(s) Status and Control function set is in accordance with the following TMN management functions:

1. Request status – Manager requests agent to send current status information.
2. Status report – Agent reports to manager the value of a monitored parameter. It may be sent on demand by manager or on a scheduled basis.
3. Schedule status report – Manager directs agent to establish a schedule for the reporting of status information.
4. Request status report schedule – Manager directs agent to send the current schedule of status reporting agent responds with the schedule.
5. Service availability timetable – Manager sends agent timetable of when a specified service is to be available for use.
6. Allow/inhibit automatic restoration – Manager directs agent to allow or inhibit automatic restoration in an M+N or duplex system.
7. Operator/release automatic restoration – Manager directs agent to switch a specified line or equipment to the redundant unit or release it from the redundant unit. For an M+N system, service is placed on the redundant unit and taken off the working unit. For a duplex system, the main unit becomes standby and the standby unit becomes the main unit.
8. Control event report – Manager selects and controls the flow of notifications from the agent to the manager.

CM.05.07: Requirement Name: Access to state information function set
Requirement Description: ITU-T M.3400 – Section 7.5.7
Test Objectives: Assure the support of access to the current state of a resource. This information should be available to queries and should also be used to determine the legality of requested state changes.

CM.05.08: Requirement Name: Notification of state changes by NEs function set
Requirement Description: ITU-T M.3400 – Section 7.5.8
Test Objectives: Assure the support for reporting of changes of state as the result of recognition that a state has changed such as a change from "enabled" to "disabled" in the event of a failure. Automatic notification of change of state may be initiated by the NE.

9.2.3 Testing Account Management

AM.01.01: Requirement Name: Planning of the usage measurement process function set
Requirement Description: ITU-T M.3400 – Section 8.1.1
Test Objectives: Assure the support of processes and systems to improve accurate and efficient usage measurement for products and services. It should provide access to information concerning the metrics of the usage data stream.

AM.01.02: Requirement Name: Management of the usage measurement process function set
Requirement Description: ITU-T M.3400 – Section 8.1.2

Test Objectives: Assure the support for the management of processes and systems to ensure accurate and efficient usage measurement for products and services. It should provide management reports that may include total number of records, time criteria, lost records, multiple records, mutilate records, etc. It should support notifications as the reports are requested or defined.

AM.01.03: Requirement Name: Usage aggregation function set
Requirement Description: ITU-T M.3400 – Section 8.1.3
Test Objectives: Assure the support of access to summaries of service-level usage events by customer by service/product as described by specific carrier-defined criteria.

AM.01.04: Requirement Name: Service usage correlation function set
Requirement Description: ITU-T M.3400 – Section 8.1.4
Test Objectives: Assure the support to associate usage data based on provider-defined criteria related to a single product/service instance but possibly across multiple networks. Correlation may associate data related to a single usage event but collected from multiple sources across networks.

AM.01.05: Requirement Name: Service usage validation function set
Requirement Description: ITU-T M.3400 – Section 8.1.5
Test Objectives: Assure the support of access to usage data that have been edited and validated to ensure that they meet service-level integrity checks and conform to semantic and syntactic rules.

AM.01.06: Requirement Name: Usage distribution function set
Requirement Description: ITU-T M.3400 – Section 8.1.6
Test Objectives: Assure the support to distribute (sends notification of) the billable and informational formatted usage data to one or more processes, as requested or defined. Distribution is tracked for purposes of settlements, noninternal audits, etc. This function set differentiates usage data and determines the disposition/treatment of the usage measurements. It should include usage deletion functionality for usage information that will not continue in the data stream.

AM.01.07: Requirement Name: Usage surveillance function set
Requirement Description: ITU-T M.3400 – Section 8.1.7
Test Objectives: Assure the support to monitor all usage data to detect deviation from established norms. It should provide access to a database containing records of translation errors, general software errors, usage information recording errors, network routing errors, and potential fraud.

AM.01.08: Requirement Name: Usage error correction function set
Requirement Description: ITU-T M.3400 – Section 8.1.8
Test Objectives: Assure the support of access to usage data records after investigation and correction of usage data records found to be suspect or in error. The correction may be based on customer and service information concerning the network resources or services that the user has requested. This function will send notification of failure to correct the usage data records.

AM.01.09: Requirement Name: Usage testing function set

Requirement Description: ITU-T M.3400 – Section 8.1.9
Test Objectives: Assure the support of access to the results of simulation of user input to the network and captures usage measurement output for the purpose of validating the processing of usage data, as well as the actual generation of the usage data. It supports notifications concerning the disposition of the test call.

AM.01.10: Requirement Name: Measurement rules identification function set
Requirement Description: ITU-T M.3400 – Section 8.1.10
Test Objectives: Assure the definition of the set of usage measurement criteria to be applied to a usage event. It supports the criteria or rules by which function sets such as Usage aggregation, Usage correlation, Usage distribution, and Usage long-term storage classify or group usage data. It should provide access to identification of customer account/configuration and identification of product/service.

AM.01.11: Requirement Name: Network usage correlation function set
Requirement Description: ITU-T M.3400 – Section 8.1.11
Test Objectives: Assure the support of access to usage data that have been correlated based on provider-defined criteria related to a single product/service instance within the network. Correlation may associate data related to a single usage event but collected from multiple sources within the network, or data from multiple usage events.

AM.01.12: Requirement Name: Usage short-term storage function set
Requirement Description: ITU-T M.3400 – Section 8.1.12
Test Objectives: Assure the support of access to usage data, records, errors, and reports for subsequent access by other functions or applications. Assists in business continuity and disaster recovery in the event that the communication path to downstream processes is corrupted or destroyed.

AM.01.13: Requirement Name: Usage long-term storage function set
Requirement Description: ITU-T M.3400 – Section 8.1.13
Test Objectives: Assure the support of access to raw usage data, records, errors (e.g. translation, software, recording, network routing, etc.), and reports. The storage requirements for this archive may be defined by regulatory, business, and/or service requirements.

AM.01.14: Requirement Name: Usage accumulation function set
Requirement Description: ITU-T M.3400 – Section 8.1.14
Test Objectives: Assure the support for collection of usage data.

AM.01.15: Requirement Name: Usage validation function set
Requirement Description: ITU-T M.3400 – Section 8.1.15
Test Objectives: Assure the support of access to usage data that have been edited and validated to ensure that it meets specific integrity checks and conforms to semantic and syntactic rules. (For example, checking each usage element to verify that a valid value has been recorded.) It supports verification that usage data is collected from scheduled NE(s) in timely fashion. Upon the detection of errors, this function reports them to the Usage error correction function.

AM.01.16: Requirement Name: Administration of usage data collection function

set
Requirement Description: ITU-T M.3400 – Section 8.1.16
Test Objectives: Assure the disposition determination of logged usage data, which should provide access to the data, and schedules reporting of bulk usage data.

AM.01.17: Requirement Name: Usage generation function set
Requirement Description: ITU-T M.3400 – Section 8.1.17
Test Objectives: Assure that the Usage Generation function set is in accordance with the following TMN management functions:

1. Create a data collection – Manager directs agent to set parameters to a charging data collection process.
2. Delete a data collection – Manager directs the agent to remove a charging data collection process.
3. Activate a data collection – Manager directs the agent to start up a defined charging data collection process.
4. De-activate a data collection – Manager directs the agent to stop a defined charging data collection process.
5. Get data collection data – Manager requests the agent to report data of the defined and/or activated data collections.
6. Set a data collection – Manager directs the agent to change parameters in a charging data collection definition.
7. Get charging record – Manager requests the agent to send a charging record, either a call record or a counter record or several records, according to the specification in the request. Agent replies with the data and saves the data.
8. Transfer charging block – Agent transfers automatically a charging block or several blocks to the manager according to the earlier activated data collection. Call records are deleted in the agent.
9. Get coin-box status – Manager requests the agent to report the status of the pay-phone coin box. Agent sends the requested status data to the manager.

AM.02.01: Requirement Name: Pricing strategy function set
Requirement Description: ITU-T M.3400 – Section 8.2.1
Test Objectives: Assure the support for management of data tables reflecting corporate strategies for the pricing of product lines.

AM.02.02: Requirement Name: Tariff and price administration function set
Requirement Description: ITU-T M.3400 – Section 8.2.2
Test Objectives: Assure that the Tariff and Price Administration function set is in accordance with the following TMN management functions:

1. Create tariff class – Manager directs agent to create a tariff class corresponding to a certain service, origination and destination.
2. Delete tariff class – Manager directs agent to delete a tariff class.
3. Set tariff class – Manager directs agent to change a tariff class.
4. Get tariff class data – Manager requests the agent to report the defined tariff class data; agent replies with the data.
5. Create a tariff – Manager directs agent to create a tariff.
6. Delete a tariff – Manager directs the agent to delete a tariff.
7. Set a tariff – Manager directs the agent to change a tariff.
8. Get tariff data – Manager requests agent to report tariff data, agent replies with the data.

9. Create tariff period of the day – Manager directs the agent to create a new tariff period of the day.
10. Delete tariff period of the day – Manager directs the agent to delete an existing tariff period of the day.
11. Set tariff period of the day – Manager directs the agent to change a tariff period of the day.
12. Set tariff period data of the day – Manager requests agent to report tariff period of the day, agent replies with the data.
13. Create day class – Manager directs the agent to create a day class into the calendar table.
14. Delete day class – Manager directs the agent to delete a day class from the calendar table.
15. Set day class – Manager directs the agent to change a day class in the calendar table.
16. Get day class data – Manager requests the agent to report a calendar table data agent replies with the data.

AM.02.03: Requirement Name: Costing function set
Requirement Description: ITU-T M.3400 – Section 8.2.3
Test Objectives: Assure the support of mechanisms for the costing (cost determination and analysis) of services and features (i.e. determination of basic switching costs, costs of Intelligent Network features, and network costs) for use in pricing and tariff filing. It may support reading of usage information from the Usage Measurements: Usage distribution function set as a component of cost tracking.

AM.02.04: Requirement Name: Settlements policy function set
Requirement Description: ITU-T M.3400 – Section 8.2.4
Test Objectives: Assure the support of access to guidelines for the apportionment of usage charges. The guidelines should reflect negotiations based on revenue and pricing that are part of business relationships with other carriers/providers.

AM.02.05: Requirement Name: Feature pricing function set
Requirement Description: ITU-T M.3400 – Section 8.2.5
Test Objectives: Assure the support for the application of corporate strategies to the pricing of individual products/services. It should supply Usage Measurement functions with the pricing information necessary to generate billing data. It should also supply the Collections and Finance functions with the requisite information to answer customer pricing questions.

AM.02.06: Requirement Name: Provision of access to tariff/price information function set
Requirement Description: ITU-T M.3400 – Section 8.2.6
Test Objectives: Assure the support for a means by which the TMN and the public may determine rates and charges.

AM.02.07: Requirement Name: Rating usage function set
Requirement Description: ITU-T M.3400 – Section 8.2.7
Test Objectives: Assure the support for the financial components of the billable records. These components may be the internal costs, initial non-discounted rates, discounted rates, rates of special offerings, wholesale or

retail rates, and/or final pricing. Rating information should be applied to the usage data obtained from the Usage Measurement functionality. This function set shall support notifications of failure to apply the financial components.

AM.02.08: Requirement Name: Totalling usage charges function set
Requirement Description: ITU-T M.3400 – Section 8.2.8
Test Objectives: Assure the support for reading bill line items, grouped by customer, and provides access to the total charge, after application of any appropriate discounts or surcharges.

AM.03.01: Requirement Name: Planning of the billing process function set
Requirement Description: ITU-T M.3400 – Section 8.3.1
Test Objectives: Assure the support for plans processes and systems to improve accurate and efficient billing and collections for products and services.

AM.03.02: Requirement Name: Management of the billing process function set
Requirement Description: ITU-T M.3400 – Section 8.3.2
Test Objectives: Assure the support for the management of processes and systems to ensure accurate and efficient billing and collections for products and services.

AM.03.03: Requirement Name: General accounting operations function set
Requirement Description: ITU-T M.3400 – Section 8.3.3
Test Objectives: Assure the support to manage the base chart of accounts for categorization, tracking and reporting of financial expenditures. It should support the monitoring of financial operations to ensure compliance to proper accounting practices. It should also support periodic reconciliation of account balances for the purpose of generating financial results.

AM.03.04: Requirement Name: General ledger function set
Requirement Description: ITU-T M.3400 – Section 8.3.4
Test Objectives: Assure the support for the tracking of equity, income from operations, costs and expenses, nonoperating income and expense, and taxes. It should also provides for movement of costs to various accounts/projects for accurate statement of costs and for corrections of incorrectly booked costs.

AM.03.05: Requirement Name: Accounts receivable function set
Requirement Description: ITU-T M.3400 – Section 8.3.5
Test Objectives: Assure the support the tracking of receipts due (including the amount, the date and identification of the account) for products and services rendered and payments received. It should support posting of transactions into the ledger. It should also support reading of invoice and payment data and provides access to summaries of such information.

AM.03.06: Requirement Name: Accounts payable function set
Requirement Description: ITU-T M.3400 – Section 8.3.6
Test Objectives: Assure the support for payment to contractors, suppliers, other service providers, insurance, principal and interest, rents and leases, taxes, utilities.
NOTE – Compare to Purchasing, a Configuration Management function set.

AM.03.07: Requirement Name: Payroll function set
Requirement Description: ITU-T M.3400 – Section 8.3.7
Test Objectives: Assure the support for the administration and payment of employee salary, etc.

AM.03.08: Requirement Name: Benefits administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.8
Test Objectives: Assure the support for the administration of employee benefits.

AM.03.09: Requirement Name: Pension administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.9
Test Objectives: Assure the support for the administration of employee pensions.

AM.03.10: Requirement Name: Taxation function set
Requirement Description: ITU-T M.3400 – Section 8.3.10
Test Objectives: Assure the support for the management and reporting of corporate tax accounting, including the determination of the proper timing for reporting income and deductions for tax purposes.

AM.03.11: Requirement Name: Human resources function set
Requirement Description: ITU-T M.3400 – Section 8.3.11
Test Objectives: Assure the support of access to the organizational structure of the company, forecasting of staffing needs, administration of employment, management of compensation, employee relations, employee assignment, and employee development.

AM.03.12: Requirement Name: Invoice assembly function set
Requirement Description: ITU-T M.3400 – Section 8.3.12
Test Objectives: Assure the support for reading the current usage charge and combines it with recurring and one time charges as well as previous debits and credits to determine a customer's account balance at billing time.

AM.03.13: Requirement Name: Sending invoice function set
Requirement Description: ITU-T M.3400 – Section 8.3.13
Test Objectives: Assure the support for reading the assembled invoices and the preparation and distribution of the formatted invoices to customers.

AM.03.14: Requirement Name: Customer tax administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.14
Test Objectives: Assure the support of access to tax tables for the computation of taxes for customer invoice components.

AM.03.15: Requirement Name: In-call service request function set
Requirement Description: ITU-T M.3400 – Section 8.3.15
Test Objectives: Assure the support for on-demand, real-time request for usage information while a call is in progress or at its completion. It may initiate the processing of the usage information while the call proceeds (processing of the usage information may be destructive or non-destructive). It should support access to the complete usage information after the conclusion of the call. It should also support a time and charges quotation at the request of the party being charged for the call.

AM.03.16: Requirement Name: Storage of invoice function set
Requirement Description: ITU-T M.3400 – Section 8.3.16
Test Objectives: Assure the support of access to the long and short term storage of billing data.

AM.03.17: Requirement Name: Receipt of payment function set
Requirement Description: ITU-T M.3400 – Section 8.3.17
Test Objectives: Assure the support for the customer interface through which customers may make valid forms of remuneration for services provided. It should support crediting the customer's account. It should also support notifications of the received payment.

AM.03.18: Requirement Name: Inquiry response function set
Requirement Description: ITU-T M.3400 – Section 8.3.18
Test Objectives: Assure the support for the interface through which customers may have access to account balance, rating, and subscription information.

AM.03.19: Requirement Name: Collections function set
Requirement Description: ITU-T M.3400 – Section 8.3.19
Test Objectives: Assure the support of access to delinquent accounts. It supports requests for collection actions.

AM.03.20: Requirement Name: Customer account administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.20
Test Objectives: Assure the support of access to the customer account, including account balance, one-time and recurring charges, and history. It should support the adjustment of customer balances according to credit, debit, and consumption information. It should also support reading of a customer service profile.

AM.03.21: Requirement Name: Customer profile administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.21
Test Objectives: Assure the support for inputs from Service Negotiation & Planning and provides access to a database for the list of services of each individual customer.

AM.04.01: Requirement Name: Budgeting function set
Requirement Description: ITU-T M.3400 – Section 8.4.1
Test Objectives: Assure the support of access to the plan or schedule that adjusts costs (capital and expense) during a certain period (typically, the accounting year) to the estimated income for that period. It should provide access to the annual (or other periodic) budget. It should support modification of the budget when variations between performance and objectives arise.

AM.04.02: Requirement Name: Auditing function set
Requirement Description: ITU-T M.3400 – Section 8.4.2
Test Objectives: Assure the support for the regular examination, checking, and adjusting of financial records.

AM.04.03: Requirement Name: Cash management function set
Requirement Description: ITU-T M.3400 – Section 8.4.3

Test Objectives: Assure the support for cash flow analysis. It supports reconciliation between payments and receipts and the identification of the potential need for borrowing to bring them in line with the budget. It supports short-term cash management (acquisition of cash needed to run the business) by borrowing against lines of credit.

AM.04.04: Requirement Name: Raising equity function set
Requirement Description: ITU-T M.3400 – Section 8.4.4
Test Objectives: Assure the support of access to data and reports for long-term cash management through investments and the liquidation of assets. It supports determination for and management of stock offerings, including SEC filings and generation of prospectuses.

AM.04.05: Requirement Name: Cost reduction function set
Requirement Description: ITU-T M.3400 – Section 8.4.5
Test Objectives: Assure the support of access to corporate policies for reducing costs and the coordination of implementation plans.

AM.04.06: Requirement Name: Profitability analysis function set
Requirement Description: ITU-T M.3400 – Section 8.4.6
Test Objectives: Assure the support of access to data and reports concerning the assessment of the revenues and expenses of products to determine the profit or loss.

AM.04.07: Requirement Name: Financial reporting function set
Requirement Description: ITU-T M.3400 – Section 8.4.7
Test Objectives: Assure the support of access to financial information to be provided to employees, stockholders, government agencies, and the public.

AM.04.08: Requirement Name: Insurance analysis function set
Requirement Description: ITU-T M.3400 – Section 8.4.8
Test Objectives: Assure the support of access to data and plans for risk assessment and the determination of insurance needs.

AM.04.09: Requirement Name: Investments function set
Requirement Description: ITU-T M.3400 – Section 8.4.9
Test Objectives: Assure the support for the management of corporate investments.

AM.04.10: Requirement Name: Assets management function set
Requirement Description: ITU-T M.3400 – Section 8.4.10
Test Objectives: Assure the support for the tracking of current and long-term assets, including inventory and depreciation.
NOTE – Compare the Material management policy function in Configuration Management.

AM.04.11: Requirement Name: Tracking of liabilities function set
Requirement Description: ITU-T M.3400 – Section 8.4.11
Test Objectives: Assure the support for the tracking of current and long-term liabilities.

9.2.4 Testing Performance Management

PM.01.01: Requirement Name: QoS performance goal setting function set
Requirement Description: ITU-T M.3400 – Section 5.1.1
Test Objectives: Assure the support for the management of guidelines for the assessment of all Quality of Service (QoS) performance measures, by area and component(s).

PM.01.02: Requirement Name: Network performance goal setting function set
Requirement Description: ITU-T M.3400 – Section 5.1.2
Test Objectives: Assure the support for the management of guidelines for the assessment of network performance quality and availability in order to support service assurance and service offerings.

PM.01.03: Requirement Name: Subscriber service quality criteria function set
Requirement Description: ITU-T M.3400 – Section 5.1.3
Test Objectives: Assure the support for a network management query feature for offering Performance Management information to a customer, such as grades of service options, performance monitoring thresholds, or the possible conditions under which rebates are awarded when service quality goals are not met.

PM.01.04: Requirement Name: QoS performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.4
Test Objectives: Assure the support of access to the assessment summary of all combined QoS performance measures, by area, by type of customer, by type of service and by network components, that compares measured quality with the quality goals.

PM.01.05: Requirement Name: Network performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.5
Test Objectives: Assure the support of access to the assessment summary of network performance quality and availability.

PM.01.16: Requirement Name: NE(s) performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.6
Test Objectives: Assure the support of access to analyses of NE quality and availability performance parameters in order to support service assurance and/or service offerings. This function set should provide information to the Network performance characterization function.

PM.01.17: Requirement Name: Data integrity check function set
Requirement Description: ITU-T M.3400 – Section 5.1.17
Test Objectives: Assure the support for the indication that performance data, such as a count, has been compromised or invalidated by re-initialization (for example, the resetting of a clock), or internal equipment failure.

PM.02.01: Requirement Name: Performance monitoring policy function set
Requirement Description: ITU-T M.3400 – Section 5.2.1
Test Objectives: Assure that the Performance Monitoring Policy function set is in accordance with the following TMN management functions:

1. Set enterprise-default PM schedule – Manager directs the agent to assign a schedule for the reporting of PM data. This schedule is to be

used, by default, across the enterprise. It may be overridden (for valid business reasons) by subordinate functionality.

2. Request enterprise-default PM schedule – Manager directs the agent to send a current PM schedule. Agent responds with the requested information. This schedule is the schedule to be used, by default, across the enterprise.
3. Set PM grade of service profile – Manager directs the agent to assign designated values to the quality parameters associated with each grade of service.
4. Request PM grade of service profile – Manager directs the agent to send current values of grade of service profiles. Agent responds with the requested information.
5. Set PM impairment criteria – Manager directs the agent to assign designated values to PM impairment criteria. These criteria are applied to PM measurements to determine whether a sequence of threshold crossing alerts indicates that an impairment of a resource is persistent.
6. Request PM impairment criteria – Manager directs the agent to send current values of PM impairment criteria. Agent responds with the requested information.
7. Set PM trend analysis pattern – Manager directs the agent to assign designated values to a PM trend analysis pattern. A PM trend analysis pattern is a set of parameters of an algorithm that analyses raw PM data from a monitoring point and characterizes the data as (for example) increasing in severity over time or cyclic or associated with service customer activity.
8. Request PM trend analysis pattern – Manager directs the agent to send current values of PM trend analysis pattern. Agent responds with the requested information.
9. Set PM correlation and filtering rules – Manager directs the agent to assign designated values to PM correlation and filtering rules. These rules are used to determine whether PM threshold crossing alerts are correlated or can be filtered.
10. Request PM correlation and filtering rules – Manager directs the agent to send current values of PM correlation and filtering rules. Agent responds with the requested information.

PM.02.02: Requirement Name: Network performance monitoring event correlation and filtering function set
Requirement Description: ITU-T M.3400 – Section 5.2.2
Test Objectives: Assure the support for the reporting of the root cause of PM threshold crossing alerts and other PM events, as inferred by an event correlation process that uses knowledge of the topology and states of a network and its component NEs, to facilitate network alarm analysis. It should provide access to information concerning identified root causes. It should also generates non-redundant notifications of trails that are found to generate persistent threshold crossing alerts.

PM.02.03: Requirement Name: Data aggregation and trending function set
Requirement Description: ITU-T M.3400 – Section 5.2.3
Test Objectives: Assure the support of access to aggregated and correlated end-to-end current and history PM information to detect and aid in the sectionalization of network faults and impairments. It should also provide access to trending information, that supports the extrapolation of historical

data to predict future performance and to identify persistent or worsening impairments.

PM.02.04: Requirement Name: Circuit-specific data collection function set
Requirement Description: ITU-T M.3400 – Section 5.2.4
Test Objectives: Assure the support for collecting all applicable data for a given circuit across multiple NEs. Information collected at the circuit level flows into the Data aggregation and trending function set.

PM.02.05: Requirement Name: Traffic status function set
Requirement Description: ITU-T M.3400 – Section 5.2.5
Test Objectives: Assure that the Traffic Status function set is in accordance with the following TMN management functions:

1. Report the service availability of NEs – Agent provides manager with the service availability status of the exchange and its major components and processors, common channel signalling systems, interface equipment and other major exchange equipment units. Such reports may be generated automatically, or in response to an operator request.
2. Report the status of controls on demand – Agent provides manager with the current status of traffic controls which have been applied by the operator, and automatic controls which have been established by the operator and applied by the exchange.
3. Report the busy/idle status of circuit groups – Agent automatically reports to manager the current busy/idle status of circuit groups for display on a terminal or other device.
4. Report the congestion status of exchanges – Agent automatically reports to manager the current congestion status of exchanges for display on a terminal or other device.
5. Report the receipt of automatic congestion control signals – Agent provides manager with current information on the hard-to-reach status of network destinations. Such information can be based on information received from distant exchanges or on information developed locally in the exchange.
6. Manually add/remove hard-to-reach status of destinations – Upon request by an operator, manager commands agent to assign or remove HTR status to destinations, and to override automatic HTR designations.
7. Report hard-to-reach status of destinations on demand – Upon request of an operator, agent reports to manager the HTR status of destinations.
8. Report the congestion status of the common channel signalling network – Agent automatically reports to manager the current congestion status of the common channel signalling network for display on a terminal or other device.
9. Report the receipt of common channel signalling network management signals – Agent provides to manager an indication that a common channel signalling network management signal has been received by the exchange, including the identity of the signalling point for which the signal relates, the type of signal and the time of its receipt.

PM.02.06: Requirement Name: Traffic performance monitoring function set
Requirement Description: ITU-T M.3400 – Section 5.2.6

Test Objectives: Assure that the Traffic Performance Monitoring function set is in accordance with the following TMN management functions:

1. Report circuit group data and parameters on a scheduled basis – Agent reports to manager circuit group traffic data and calculated network management parameters automatically according to a schedule.
2. Report circuit group data and parameters on demand – Agent reports to manager circuit group traffic data and calculated network monitoring parameters in response to an operator request.
3. Report exchange load measurements on a scheduled basis – Agent reports to manager measurements of the traffic load on the exchange and its major components according to a schedule.
4. Report exchange load measurements on demand – Agent reports to manager measurements of traffic load on the exchange and its major components in response to an operator request.
5. Report exchange congestion on a scheduled basis – Agent reports to manager measurements of exchange switching congestion according to a schedule.
6. Report exchange congestion measurements on demand – Agent reports to manager measurements of exchange switching congestion in response to an operator request.
7. Report common channel signalling network load measurements on a scheduled basis – Agent reports to manager measurements of CCSS traffic according to a schedule.
8. Report common channel signalling network load measurements on demand – Agent reports to manager CCSS traffic measurements in response to an operator request.
9. Report common channel signalling network congestion measurements on a scheduled basis – Agent reports to manager CCSS network congestion measurements according to a schedule.
10. Report common channel signalling network congestion measurements on demand – Agent reports to manager CCSS congestion measurements in response to an operator request.
11. Report data on the performance of controls on a scheduled basis – Agent reports to manager data on traffic affected by network management controls according to a schedule.
12. Report data on the performance of controls on demand – Agent reports to manager data on traffic affected by network management controls in response to an operator request.

PM.02.07: Requirement Name: NE(s) threshold crossing alert processing function set
Requirement Description: ITU-T M.3400 – Section 5.2.7
Test Objectives: Assure the support of access to the root cause of PM threshold crossing alerts and other PM events, as inferred by an event correlation process that uses knowledge of the internal topology and states of an NE or set of NEs in a subnetwork. It should also provide access to processed NE threshold crossing alerts, that is those that are found to be persistent and that survive after those that are associated with alarms or threshold crossing alerts on supporting facilities are filtered out.

PM.02.08: Requirement Name: NE(s) trend analysis function set
Requirement Description: ITU-T M.3400 – Section 5.2.8

Test Objectives: Assure the support for reporting of trends that are detected by processing the historical data of an NE or group of NEs.

PM.02.09: Requirement Name: Performance monitoring data accumulation function set
Requirement Description: ITU-T M.3400 – Section 5.2.9
Test Objectives: Assure that the Performance Monitoring Data Accumulation function set is in accordance with the following TMN management functions:

1. Request PM data – Manager request the agent to send current PM data.
2. Report PM data – Agent sends performance data to the manager. It may be generated routinely by the agent, sent upon demand by the manager or by exception when a parameter threshold has been exceeded.
3. Allow/inhibit PM data – Manager directs the agent to start/stop the collection of PM data.
4. Reset PM data – Manager directs agent to reset storage registers for PM data.

PM.02.10: Requirement Name: Detection, counting, storage and reporting function set
Requirement Description: ITU-T M.3400 – Section 5.2.10
Test Objectives: Assure the support for reporting of results of the continuous detection, collection, and reporting of performance primitives, i.e. data or measurements, associated with a transmission, traffic, or service entity. Storage should imply that performance registers within an NE are readable on demand without resetting the count. Reporting should imply that an NE reports any performance parameters on demand, as well as reports periodically via scheduling.

PM.03.01: Requirement Name: Network traffic management policy function set
Requirement Description: ITU-T M.3400 – Section 5.3.1
Test Objectives: Assure the support for managing domains of control over different parts of the network and establishes plans for anticipated conditions of congestion (for example, storm patterns that are typical of the region and focused demands that result from promotions and surveys).

PM.03.02: Requirement Name: Traffic control function set
Requirement Description: ITU-T M.3400 – Section 5.3.2
Test Objectives: Assure that the Traffic Control function set is in accordance with the following TMN management functions:

1. Apply/modify/remove a manual control – Upon request from an operator, manager directs agent to modify manual network management traffic controls.
2. Establish/modify/remove an automatic control – Upon request from an operator, manager directs agent to modify automatic network management traffic controls.
3. Activate/deactivate an automatic control – Manager directs agent to activate or deactivate an automatic control that has been previously established.
4. Apply/modify/remove a special recorded announcement – Upon request from an operator, manager directs agent to establish a special

recorded announcement and to specify the type of traffic that is to be routed to the special announcement.

PM.03.03: Requirement Name: Traffic administration function set
Requirement Description: ITU-T M.3400 – Section 5.3.3
Test Objectives: Assure that the Tariff Administration function set is in accordance with the following TMN management functions:

1. Establish/change/remove a measurement schedule – Upon request from an operator, manager directs agent to establish, change or traffic measurement schedules in the exchange or operations system which set the type of measurements to be made, the periodicity of the measurements and the objects and entities for the measurements.
2. Establish/update a network management database – Manager directs agent to establish or update a database in the exchange or operations system of network statistics and information necessary to perform the network management function.
3. Establish/change/remove thresholds for status reporting, data reporting and HTR determination – Upon request from an operator, manager directs agent to establish, change or remove values for the various thresholds in the exchange or operations system for data calculation and reporting, status reporting and automatic control activation.
4. Establish/change/remove schedules for status and data reporting – Upon request from an operator, manager directs agent to establish, change or remove schedules in the exchange or operations systems for the reporting of status and network performance data.
5. Report routing table information on demand – Upon request from an operator, manager directs agent to establish, change or remove routing table information that resides in the exchange of operations system in response to an operator request.

PM.03.04: Requirement Name: Performance administration function set
Requirement Description: ITU-T M.3400 – Section 5.3.4
Test Objectives: Assure that the Performance Administration function set is in accordance with the following TMN management functions:

1. Schedule Performance Monitoring (PM) data report – Manager directs agent to establish a schedule for the reporting of PM data.
2. Request PM data report schedule – Manager directs agent to send the current PM data reporting schedule. Agent responds with the schedule.
3. Set PM attributes – Manager directs agent to assign designated values to PM attributes.
4. Request PM attributes – Manager requests agent to send current PM attributes.
5. PM attributes report – Agent sends the currently assigned PM attributes to manager.
6. Assign PM thresholds – Manager directs agent to set or change the PM parameter threshold.
7. Suspend/resume a PM data collection – Manager instructs agent to suspend/resume the PM data collection activity for a given monitored entity or set of monitored entities.

8. Screen PM data storage – Manager instructs the agent to originate historical data based on some screening criteria (e.g. suppress "all-zero" data).
9. Assign PM data collection interval – Manager instructs the agent about the duration of the PM data collection interval for a given entity or set of entities.
10. Request PM thresholds – Manager directs agent to send the current PM threshold.
11. Schedule QoS test calls – Manager directs agent to establish a schedule for the execution of QoS test calls.

PM.03.05: Requirement Name: Execution of traffic control function set
Requirement Description: ITU-T M.3400 – Section 5.3.5
Test Objectives: Assure the support for commands to change traffic controls and provides access to data concerning status and execution of the controls.

PM.03.06: Requirement Name: Audit report function set
Requirement Description: ITU-T M.3400 – Section 5.3.6
Test Objectives: Assure the support for reports on control information available at the NE.

PM.04.01: Requirement Name: Recommendations for performance improvement function set
Requirement Description: ITU-T M.3400 – Section 5.4.1
Test Objectives: Assure the support for generation of recommended steps, such as changes in procedure, augmentation or redistribution of capital or labour, etc., to improve quality in the future, as determined by improvements in performance measurements.

PM.04.02: Requirement Name: Exception threshold policy function set
Requirement Description: ITU-T M.3400 – Section 5.4.2
Test Objectives: Assure the support for managing conditions for taking corrective actions for exceptions to acceptable performance measurements, together with a designation of the type of action to be taken.

PM.04.03: Requirement Name: Traffic forecasting function set
Requirement Description: ITU-T M.3400 – Section 5.4.3
Test Objectives: Assure the support for reports on predicted changes in demand, from a combination of extrapolation of history and an evaluation of business factors. The prediction is needed far enough into the future that action may be taken to maintain quality targets.

PM.04.04: Requirement Name: Customer service performance summary (excludes traffic) function set
Requirement Description: ITU-T M.3400 – Section 5.4.4
Test Objectives: Assure the support for generation of reports on summaries of measurements for the purpose of evaluating the performance of a particular transport service or group of services. The customer can be provided access to the summary in order to verify that guaranteed service levels have been met, or to enable the customer to evaluate their own networks.

PM.04.05: Requirement Name: Customer traffic performance summary function set

Requirement Description: ITU-T M.3400 – Section 5.4.5
Test Objectives: Assure the support of access to a scheduled or exception report of offered traffic, usage and measures of congestion on a leased circuit, a group of leased circuits, a hunt group, or a leased physical or virtual network.

PM.04.06: Requirement Name: Traffic exception analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.6
Test Objectives: Assure the support for reporting analysed traffic data from a network or part of a network in order to detect and report on exceptional conditions due to unusual demand or reduced capacity. Traffic exception analysis is analysis of traffic patterns to detect blocking conditions that exceed thresholds. Reports of traffic blocking conditions that exceed thresholds should be generated. They should provide sufficient supporting information to reveal the extent of congestion and to support a determination of remedial action (re-routing, improved maintenance, additional capacity in switches or interexchange circuits, public service emergency announcements, etc.).

PM.04.07: Requirement Name: Traffic capacity analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.7
Test Objectives: Assure the support for generation of reports to estimate the level of offered traffic that can be carried by the current resources at the desired level of QoS.

PM.04.08: Requirement Name: Network performance characterization function set
Requirement Description: ITU-T M.3400 – Section 5.4.8
Test Objectives: Assure the support for generation of reports to characterize end-to-end performance of dedicated digital networks, which includes Network Interface-to-Network Interface, and Network Interface-to-Inter-Network Interface (point of termination), in relation to long-term (i.e. 30 or more days) accuracy and availability objectives.

PM.04.09: Requirement Name: NE(s) performance characterization function set
Requirement Description: ITU-T M.3400 – Section 5.4.9
Test Objectives: Assure that the NE(s) Performance Characterization function set is in accordance with the following TMN management functions:

1. Report PM data – Agent reports PM data to manager.
2. Report PM threshold violation – Agent informs the manager of a PM parameter threshold violation having occurred in a specific monitored entity.

PM.04.10: Requirement Name: NE(s) traffic exception analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.10
Test Objectives: Assure the support for collecting and analysing traffic data from an NE or group of NEs. Reports should be available on exceptional conditions due to unusual demand or reduced capacity.

PM.04.11: Requirement Name: NE(s) traffic capacity analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.11
Test Objectives: Assure the support for reporting analysed traffic data from an NE or a group of NEs in order to determine the traffic capacity for the measured mix of types of usage.

9.2.5 Testing Security Management

SM.01.01: Requirement Name: Legal review function set
Requirement Description: ITU-T M.3400 – Section 9.1.1
Test Objectives: Assure the support of access to data concerning legal review of corporate documents, service offerings and policies to protect the enterprise against claims and litigation.

SM.01.02: Requirement Name: Physical access security function set
Requirement Description: ITU-T M.3400 – Section 9.1.2
Test Objectives: Assure the support for coordination of the installation, maintenance and monitoring of all equipment used to restrict or validate access (e.g. electronic access systems requiring a coded badge or other device to validate person seeking access, metal detectors, etc.).

SM.01.03: Requirement Name: Guarding function set
Requirement Description: ITU-T M.3400 – Section 9.1.3
Test Objectives: Assure the support for human monitoring of access such as checking identification badges or checking bags and packages for people entering and leaving a building.

SM.01.04: Requirement Name: Personnel risk analysis function set
Requirement Description: ITU-T M.3400 – Section 9.1.4
Test Objectives: Assure the support for requests for checking the trustworthiness of current and prospective employees. The checks are similar to those for Security screening (for customers), but are usually more thorough.

SM.01.05: Requirement Name: Security screening function set
Requirement Description: ITU-T M.3400 – Section 9.1.5
Test Objectives: Assure the support for requests for validating that a customer is trustworthy (e.g. has a good credit rating that indicates an acceptable risk for providing service) and associated responses. It supports reading of appropriate databases.

SM.02.01: Requirement Name: Investigation of changes in revenue patterns function set
Requirement Description: ITU-T M.3400 – Section 9.2.1
Test Objectives: Assure the support for analysis of significant shifts in revenue that might indicate fraud or theft of service.

SM.02.02: Requirement Name: Support element protection function set
Requirement Description: ITU-T M.3400 – Section 9.2.2
Test Objectives: Assure the support for the determination of need, monitoring and analysis of alarm systems that support structures that house network equipment. These alarms may include power, HVAC (Heating, Ventilation, and Air Conditioning), fire, flood, and open-door-or-cabinet systems.

SM.02.03: Requirement Name: Customer security alarm function set
Requirement Description: ITU-T M.3400 – Section 9.2.3

Test Objectives: Assure the support of access by customers to security alarm information that indicates security attacks on their portion of the network.

SM.02.04: Requirement Name: Customer (external user) profiling function set
Requirement Description: ITU-T M.3400 – Section 9.2.4
Test Objectives: Assure that the Customer (external user) Profiling function set is in accordance with the following TMN management function:

1. Report usage status – Agent provides manager with a record that contains information of a statistical nature relevant to security.

SM.02.05: Requirement Name: Customer usage pattern analysis function set
Requirement Description: ITU-T M.3400 – Section 9.2.5
Test Objectives: Assure the support for reading of usage data and customer profiles from other functions. It supports the recording of service irregularities or anomalies such as billing and usage abnormalities. It provides access to such records.

SM.02.06: Requirement Name: Investigation of theft of service function set
Requirement Description: ITU-T M.3400 – Section 9.2.6
Test Objectives: Assure the support for investigation of customer and internal users whose usage patterns indicate possible fraud or theft of service. It may include requests for credit checking, and employment record checking.

SM.02.07: Requirement Name: Internal traffic and activity pattern analysis function set
Requirement Description: ITU-T M.3400 – Section 9.2.7
Test Objectives: Assure the support for the collection of audit trail information and the recording of anomalies or abnormalities that may indicate a breach of security or theft of customer services through employee action. It provides access to such data.

SM.02.08: Requirement Name: Network security alarm function set
Requirement Description: ITU-T M.3400 – Section 9.2.8
Test Objectives: Assure that the Network Security Alarm function set is in accordance with the following TMN management functions:

1. Request audit trail history – Manager requests the agent to send specified alarm information history; agent responds with the specified information.
2. Report security alarm – Agent notifies manager of security alarm information (including identification of the NE) upon the occurrence of a security alarm.
3. Audit trail report – Agent automatically reports to manager the result of audit trails.

SM.02.09: Requirement Name: Software intrusion audit function set
Requirement Description: ITU-T M.3400 – Section 9.2.9
Test Objectives: Assure the support of checks for signs of software intrusion (e.g. the presence of a known virus) in the TMN. Such checks can apply to any TMN system. They can be regularly scheduled and/or they may be triggered by security events.

SM.02.10: Requirement Name: Support element security alarm reporting function set

Requirement Description: ITU-T M.3400 – Section 9.2.10
Test Objectives: Assure the support of access to report information about security alarms so that containment and recovery activities may be initiated. It may include the reporting of environment alarms (e.g. fire or moisture) and intrusion detection alarms.

SM.03.01: Requirement Name: Protected storage of business data function set
Requirement Description: ITU-T M.3400 – Section 9.3.1
Test Objectives: Assure the support for the access and mechanisms, such as maintaining back copies of data and monitoring for data corruption, to secure business data.

SM.03.02: Requirement Name: Exception report action function set
Requirement Description: ITU-T M.3400 – Section 9.3.2
Test Objectives: Assure the support for exception reports such as security alarms. It also supports requests for action to limit the security breach such as isolation of equipment or data so that corruption is not propagated and requests for restoration of any corrupted data or equipment.

SM.03.03: Requirement Name: Theft of service action function set
Requirement Description: ITU-T M.3400 – Section 9.3.3
Test Objectives: Assure the support for receiving input on usage anomalies to initiate action to limit the security breach (e.g. remove user's access privileges, etc.). It should support requests to restore any corrupted data or equipment. It may also support requests for the initiation of litigation against a perpetrator of an illegal action.

SM.03.04: Requirement Name: Legal action function set
Requirement Description: ITU-T M.3400 – Section 9.3.4
Test Objectives: Assure the support for litigation against a perpetrator of an illegal action. This may be done in cooperation with law enforcement agencies.

SM.03.05: Requirement Name: Apprehending function set
Requirement Description: ITU-T M.3400 – Section 9.3.5
Test Objectives: Assure the support for actions to catch an intruder. This may be done in cooperation with law enforcement agencies. It may support the identification of an intruder (for example, by analyzing security logs, monitoring targets of intrusion or feeding misinformation to a suspected intruder).

SM.03.06: Requirement Name: Service intrusion recovery function set
Requirement Description: ITU-T M.3400 – Section 9.3.6
Test Objectives: Assure the support for requests to access backup files in order to restore service after detection of a security violation.

SM.03.07: Requirement Name: Administration of customer revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.7
Test Objectives: Assure the support of access to a list of all customer public keys and access control certificates for the current time period that are known or suspected of being invalid due to security violation (e.g. stolen secret keys) or administrative procedures (e.g. a customer has moved elsewhere).

SM.03.08: Requirement Name: Protected storage of customer data function set
Requirement Description: ITU-T M.3400 – Section 9.3.8
Test Objectives: Assure the support for the backup and restoration of stored customer data that can be used in support of intrusion recovery.

SM.03.09: Requirement Name: Severing external connections function set
Requirement Description: ITU-T M.3400 – Section 9.3.9
Test Objectives: Assure the support of requests for the severance of connections with a customer in an attempt to contain data and system corruption as the result of a detected security violation. It supports commands to carry out the request.

SM.03.10: Requirement Name: Network intrusion recovery function set
Requirement Description: ITU-T M.3400 – Section 9.3.10
Test Objectives: Assure the support of requests for restoration of the network configuration after detection of a security violation.

SM.03.11: Requirement Name: Administration of network revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.11
Test Objectives: Assure the support of access to a list of all network public keys and access control certificates for the current time period that are known or suspected of being invalid due to security violation (e.g. stolen secret keys) or administrative procedures (e.g. a system has been replaced).

SM.03.12: Requirement Name: Protected storage of network configuration data function set
Requirement Description: ITU-T M.3400 – Section 9.3.12
Test Objectives: Assure the support for the storage of network configuration data that can be used in support of intrusion recovery. It should allow for backup of such data, and for restoration of such backed up data upon request.

SM.03.13: Requirement Name: Severing internal connections function set
Requirement Description: ITU-T M.3400 – Section 9.3.13
Test Objectives: Assure the support for the severance of internal user connections in an attempt to contain data and system corruption as the result of a detected security violation.

SM.03.14: Requirement Name: NE(s) intrusion recovery function set
Requirement Description: ITU-T M.3400 – Section 9.3.14
Test Objectives: Assure the support for the access to backup files in order to restore NE or element management information after detection of a security violation.

SM.03.15: Requirement Name: Administration of NE(s) revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.15
Test Objectives: Assure the support for the access to a list of all keys and access control certificates used for NE and element management access that are known or suspected of being invalid due to security violation (e.g. stolen secret keys) or administrative procedures (e.g. an element management system or NE has been replaced).

SM.03.16: Requirement Name: Protected storage of NE(s) configuration data function set
Requirement Description: ITU-T M.3400 – Section 9.3.16
Test Objectives: Assure the support for data storage and provides access to that data for backup in support of intrusion recovery.

SM.04.01: Requirement Name: Security policy function set
Requirement Description: ITU-T M.3400 – Section 9.4.1
Test Objectives: Assure the support for the access to company guidelines for establishing and maintaining a secure environment for personnel, hardware, and software.

SM.04.02: Requirement Name: Disaster recovery planning function set
Requirement Description: ITU-T M.3400 – Section 9.4.2
Test Objectives: Assure the support of access to methods and procedures to be used in restoring the network in the event of a security breach and the resulting corruption of data.

SM.04.03: Requirement Name: Manage guards function set
Requirement Description: ITU-T M.3400 – Section 9.4.3
Test Objectives: Assure the support of access to information about the management of physical and mechanized devices used to provide security.

SM.04.04: Requirement Name: Audit trial analysis function set
Requirement Description: ITU-T M.3400 – Section 9.4.4
Test Objectives: Assure the support of access to methods and procedures for audit trail information to be collected and evaluated to identify possible and/or potential security violations by individuals or groups of users.

SM.04.05: Requirement Name: Security alarm analysis function set
Requirement Description: ITU-T M.3400 – Section 9.4.5
Test Objectives: Assure the support of access to guidelines for the monitoring, evaluating, and correlating security alarms.

SM.04.06: Requirement Name: Assessment of corporate data integrity function set
Requirement Description: ITU-T M.3400 – Section 9.4.6
Test Objectives: Assure the support of access to information to determine the need for security, monitoring, and analysis of security measures instituted to protect corporate data from unauthorized access, altering, tampering, and/or corruption.

SM.04.07: Requirement Name: Administration of external authentication function set
Requirement Description: ITU-T M.3400 – Section 9.4.7
Test Objectives: Assure the support of requests for and distributes codes for verification that a customer or user of a peer Administration is who they present themselves to be. It should also support an authentication path involving external authenticators. If a customer has been authenticated by an authentication agent outside the TMN, this function shall support the certification, if appropriate, that the external authentication agent is a valid entity for providing that kind of authentication.

SM.04.08: Requirement Name: Administration of external access control function set
Requirement Description: ITU-T M.3400 – Section 9.4.8
Test Objectives: Assure the support of requests for and distributes permissions (in accordance with security policy) for control over what a customer or user of a peer Administration can do with any given resource and includes establishing and validating customer permissions and credentials.

SM.04.09: Requirement Name: Administration of external certification function set
Requirement Description: ITU-T M.3400 – Section 9.4.9
Test Objectives: Assure the support of requests for and distributes permissions (in accordance with security policy) for control over what a customer or user of a peer Administration can do with any given resource and includes establishing and validating customer permissions and credentials.

SM.04.10: Requirement Name: Administration of external encryption and keys function set
Requirement Description: ITU-T M.3400 – Section 9.4.10
Test Objectives: Assure the support of requests for and distributes encryption keys to be used in communications between an external customer or user of a peer Administration and a TMN (such keys may be used for authentication, integrity, confidentiality and non-repudiation).

SM.04.11: Requirement Name: Administration of external security protocols function set
Requirement Description: ITU-T M.3400 – Section 9.4.11
Test Objectives: Assure the support for the management of joint implementation agreements with other jurisdictions to assure interoperability of security protocols. For example, it assures that both communicating parties use the same encryption algorithm with the same set of options and parameters. Further, it assures agreement on the kind of security information that shall be provided for authentication. It should also support the management for the administration of external security protocols.

SM.04.12: Requirement Name: Customer audit trial function set
Requirement Description: ITU-T M.3400 – Section 9.4.12
Test Objectives: Assure the support for a customer to establish and configure audit trails to obtain information about service usage. It should allow a customer access to usage and security event information related to their portion of the network.

SM.04.13: Requirement Name: Customer security alarm management function set
Requirement Description: ITU-T M.3400 – Section 9.4.13
Test Objectives: Assure the support for the customer access to security alarm information that indicates security attacks on their portion of the network.

SM.04.14: Requirement Name: Testing of audit trail mechanism function set
Requirement Description: ITU-T M.3400 – Section 9.4.14
Test Objectives: Assure the support for testing to ascertain that designated events are recorded in a security log.

SM.04.15: Requirement Name: Administration of internal authentication function set
Requirement Description: ITU-T M.3400 – Section 9.4.15
Test Objectives: Assure the support for receiving requests for and distributes codes for verification that internal users are who they present themselves to be.

SM.04.16: Requirement Name: Administration of internal access control function set
Requirement Description: ITU-T M.3400 – Section 9.4.16
Test Objectives: Assure that the Administration of Internal Access Control function set is in accordance with the following TMN management function:

1. Change permission – Manager requests agent to change a permission or set of permissions.

SM.04.17: Requirement Name: Administration of internal certification function set
Requirement Description: ITU-T M.3400 – Section 9.4.17
Test Objectives: Assure the support of requests for and distributes Access Control Certificates that permit internal users access to previously agreed upon sets of capabilities.

SM.04.18: Requirement Name: Administration of internal encryption and keys function set
Requirement Description: ITU-T M.3400 – Section 9.4.18
Test Objectives: Assure the support of requests for and distributes encryption keys to be used in communications between internal users (such keys may be used for authentication, integrity and confidentiality). It should provide information on which encryption algorithms are to be used and in which mode.

SM.04.19: Requirement Name: Network audit trail management function set
Requirement Description: ITU-T M.3400 – Section 9.4.19
Test Objectives: Assure the support for internal users, generally security personnel, to establish and configure audit trails to obtain information about network usage. This function should collect and allow an internal user access to network usage and security event information.

SM.04.20: Requirement Name: Network security alarm management function set
Requirement Description: ITU-T M.3400 – Section 9.4.20
Test Objectives: Assure the support for the collection of security alarm information that indicates network security violations. It should allow an internal user access to such data.

SM.04.21: Requirement Name: NE(s) audit trail management function set
Requirement Description: ITU-T M.3400 – Section 9.4.21
Test Objectives: Assure that the NE(s) Audit Trail Management function set is in accordance with the following TMN management functions:

1. Security audit request – Manager requests agent to report security audit.
2. Allow/inhibit logging – Manager instructs the agent to allow or inhibit logging of log records security alarms.

3. Condition logging – Manager instructs the agent to assign log attributes as specified by the manager what information to log.
4. Allow/inhibit audit trail – Manager directs the agent to allow/inhibit audit trail.
5. Schedule audit trail – Manager directs agent to establish a schedule to initiate, suspend or resume audit trails.
6. Report audit trail schedule – Manager directs agent to send the current audit trail schedule. Agent responds with the schedule.
7. Report audit trail status – Agent reports to manager the current status of audit trail.

SM.04.22: Requirement Name: NE(s) security alarm management function set
Requirement Description: ITU-T M.3400 – Section 9.4.22
Test Objectives: Assure the support for the collection of security alarms detected by lower level functions. It should provide access to such information, possibly including information resulting from the correlation of such alarms.

SM.04.23: Requirement Name: Administration of keys for NEs function set
Requirement Description: ITU-T M.3400 – Section 9.4.23
Test Objectives: Assure the support of requests for the generation of encryption keys to be used in communications between NEs or between an NE and an element management system or other building block. It should also support the distribution of these keys to NEs and communicating entities. Such keys may be used for authentication, integrity and confidentiality.

SM.04.24: Requirement Name: Administration of keys by an NE function set
Requirement Description: ITU-T M.3400 – Section 9.4.24
Test Objectives: Assure the support of requests for the generation within an NE of encryption keys to be used in communications between NEs or between an NE and an element management system or other building block. It should also support the distribution of these keys to communicating entities. Such keys may be used for authentication, integrity and confidentiality.

9.3 References

[1] MUSE1: TF1.3 - OAM and NSM chain automation for multidomain/ multi-provider access networks (MUSE_DTF1.3_Issue2_V01.pdf)

[2] ITU-T M.3400: TMN management functions

[3] ITU-T M.3050: Enhanced Telecom Operations Map (eTOM)

[4] TMF – GB921: Enhanced Telecom Operations Map (eTOM)

[5] DSL Forum – TR064: LAN-Side DSL CPE Configuration

[6] DSL Forum – TR069: CPE WAN Management Protocol

[7] DSL Forum – TR089: Data Model for TR-069

10 XDSL SPECIFIC TESTING

10.1 Introduction

This chapter 10 summarizes a wide range of test objectives for full service, end-to-end access solutions that are based on xDSL equipment. The aim is to test all kinds of xDSL properties, mainly dedicated to the physical layer.

The range of properties that should be tested covers many aspects of xDSL. Many of these properties have already been identified in various standards, and these standards have also set requirements for (different) xDSL transceivers. When appropriate, we refer to relevant standards that specify those properties in much more detail, because the aim of this current document is not to duplicate these standards. A single standard covering all physical layer properties does not exist, and therefore we have not restricted this chapter to one of them. Nevertheless, the scope of this document is not limited to already existing documents but encompasses new xDSL test aspects that shall be covered by future international test plans.

The xDSL properties to be tested are organized in a more generic way:

- Testing Management capabilities
- Testing Usability
- Testing Transmitted signal characteristics
- Testing Performance under noisy stress conditions

The objective is to test at least a subset of all the properties summarized in this chapter.

The selection of such a subset will vary with the application of an xDSL test. The same applies for the amount of detail and thoroughness of testing each property. Some of them are so laborious to test that it becomes essential to decide at the beginning of a test what is really required for a particular test application. For the purpose of this document, we make a distinction between the following kinds of tests:

- Functional testing
- Conformance testing

These words may cause some confusion and therefore we specify first what is meant by this, followed by a discussion on what kind of tests are adequate for MUSE.

The test objectives in this chapter are (roughly) categorised as:

- Test objectives to be verified: those ones which are usually validated by verification (see table 11-3).
- Test objective to be measured: those ones which are usually validated by measurement (see table 11-4).

This classification is more or less generally valid, but shall not be taken as rigid. In fact, more than one test procedure may be applied to validate an objective, and some objectives can be validated as well as measured. Moreover, sometimes the lack of certain monitoring capabilities on the equipment under test impedes a simple verification and compels to perform an explicit measurement.

10.1.1 Functional testing

Functional tests are meant for identifying if a specific xDSL based solution can serve as an adequate transport platform for a full service, end to end access network. Possible applications for functional tests are (a) to debug solutions that are under development, (b) to identify strong and weak points of a solution to enable strategic decisions on migration scenarios, or (c) to select one solution out of many offers from different vendors.
As at this stage time-to-market (for an equipment vendor) or time-to-deployment (for a network operator) are fundamental hence test lists must be more oriented to the actual operation of the equipment both in terms of basic interoperability and of achieved performances.
In these cases, the range of properties that are to be tested should be made as broad as possible. However, it may be adequate to limit the amount of detail for testing a single property. This holds for *operability tests*, characterized by interconnecting a matched set of equipment, as well as for *interoperability tests,* characterized by interconnecting equipment from different vendors.

10.1.2 Conformance testing

Conformance tests are meant to certify that a specific xDSL based solution complies with all mandatory requirements from a standard. Possible applications for conformance tests are (a) to enable vendors to guarantee that the products they sell do comply with such a standard, or (b) to enable operators to verify if the products they buy do indeed comply.
In these cases, the range of properties that are to be tested are usually more limited and restricted then those of a functional test. However, conformance testing is very punctual and usually specified in great detail to enable reproducible results in different laboratories. For these reasons it may be quite time consuming.
Hence this testing approach is usually applied in the development and pre-release testing of an (xDSL chipset) implementation.

An example that may illustrate how laborious a conformance test can be is for instance a conformance test to prove compliance with the ETSI performance requirements on ADSL. A full test incorporates 8 test loops, times 4 stationary noise models, times 9 bit rates for downstream and 6 bit rates for upstream. So 480 tests for a single property: performance!

10.1.3 Choosing between functional and conformance testing

Both functional and conformance tests have their pros and cons, and each of these tests serve its own range of test applications. In general, functional tests cover wide ranges of properties that are to be tested, but each of these tests may not be in-depth. The test conditions may even be matched to the deployment of interest (country/operator specific). On the other hand, conformance tests may be more restricted to a subset of these properties and test conditions, but can be more elaborating.
We believe that functional tests are more appropriated to the MUSE lab trials, but this can be decided on a per-case basis. When appropriated, this chapter refers to conformance tests in standards or provides solutions to compare the results of functional tests under different test conditions in different laboratories.
The DSL Forum and ETSI have published different documents e.g. [x1, x2, x3, x4, x11, x12, x13] with test plans that are very comprehensive, very laborious and specified in great detail. The physical layer tests in the above mentioned ETSI documents have *operability tests* in mind, but do not exclude interoperability tests for performance. More specifically DSL Forum TR-067 [x11] is a good example of Interoperability Test Plan. It covers a wider range of

properties that should be tested and has reduced the complexity of ETSI performance tests significantly (single loop, single noise model without any length dependency), and sets (sometimes) higher performance requirements (e.g. for ADSL).

10.2 Testing management capabilities

A first group of xDSL properties that should be tested is related to all kinds of xDSL-specific capabilities that are to be supported by the management system. We have made a distinction between:

- Capabilities for configuration management
- Capabilities for monitoring and diagnostics

The first group deals with settings only, and it can only be verified if a specific property is supported or not. In many cases it is not needed to stress the modem for that.
The second group deals with all kinds of information and alarms, originating in the physical layer, but reported by the management system. In these cases, it may be relevant to stress the modem under test with a test loop and noise.

10.2.1 Testing configuration management

Configuration management should be capable of configuring all kinds of *line parameters* as well as *channel parameters*.

10.2.2 Line configuration

Line configuration is to control physical layer properties. Therefore it should be tested, to what extent these properties are configurable from the management system and how flexible this configuration can be changed. This includes:

- the capability to configure the mode of operation;
- the capability to configure signal power;
- the capability to configure signal PSD (PSD shaping);
- the capability to configure the *target* noise margin;
- the capability to configure rate adaptation mechanisms.

Line configuration is assumed to be individual for each line, and should not be restricted to common settings for all xDSL transceivers that are packed together in the same DSLAM.

Testing Mode of Operation management configuration
With the advent of second generation ADSL and VDSL, systems support multiple modes of operation. It is then necessary to verify the ability to configure the set of modes of operation.

TEST: It should be tested to what extent the mode of operation can be configured:

- Is it possible to configure a set of modes of operation for the modem? Can this set be composed of only one mode (single mode operation)

Testing Power management configuration
A primary objective for testing is to verify to what extent a management system can control the transmitted power of an xDSL modem under test. First generation xDSL modems operate in full-power state day and night, even when not in use. With several millions of deployed DSL modems, a significant amount of energy can be saved if the modems engage in as standby/sleep state just like computers. Furthermore from a spectral management point of view, the cross talk reduces when unused modems are sleeping. Second generation DSL (ADSL2/2+, VDSL2) supports power management to reduce overall power consumption

while maintaining the always-on functionality. They can make a distinction between the following states:

- *L0 state* (Full On); This line state occurs when the line has full transmission
- *L1/L2 state* (Low Power); These line states occur when reduced transmission only is required for the purposes like. OAM, higher layer connection and session control. The L1/L2 entry/exit mechanisms and resulting bit rate adaptations are accomplished without any service interruption or bit error.
  L1 applies only to G.992.2, L2 applies to G.992.3, G.992.4 and G.992.5.
- *L3 state* (Idle); This line state occurs when there is no signal on the line at all.
  L3 applies to G.992.3, G.992.4 and G.992.5 (ADSL2/2+) and to G.993.2 (VDSL2).

TEST: Relevant Configuration Parameters to be verified or measured are:

§ *Power management states*: What Power management states are supported? Do they support all L0, L1 or L2 as well as L3 states? Do they support them on the near-end and/or on the far end transceiver units?
§ *Power management timers*: Is it possible to configure the parameters L3-to-L0-Time, L2-Entry-Time and L3-Entry-Time?
§ *L2 mode maximum power reduction*: Is it possible to configure the parameter L2-ATPR?

Testing PSD configuration

For various spectral management purposes, it is desirable that the PSD (Power Spectral Density) can be shaped to decrease crosstalk to other wire pairs or to enable higher upstream bit rates (at the cost of downstream). Especially DMT-based solutions (like ADSL) of a second generation may support advanced features for PSD configuration, but the presence of build-in filters may restrict these capabilities.

New deployment scenarios (e.g. FTTCab, FTTB) for VDSL2 typically require the coexistence with ADSL and ADSL2+ systems deployed from the CO. For such needs specific PSD shaping mechanisms in the frequency range up to 2.2 MHz have been defined (DPBO). Furthermore upstream PSD shaping is defined specifically for VDSL2 in order to preserve the US performances of neighbour (both VDSL2 and legacy) systems (UPBO). For more details about power back-off refer to section 10.4.2.

TEST: It should be tested to what extent the transmit PSD can be configured:

§ Is it possible to control the maximum nominal transmit PSD in the downstream and upstream direction during initialization and show time (in dBm/Hz). If yes, over what range?
§ Is it possible to control the maximum nominal Aggregate Transmit Power for upstream and downstream? If yes, over what range?
§ Is it possible to control the transmit spectrum for upstream and downstream by applying a Band Plan[9]?
§ Is it possible to control the transmit spectrum for downstream by applying a DPBO mechanism? Can this be done by means of a predefined (build-in) “standard” PSD shape? Can this be done by means of a flexibly customisable PSD shape?
§ Is it possible to control the transmit spectrum for upstream by applying a UPBO mechanism? Can this be done by means of a predefined (build-in) “standard” PSD shape? Can this be done by means of a flexibly customisable PSD shape?

[9] ITU-T G.993.2 specifies the Band Plans for VDSL2 in terms of used downstream and upstream bands; furthermore the use (or not) of the lowest frequency band US0 is specified and its type: A for compatibility with legacy POTS services and B for compatibility with ISDN ones.

- Is it possible to control the shape of the transmit spectrum, e.g. by reducing the levels of individual DMT tones ("sub-carrier Masking"). If yes, over what range?
- Is it possible to control the shape of the transmit spectrum, e.g. by notching it over defined frequency ranges for coexistence with radio stations and resilience to Radio Frequency Interferers (RFI). If yes, over what range?
- Beyond the above, is it possible to change these shapes according to predefined (build-in) "standard" profiles?

Testing the configuration of target Noise Margin

If a transceiver adapts its rate to a maximum "safe" value for particular operational conditions, then it accounts for some noise margin. A safe value of 6 dB margin is commonly used, but higher margins bring more robustness at the cost of lower bit rates. In case an xDSL modem supports the rate adaptation capability, the following configuration parameters are defined to control the noise margin in the receive direction of the xTU:

- Target Downstream & upstream Noise Margin: This is the noise margin the xTU shall achieve, relative to the BER requirement for each of the bearer channels to successfully complete initialization.
- Maximum Downstream & upstream Noise Margin: This is the maximum noise margin the xTU receiver shall try to sustain. If the noise margin is above this level, the xTU shall request the opposite xTU to reduce its transmit power.
- Minimum Downstream & upstream Noise Margin: This is the minimum noise margin the xTU shall tolerate. If the noise margin falls below this level, the xTU requests the opposite xTU to increase the transmit power. If this power increase is not possible, the xTU shall fail and attempt to re-initialize.

TEST: It should be verified if the above defined parameters are supported and can be configured by the management system.

Rate Adaptation Parameters

Some xDSL modems support rate adaptation, which means that they can automatically find a maximum bit rate for the downstream and upstream transmit direction that can be transported at a safe noise margin. Different modes of Rate Adaptation can be distinguished:

- Mode 1: MANUAL - Rate changed manually, no automatic rate adaptation.
- Mode 2: AT_INIT- Rate automatically selected at start-up only and does not change after that.
- Mode 3: DYNAMIC – Data rate is automatically selected at initialization and is continuously adapted during operation; this is also known as Seamless Rate Adaptation. The data rate can vary between the maximum and minimum data rate.

The SRA feature is especially important for high-rate capable DSL flavours (such as ADSL2+ and VDSL2), used with rate-adaptive line profiles with a wide bitrate interval; infect the ability to continuously adapt the bitrate to line conditions without dropping out of showtime allows to fully exploit the bandwidth potential of ADSL2+ and VDSL2.

Rate adaptation in the dynamic mode is performed when the conditions for upshift or downshift are satisfied by Noise Margin and Minimum Time Interval. This means:

- Dynamic Mode Upshift action: A data rate Upshift action is allowed when the noise margin is above the Upshift Noise Margin during Minimum Time Interval for Upshift Rate Adaptation.
- Dynamic Mode Downshift action: A data rate Downshift action is allowed when the noise margin is below the Downshift Noise Margin during Minimum Time Interval for Downshift Rate Adaptation.

TEST: The following properties should be verified:

- *Downstream & upstream Rate Adaptation Mode:*

Which adaptation modes are supported?

- *Downshift and Upshift Noise Margin:* If the DYNAMIC mode is supported, does the system adapt the bitrate upon variation of the noise margin above the Upshift Noise Margin or below the Downshift Noise Margin?
- *Response time of rate adaptation:* If the DYNAMIC mode is supported, what is the time interval ranges that is supported? In other words; how rapidly can the modem re-adapt to an increase or decrease in noise level?

10.2.3 Channel configuration

Another objective for testing is to identify to what extent an xDSL-based solution supports multiple transportation channels. In most cases there is only a single wire pair, but xDSL systems can emulate more bearer channels over a single line. A bearer channel is described by its data mode (ATM or PTM), latency, robustness against a burst of impulses on the line, and the bitrate.
The triple or multi-play services (e.g. voice, interactive gaming, web browsing and broadcast video) have different requirements on latency, bit errors and impulse protection. If multi-play services are carried on the same latency path, the DSL system would need to be simultaneously configured for low latency and high robustness against a burst of impulses on the line. When both requirements are enforced to one channel, it will result in very inefficient bandwidth utilization due to high redundancy for Forward Error Correction. This inefficiency can be combated by assigning a dedicated low latency channel for voice and gaming and a dedicated robust channel for the bit error sensitive service like broadcast video can improve the quality of service of multi-play and the bitrate performance.

The first generation ADSL technologies supported two channels: one could be configured as a “low latency” channel at the cost of limited error correction, while the other one could be made more robust against bursts of impulse noise at the cost of more latency.

- More robustness against a burst of impulses on the line, at the cost of latency, can be achieved by *Interleaving* the data bits through a channel. This is a reordering of transmitted bytes by interleaving dept D over a number of xDSL physical layer DMT symbols., so that the adjacent bytes in the transmitted data stream are not from the same DMT symbols which, reduces the probability of failure in the presence of impulse noise. Interleaving is performed by a buffer which introduces an interleaving delay depending on the interleaving dept. One bearer channel may be configured (if desired) with interleaving resulting in a delay corresponding to the configured interleaving dept. The second latency path is always fast, i.e., no interleaving is provided.
- More robustness against (stationary) cross talk noise, at the cost of latency and data rate can be achieved by adding overhead bits for error correction. Each bearer channel may be configured (if desired) with different kind of error correction.

SDSL supports multiple channels as well, for instance one (or more) dedicated to voice (with life-line functionality, when remote power feeding is applied) and another one to data (that will fail when the local power goes down).

The second generation ADSL and VDSL technologies [x21, x22] are supporting more flexible configuration schemes. If desired, up to four generic channels can be configured independently with respect to latency, data rate and Bit Error Ratio. This is illustrated in figure 10-1.
The requirements for managing second generation ADSL and VDSL technologies are captured in the revised draft of ITU-T G.997.1 [x22].

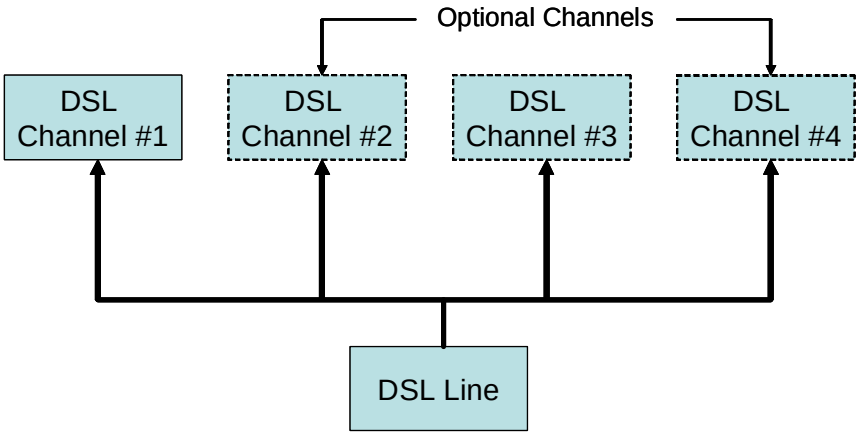


Figure 10-1: Bearer channel arrangement in the second generation ADSL and VDSL technologies

The second generation DSL technologies have a dedicated channel configuration parameter to improve the resistance against impulsive noise significantly. This channel configuration parameter is called Impulse Noise Protection (INP). The definition for INP is the following:

INP is the number of DMT symbols in one interleaving delay period for which errors can be completely corrected by the error correcting code.

The price that most be paid for more impulse noise protection can be expressed in bitrate and or delay, the general is:

$$INP = 2 \times delay \times FEC\,overhead \qquad \text{(Equation x1)}$$

Equation x1 shows that the INP can be increased by adding Reed Solomon redundancy bytes (overhead) and or a longer interleaving delay. The interleaving delay parameter gives the delay caused by the interleaving buffer in milliseconds.

TEST: The following properties should be verified:

- How many bearer channels are supported?
- Is it possible to configure each channel individually, and which of the following settings are configurable by the management system?
  - Minimum Data Rate downstream & upstream
  - Target Data Rate downstream & upstream
  - Maximum Data Rate downstream & upstream
  - Rate Adaptation Ratio downstream & upstream
  - Minimum Data Rate in low power state downstream
  - Maximum Interleave Delay downstream & upstream
  - Minimum Impulse Noise Protection (INP) downstream & upstream

10.2.4 Testing monitoring capabilities

The management system should be capable of reporting all kind of values, related to the operational condition, and to generate all kinds of alarms in case of failure.

10.2.4.1 Reported Line parameters

The reported line parameters indicate the actual values at which the xDSL link was established. These parameters are of great importance to monitor the reliability of a link. Furthermore, it enables the qualification of individual loops by learning if delivery of higher bit

rates is feasible to the attached customer or not. In addition it is a good facility to speed-up (time-consuming) performance tests in a lab environment.

TEST: It should be verified to what extent the following capabilities are supported by the xDSL system under test:

- *About downstream and upstream signal-to-noise ratio margin:*
  - Does the management system report the actual noise margin, being the amount of dB by which the received noise may increase before the BER falls below a defined threshold (typically 10^{-7})?
  - Does it report the margin for the xTU-C unit as well for the xTU-R unit?
  - Over what range can it be reported, and with what resolution? (NOTE: commonly deployed ADSL transceivers report between 0-31 dB, in 1 dB steps, while a range between 0-63 dB in 0.1 dB steps may be preferred)
- *About downstream and Upstream Maximum Attainable Data Rate:*
  - Does the management system report the maximum (payload/net) data rate that can safely offered on that line?
  - Does it report this for the xTU-C unit as well for the xTU-R unit?
- *About downstream and Upstream Actual Aggregate Transmit Power:*
  - Does the management system report the actual total transmit power , as it can be measured at the U-interface (line output)?
  - Does it report this for the xTU-C unit as well for the xTU-R unit?
- *About actual Data Rate:*
  - Does the management system reports the actual net data rate of each bearer channel at which it operates (excluding rate in L1 and L2 states). In L1 or L2 states, the parameter contains the net data rate in the previous L0 state.
- *About actual INP*
  - Does the management system report the actual upstream and downstream INP values?
- *About actual interleaving delay*
  - Does the management system reports the actual interleaving delay for the upstream and downstream direction?

10.2.4.2 Reported Fault Parameters

Reporting all kinds of failures is an essential capability. The failures can be divided in Line Near-end failures and Line Far-end failures. Both contain:

- Loss of signal (LOS) failure
- Loss of frame (LOF) failure
- Loss of power (LOP) failure
- Line Initialization (LINIT) failure

TEST: What capabilities on fault detection are supported by the system under test?

10.2.4.3 Reported Diagnostic Parameters

Reporting diagnostic parameters is of great importance. Diagnostic parameters enhance the service maintenance, diagnostics and enables effective loop qualification and monitoring. A detailed description and complete list of the diagnostic parameters is given in clause 7.5 of [x22]. In [x23] the pre-loop qualification and how to use these diagnostic parameters is described in detail. In [x23] these parameters are called Double Ended Line Testing (DELT) parameters. DELT is a test of a copper loop and the overlying xDSL link performed by combination of xTU-C and xTU-R modems. Because of its dual nature, DELT can only be used when the DSL line is up. In [x23] another test is described where only the xTU-C is

connected with the local loop. This test is called Single Ended Line Testing (SELT). SELT tests the electrical characteristics of a copper loop (TDR, FDR) performed by suitable equipment (e.g. an xDSL modem) without the need of a counterpart peer.

Another set of measurements that can be performed over the copper loop is called MEtallic Line Testing (MELT), which encompasses AC/DC foreign voltages, frequency of foreign voltages, loop resistance, insulation resistance and capacitance as measured between the wires or to ground. In current networks this kind of measurements are performed in the narrow-band range and the related functionalities are available on POTS/ISDN cards of Local Exchange equipment. The evolution towards all-IP networks, replacing legacy voice services with VoIP ones, may require the availability of MELT functionalities on the xDSL line cards of DSLAMs. The requirement of these functionalities and the actual set of parameters to be supported by an xDSL transceiver is still under definition in the G.LT project of ITU-T, hence testing about MELT parameters is left for further study in this document.

Here a brief overview of the diagnostic parameters that shall be reported by the xDSL management:

- Channel Characteristics Function H(f) per sub-carrier (CCF-ps); H(f) can be used for analyzing the physical copper loop condition.
- Quiet Line Noise PSD QLN(f) per sub-carrier (QLN-ps); QLN(f) can be used for analyzing the crosstalk
- Signal-to-Noise Ratio SNR(f) per sub-carrier (SNR-ps); SNR(f) can be used for analyzing time dependent changes in crosstalk levels and line attenuation (such as due to moisture and temperature variations)
- Line Attenuation (LATN); LATN can be used for determining the length of the line.
- Signal-to-Noise Margin (SNRM); SNRM can be used in analyzing the performance of the corresponding xDSL line.
- Impulse Noise Monitor (INM): provides information (independent of current FEC and interleaver settings) for operator to determine the required INP_min and Delay_max setting. Using different parameters related to the “Number of severely degraded symbols during interleaved period”.

TEST: What diagnostic parameters are supported by the system under test? Depending on the importance of the parameter, it could be necessary to test the reported value of the concerning diagnostic parameter. For example: the LATN is an important diagnostic parameter for determining the cable length for purpose of pre loop qualification. Because of its importance the reported value should be validated by measurements.

10.3 Testing Usability

Usability is, within the context of this chapter, a list of physical layer properties that improves user friendliness towards the end-user.

- Auto configuration; is it plug & play? Auto-configuration on the DSL physical layer should be for the end-user a non-issue. The xDSL management system takes care of the communication between the xTU-C and xTU-R necessary for the start-up of the DSL line. When the xTU-C is properly configured, the xTU-C and xTU-R are interoperable and the circumstances are not to tough, the DSL line will start-up automatically. The higher layers will need more user effort if auto configuration on these layers is not implemented. Auto configuration on the higher layers, Ethernet, ATM and IP is outside the scope of this section, see chapter 6 on connectivity. DSL Forum TR-69 [x13] gives a good reference for all the issues of auto configuration on the higher layers.
- Cold and warm start-up times
- Status information of the link to the end user

TEST: It should be verified to what extent the following capabilities are supported by the xDSL system under test:

- Does it function properly for the end user without a lot of difficult configuration work; in other words: Plug and play and auto-configuration.
- How long must be waited before the connection is up and running; In other words: Cold and warm start-up times.
- What status information about the link is made available for the end user? How easy/clear is it for the end-user to identify if the link is still operational, so that failures in connectivity are within its home network or PC?
- What additional features for the end-user are build-in?

10.4 Testing Transceiver signal characteristics

When signals from xDSL transceivers are injected into a twisted pair cable, a fraction of the injected power will couple into other wire pairs. This concept is well known as crosstalk, and crosstalk noise impairs the transmission in systems of other wire pairs. The result is that the maximum bit rate of these systems is limited by this, and that the crosstalk noise has to be bounded to enable other systems to operate well.

Spectral management (SpM) is the art of making efficient use of available copper resources, including finding ways for bounding this crosstalk to achieve this goal. An efficient way to bound crosstalk is bounding the levels of each signal being injected.
Many countries implemented so called “access rules” as part of their SpM approach, for bounding the maximum spectral pollution. These rules are essentially a specification of the maximum aggregate power of a signal, and of the maximum spectral power in a narrow band, up to 30 MHz. An example of how to specify these limits for a specific signal can be fount in the ETSI Spectral management standard, part 1 (see [x5]).

Transmit signals of xDSL transceivers have to comply with these access rules, that are mandatory and country specific. Therefore it is essential to test transceiver signal characteristics, to learn if it is applicable in a country of interest.
Being compliant with an xDSL product standard, does not mean that it also complies with an access rule in a specific country.

An example is HDSL.2B1Q/2 (a two-pair HDSL system, using 2B1Q line code) that is not allowed to be deployed in the Netherlands (use HDSL.CAP/2 instead), while this product is allowed in many other countries.
If transceiver implementations under test are equipped with steeper filtering (not required by its standard) then their transmit signal may fall in a category that is allowed. Therefore testing signal characteristics should not be restricted to verify if they meet the specs in a product standard, but their capability of supporting non-standard PSD’s should be tested as well, including the flexibility of defining deviated spectra.

10.4.1 Total transmit power

The total transmit power is the power aggregated over a frequency band that is significantly wider then the transition band. For example, when this is to be measured for ADSL, the frequency band should exceed a range between 3 kHz and 4 MHz.
Specific characteristics of the test setup (load impedance, pass-band) need to be precisely defined and fulfilled. Only in case the measurement is exactly performed conforming to the prescriptions, a verdict may be made.

TEST: It should be measured what the actual power levels are, when the transceiver under test is terminated with a well defined impedance:

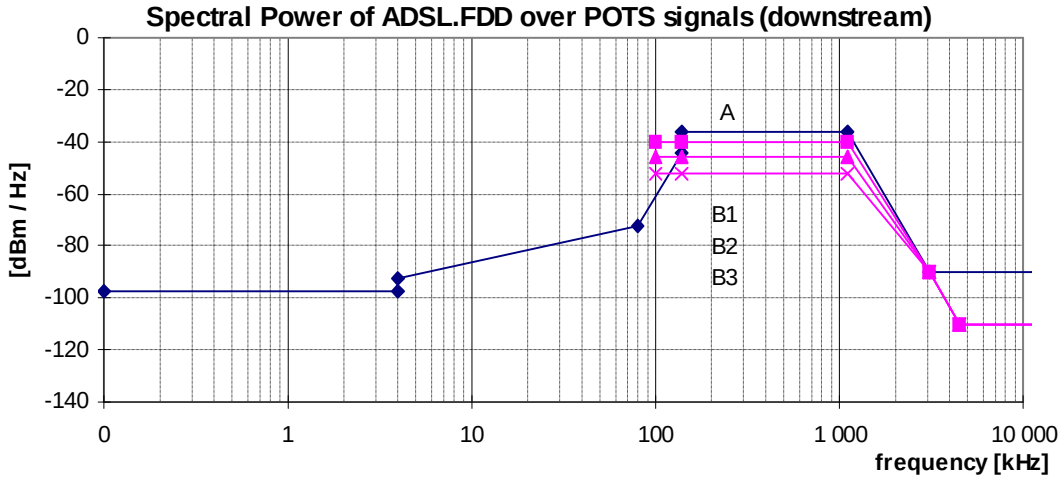
- § What is the aggregate power in downstream direction?
- § What is the aggregate power in upstream direction?

10.4.2 Power Spectral Density

The PSD of a transmitted signal will change with the time, and will have an expected average value and a worst case maximum value. When this signal has to comply with the specification in some document (product standards or access rule), then it is usually specified that the worst case maximum should not exceed a well defined “PSD Mask”.PSD masks
An example of such a mask specification, dedicated to ADSL.FDD over POTS, is given below in table 10-1 and figure 10-2, and taken from [x5].

Centre frequency f	Impedance R	Signal Level P	Power bandwidth B	Spectral Power P/B	
0,1 kHz 1 kHz	600 600	-77,5 dBm -77,5 dBm	100 Hz 100 Hz	-97,5 dBm/Hz -97,5 dBm/Hz	A
1 kHz 4 kHz	600 600	-67,5 dBm -67,5 dBm	1 kHz 1 kHz	-97,5 dBm/Hz -97,5 dBm/Hz	
4 kHz 80 kHz 137,9 kHz 138 kHz 1 104 kHz 3 093 kHz 11 040 kHz 30 000 kHz	100 100 Ω 100 Ω 100 Ω 100 100 100 100	-52,5 dBm -32,5 dBm -4,2 dBm +3,5 dBm +3,5 dBm -50 dBm -50 dBm -50 dBm	10 kHz 10 kHz 10 kHz 10 kHz 10 kHz 10 kHz 10 kHz 10 kHz	-92,5 dBm/Hz -72,5 dBm/Hz -44,2 dBm/Hz -36,5 dBm/Hz -36,5 dBm/Hz -90 dBm/Hz -90 dBm/Hz -90 dBm/Hz	
170 kHz 1 104 kHz 3 093 kHz	100 100 100	P_{BO} + 50 dBm P_{BO} + 50 dBm -40 dBm	100 kHz 100 kHz 100 kHz	P_{BO} dBm/Hz P_{BO} dBm/Hz -90 dBm/Hz	B
3 093 kHz 4 545 kHz 30 000 kHz	100 100 100	-30 dBm -50 dBm -50 dBm	1 MHz 1 MHz 1 MHz	-90 dBm/Hz -110 dBm/Hz -110 dBm/Hz	
NOTE: The values for parameter P_{BO} are defined in, and are dependent from the received upstream power (Power back-off).					

Table 10-1: Break points of the narrow-band power limits



NOTE: The maximum spectral power varies with the value of parameter P_{BO}, as defined in table 10-2. Only the curves for the values P_{BO} = -40 dBm/Hz, P_{BO} = -46 dBm/Hz, and P_{BO} = -52 dBm/Hz are shown here.

Figure 10-2: Spectral Power, for ADSL.FDD over POTS signals, as specified in [x5].

10.4.3 Power adaption

Frequency independent (power-cut-back, PCB)

The PSD mask is often not a static mask. For instance the downstream PSD of ADSL has to reduce in level when the line is relatively short to prevent signal distortion at the downstream receiver. The table below shows that the downstream transmit PSD has to reduce if the received upstream power exceeds some specified level. Note that the PSD reduction is frequency independed which is called “power cut back”.

Upstream received power [dBm]	< 3	< 4	< 5	< 6	< 7	< 8	< 9
Parameter P_{BO} [dBm/Hz]	-40	-42	-44	-46	-48	-50	-52

Table 10-2 Definition of parameter P_{BO}, as used in table 10-1 (Power Back-off, or Power Cut-Back)

Frequency dependent (power-back-off, PBO)

For VDSL2 a frequency depended mechanism is specified reducing the power of the upstream and downstream PSD masks, called Upstream power back-off (UPBO) and Downstream power back-off (DPBO).

The UPBO specified for VDSL2 is pointed out to solve the Near-Far problem on the VDSL2 upstream performance. Figure 10-3 depicts schematically the situation. That is, if all the CPEs which are connected to the same cabinet but at different cable lengths will transmit their upstream PSD at full power level, the upstream VDSL2 connections on shorter cable lengths will have a very strong received signal while the connection on the longer cable will have a severe degradation in the upstream performance due to the FEXT contributions from the VDSL2 connections on shorter cable lengths.

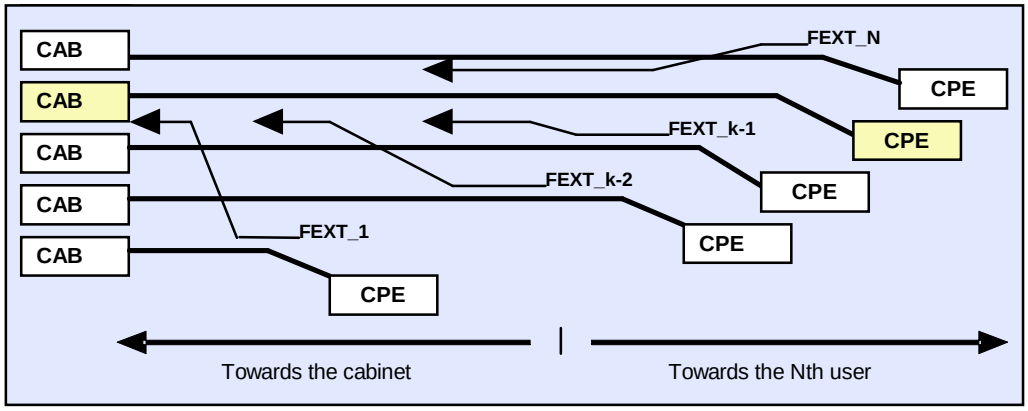


Figure 10-3 : Example of the Near-Far problem of the VDSL2 upstream performance.

UPBO tries to reduce the power level of the upstream transmit PSD of the shorter lines. This will result in reduced FEXT crosstalk noise on the long VDSL2 connections which improves significantly the upstream performance of these longer connections. Note that the PSD level adaption is frequency depended according to the cable attenuation characteristics.

The DPBO specified for VDSL2 is aimed to solve the spectral compatibility issue between legacy DSL technologies deployed from the CO and VDSL2 systems deployed from the Cabinet. For example, the spectra for VDSL2 and ADSL2+ show an overlap in frequency range up to 2.2 MHz. Consequently, VDSL2 has a severely detrimental impact on the ADSL2+ performance. At the same time the impact of ADSL2+ on VDSL2 is of a much lesser extent. This effect is illustrated in figure 10-4.

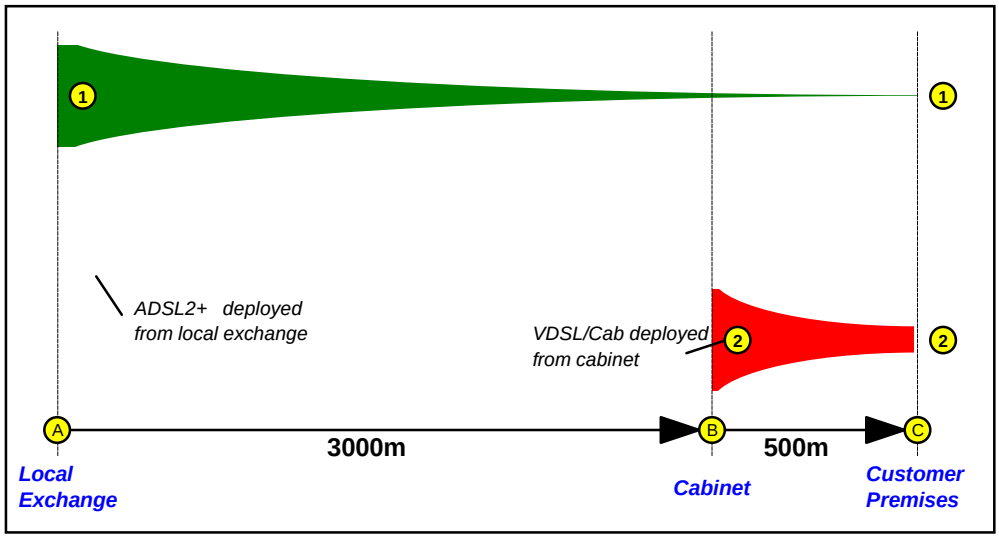


Figure 10-4: The problem of simultaneous roll-out from CO and cabinet: strong crosstalk from the cabinet based equipment (VDSL2) overwhelms the weakened (ADSL2+) signal from the CO. Consequence: A reduction of the performance of the CO based (ADSL2+) service.

This DPBO solution that mitigates the spectral incompatibility between ADSL2+ and VDSL2 is also known as *PSD shaping*. By shaping the downstream VDSL2 PSD in such a way that it matches the weakened ADSL2+ downstream signal at the cabinet, the shaped VDSL2 system will appear to other ADSL2+ systems as just another ADSL2+ system.

The shaped PSD signal description changes with the so called *attenuation distance* between local exchange and cabinet. Figure 10-5 shows examples of a few PSD shapes associated with different attenuation distances, as illustrated in Figure 10-6.

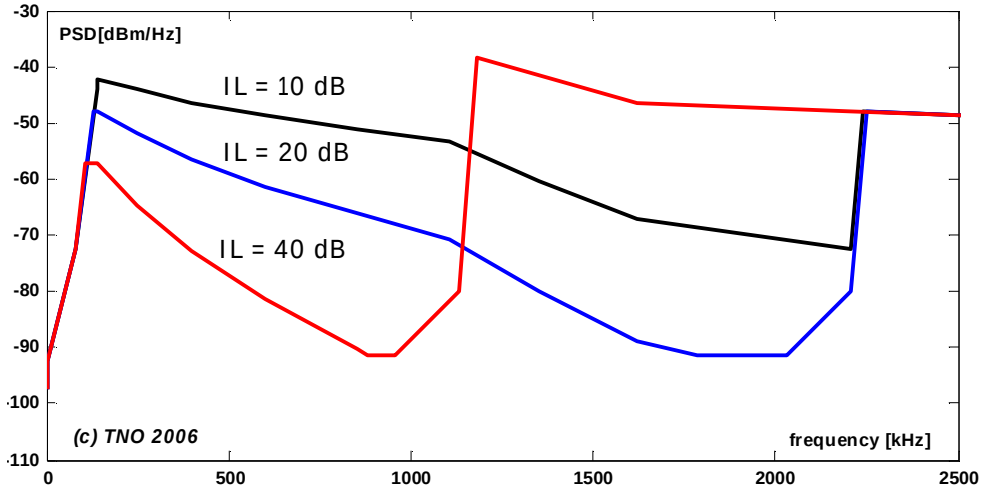


Figure 10-5: Different PSD shapes, to be used for different attenuation distances

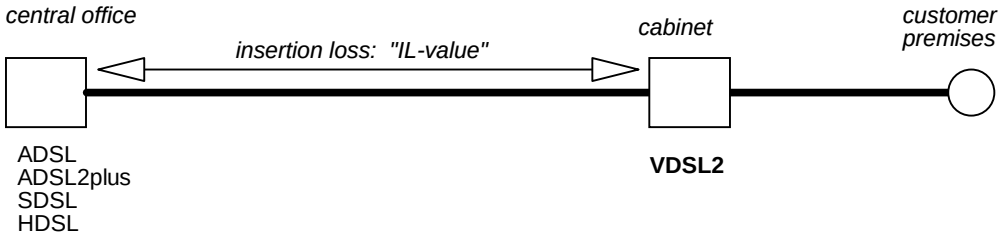


Figure 10-6: Attenuation distance is the insertion loss (IL) between central office and cabinet, measured at 300 kHz.

The shape downstream VDSL2 PSD is defined by breakpoints or by the cable parameters of the cable between the central office and the cabinet (so-called A, B, C parameters) which define the attenuation characteristics.

TEST: It should be measured what the actual shaped spectrum is:

- Does the shaped PSD obey the mask?
- How accurate does the actual shaped PSD "follow" the configured shaped PSD mask, How well does the actual shaped PSD use the available spectrum?
- What are the out-of band PSDs (up to 30 MHz)?
- Are there total power limitations that force the system to use a lower PSD template using an algorithm e.g., water filling?
- How do these PSDs change when instructed so via configuration management?; For instance when switching off individual carriers in the case of DMT-base transceiver?
- Are all the mandatory needed shapes supported?

10.4.4 Power management

First generation ADSL supports only an "on" and an "off" state. Second generation (A)DSL supports more advanced power management functionality, for instance to reduce overall power consumption while maintaining the always-on functionality. A second

generation (A)DSL line has three possible power management states, namely: L0, L1/L2 and L3, as explained in the section “Testing Configuration Management”.
For VDSL2 only L0 and L3 states are defined.
Requirements can be defined on timers, power levels and functionality e.g. service interruptions and bit errors.

TEST: The following power management properties should be measured:
- The actual power levels for each power level
- *L3-to-L0-Time*; What is the minimum time (in seconds) that is required to Exit an transceiver from the L3 (Idle) state into the L0 (Full Active) state? This transition requires the optional short initialization procedure.
- *L2-Entry-Time*; What is the minimum time (in seconds) to transit from the L0 (Full On) state into the L2 (Low Power) state?
- *L3-Entry-Time*; What is the minimum time (in seconds) to transit from the L0 (Full On) or the L2 (Low Power) state into the L3 (Idle) state? This transition requires the shut down procedure.
- *L2-ATPR*; What is the maximum reduction (in dB) of aggregate transmit power that can be achieved through a single Power Trim in the L2 state?
- Does a state transition event pass without a service interruption?
- Does a state transition event pass without any bit error?

10.4.5 Power consumption

The power consumption is not a parameter specific of DSL systems only. Nonetheless, as DSL circuitry dominates the power consumption budget of a DSLAM, this figure of merit is important for assessing an equipment that may be used in a remote location with power feeding/consumption/dissipation restrictions. This is certainly the case for new deployment scenarios (FTTCab, FTTB) of VDSL2 DSLAMs.
Generally speaking, this is a very sensitive subject for the EC which is promoting a Code of Conduct defining the guidelines and requirements about power consumption of telecommunication equipment.

TEST: The following power consumption figures should be measured:
- The overall power consumption of a fully equipped and operating DSLAM
- The power consumption of a single DSL line in a defined operation mode

10.5 Testing performance under noisy stress conditions

Existing access network cables are designed to facilitate a low crosstalk coupling at low frequencies (telephony band), but the frequency of signals in cables increases substantially due to the introduction of broadband transmission systems. The consequence will be a substantial increase of the total crosstalk noise power in each wire pair.

Existing transmission systems are designed to cope (to some extent) with this type of impairment, which anyhow puts a limit on the maximum bit rate that can be transported through a cable at given cable length (or the maximum length that can be reached at given bit rate). Above some impairment level, the reliability of installed systems becomes poor, and they will even fail when the impairment level will be increased any further.

The purpose of transmission performance tests is to stress xDSL transceivers in a way that is representative to the deployment in operational access networks, and to measure parameters like reach, bit rate or noise margin under these stress conditions.

10.5.1 Basic test setup and stress conditions

The usual approach is to attenuate the transmitted signal with a test loop and to impair the attenuated signal by injecting noise near the receiver input. The loop is to cause amplitude distortion due to insertion loss, echo due to impedance mismatch, and phase distortion due to delay. The noise represents crosstalk noise, RFI ingress noise, impulse noise, etc.
These setups are described in great detail in various standards, but they are in essential all similar. Figure 10-8 illustrates a basic test set-up based on the functional description of the test set-up taken from [x1, x2, x3].
The splitter is a fundamental part of some xDSL solutions (e.g. ADSL and VDSL), and these solutions should not be tested without splitters. This is obvious in case the splitter is an integral part of the modem under test (internal splitter), but when external splitters are required, these splitters are to be inserted between test loop and injection point.
For proper execution of certain tests, specific monitoring capabilities on the xTU-C and xTU-R are necessary.

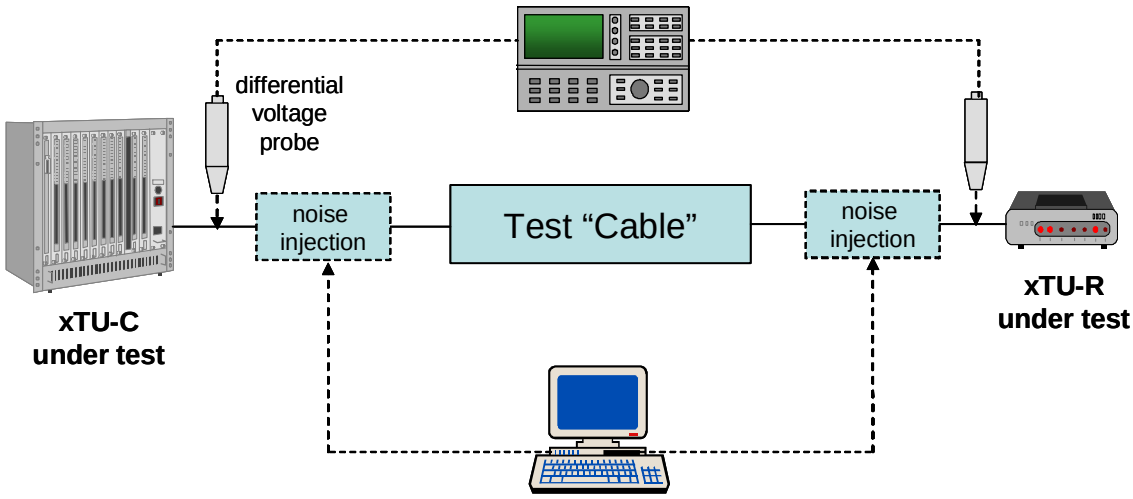


Figure 10-7: Functional description of the set-up of the performance tests.

The above test setup allows covering all kinds of bad-case conditions. This includes:

- loops that are long enough to measure the reach of the modem at given bit rate and noise margin;
- stationary noise that is high enough to measure the impact of medium or high penetration scenarios (a mix of many xDSL systems connected to the same cable);
- non-stationary noise, that is stressful enough to measure the impact of all kinds of impairment that is bursty, impulsive or just time-varying in nature.

For the purpose of ***conformance testing***, various xDSL standards have defined a range of test loops and noise models in great detail e.g. [x1, x2, x3, x11, x14].

§ ETSI has defined a range of test loops for proving *operability* to cover a variety of cables being used in Europe. The characteristic impedance of most European loops ranges between 100Ω and 150Ω, and values below 80Ω and above 180Ω have been reported as well. In early ETSI standards they were just a mix of loops, in the assumption that a large variety of sections with different wire gauges (=diameter) will be adequate to emulate most loops in Europe. The result is sometimes up to eight loops. More recently developed loop sets can do a better job with fewer loops because they where selected because of their impedance instead of there wire gauge. The result was only four loops. Because of historical reasons, HDSL, ADSL and SDSL loops from ETSI are still based on these early standards.
VDSL(2) loops from ETSI are more recently developed. Some loop types are the same as those defined for previous DSL flavours with the simple extension of the related model up to relevant VDSL(2) frequencies (e.g.: PE 0.4 mm). Other loop types are instead taken into consideration only for VDSL(2) (e.g. TP100 and TP150).

§ ETSI has also defined a range of (stationary) noise models for proving *operability* to cover a variety of technology mixtures as well as the observation that in some countries (like in The Netherlands) up to 900 wire pairs are layered in the same concentric bundle. These noise models are length dependent and identified by ETSI as “medium penetration” (based on about 50 disturbers) or as “high penetration” (based on about 180 disturbers).
ETSI has applied a similar approach for the definition of noise models for VDSL2 by defining “medium density” (MD, for short-term) and “high density” (HD, for long-term) noise models specifying the mix of self and alien disturbers.
To take into account for the foreseen VDSL2 deployment scenarios (e.g. FTTEx, FTTCab, FTTB), for each density, three mixes, characterising different network topologies, have been defined: one exchange side mix (EX) and two cabinet mixes (CAB27 and CAB72). These latter two consider a different distance between the CO and the Cabinet (respectively 1492m and 3987m of TP100 loop); this is relevant to calculate the attenuation of downstream alien disturbers injected at CO.
The following table gives a list of the ETSI noise models for VDSL2, the number of disturbers and the ratio between self (VDSL2) and alien (non VDSL2) ones:

	MD_EX	**MD_CAB27**	**MD_CAB72**	**HD_EX**	**HD_CAB27**	**HD_CAB72**
Number of disturbers	25	25	25	280	120	120
Ratio of self vs alien disturbers	13:12	15:10	15:10	70:210	60:60	60:60

Along with each single mix, the ETSI framework provides the PSDs of the LT and NT alien disturbers calculated at the sections where the VTU-C and VTU-R under test are respectively deployed.

The PSDs of VDSL2 self disturbers are not given as they depend on the hypotheses made on the spectrum configuration (profile, Band Plan, possible shaping, etc.) of the disturbing systems.

§ DSL Forum has selected from the ETSI framework only one combination (one ‘penetration’ scenario, one loop, one noise model) for defining performance objectives for ADSL and ADSL2+ *interoperability*.

For VDSL2 the ETSI framework has been adopted as well, but further assumptions where made to derive a useful and effective model for VDSL2 Performance Test Plans.

One first assumption is to adopt the “medium density” (MD) scenario from the ETSI framework.
Secondly, as VDSL2 system may implement one or more band profiles using the frequency spectrum up to 8, 12, 17 or 30 MHz, it is reasonable to associate them to the deployment scenario they are typically suitable with, leading to the following mapping:

Type of VDSL2 profile	Typical deployment scenario	Associated ETSI mix (and alien disturbers PSDs)
up to 8 MHz	FTTEx	MD_EX
up to 12 MHz	FTTCab	MD_Cab27
up to 17 MHz		
up to 30 MHz	FTTB	MD_Cab72[10] (note)

Finally, the basic PSD mask of a single VDSL2 self disturber (not explicitly given in the ETSI framework) has been defined to be equal to the one configured for the VDSL2 system under test (profile, Band Plan, possible shaping, etc.).
The following picture shows the relationship between the ETSI VDSL2 noise models and those derived for the DSL Forum VDSL2 Test Plans.

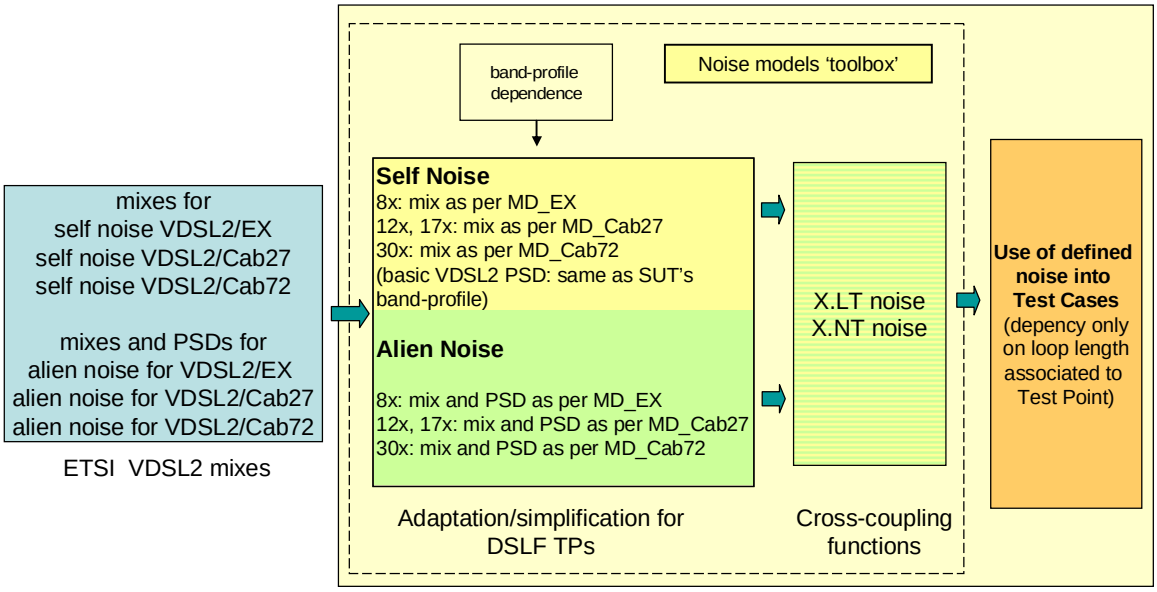


Figure 10-8: relationship between ETSI VDSL2 noise models and DSL Forum derived ones

§ For testing the DSL system on its capability to mitigate the impact of impulse noise, the DSL Forum describes performance tests under Repetitive Electrical Impulse Noise (REIN) and isolated noise bursts (SHINE).

The REIN model is defined as a “Burst of pseudo random AWGN” of 100us duration and repetition rate of 100/120Hz at a level of –90dBm/Hz differential mode. In case of ETSI conformance testing, the test setup should include all the above mentioned standard loops and noise models, to test if the reach or bit rate or noise margin meets the minimum

[10] The FTTB scenario is best described by the ETSI Cab72 mix (one may call it “deep-Cabinet” mix) which represents a topology with the VDSL2 system deployed very far from the location of the Central Office.

requirements from these standards. While in case of the DSL Forum, the test plans are based on simplified loop&noise environments that allow to perform tests in a time effective way.

For the purpose of ***functional testing***, the above loops and noise models are probably too laborious, and probably too inadequate to meet country-specific needs. In those cases, it is recommended to apply country-specific loops, and stationary crosstalk noise that is considered as representative for that country. When required, add non-standard noise models that are considered as adequate for the time being.

However, the use of (a sub set) of the "standard" stress conditions may be adequate as well. In the perspective of a pan European specification of a MUSE architecture it is also appropriate to refer to commonly accepted test loops and noise models such as those defined in [x1, x2, x3] and adopted in [x10].
Beyond the scope of MUSE, this approach has proved to be successful to build up the DSLF Independent Test Lab Program for modem validation and more specifically to foster ADSL interoperability and improvements by defining performance objectives that are accepted by the industry. The use of standard test conditions allows operators and other players to directly compare results on common and insensitive loop&noise environments.
Furthermore such DSLF tests can be exploited by vendors as a one-stop shop test model that allows them to present the same results to many operators for a pre-screening of their product.

A disadvantage of using country-specific stress conditions is the difficulty to inter-compare test results from different laboratories. The test objectives below give guidance on how to enable inter-comparison, even when tested under different stress conditions.

10.5.2 Testing margin under stationary cross talk noise conditions

A performance parameter that is meaningful for all xDSL systems is the actual noise margin at given bit rate, under specified stress conditions. It is essentially the amount of dB that the noise can increase, up to the point where the bit-error rate becomes worse then a predefined value.
Such a value can be a BER value of 10^{-7} (that is commonly used, but difficult to detect in a reproducible way) or values that are much worse (up to loss of synchronization) to simplify measurements.

TEST: It should be measured what the noise margins at given bit rate are:

- What is the noise margin, up to BER=10^{-7}, for a variety of stress conditions (loops, noise)?
- What is the noise margin, up to the "sync-loss" point, and how much dB is this higher than the previous noise margin (related to BER=10^{-7})?
- What is the relation between the measured noise margin, and the reported noise margin (by the management system). How accurate are these diagnostic tools?
- If the noise margin is tested at some stress condition, but the noise was kept significantly lower during start-up of the modem, will this change the noise margin of the modem?

10.5.3 Testing bit rate under stationary crosstalk noise conditions

Some modems support the principle of rate adaptation, and can determine the maximum attainable upstream and downstream bit rate for the actual stress conditions at a target noise margin (e.g. of 6dB). This is a common capability of many ADSL/VDSL modems, but uncommon for SDSL and HDSL.
These capabilities reduce the overall measurement effort significantly. For a specific test loop (with selectable length) and a noise model based on a fixed mix of disturbers it is now simple to measure the maximum bit rate. The "rate-adaptive" capability enables to measure a so-called rate-reach curve, by varying the loop length and the cross talk noise associated with that length.
Rate-reach tests return an all-round characterization of the xDSL system transmission capability over a wide loop range. This is certainly relevant for implementation validation and comparison. Furthermore with the deployment of high-rate capable DSL flavours (such as ADSL2+ and VDSL2), marketing and technical reasons have brought operators to use rate-adaptive line profiles with a wide bitrate interval (up to the maximum rate achievable by the specific DSL flavour). Under this perspective "rate-reach tests" become even more relevant not only for the all-round characterisation of an implementation but also for gathering performance and penetration results useful for deployment planning purposes.

TEST: It should be measured what the max bit rates are for a variety of stress conditions:

- What is the maximum bit rate, at a target noise margin (e.g. 6 dB), as a function of the loop length, but at a well defined stress scenario?
- The same question as above, but for other stress scenarios (other loop types, or other disturber mixtures)
- Do the actual noise margin and the target noise margin correspond, what is the difference?
- What is the gap in noise margin between the system under test, and a hypothetical system that performs at the theoretical maximum bit rate (Shannon limit), operating at the same bit rate, noise margin and signal spectrum?

Inter-comparing test results: The comparison of the performance of a system under test and of a hypothetical system performing at Shannon limit, enables a convenient comparison of test results with other labs/countries using other stress conditions. A diagram with the measured curve and a hypothetical curve (e.g. Shannon limit minus 7 dB) shows how close the system under test approaches this Shannon limit. Figure 10-9 depicts an example of such a diagram.
The "Shifted Shannon" receiver model (see ETSI TS 101 830-2) can be used a reference. Technical details are elaborated in another MUSE deliverable DTF4.2: "Test Methods".

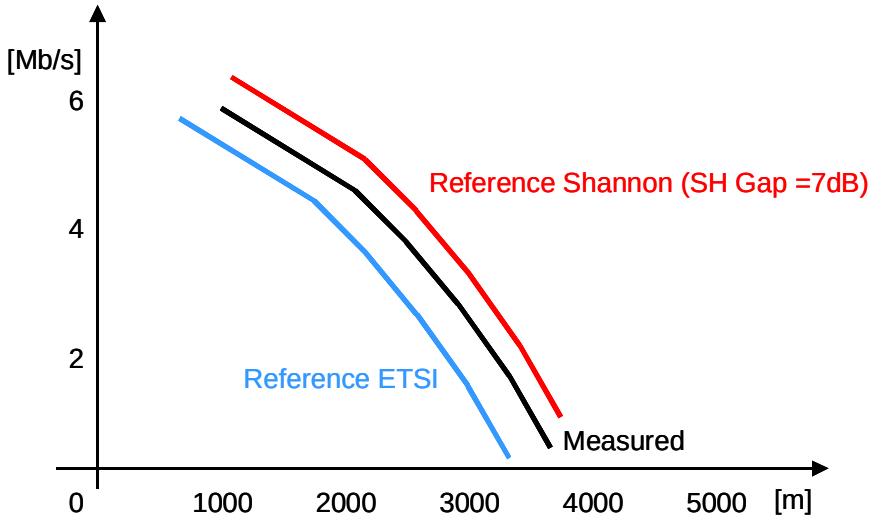


Figure 10-9: Example of performance comparison with other labs/countries

10.5.4 Testing Reach under stationary crosstalk noise conditions

Another way of characterizing the performance is measuring the reach at given bit rate and target noise margin. It would require a test loop that can be varied in length with small steps, to find the maximum length that can still fulfil the target noise margin.
Such an approach can be inconvenient in practice (especially when the test setup is based on real cables in stead of a cable simulator). Therefore, an alternative would be to measure the noise margin at two fixed loop lengths (one being a slightly shorter, and another a slightly longer then the expected reach) and to extract the actual reach by interpolating these two measurements.

Although loop-reach measurements may seem to be superfluous when rate-reach measurements are being performed as well, this is not always the case. Rate-reach measurements may be less accurate than loop-reach tests, when the first is measured by using the “rate-adaptive” capabilities of the modem under test (rate adaptive mechanisms do not measure the actual noise margin, but estimate them).
The elaboration of a more accurate loop-reach measurement may be relevant in case of conformance tests that are to verify the reach as a performance objective. (*A quick alternative could also be a margin test, in stead of a loop-reach test, to verify if the actual noise margin is above the target noise margin at the required minimum reach.*)
As said in the previous section, the wide adoption of rate-adaptive line profiles for high-rate capable DSL flavours (such as ADSL2+ and VDSL2) may suggest to give less relevance to “loop-reach tests”, performed with fixed rate line profiles, when it comes deployment validation testing. This mindset has been considered for example in the development of DSL Forum’s VDSL2 Test Plans in order to keep the amount of Test Cases at a reasonable level in a context where the number of applicable VDSL2 profiles acts as a multiplying factor on the overall number of Test Cases.

TEST: It should be verified what the reach is for various stress scenarios:

- What is the maximum loop length, at a target bit rate and noise margin (e.g. 6 dB), at a well defined stress scenario?
- The same question as above, but for other stress scenarios (other loop types, or other disturber mixtures)

10.5.5 Testing performance under other noise conditions

The above test objectives are all based on stationary (cross talk) noise. The specification of this type of impairment is described in great detail in various xDSL standards, and the associated noise models are considered as mature.
However, stationary noise is an oversimplification of reality, and therefore the use of more advanced noise models are desired for testing. Examples are:

- impulse noise (e.g.: Cook impulse, REIN, SHINE, etc)
- noise that represent non-stationary behaviour of modems that switch between high power and lower power modes;
- noise that can do a fair representation of RFI ingress noise, both differential mode as well as common mode.
- non-stationary noise related to slow varying signals associated with transients typical of POTS/ISDN legacy telephone services (ringing, on hook/off-hook events, pulse/tone dialing on POTS/ISDN telephone);

Along with typical performance tests, such as rate-reach or loop-reach ones, it is relevant to verify if the system is able to synchronise under the above stress conditions which may be particularly harsh.
Tests performed under the above noise conditions are important both to assess implementations' robustness and performances under these other realistic field conditions and to verify the implementation and effectiveness of features specified to contrast such type of noises (e.g.: INP, RFI ingress and egress control).

Impulsive Noise
The next generation DSL systems support Impulse Noise Protection (INP) that will mitigate the impact of impulsive noise. The mechanism behind INP can be the combination of Reed Solomon Forward Error Correction and interleaving. In that case, the INP performance depends on the limitations of the framing parameters, e.g., the interleaving dept and 1/S (the maximum number of FEC codewords that the modem is capable of transmitting during one DMT symbol). Other mechanisms which are still under study within the standardisation are Frame Blanking, Frame Repetition and data retransmission.
The use of INP will have impact on the maximum attainable bitrate due to extra overhead (Reed Solomon) or retransmissions.

The performance in case of impulse noise is twofold:

1. What is the maximum bitrate performance in case of the required INP_min and Delay_max setting?
2. What is the achieved resistance against impulse noise? Can the DSL system mitigate the impact of impulse noise according to the INP setting expectations?

TEST: The following should be verified under a variety of stress conditions other than typical stationary noise ones:

- Is the system able to synchronise at the specified loop length, at a well defined stress scenario other than typical stationary noise ones?
- What is the required INP_min and Delay_max setting that will mitigate the impact of impulsive noise to an acceptable level?
- What is the achieved resistance against impulse noise, expressed in, e.g., code violations cause by the impulsive noise?
- What is the maximum bit rate, at a target noise margin (e.g. 6 dB) and required INP_min and Delay_max, as a function of the loop length, for a defined stress scenario other than typical stationary noise ones?

- What is the maximum loop length, at a target bit rate and noise margin (e.g. 6 dB) and required INP_min and Delay_max, at a well defined stress scenario other than typical stationary noise ones?

RFI Noise

The next generation DSL systems allow configuring RFI band notching in order to protect them selves from narrow-spectrum disturbances induced on the loop by the electromagnetic environment (typically radio stations). Essentially the system is configured to introduce a notch in a so called RFI band (e.g. corresponding to HAM bands), thus avoiding the use of those frequencies for transmission.
Under this perspective, tests with configured RFI notching are performed without the explicit application of a narrow-spectrum disturbance on the line.

TEST: The following should be verified under different configurations of RFI notching:

- Is the system able to synchronise with the required noise margin?
- What is the maximum bit rate, at a target noise margin (e.g. 6 dB) as a function of the loop length?

Non-stationary noise generated by POTS/ISDN signal transients

The coexistence of DSL services with POTS/ISDN legacy telephone services may lead to non-stationary noise impairments experienced by the DSL transceiver. This non-stationary noise conditions are related to slow varying signals associated with transients typical of POTS/ISDN legacy telephone services (ringing, on-hook/off-hook events, pulse/tone dialling on the telephone) only partly filtered by the splitter.
The combined effect of these transients along with the filtering of a splitter (compliant to specific electrical requirements under such transients) should be expressed in the resulting model(s) of the “POTS/ISDN transients non-stationary noise”.
This is especially relevant on the QoE of services like VoIP and Video (over DSL) which are particularly sensitive to errors.

TEST: The following should be verified under a variety of “POTS/ISDN transients non-stationary noise” conditions:

- When the transient noise is during the synchronisation phase, is the system able to synchronise with the required noise margin?
- When the transient noise is during the synchronisation phase, what is the maximum bit rate, at a target noise margin (e.g. 6 dB) as a function of the loop length?
- When the transient noise is applied after the synchronisation, is the system able to stay in showtime?
- When the transient noise is applied after the synchronisation, what is the amount of observed Code Violations (CVs) as a result of not corrected frame errors?

10.5.6 Testing minimum required performance

The objective of a conformance test is to provide a simple “pass/fail” answer to the question if the performance of a modem is above a minimum required performance. For such a test application, it is usually too elaborating to measure margin, bit rate and/or reach as intermediate test result.
In a so-called “spot-performance” test, it is only to be verified if the modem under test remains operational when the test conditions have cycled through a specified list of individual steps, under fully restrictive test conditions. For instance, ETSI (or DSL-forum) have defined certifying documents, describing a discrete set of test loops (with fixed length), noise models,

bit rates, target margins (e.g. 6 dB), etc. Each spot-performance test cycles through steps like: (a) select one of the specified loops, (b) inject one of specified noise, (c) activate modem at one of the specified bit rates, (d) increase the noise by the target margin, (e) validate if the modem remains operational.
The advantage of above approach is a significant simplification, since each spot performance test verifies only if the margin remains above 0 dB.

TEST: It should be verified if the modem-under-test remains operational for each spot-performance test, as specified in a certifying document. Such a document also covers fully restrictive test conditions, pass/fail criteria, etc.

- Single spot-performance test: will the modem remain operational when the test conditions (stress scenario, modem start-up, modem bit rate, …) have cycled through a list of specified steps?
- Range of spot-performance tests: will the modem pass X percent of a range of the above-mentioned spot-performance tests?

NOTE: A modem may be declared as “conformant to the standard” if it passes all (or most) of the specified spot-performance tests.

10.6 Summary

Table 10-3 gives a summary of the xDSL objectives that should be tested.
It has to be said that when it comes to the definition of Test Methodology and its actual implementation into a Test Campaign, test objectives might be verified in an aggregate way, i.e. one test may be defined and performed in such way that a positive result ensures that more than one test objective is passed.
This is quite useful in terms of ease and time effectiveness of the test campaign.

	Test Objective
Testing management capabilities	
Line configuration	*Mode of operation*
	Power management state forced
	L0-Time
	L2-Time
	L2-ATPR
	Downstream maximum nominal Power spectral Density
	Upstream maximum nominal Power spectral Density
	Downstream Maximum nominal Aggregate Transmit Power
	Upstream Maximum nominal Aggregate Transmit Power
	Downstream Sub-carrier Masking
	Upstream Sub-carrier Masking
	PSD shape: Downstream Power Back-off
	PSD shape: Upstream Power Back-off
	PSD shape: Custom shape with break-points
	Ingress and egress RFI ranges
	Target Downstream NM
	Target Upstream NM
	Maximum Downstream NM
	Maximum Upstream NM
	Minimum Downstream NM
	Minimum Upstream NM
	Downstream Rate adaptation mode
	Upstream Rate adaptation mode
	Downstream Up-shift Noise Margin
	Upstream Up-shift Noise Margin
	Downstream Down-shift Noise Margin
	Upstream Down-shift Noise Margin
	Minimum Time Interval for Downstream Up-shift NM
	Minimum Time Interval for Upstream Up-shift NM
	Minimum Time Interval for Downstream Down-shift NM
	Minimum Time Interval for Upstream Down-shift NM
Channel Configuration	*Downstream Minimum Data Rate*
	Upstream Minimum Data Rate
	Downstream Target Data Rate
	Upstream Target Data Rate
	Downstream Maximum Data Rate
	Upstream Maximum Data Rate
	Downstream Rate Adaptation Ratio
	Upstream Rate Adaptation Ratio
	Minimum Data Rate in low power state downstream
	Downstream Maximum Interleave Delay
	Upstream Maximum Interleave Delay
	Downstream Minimum Impulse Noise Protection
	Upstream Minimum Impulse Noise Protection

Table 10-3a: xDSL Objectives to be verified

Testing monitoring capabilities	
Line Parameters	*Downstream Signal-to-Noise Ratio Margin*
	Upstream Signal-to-Noise Ratio Margin
	Downstream Attainable bit Rate
	Upstream Attainable bit Rate
	Downstream Maximum Actual Aggregate Transmit Power
	Upstream Maximum Actual Aggregate Transmit Power
	Downstream Actual data Rate
	Upstream Actual data Rate
Fault management	*LOS*
	LOF
	LOP
	LINIT
Diagnostic Parameters	*Channel Characteristics Function H(f) per subcarrier (CCF-ps)*
	Quiet Line Noise PSD QLN(f) per subcarrier (QLN-ps)
	Signal-to-Noise Ratio SNR(f) per subcarrier (SNR-ps)
	Line Attenuation (LATN
	Signal-to-Noise Margin (SNRM
	INP_min (INM)
	Delay_max (INM)
Testing Usability	
	Auto-Configuration (Plug And play)
	Cold and warm startup times
	Status information of the link to the end user

Table 10-3b: xDSL Objectives to be verified

Table 10-4 gives a summary of the xDSL objectives that need to be measured.
This section describes test objectives which, given their nature, are usually validated by measurement. For this reason the test setup and related test procedure shall be precisely defined for measurement accuracy and repeatability.

	Test Objective
Testing Transceiver signal characteristics	
Total transmit power	Downstream Total Transmit power
	Upstream Total Transmit power
Power Spectral Density	Downstream Power Spectral Density
	Upstream Power Spectral Density
Power Management	*The actual power levels for each power level*
Power consumption	*The overall and per line power consumption*
Testing performance under noisy stress conditions	
Measuring performance under stationary cross talk noise conditions	Measuring Margin
	Measuring bit rate
	Measuring Reach

Measuring performance under other noise conditions	Ability to synchronise
	Measuring bit rate
	Measuring Reach
Verifying minimum performance requirements	Will the modem pass “X” percent of the specified spot-performance tests

Table 10-4: xDSL Objectives to be measured

10.7 References

[x1] ETSI TS 101 388 (V1.3.1): “Transmission and multiplexing: Access transmission on metallic access cables; Asymmetric Digital Subscriber Line (ADSL)-European specific objectives”.
[x2] ETSI TS 101 524 (V1.1.3): “Transmission and multiplexing: Access transmission on metallic access cables; Symmetric single pair high bit rate Digital Subscriber Line (SDSL).
[x3] ETSI TS 101 270-1 (V2.0.10): “Transmission and multiplexing: Access transmission on metallic access cables; very high speed Digital Subscriber Line (VDSL); part 1: functional objectives.
[x4] ETSI TS 101 270-2 (V2.0.8): “Transmission and multiplexing: Access transmission on metallic access cables; very high speed Digital Subscriber Line (VDSL); part 2: transceiver specification.
[x5] ETSI TR 101 830-1: “Transmission and multiplexing; Spectral Management on metallic access networks: Part1 Definitions and signal library”.
[x6] ETSI TR 101 830-2 - DRAFT: “Transmission and multiplexing; Spectral Management on metallic access networks: Part2 Technical methods for performance evaluations” (work item DTS/TM-06030, file m01p20a8.pdf, July 2004).
[x7] DSL Forum TR-023, Overview of ADSL Testing, May 1999.
[x8] DSL Forum TR-029, ADSL Dynamic Interoperability Testing, February 2000.
[x9] DSL Forum TR-030, ADSL EMS to NMS Functional Requirements, February 2000.
[x10] DSL Forum TR-048, ADSL Interoperability Test Plan, April 2002.
[x11] DSL Forum TR-067, ADSL Interoperability Test Plan, May 2004.
[x12] DSL Forum TR-060, Interoperability test plan for SHDSL, November 2003.
[x13] DSL Forum TR-069, CPE WAN Management Protocol, May 2004.
[x14] DSL Forum WT-072v4, VDSL Interoperability Test Suite, May 2003.
[x15] DSL Forum WT-090, Protocol Independent Object Model for Managing Next Generation ADSL Technologies, June 2004.
[x16] DSL Forum WT-100v1, ADSL2/ADSL2plus Interoperability Test Plan
[x17] DSL Forum, New tests for WT-100: Tests for ADSL2 specific features, August 17-19, 2004.
[x18] DSL Forum PD-013v8, Interoperability Test Plan for ADSL2/ADSL2plus plug fests, July 2004.
[x19] ITU-T G.992.3 (07/2002), Asymmetric digital subscriber line (ADSL) transceivers – 2 (ADSL2).
[x20] ITU-T G.992.5 (05/2003), Asymmetric digital subscriber line (ADSL) transceivers – 2 plus (ADSL2+).
[x21] ITU-T G.996.1 (2001), Access networks: Test procedures for digital subscriber line (DSL) transceivers.
[x22] ITU-T G.997.1 (2001), Access networks: Physical layer management for digital subscriber line (DSL) transceivers.

[x23] Muse M C2.2 (2004), Position paper on loop qualification and monitoring outlining general features the developed loop qualification and monitoring solution should fulfill.
[x24] ITU-T G.993.2 (2006), Very high speed digital subscriber line transceivers 2 (VDSL2).

11 FIBRE SPECIFIC TESTING

11.1 Introduction

When speaking about testing of fibre-based systems, a wide range of different solutions have to be considered. As shown in Figures 11-**1**a-e, in addition to pure fibre systems e.g. GPON, all types of hybrid solutions have to be addressed like hybrid fibre-copper systems e.g. twisted pair: VDSL over optics, optical Ethernet + VDSL and hybrid fibre-radio systems (radio over fibre). Due to different transmission schemes, different test approaches are required. Because the following chapter is devoted to optical segments of E2E systems, the presented tests focus mainly on the performance and quality of optical domains seen from **external interfaces** (Figures 11-**1**a-e) that act as points of contact between the optical subsystem and the remaining system.
When testing optical systems, there is also wide range of different aspects involved, and not all aspects summarized in this chapter apply to specificl SUT. Before testing, we should characterize the specific SUT and then select adequate tests. In order to structure these test aspects, we have organized this chapter according to the following division:

- External interfacing aspects (see Figures 11-**1**a-e)
  - Analogue interfacing (layer 1)
  - Framed digital interfacing (layer 2)
  - Digital interfacing (layer 1)
- Optical technology aspects
  - Optical modulation (analogue optical, digital optical)- see Figures 11-**1**a-e
  - Optical architecture (P2P, P2MP)
  - Optical multiplexing (non-WDM, xWDM)

Each of these aspects entails different parameters to be tested.

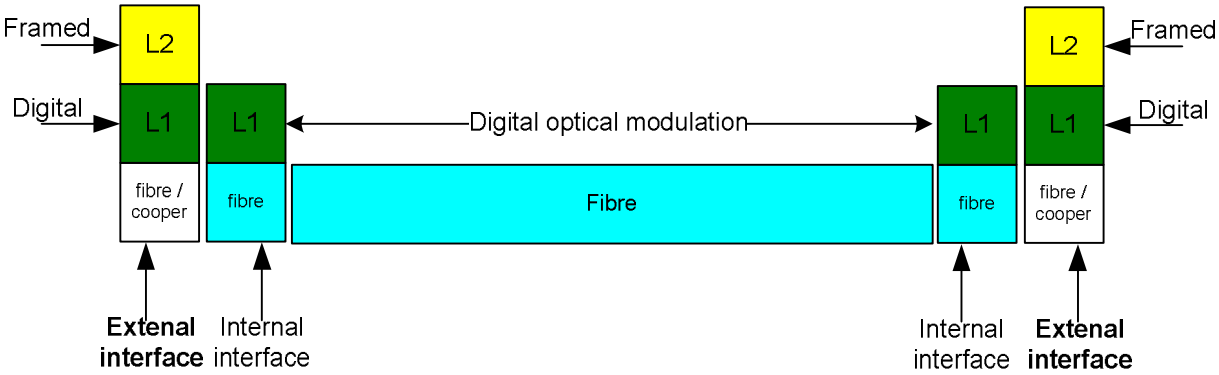


Figure 11-1a: Pure fibre (e.g data transmission over GPON)

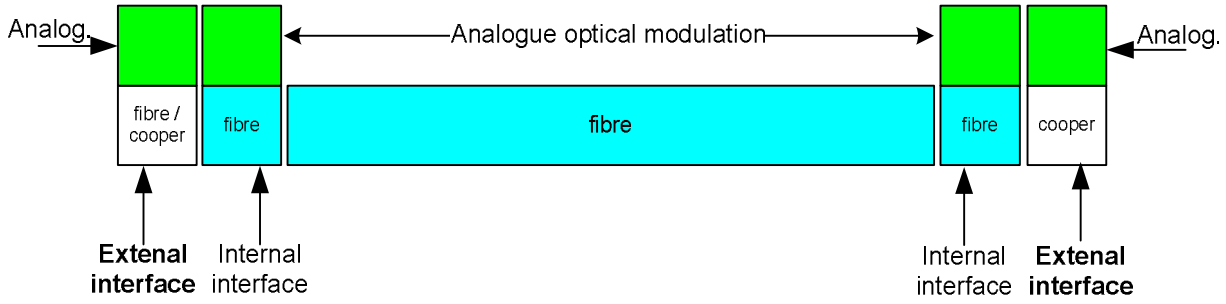


Figure 11-1b: Pure fibre (e.g. analogue TV over PON)

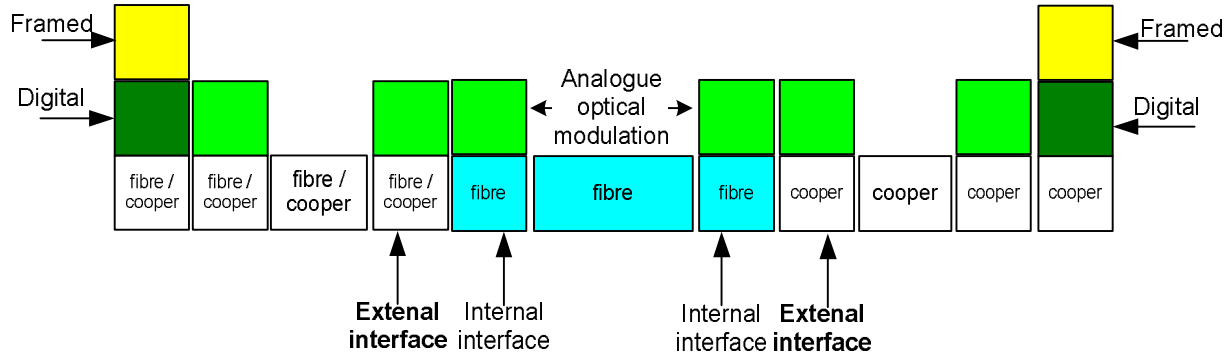


Figure 11-1c: Fibre + Cooper (e.g. VDSL over Optic)

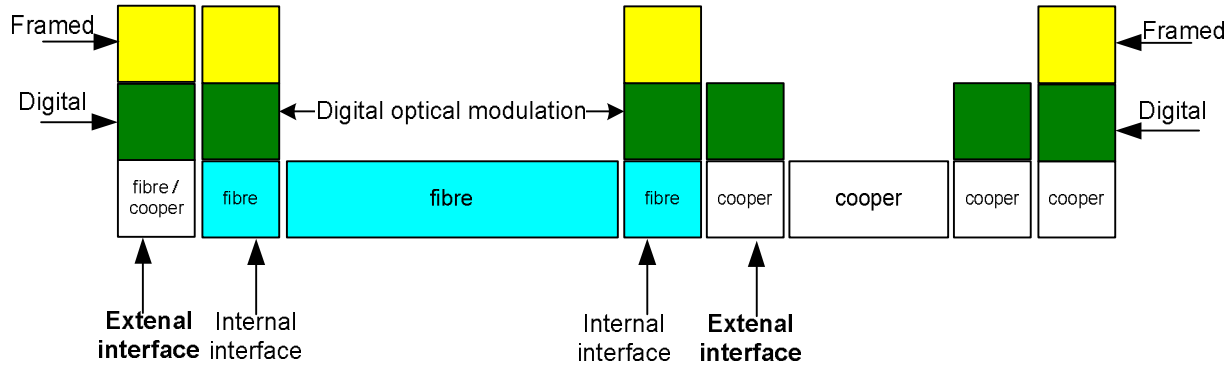


Figure 11-1d: Fibre +Cooper (e.g. P2P GbE (FTTC) + VDSL)

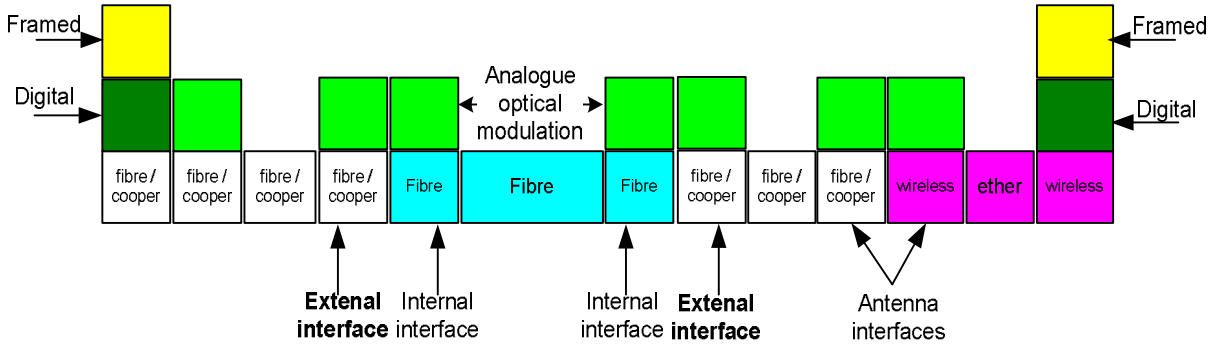


Figure 11-1e: Fibre + Ether (e.g. Radio over Fibre)

One of the challenges of the document is to characterize the system as a whole ("holistic" view). Therefore, the optical system is considered as a "black box" with external interfaces. The "black box" realizes the transmission between these external interfaces at some quality level. The set of parameters that describe the performance and quality of the transmission is a **set performance and quality parameters** (see Figure 11-**2**). These parameters describe the optical system as a whole, they refer to the measurements done at the external interfaces of the optical system. The set of these parameters do not depend on the technology used in the "black box", however the value of these parameters depends strongly on what is inside the "black box". Although these parameters give enough information to provide services on defined quality level, to test the abilities of optical system in terms of physical layer configuration usually more information about the optical system is required. For this reason, the parameters that describe elements, their behavior and the transmission properties of the "black box", are called **"optical technology parameters"** here (see Figure 11-**2**). Furthermore, "optical technology parameters" are divided into **"specific parameters"** and **"common parameters"**. "Specific parameters" strongly depend on the technology used inside the "black box" - type of optical modulation, type of architecture and type of multiplexing technologies (e.g. extinction ratio- specific for digital optical modulation, maximum split ratio- specific for P2MP architecture). "Common parameters" are relevant for many optical systems, independent of the technology used inside the "black box" (e.g. output power, receiver sensitivity, wavelength etc.) The values of the "optical technology parameters" have an obvious impact on the values of "performance and quality parameters", however this impact is not directly, it is rather complex.
The interrelation between different parameters is presented in Figure 12-**2**. The impact of optical technology parameters on performance & quality parameters will be explained in the following parts of this chapter.

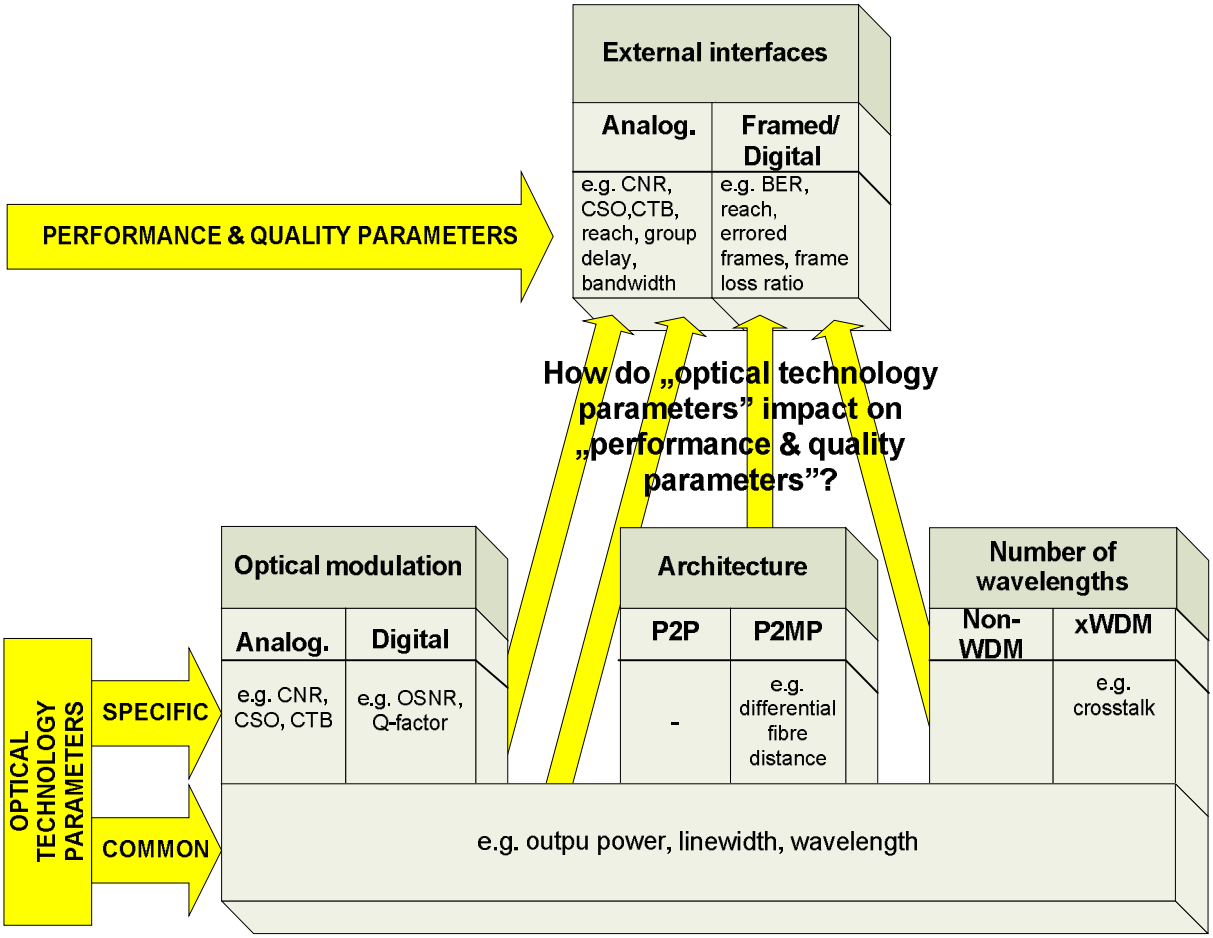


Figure 11-2: Interrelation of testing parameters for fibre optic systems

Next paragraphs of this chapter present a wide range of different test objectives which schould be considered depending on the individual properties of tested optical system.

11.2 Overall testing plan

The overall testing plan is presented below:

1. **Define the SUT**

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM

2. **Define a set of parameters** by selecting these parameters (mentioned in the following chapters), which apply to the SUT properties (it also includes common parameters)

3. **Decide** which parameters are important for your testing goals. Since the importance of selected parameters may vary depending on the SUT, the parameters have been assigned to one of three priorities:
   - High-essential
   - Medium-recommended
   - Low-optional

4. **Select the tests** according to the chosen parameters;
   Proposed sequence of tests:
   a. Functional tests
   b. Element specific tests
   c. External interface-performance and quality tests
   d. Specific optical technology tests

5. **Execute tests**

11.3 Functional tests

11.3.1 Testing management capabilities

In this paragraph, we discuss capabilities of management mechanisms that should be tested in fibre optic systems, especially configuration management and monitoring.

11.3.1.1 Configuration management

Configuration management should consider aspects like transmission quality, access control lists, user configuration, service configuration, etc. However, this paragraph deals with tests that characterize fibre optic systems. These tests are based on verification, whether specific optical properties in relation to configuration management are supported or not. The importance (high, medium, low) of parameters to be tested depends on individual needs /requirements of the tester.

TEST: Check the possibility of following configurations and their real impact on optical system behaviour:

Item	Applicable to	Comments
Accuracy of laser output power	Common	
Path switching from the active to the stand-by mode (on demand)	Common	
Port configuration: enable, disable, loopback	Common	
Laser wavelength accuracy	No. of λ: xWDM	
Adjustment of the optical signal degradation threshold	Optical modulation: digital	Represents the BER threshold used to detect signal degradation (SD) alarms for optical device
Change of the port data rate	Optical modulation: digital	eg. for multirate SFP transceivers (FE/GbE)
-FEC configuration for downstream direction: disable/enable -FEC configuration for upstream direction: disable/enable	Optical modulation: digital	
Automatic synchronization of system elements	Architecture:P2MP Optical modulation: digital	
Synchronization of system elements (on demand)	Architecture:P2MP Optical modulation: digital	
Encryption configuration in downstream direction of P2MP system: disable/enable	Architecture:P2MP Optical modulation: digital	e.g. Advanced Encryption Standard-AES in GPON
Configuration of the “Polling Period”	Architecture:P2MP Optical modulation: digital	The period between two consecutive times, the ONU autodetection procedure on the PON system is executed. The period is called “Polling Period” (ITU-T G.984.3)
Multicast GEM Port ID configuration	Architecture:P2MP Optical modulation: digital	Used in GPON to specify the GEM Port ID that carries multicast traffic

11.3.2 Monitoring capabilities

In order to manage faults in optical networks, specific monitoring tools should be used, e.g. OAM protocols can be used to diagnose and repair network failures. An appropriate level of optical monitoring gives some insight to optical networks ensuring that the optical system is properly configured and some performance parameters are appropriate for a reliable service delivery. These tools allow for performance monitoring, failure detection and alarm generation. Alarms and performance monitoring features of fibre optic networks should be tested to guarantee their efficiency.

TEST: Check supported monitoring capabilities:

Item	Applicable to	Comments
Loss of optical signal alarm	Common	
Degradation of optical signal alarm	Common	
Laser ON/OFF status	Common	
Detector saturation alarm	Common	
Switching protection status	Common	
Received power level at the internal interface of optical system	Common	
Frame loss ratio	Optical modulation: digital	
Errored frames	Optical modulation: digital	
Bit error rate	Optical modulation: digital	
Distance range calculation	Architecture: P2MP	

For example, the diagnostic tool in PONs may use information transmitted through the OMCI ONU Management and Control Interface (G983.2) link

11.3.3 Security tests

11.3.3.1 Architecture specific security

The fibre specific security related problems should be limited, since it is a wire line technology. However, some attention should be paid to P2MP architectures.
Two basic issues should be considered:

A) Data security – user data may be tapped

B) Fibre optic specific security –user data/signal may be disturbed or damaged

A) Data security

A problem with P2MP systems is that data can theoretically be tapped by any ONU. This especially true for single wavelength systems (non-WDM), where signal in downstream direction is transmitted from OLT to many ONU's on the same wavelength. To prevent this security gap different counter measures like encryption, access lists, etc. are used in PON systems. A detailed description of security objectives requires further studies.

TEST: Data transmission security in P2MP system.

Item	Applicable to	Comments
Data transmission security	Architecture: P2MP No. of λ: non-WDM (downstream) Optical modulation: digital External interfaces: digital/digital framed	

B) Fibre optic specific security

In the following section we describe three events, which can disturb an optical access system significantly:

- The OLT receiver is disturbed by an **ONU malfunction** (laser does not work in burst mode (ON/OFF) but is permanently switched ON). In this case, the OLT receives an interfering signal in parallel to a regular ONU signal. This can strongly reduce the CNR/OSNR (depending on optical modulation type: analogue/digital). As a result, downstream and upstream transmission of the entire PON could be disturbed or even impossible.
- The OLT receiver is disturbed by the insertion of an **additional laser** at the user site. Considering laser wavelengths within the ONU transmitter specification the situation corresponds to the ONU malfunction scenario above.
- The OLT transmitter is disturbed by the insertion of an **additional laser** at the user site. Considering laser wavelengths within the OLT transmitter specification, the disturbing user could cause power and wavelength fluctuations of the OLT light source. As a result, the CNR/OSNR at the ONUs could be reduced.

In a test scenario, insertion of an additional laser at user site can also simulate an ONU malfunction. These tests can be done especially for systems, which have implemented mechanisms for monitoring of potential threats in the network.

TEST: Check whether the following events have any impact on the transmission performance and quality:

Event	Applicable to	Result
Insertion of an additional laser at user site working at following wavelengths: λ_1 or λ_2	No. of λ: (λ_1-down)- non-WDM (λ_2- up)- non-WDM Architecture:P2MP	Transmission within the entire PON could be impossible.
Insertion of an additional laser at user site working at λ_1… λ_n	No. of λ: (λ_1 - down)- non-WDM (λ_2…λ_n - up)- xWDM Architecture:P2MP	Transmission within the entire PON could be impossible.
1) Insertion of an additional laser at user site working at λ_1 2) Insertion of an additional laser at user site working at one of following wavelengths:	No. of λ: (λ_2…λ_n -down)-xWDM (λ_1 - up)-non-WDM Architecture:P2MP	1) Transmission within the entire PON could be impossible. 2) Operation of individual ONU's could be impossible.

$\lambda_2 \ldots \lambda_n$		
Insertion of an additional laser at user site working at one of following wavelengths: $\lambda_{1 \ldots} \lambda_{i+k}$	No. of λ: xWDM ($\lambda_1 \ldots \lambda_n$ - down)-xWDM ($\lambda_i \ldots \lambda_{i+k}$ -up)- non-WDM Architecture:P2MP	Operation of individual ONU's could be impossible.

11.3.3.2 Laser safety requirements

Laser safety requirements play an important role in designing xWDM systems. In optical access systems using xWDM the launched power per channel might be limited due to safety demands.
According to [Fib4] and [Fib5], lasers are classified into different safety categories. The following table gives an overview for the relevant classes with a short description.

Class	Description
1	Safe under reasonably foreseeable conditions, including use of optical instruments
1M	Lasers that are safe for viewing with the unaided eye
3R	Usually safe when handled carefully
3B	Potentially hazardous when beam or specular reflections are viewed directly
4	Hazardous to eye and skin, even diffuse reflections

Depending on laser class and wavelength, IEC standards [Fib4] and [Fib5] define an accessible emission limit (AEL) and a maximum power levels for communication fibres respectively. A summary of the maximum ratings is given in the following table. The maximum power was calculated for a single mode fibre with a mode field diameter of 11µm.

Laser class	Wavelength [nm]	Accessible emission limit (AEL) [mW]	Max. power for communication fibre*) [mW]
1	1270…1400	15.6	15.6
	1400…1610	10	10
1M	1270…1400	15.6	43
	1400…1610	10	112
3R	1270…1400	80	80
	1400…1610	50	NA (see 1M)
3B	1270…1610	500	500

*) worst-case value for a single mode fibre with a mode field diameter of 11µm.

TEST: Ensure that the network design complies with laser safety regulations.

11.3.4 Redundancy tests

Fibre breaks and other physical layer failures account for the vast majority of all network failures. Fibre protection is therefore essential for achieving high network availabilities. Ethernet-based services can be protected through protocols such as IEEE 802.3ad (LACP), IEEE 802.1d-2004 (RSTP) or IEEE 802.17 (RPR).
On the physical layer we can distinguish between two main approaches:

- The 1:1 protection mechanism (cold stand-by) is based on the creation of two disjoint paths for the protected link or link section. Devices located on both sides of the link/section select one operating link/section, while the other link/section is temporarily unused. To coordinate this procedure some kind of protocol is needed.
- The 1+1 protection mechanism (hot stand-by) splits the signal and transmits it over two disjoint paths to the receiver. A device at the receiver site selects one signal.

Of course, there are much more protection mechanisms, depending on the network complexity. But usually they are based on the basic mechanisms described above.
The most important aspect to be tested is switching time (restoration of transmission) in case of fibre failures.

TESTS: The following aspects should be verified:

Item	Applicable to	Comments
Feasibility of redundancy/resilience in different parts of optical network	common	
Switching from the stand-by to the active mode in case of failures. The transmission restoration time should be measured.	common	

11.4 External interface aspects

This point focuses on performance and quality tests of optical system seen from the external interfaces (see Figure 11-**3**).

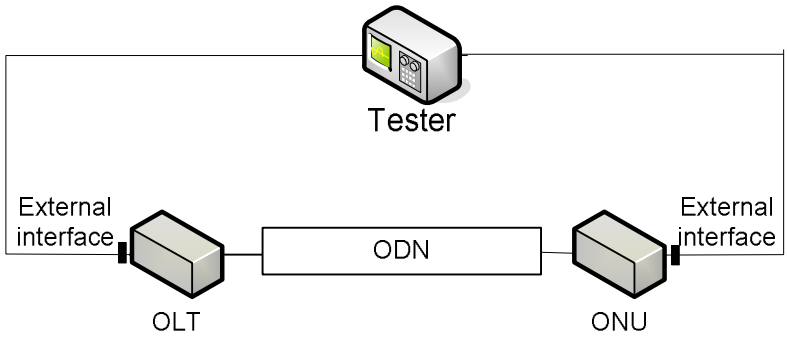


Figure 11-3: Simplified diagram of the test configuration

The key for the differentiation of the external interfaces is the signal type (analogue/digital/framed digital), which is present at the ends of the optical system.
From the external interfaces point of view (see Figures 11-**1**a-e), optical systems can transmit:

a. analogue signals (layer 1) – analogue external interfaces on both sides of the optical system (e.g. xDSL over Optics, Radio over Fibre, or Analogue TV over PON)
b. digital signals (layer 1) – digital external interfaces on both sides of the optical system (e.g. P2P Optical Ethernet with VDSL external interfaces, E1, STM1)
c. framed digital traffic (layer 2) – framed external interfaces on both sides of the optical system (e.g. GPON, P2P Optical Ethernet)

Depending on the external interface type (analogue, digital or framed digital) different performance & quality parameters should be considered. The results obtained from these tests give information about the overall performance of the fibre optic system, but provide little help when the performance lags behind the expectations for different border conditions. Based on these tests we could make some preliminary analysis whether a tested system is able to provide special services or not.

11.4.1 Analogue external interfaces

An analogue external interface is able to transmit/receive analogue signals. To characterize analogue external interfaces, the following evaluation parameters should be considered:

CNR
In analogue communications, CNR is a measure of the carrier strength relative to the background noise in the bandwidth of interest. This is a key parameter in terms of analogue transmission and characterizes the quality of the signal.

TEST: CNR should be tested at the external interfaces considering impact of many parameters e.g.:

- optical reach
- splitting ratio (in case of P2MP networks)
- differential fibre distance (in case of P2MP networks)
- optical return loss (in case of analogue modulation as well as modulation independent in conjunction with optical circulators)

Moreover, CNR is subject of receiver sensitivity tests.

Linearity
In analogue transmission, composite second-order (CSO) distortion is the ratio of the carrier to composite second-order distortion products. Composite triple beat (CTB) distortion, also called composite third-order beat, is the ratio of carrier to composite third order distortion products. Both distortions result from multiple carriers experiencing second and third order non-linearities, which generate multiple distortion products. These distortion products are the result of the nonlinear transfer characteristic of amplifiers, attenuators, fibres and other passive devices.

TEST: CSO and CTB should be tested at the external interfaces considering impact of various parameters like in CNR test case.
Furthermore, linearity as well as CNR is subject of receiver sensitivity tests.

Group delay
Group delay is the effective time delay as a function of frequency of the transmitted signal. The transmission delay has a large impact on the services supported by the optical network.

TEST: Measure the group delay of the optical system considering impact of optical reach

Transmission bandwidth
Transmission bandwidth is the frequency range between two points where the signal is a fraction (e.g. -3 dB) of the maximum signal strength (in that case 3dB-bandwidth). Transmission bandwidth represents the useful frequency range for signal transmission.

TEST: Verify the transmission bandwidth of a system in a specific configuration

Optical reach (for analogue external interfaces)
Optical reach is the maximum length of an optical path that still ensures a required signal transmission performance (the required value of CNR and linearity (CSO/CTB) at the analogue external interfaces)

TEST: Verify the optical reach of a system consdering impact of various parameters e.g:

- splitting ratio (in case of P2MP)
- optical return loss (in case of analogue modulation as well as modulation independent in conjunction with optical circulators)
- wavelength (in case of multi wavelength transmission -xWDM)

TESTS: Performance & quality parameters for analogue external interfaces are compiled in the table below:

Item	Unit	Applicable to	Comments
CNR	dB	Analogue external interfaces	Considering impact of optical reach, splitting ratio, differential fibre distance, ORL
Linearity (CSO/CTB)	dB		Considering impact of optical reach, splitting ratio, ORL
Group delay	ns		Considering impact of optical reach
Transmission bandwidth	Hz		Tested in specific configuration
Optical reach	km		Considering impact of splitting ratio, ORL, wavelength

11.4.2 Framed digital external interfaces

For framed digital interfaces the following evaluation parameters should be considered:

Errored frames
Errored frames - frames which are over-sized, under-sized, misaligned or with a faulty FCS (Frame Check Sequence) [Fib15].

TEST: Verify errored frames with respect to the impact of various parameters e.g:

- optical reach
- bitrate
- splitting ratio (in case of P2MP networks)
- differential fibre distance (in case of P2MP networks)
- optical return loss (in conjunction with optical circulators)
- wavelength (in case of multi wavelength transmission)

Frame loss ratio

Frame loss is a percentage of frames that should have been forwarded by a network device under steady state (constant) load but were not forwarded due to a lack of resources [Fib9]. In terms of fibre optic systems it is useful to evaluate this parameter e.g. for MAC protocol performance (TDMA reliability, differential fibre distance etc.).

TEST: Verify the frame loss ratio for tests on TDMA reliability, differential fibre distance throughput, maximum system capacity

Throughput
Throughput is the maximum rate at which none of the offered frames are dropped by the device [Fib9].

TEST: Verify the impact of various parameters (similar to the errored frames test) on throughput

Maximum system capacity (for framed digital external interfaces)
System capacity means the total throughput of the optical system. It is the sum of throughputs between all external interfaces assigned to one fibre optic system. For example, in order to measure the maximum upstream and downstream system capacity of a GPON (theoretically 1,2 and 2,4 Gbps), three 1 GbE interfaces at the OLT and 24 Fast Ethernet interfaces at the ONU sites are to be considered. In such a configuration, the throughput tests on all employed interfaces should be performed (OLT-ONU) and the results should be summed (at the OLT site for upstream and ONU for downstream).

TEST: Verify the maximum system capability for specific physical configurations

Frame delay
Frame delay refers to the time it takes to transmit a frame across an optical network from source to destination (between external interfaces).
The term frame delay is often used interchangeably with latency. The definition of latency [Fib9] may be quoted: “The time interval starting when the last bit of the input frame optical reaches the input port and ending when the first bit of the output frame is seen on the output port.” In this definition, input and output ports should be treated as framed external interfaces.

TEST: Verify the frame delay of the optical system considering impact of optical reach and throughput

Optical reach (for framed digital external interfaces)
Optical reach is the maximum length of an optical path that still ensures a required signal transmission performance (minimum required number of errored frames at the framed digital external interfaces)

TEST: Verify the optical reach of the system in terms of various parameters:

- bitrate
- splitting ratio (in case of P2MP networks)
- differential fibre distance (in case of P2MP networks)
- optical return loss (in case of analogue modulation as well as modulation independent in conjunction with optical circulators)
- wavelength (in case of multi wavelength transmission)

TESTS: Performance & quality parameters for framed external interfaces are compiled in the table below:

Item	Unit	Applicable to	Comments
Errored frames	frame	Framed external interfaces	Considering impact of bitrate, optical reach, splitting ratio, differential fibre distance, ORL, wavelength
Frame loss ratio	%		Checked in such tests as TDMA reliability, differential fibre distance, throughput, maximum system capacity
Throughput	Mbit/s		Considering impact of bitrate, optical reach, splitting ratio, differential fibre distance, ORL, wavelength
System capacity	Mbit/s		Tested in specific physical configurations
Frame delay	ms		Considering impact of optical reach and throughput
Optical reach	km		Considering impact of bitrate, splitting ratio, differential fibre distance, ORL, wavelength

11.4.3 Digital external interfaces

BER
The bit error ratio (BER) is a fundamental performance measure in digital transmission systems. Due to interrelated signal impairments, there is no straightforward relation between BER and optical transmission characteristics. BER measurements are out-of-service measurements, since they rely on a bit-by-bit comparison between the received bit stream and a known test pattern [Fib13].

TEST: BER should be tested in terms of various parameters e.g.:

- optical reach
- bitrate
- splitting ratio (in case of P2MP networks)
- differential fibre distance (in case of P2MP networks)
- optical return loss (in conjunction with optical circulators)
- wavelength (in case of multi wavelength transmission)

NOTE: For a complete system BER can easily be tested only in conjunction with PDH/SDH interfaces (e.g. E1, STM-1). Tests with VDSL external interfaces (e.g. P2P optical Ethernet with VDSL external interfaces) represent a different (mixed) approach and require further studies.

Maximum system capacity (for digital external interfaces)
System capacity means the total bitrate of the optical system. It is the sum of bitrates between all external interfaces assigned to one fibre optic system. For example, in order to measure the maximum upstream and downstream system capacity of a BPON (e.g. theoretically 155 and 622 Mbps), 1 x STM-4 interface at the OLT and 4 x STM-1 interfaces at the ONU sites are to be considered. In such a configuration, the throughput tests on all

employed interfaces should be performed (OLT-ONU) and the results should be summed (at the OLT site for upstream and ONU for downstream).

TEST: Verify the maximum system capability for specific physical configurations

Delay
TEST: Verify the signal delay between external interfaces considering impact of optical reach

Optical reach (for digital external interfaces)
Optical reach is a maximum length of an optical path to achieve a given BER at the external interfaces of an optical access system.

TEST: Verify the optical reach of the system in terms of various parameters:

- bitrate
- splitting ratio (in case of P2MP)
- differential fibre distance (in case of P2MP networks)
- optical return loss (in case of analogue modulation as well as modulation independent in conjunction with optical circulators)
- wavelength (in case of multi wavelength transmission)

TESTS: Performance & quality parameters for digital external interfaces are compiled in the table below:

Item	Unit	Applicable to	Comments
BER		Digital external interfaces	Considering impact of bitrate, optical reach, splitting ratio, differential fibre distance, ORL, wavelength
System capacity	Mbit/s		Tested in specific physical configurations
Delay	ms		Considering impact of optical reach
Optical reach	km		Considering impact of bitrate, splitting ratio, differential fibre distance, ORL, wavelength)

11.5 Optical technology aspects

In order to provide a generic overview, the main parameters characterizing the quality of optical transmission systems are discussed below. They are split into the groups element specific testing parameters that describe each constituting part of the network (transmitter, ODN, receiver) and optical technology specific testing parameters that decribe different types of optical modulation, architecture and xWDM. For system evaluation purposes the relevance of these parameters is indicated by the priorities

- High
- Medium
- Low

Parameters with high priority are essential to evaluate optical systems (e.g. transmitted power, receiver sensitivity, insertion loss).

Parameters with medium priority are recommended due to their complementary impact on system performance and quality (e.g. total jitter or extinction ratio with direct impact on BER/errored frames).
Parameters with low priority are optional, for in-depth studies. These parameters can be tested to get detailed information about specific system domains. Since each parameter has a dedicated impact on system performance and quality, such information could be useful to find possible weak points and corresponding counter actions.

11.5.1 Element specific aspects

11.5.1.1 Optical transmitter

The most relevant parameters for transmitters in terms of system quality and performance are output power, wavelength, linewidth and isolation. The list of potential physical layer parameters may be longer, but we are focusing on the most important ones to evaluate the physical layer system performance.

Output power
Minimum mean output power is the minimum value of the average power of a pseudo-random data sequence launched into an optical fibre [Fib1].

Maximum mean output power is the maximum value of the average power of a pseudo-random data sequence launched into an optical fibre [Fib1].

Output power is a basic parameter with direct impact on many parameters like total power budget, OSNR/CNR (digital/analogue), optical reach as well as with indirect impact on the available bitrate (photons per bit).

Wavelength
By wavelength we mean the peak/centre wavelength emitted by the transmitter (depending on used laser SLM/MLM). Wavelength has significant influence on attenuation and dispersion caused by fibre in the ODN and on optical reach of the system. Furthermore, this parameter has an impact on performance of used optical components in the ODN (e.g. splitters, filters, amplifier gain).

Linewidth
The most relevant parameters that characterize linewidth are RMS width (root-mean square width) in case of MLM lasers and “-20 dB width” for SLM lasers. The RMS width or the standard deviation σ (in nm) of the spectra distribution of MLM laser considers all laser modes, which are not more than 20 dB down from the peak mode. Only a system with an MLM laser at 1310 nm requires this specification. In turn, the -20 dB spectral width (in nm) of an SLM laser is specified by the full width of the central wavelength peak, measured 20 dB down from the maximum amplitude of the central wavelength under standard operating conditions [Fib1].
Signals with a large linewidth are more susceptible to ODN dispersion effects limiting the system performance.

Side mode suppression ratio
The side mode suppression ratio (SMSR) is defined as the ratio of the largest peak of the total source spectrum to the second largest peak. The spectral resolution of the measurement shall be better (i.e. the optical filter bandwidth shall be less) than the maximum spectral width of the peak, as defined above. The second largest peak may be close to the main peak or more distant [Fib1]. Transmitters for high-end optical communication systems

typically need a side mode suppression ratio >30 dB. Lower SMSR values may lead to intolerable intensity noise (mode partition noise) with negative effects on OSNR/CNR and the crosstalk behavior in xWDM systems.

Isolation

In case of WDM systems, it is important to assure adequate isolation between adjacent wavelengths. Poor isolation can lead to crosstalk with negative effects on CNR (analogue transmission) and on BER/errored frames (digital/framed digital transmission).

Temperature coefficient optical power/wavelength

With regard to systems that have to cope with variable temperature conditions (e.g. street cabinets) it could be relevant to measure power and wavelength dependencies.

TESTS: Parameters in terms of optical transmitter are compiled in the following table:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interface	Digital/Framed dig. external interface		
Output power (MIN/MAX)	dBm	High	CNR, optical reach	BER, errored frames, optical reach, throughput	common	
Wavelength	nm	High	Optical reach, crosstalk	Optical reach, crosstalk		
Linewidth (RMS/-20 dB width)	nm	Medium	Optical reach, crosstalk	BER, errored frames, optical reach, crosstalk		RMS is considered for MLM lasers and "-20dB width" for SLM lasers
SMSR	dB	Medium	CNR, crosstalk	BER, errored frames, crosstalk		Optical transmitter: SLM
Isolation	dB	Medium	CNR, crosstalk	BER, errored frames, crosstalk	No. of λ: xWDM	
T° coef. optical power	dB/°C	Low	CNR, optical reach	BER, errored frames, optical reach, throughput	common	
T° coef. wavelength	nm/°C	Low	Optical reach, crosstalk	Optical reach, crosstalk		

11.5.1.2 ODN requirements

There is no interest to describe in-depth ODN tests in this document, however since the ODN is part of test set-up it may play an important role with respect to the evaluation of test results. Furthermore, in accordance with the test methodology, the ODN used for testing should meet specific requirements to assure the reproducibility of testing conditions and comparison of measurements.

There are many parameters to describe the ODN. For practical reasons, they can be divided in two sets:

- optical transmission parameters
- component oriented parameters

Optical transmission parameters may describe both, components and ODN as a whole including insertion loss, optical return loss, spectral response, PMD (entire path), chromatic dispersion (entire path), wavelength isolation (entire system).

Component oriented parameters only refer to particular elements of the ODN including fibre attenuation, amplifier gain, and uniformity.
In order to assure the reproducibility of tests conditions and the comparability of measurements, it seems sufficient to consider optical transmission parameters. However, the impact of component oriented parameterson optical transmission parameters will exemplarily be explained in the following paragraphs.
An overview of linear and non-linear effects affecting the signal quality in the fibre is given in Figure 11-**4**. With less optical power and a lower number of channels (wavelengths), the system performance suffers mainly linear effects. With higher optical power and more channels (wavelengths), the influence of non-linear effects on signal quality is increasing.

To find out more about general requirements on ODN components please refer to [Fib11].

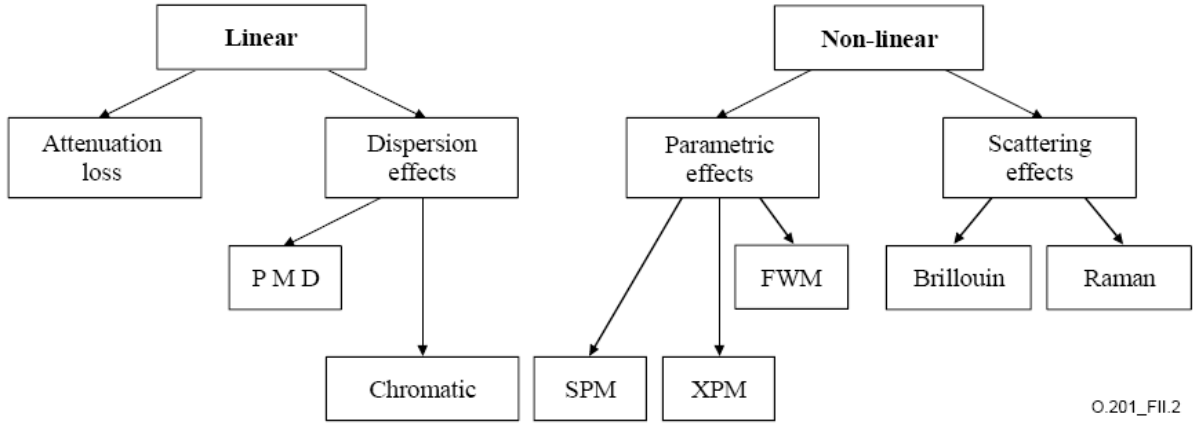


Figure 11-4: Sources of impairments in optical transmission systems [Fib13].

Insertion Loss (IL)
IL is defined as the total optical power loss caused by insertion of an optical component in the ODN, such as a connector, splice or a splitter [Fib2]. It is an important parameter that characterizes the ODN and has a direct impact on optical reach, OSNR/CNR and BER/Errored Frames (in case of digital/framed digital external interfaces).
Insertion loss depends on the ODN configuration:

- For a single wavelength P2P network, the IL depends on fibre type, signal wavelength, optical path length, amplifier gain, and connector as well as splice losses.
- For a single wavelength P2MP network (typically a PON), the additional power loss of the splitter have to be considered compared to P2P networks. Depending on the design of the power splitters, different branches of P2MP network may have different IL and should be measured separately.
- In xWDM infrastructures, specific xWDM components influence the IL e.g. fixed or tuneable filters, WDM splitters and AWG. Complementary factors also have an impact on IL e.g. fibre type, signal wavelength, optical path length, amplifier gain, connector as well as splices losses.

Moreover, the following parameters have an impact on the IL:

Parameter	Description
Amplifier gain	Gain for optical amplifiers is the ratio of output power to input power, specified in the small signal, linear gain region, with a signal applied at the input. Gain varies with wavelength, with a peak near 1535 nm. The exact shape of the gain profile depends on the length and doping of the fibre amplifier, the pump power, and the input power. As input powers increase, the variation of gain

	with wavelength declines, giving a more uniform gain spectrum [Fib7].
Fibre attenuation	Representative values of concatenated optical fibres [Fib12]: • 1260–1360nm: 0.5 dB/km • 1530–1565nm: 0.275 dB/km • 1565–1625nm: 0.35 dB/km
Uniformity	Uniformity is applied to splitters having the same splitting ratio determining the power distribution on the output ports. It can also be calculated based on the highest and lowest insertion losses. Uniformity could cause an unequal loss in each branch of a PON.
Temperature	The specifications of ODN components (e.g. connectors, fibre) are temperature dependent, which could cause IL variations.

Sensitivity to reflections

Reflections are caused by refractive index discontinuities along optical paths. Uncontrolled they can degrade the system performance (e.g. BER or CNR) because of their disturbing effects on the operation of optical sources or amplifiers. Multiple reflections can lead to interferometric noise at the receiver [Fib1]. Reflections may occur in different forms:

- Reflectance
- Optical Return Loss (ORL)

Reflectance is the ratio of power reflected to the incident power at a connector junction or other component or device [Fib2].

ORL is the ratio of optical power arriving at the interface to the optical power reflected back from the same interface [Fib2].
Reflectance denotes the reflection at any discrete reflection point, whereas the ORL is the total returned power of a fibre including both discrete reflections and distributed backscattering such as Rayleigh scattering.
Reflections are especially important in P2MP systems where multiple reflections occur. According to ITU-T G.982 all discrete reflections between reference points S and R (internal interfaces), including unused branches of branching devices, shall exhibit a reflectance better than –35 dB. A maximum discrete reflectance of –50 dB is recommended for fusion splices, to accommodate current and future applications in optical access networks. According to ITU-T G.983.1, the overall ORL specification at point R/S (internal interfaces) should be better than 32 dB.
Due to more demanding requirements with respect to CNR/OSNR at the receiver, optical systems with analogue modulation are more sensitive to ORL than systems with digital modulation.
An exception is the usage of optical circulators in the ODN. In this case, the ORL is also important for digital modulation type. Figure 11-**5** illustrates an optical system with two circulators at OLT and ONU side respectively. The reflected signal (e.g. from a fibre connector like FC/PC) has a relatively high power (point of reflection close to the transmitter) which disturbs the strongly attenuated signal from the ONU Tx. Both signals are received by the OLT and as a result, the OSNR at the OLT is strongly reduced.

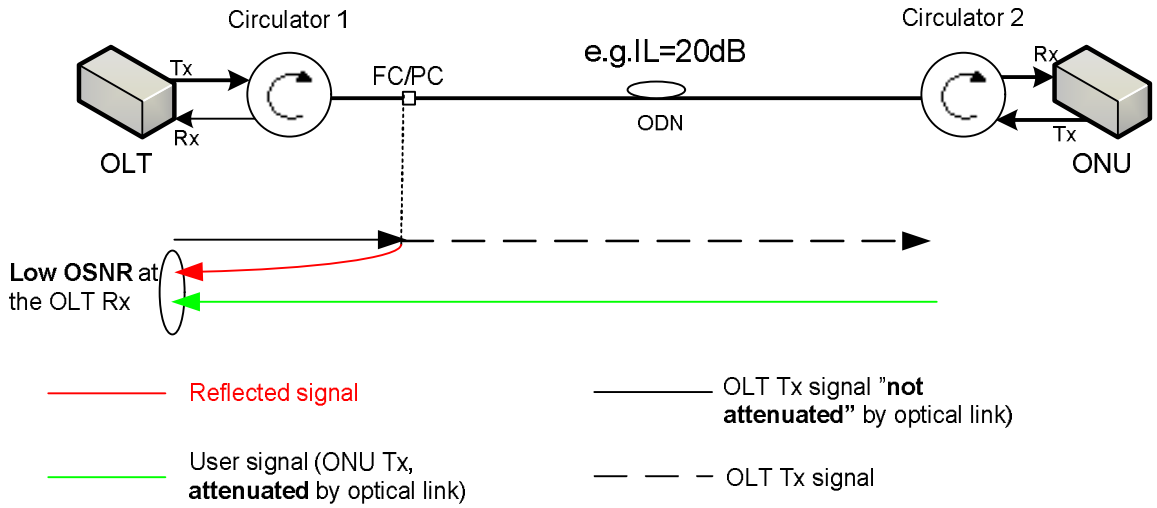


Figure 11-6: Impact of reflections within optical system with optical circulator

Sensitivity to polarization mode dispersion (PMD)

PMD occurs when different planes of light travel along a fibre at slightly different speeds, [Fib3]. Depending on the fibre type, PMD becomes an increasingly serious as the bitrate and the length of optical transmission systems increase (e.g. 10Gbit/s and 100km). Without any compensation, PMD can lead to additional bit errors at the receiver (increased BER/errored frames).

Considering analogue signals, excessive levels of PMD, combined with laser chirp and chromatic dispersion, can create CSO/CTB distortions and CNR reductions.

Sensitivity to chromatic dispersion

Chromatic dispersion occurs because wavelengths travel through the fibre at different speeds, even within the same mode. Standard single-mode fibres exhibit zero dispersion around 1310 nm. Depending on wavelength, bitrate and optical reach, chromatic dispersion causes pulse distortions, which leads to additional bit errors at the receiver (increased BER). In analogue transmission, dispersion can cause significantly distorted waveforms and can result in unacceptable levels of (CSO/CTB) [Fib3].

Noise figure (NF)

NF is the increase in noise power of a device from the input to the output (e.g. optical amplifier). The definition is [Fib9]:

$NF = SNR_{IN} / SNR_{OUT}$

Where $SNR_{IN/OUT}$ is the SNR at the input/output port respectively. The SNR_{OUT} at the amplifier output is lower than SNR_{IN} at the input due to presence of ASE (Amplified Spontaneous Emission).

In general, this parameter refers to amplifiers, but applies also to ODN/amplifier combinations. In such cases, SNR_{IN} should be measured at the input of the ODN (transmitter side) and SNR_{OUT} at the output of the ODN (receiver side).

Wavelength isolation

Wavelength isolation is a measure to describe the separation of a given wavelength at the output of a wavelength division demultiplexer. It is the ratio of the optical power at two output

ports. In the case of WDM networks, the channel separation has to be guaranteed in order to avoid crosstalk (referred to as far-end crosstalk) between adjacent wavelength channels. Poor wavelength isolation reduces the OSNR.

Wavelength conversion

Conversion of optical signals from one wavelength to another one is used to enable flexible lightpath establishment and efficient wavelength utilization. Such a conversion process is called wavelength conversion.

$\Delta \lambda = | \lambda_2 - \lambda_1|$
λ_1 - optical wavelength before conversion
λ_2 - optical wavelength after conversion

In general, there are two approaches to realize wavelength conversion, namely OEO-based wavelength conversion and all-optical wavelength conversion.

OEO wavelength conversion is a two-step process. First, the optical signal is converted into an electronic format and second, the electronic signal is used to modulate a laser with another emission wavelength. For instance, such type of conversion will be used in MUSE SPE.

All-optical wavelength conversion is a more advanced conversion schemes not considered in MUSE. All optical conversion in general utilizes some nonlinear optical effects in optical components. These effects include four wave mixing (FWM), cross-phase modulation (XPM), etc.

In comparison to signal before conversion, signal after covnerion have different optical properties (e.g. different wavelength, different linewidth, different optical power etc.). For this reason signal after conversion should be treated separately and measured again. For test details, please reffer to previous paragraph “Optical transmitter”.

Spectral Response
Spectral response gives us information about range of wavelengths that pass through an ODN component in desirable way (e.g. max -3dB from peak wavelength). In case of filters it is the ratio of output power to input power depending on wavelength.

TESTS: Crucial ODN tests are compiled in the following table:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
IL	dB	High	CNR, optical reach	BER, errored frames, optical reach, throughput	Common	
ORL	dB	High/ medium	CNR, optical reach	BER, throughput, errored frames,optical reach	Common	In general, this parameter is more significant in analogue than in digital optical modulation schemes
Sensitivity to PMD	Ps	Medium	CNR, optical reach	BER, errored frame, optical reach, throughput	Common	
Sensitivity to CD	ps	Medium	CNR, optical reach	BER, errored frames, optical reach, throughput	Common	
NF	dB	Medium	CNR, optical reach	BER, errored frame, Optical reach	Common	ODN: with amplifier
Wavelength isolation	dB	Medium	CNR, optical reach, crosstalk	BER, Errored Frames, optical reach, crosstalk	No. of λ: xWDM	e.g WDM splitter
Wavelength conversion	nm	Medium	CNR, optical reach, crosstalk	BER, errored frames, optical reach, crosstalk	No. of λ: xWDM	e.g transponder
Spectral response	dB vs. nm	Medium	CNR, optical reach	BER, errored frames, optical reach	No. of λ: xWDM	

11.5.1.3 Optical receiver

A list of parameters to be tested is described below:

Sensitivity (Receiver Sensitivity)

In digital transmission, receiver sensitivity is defined as the minimum average received power to achieve a BER of e.g.10^{-10}. It takes into account power penalties caused by use of a transmitter under standard operating conditions with worst-case values of extinction ratio, pulse rise and fall times, optical return loss at the transmitter, receiver connector degradation and measurement tolerances [Fib10]. The receiver sensitivity does not include power penalties associated with dispersion, jitter, or reflections from the optical path; these effects are specified separately in the allocation of maximum optical path penalty (described in next paragraph “Digital optical modulation”.

In analogue transmission, receiver sensitivity is the minimum value of received optical power to allow correct operation (e.g. the required value of CNR and linearity (CSO/CTB) at the external interfaces of optical system must be achieved).

Sensitivity is a basic parameter for calculating the power budget. Furthermore, it has direct influence on the optical reach of an optical system.

Saturation (Receiver Saturation)
Receiver saturation power is the maximum allowed input power, to prevent receiver saturation. In PON systems, the receiver should be robust against increased optical power levels for the period of start-up or potential collisions during ranging, for which a BER of 10^{-10} is not guaranteed [Fib10]. Receiver saturation threshold considerations are of importance for the operation of short haul systems.

Temperature coefficient of Receiver Sensitivity
The test of the temperature coefficient applies to systems that have to cope with variable temperature conditions (e.g. street cabinets). Sensitivity variations influence the optical budget and in consequence, the optical reach. This test is important for the design of optical systems, especially for the characterization of components that operate at non-wheatherprotected locations.

TESTS: Transmitter parameters are compiled in the following table:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
Sensitivity	dBm	High	Optical reach	Optical reach	common	
Saturation	dBm	Medium	CNR, linearity, ptical reach	BER, errored frames, optical reach		
T° coef. sensitivity	°C	Low	Optical reach	Optical reach		

11.5.2 Optical technology specific aspects

11.5.2.1 Type of optical modulation

This paragraph specifies some parameters that can be tested inside optical systems and which are useful for system evaluations. Depending on the optical modulation type: analogue or digital (see Figures 11-**1**a-e), different approaches are required and should be treated separately. Regardless of the optical modulation type, measurements of different parameters can be done in different locations of optical path. (Figure 11-6).

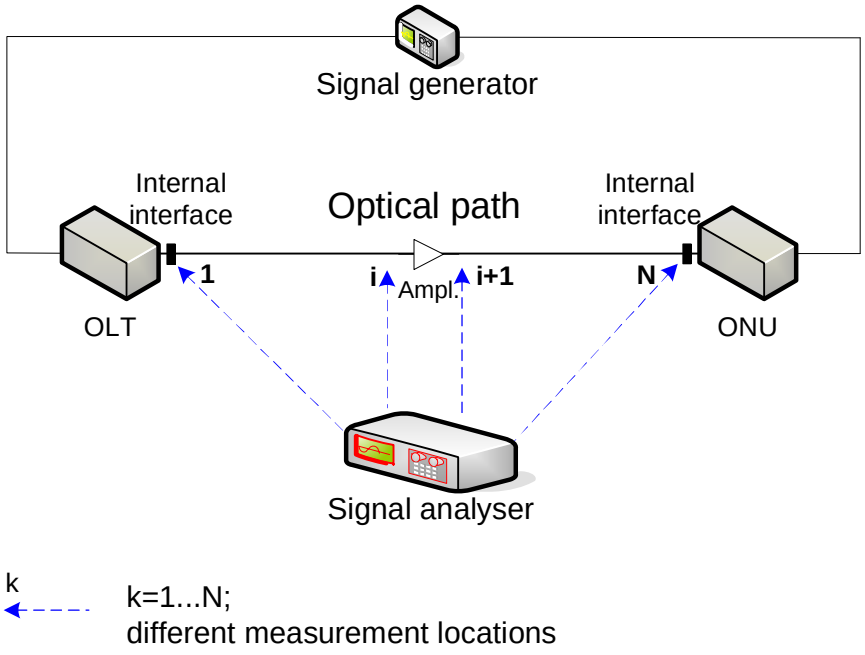


Figure 11-6: Different measurement locations

11.5.2.1.1 Analogue optical modulation

In analogue modulation, the following parameters should be considered:

CNR (inside the optical system)
In analogue communication systems, carrier-to-noise ratio (CNR) is a measure of carrier strength relative to background noise in the bandwidth of interest. One should note that the measurement of CNR is carried out to evaluate the optical system from analogue external interfaces point of view. However, the evaluation with respect to optical system segments is also worth considering. CNR can be tested in different domains of the optical path: at the internal interface (transmitter side) as a reference point, at the input and output port of optical components with impact on CNR (e.g. amplifier-noise figure) and at the internal interface (receiver side). By comparison of CNR values the impact of individual components could be calculated.
TEST: CNR at different points of the optical path (see Figure 11-6).

Linearity
Linearity is defined in paragraph 11.4.1 “Analogue external interfaces”. Measurements in terms of linearity of optical systems allow, similar to CNR measurements, the evaluation of the impact of individual elements on CSO and CTB.
TEST: CSO and CTB can be tested simultaneously with CNR in different segments of the optical path (see Figure 11-6).

Optical Power Budget – Analogue modulation
Optical power budget is the allocation of available optical power (launched into a given fibre by a given source) among various loss-producing mechanisms such as launch coupling loss, fibre attenuation, splice losses, and connector losses, in order to ensure that adequate signal strength (optical power) is available at the receiver [Fib2]. Optical power budget is calculated as a difference between optical power launched into the fibre and **receiver sensitivity for analogue signals** (see paragraph 11.5.1.3 “Optical receiver”).

TEST: Calculate the optical power budget

TESTS: This table lists the parameters that are described above for analogue optical modulation:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
CNR	dB	Medium	CNR, optical reach	n/a	Optical modulation: analogue	Tested in different segments of the optical path
Linearity: CSO/CTB	dB	Medium	Linearity: CSO/CTB, optical reach	n/a		Tested in different segments of optical path
Optical power budget	dB	High	optical reach	n/a		

11.5.2.1.2 Digital optical modulation

For optical system with digital modulation, the following parameters should be considered:

OSNR
In digital communications, the signal-to-noise (SNR) ratio is a measure of the signal strength relative to background noise. The OSNR (Optical SNR) has a direct impact on the BER. For this reason, it is relevant to know the relation between OSNR at the internal interface (receiver side) and the BER. For in-depth studies, the measurement of the OSNR at different locations of the optical path can be considered. For example: at the internal interface (transmitter side) as a reference point, at the input and output port of an optical component that influences the OSNR (e.g. amplifier) and at the internal interface (receiver side).

TEST: OSNR should to be tested at the internal interface (receiver side). For deeper studies, OSNR can be tested at different segments of optical path (see Figure 11-6).

Optical power budget- Digital modulation
Optical power budget is the allocation of available optical power (launched into a given fibre by a given source) among various loss-producing mechanisms such as launch coupling loss, fibre attenuation, splice losses, and connector losses, in order to ensure that adequate signal strength (optical power) is available at the receiver [Fib2]. Optical power budget is calculated as a difference between optical powers launched into the fibre and **receiver sensitivity for digital transmission**. Optical power budget calculation should also include power penalties associated with dispersion, jitter, or reflections from the ODN.

TEST: Calculate the optical power budget

Optical path penalty

The path penalty is the apparent reduction of receiver sensitivity due to distortion of the signal waveform during its transmission over the optical path. It is manifested as a shift of the system's BER-curves towards higher input power levels. This corresponds to a positive path penalty. Negative path penalties may exist under some circumstances, but should be small. (A negative path penalty indicates that a less than perfect transmitter eye has been partially

improved by the path dependent distortions.) Ideally, the BER-curves should only be translated, but shape variations are not uncommon, and may indicate the emergence of BER-floors. Since the path penalty is a change in the receiver's sensitivity, it is measured at a BER-level of e.g. 10^{-10}. A maximum path penalty of 1 dB for low-dispersion systems is allowed. The path penalties are not made proportional to the target distances to avoid operating systems with high penalties. The average value of the random dispersion penalties due to PMD is included in the allowed path penalty. In this respect, the transmitter/receiver combination is required to tolerate an actual DGD of 0.3 bit period with a maximum sensitivity degradation of 1 dB (with 50% of optical power in each principal state of polarization). For a well-designed receiver, this corresponds to a penalty of 0.1-0.2 dB for a DGD of 0.1 bit period [Fib1].

TEST: Verify the Optical Path Penalty

Eye diagram

An eye diagram is useful to characterize a digital signal for its quality and timing performance. The eye diagram is used to measure how well the transmitted bits are separated and hence how easy it will be to recover the data at the receiver end. Figure 11-**7** shows a number of parameters, which could be derived from the eye diagram shape. The open part of the eye represents the area where signal can be reliable detected. The horizontal bands at the 'Zero' and 'Mark' level represent the amount of signal variation. The variation is seen in the scatter diagram and is directly related to the OSNR of the signal. A small band means less noise and a high OSNR. The slope of the eye determines how sensitive the signal is to timing errors. The width of the crossover represents the amount of jitter present in the signal.

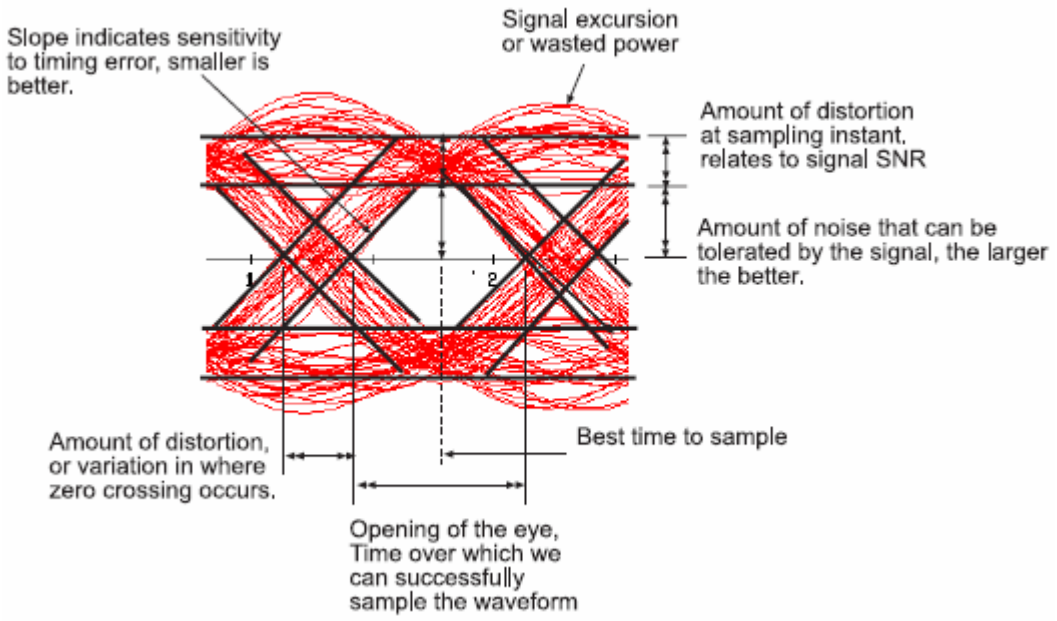


Figure 11-7: Eye diagram parameters

The eye diagram may be used for testing the signal at the transmitter and receiver side (ref. point 1 and N of Figure 11-6). These two tests can be an indicator for problems in the optical system.

Common ways of characterizing an eye are to measure the extinction ratio, total jitter at the middle of the crossing point of the eye and rise/fall time. Furthermore, to calculate the statistical BER, also Q-factor parameter can be measured.

Extinction Ratio

The extinction ratio (EX) is defined as:

$$EX = 10 \cdot \log\left(\frac{A}{B}\right)$$

In the above definition of EX, A is the average optical power level at the centre of a logical "1" and B is the average optical power level at the centre of a logical "0" [Fib1].

The extinction ratio is used to describe the efficiency with which the transmitted optical power is modulated over the fibre-optic transport. The value of EX has influence on the ability of correct detection at the receiver and in consequence on BER.

Total jitter (TJ)

Jitter is commonly defined as “The deviation from the ideal timing of an event. The reference event is the differential zero crossing for electrical signals and the nominal receiver threshold power for optical systems” [Fib17]. Total jitter is composed of both deterministic and random jitter.

Deterministic jitter (DJ) is a jitter with non-Gaussian probability density function; it is always bounded in amplitude and has specific causes (e.g. Simultaneously Switching Outputs-SSO, device function dependency-pattern dependant jitter and other regularly occurring interference signals).

Random jitter (RJ) is characterized by Gaussian distribution and is determined for desirable BER (e.g. 10^{-12}). In contrast to DJ, RJ is unbounded and therefore directly affects long-term reliability.

TJ has an influence on the BER performance. A relation between TJ and BER could be depicted on so-called bathtube curve. For more information about bathtube curve please refer to [Fib16].

Rise time

In the approximation of a step function, the time required for a signal to change from a specified low value to a specified high value. Typically, these values are 10% and 90% of the step height [Fib2].

Fall time

The time required for the amplitude of a pulse to decrease (fall) from a specified value (usually 90% of the peak value exclusive of overshoot or undershoot) to another specified value (usually 10% of the peak value exclusive of overshoot or undershoot) [Fib2].

Rise and fall time have an influence on the ability of transmission at given bitrate and in the end on BER.

Q-factor

A Q-factor is defined as the electrical signal-to-noise ratio (ESNR) at the decision circuit of a digital signal receiver [Fib13]:

$$Q = \frac{m_1 - m_0}{s_1 + s_0}$$

Where μ_1 and μ_0 are the mean voltage level of the “1” and “0” levels. Both σ_1 and σ_0 are the standard deviations of the noise distribution on the 1 and 0 levels. Q-factor measurement is an established method for characterization of optical channels.

The Q-factor is a comprehensive measure for the signal quality of an optical channel taking into account the effects of noise, filtering and linear/non-linear distortions on the pulse shape, which is not possible with simple optical parameters alone [Fib14]. The ESNR reflects all impairing optical and electrical defects at the electrical interface. In the absence of true BER measurement, (e.g. due to test time, test access, etc.) the Q-factor method can be used to

provide an estimation of the performance than can be expected in-service. Particularly at low bit error rates the method has the advantage of taking less time than a traditional BER measurement, where bit errors need to be counted over a statistically significant time period [Fib13]. Statistical BER is calculated by mathematical transformation of Q-factor. Figure 11-**8** shows a graphical representation of BER calculations.

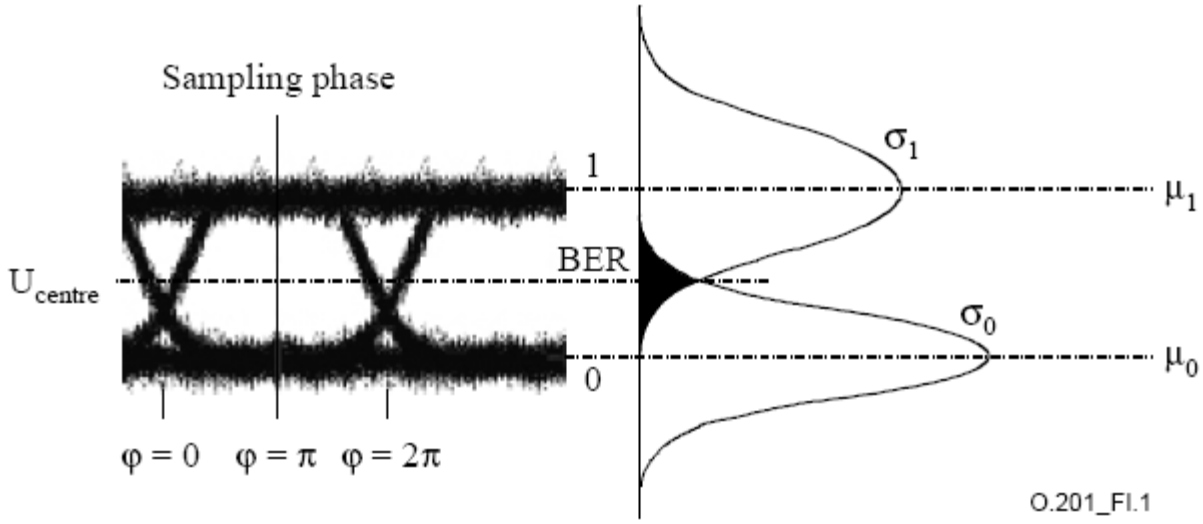


Figure 11-8: Relationship between probability density function and bit error ratio [Fib13]

TEST: Analysis of the overall shape of eye diagram and the following parameters:

- Rise/fall times (tested at the transmitter side, ref. point 1 or N of Figure 11-6)
- Total jitter at the middle of the crossing point of the eye (tested at the transmitter side, ref. point 1 or N of Figure 11-6)
- Extinction ratio (tested at the transmitter side, ref. point 1 or N of Figure 11-6)
- Q-factor should be tested at the receiver side (ref. point 1 or N of Figure 11-6) to calculate the statistical BER for an optical system when real BER (between external interfaces) test can not be performed. The proposed test configurations are identical with the external interfacing BER test.

TESTS: This table lists the parameters that are described above for digital modulation:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
OSNR	dB	Medium	CNR	BER, errored frames	Optical modulation: digital	Tested in different segments of the optical path
Optical power budget	dB	High	Optical reach	Optical reach		
Optical path penalty	dB	High	Optical reach	Optical reach		
Eye diagram shape	-	Medium	Optical reach	BER, errored frames		Tested on the transmitter side (internal interface)
Extinction ratio	dB	Medium	Optical reach	BER, Errored Frames		
Total jitter	UI	Medium	Optical reach	BER, errored frames		
Rise/fall time	Ns	Medium	Optical reach	BER, erroreds frames		
Q-factor	dB	High	Optical reach	BER, errored frames		Tested on the receiver side (internal interface) to calculate statistical BER in optical systems

11.5.2.2 Architecture aspects: P2MP specific testing

TDMA reliability

In P2MP architecture where multiple ONUs work at the same wavelength (non-WDM systems), the TDMA (Time Division Multiple Access) is the basic mechanism to avoid collision. One should check, if the TDMA mechanism is properly implemented. For this reason, it should be tested whether the traffic of one ONU is not affected by traffic of other ONUs (i.e. no collision between the frames).

TEST: Verify that the traffic from one ONU is not affected by traffic of other ONU for different system and ODN configurations.

Differential fibre distance

In P2MP architecture, an OLT is connected to several ONUs. The differential fibre distance is the difference in the distance between the nearest and furthest ONU from the OLT [Fib17]. This parameter is crucial for network planning. For higher differential fibre distances, a more flexible design of the network is needed.

TEST: Verify the maximum differential fibre distance between ONUs for which the system could work without errors.

Split ratio/ max number of ONUs

By split ratio is meant the maximum number of ONUs working simultaneously. Each P2MP system can deal with different split ratio. Split ratio depends on power budget and MAC properties. A fully loaded system can behave unstable and therefore such cases should be tested.

TEST: Verify the ability to work stable and flawlessly for a system with maximum split ratio or maximum number of ONUs working simultaneously.

TESTS: This table lists the tests that are described above for P2MP characterization:

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
TDMA reliability	-	High	n/a	BER, errored frames, Packet Loss	Architecture: P2MP Optical modulation: digital	
Differential fibre distance	km	High	CNR, optical reach	BER, errored frames, packet loss, optical reach	Architecture: P2MP	
Splitting ratio/ number of ONUs	-	High	CNR, optical reach	System capacity, errored frames, packet loss, optical reach	Architecture: P2MP	

11.5.2.3 xWDM system specific testing

Crosstalk

In xWDM systems where at least two signals at different wavelengths are transmitted in the same direction, phenomena such as crosstalk from adjacent signals may cause transmission errors. A sufficient isolation between adjacent wavelength channels should be considered as a part of the ODN requirements. Nevertheless, even if the ODN meets the requirements for wavelength isolation the possible impact of the adjacent wavelength channels should be tested.

The test objectives are:

a) to check if there is a decrease in signal quality if a signal in an adjacent channel is added.

b) to check the performance of the system when all wavelength channels are operating

The evaluation criterion should be the performance & quality parameters: BER, errored Frames or CNR.

The test of channels spacing or conformance to a wavelength grid makes sense only in case of DWDM and CWDM systems.

TEST: Verify the transmission quality on adjacent wavelengths.

Item	Unit	Priority	Impact on:		Applicable to	Comments
			Analogue external interfacing	Digital/Framed dig. external interfacing		
Crosstalk	-	High	CNR, optical reach	BER, errored frames, optical reach	No. of λ: xWDM	

11.6 Inventory of standards and other documents

Different committees have standardized optical access. The current chapter summarizes the past and running study group, as well as corresponding documents, that are relevant for the optical access technical evaluation (performances requirements, measurement methods).

IEEE

IEEE802.3ah: Ethernet in the First Mile Committee has built up a set of specifications that are relevant for implementation of an optical access network. Indeed IEEE802.3ah defines the requirements for Ethernet-based optical systems (PON p2mp and p2p, SMF or MMF).

- 1 Gbps EPON (1000Base-PX10), Single Fibre P2MP : clause 60
- 1Gbps EPON (1000Base-PX20), Single Fibre P2MP : clause 60
- 100 Mbps Single Fibre P2P (100Base-LX) : clause 58
- 100 Mbps Dual Fibre P2P (100Base-BX): clause 58
- 1 Gbps Single Fibre P2P (1000Base-LX10) : clause 59
- 1 Gbps Dual Fibre P2P (1000Base-BX10) : clause 59

IEEE802.17: Resilient packet rings (RPR) has been standardized in RPR P802.17/D3.3. RPR itself refers to the PHY of other standards like GBE and 10 GbE.
(Ref. http://www.ieee802.org/17/)

ITU / FSAN

ITU-T has been involved in optical transmission standardization for many years particularly when specifying SDH optical links.
Regarding PON systems, G.983 series consist of some useful tool, when specifying the system performances, especially if WDM techniques are implemented over the access network.
Moreover, series O could provide some useful tools for tests achievement.

- ITU-T G.983.1 (+ amd1, amd2) : 155, 622, and 1244 Mbps BPON Single fibre P2MP
- ITU-T G.984.1: 1.25 Gbps GPON Single Fibre P2MP
- ITU-T G.985: 125 Mbps Single Fibre P2P
- TTC TS-1000: 125 Mbps Single Fibre P2P.

Telcordia Technologies

Telcordia in GR-468 describes the Generic Reliability Assurance Requirements for optoelectronic devices used in telecom equipment.
A second issue of GR-909 Fibre in the Loop System Generic Requirements will be updated to take recent advances of low cost FTTP systems into account. (Estimated completion date Issue 2:June 2004) GR-909 will provide a framework allowing for both G983 of ITU and IEEE 802.ah FTTP systems.
In order to facilitate a further cost reduction of e.g. transceivers it is essential to relax test requirements (e.g. 85/85 tests are unnecessary demanding).
Reference: http://www.telcordia.com

11.7 References

[Fib1] ITU-T G.693 “Optical interfaces for intra-office systems”
[Fib2] The Alliance for Telecommunications Industry Solutions (ATIS), http://www.atis.org/tg2k/
[Fib3] The International Engineering Consortium (IEC), http://www.iec.org/
[Fib4] IEC EN 60825:2002 Part 1: “Safety of Laser Products Part 1: Equipment Classification, Requirements and User Guide
[Fib5] IEC EN 60825-2:2003(Draft): “Safety of Laser Products Part 2: Safety of Optical Fibre Communication Systems
[Fib6] http://www.complextoreal.com/chapters/eye.pdf
[Fib7] Laser Focus World, Jeff Hecht, March, 2002
[Fib8] P. C. Becker, N. A. Olsson, J. R. Simpson: Erbium-Doped Fibre Amplifiers Fundamentals and Technology, Academic Press, San Diego, 1999.
[Fib9] RFC 1242, Benchmarking Terminology for Network Interconnection Devices
[Fib10] ITU-T G.983.1 Broadband optical access systems based on Passive Optical Networks
[Fib11] ITU-T G.671 Transmission characteristics of optical components and subsystems
[Fib12] ITU-T G.652.2 Characteristics of single-mode optical fibre and cable
[Fib13] ITU-T O.201 Q-factor test equipment to estimate the transmission performance of optical channels
[Fib14] ITU-T G.697 Optical monitoring for DWDM systems
[Fib15] RFC 2285, Benchmarking Terminology for LAN Switching Devices
[Fib16] Agilent Webcast Template 2.0 Instructions, Introduction to Jitter and Jitter Measurements, Agilent Technologies 2004
[Fib17] ITU-T 984.1, Gigabit-capable Passive Optical Networks (GPON): General characteristics
[Fib18] Fibre channel—methodologies for jitter specification, Fibre Channel Jitter Working Group, Document T11.2/ Project 1230/, Revision 10, American National Standards Institute, June 9, 1999, p 7.