

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

Part 2: Test methods

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

Kamal Ahmed – TNO
Editor D.TF4.2 "Test Suite, Part 2: Test Methods"
(e-mail: kamal.ahmed@tno.nl)

Plus TF4 Team (see contributing authors per chapter)

Identifier:	Deliverable D TF4.4b
Class:	Report
Version:	Final, December 2007 (V13)
Version Date:	December 20th, 2007
Distribution:	Public
Responsible Partner:	TNO
Filename:	MUSE_TestSuite_Part2

DOCUMENT INFORMATION

Project ref. No.	IST-6thFP-26442
Project acronym	MUSE
Project full title	Multi-Service Access Everywhere
Security (distribution level)	Consortium
Contractual delivery date	June 2007
Actual delivery date	July 12th, 2007 (Final Dec 2007)
Deliverable number	DTF4.4b
Deliverable name	Test Suite for Full-Service End-to-End Analysis of Access Solutions, Part 2
Type	Report
Status & version	Version December 2007 - V13
Number of pages	384
WP / TF contributing	TF4
WP / TF responsible	TF4
Editor(s)	Kamal Ahmed (TNO), compiled from various focus documents (*Federiko Krommendijk, 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 2” of this “test suite” describes *how* should be tested (the methods) while the accompanying “part 1” is dedicated on *what* should be tested (the objectives).

Contributing Authors per Chapter

chapter		Names
1	intro	Rob van den Brink (TNO).
2	def	All
3	qos	Rob Kooij (TNO), Jeroen van Vugt (TNO), Kamal Ahmed (TNO), Kjell Brunnström (ACR), Tanja Kauppinen (ACR), Stéphane Junique (ACR), Georgina Gallizo (TID), António Gamelas (PT)
4	con/S	Pieter Liefooghe (IME), Brecht Vermeulen (IME), Björn Nagel (DT), Arnaud Riaudel (FT), Frank Geilhardt (DT)
5	con/N	Pieter Liefooghe (IME), Brecht Vermeulen (IME), Björn Nagel (DT), Arnaud Riaudel (FT), Frank Geilhardt (DT)
6	con/RG	Johannes Deleu (IBBT), Brecht Vermeulen (IBBT), Alex De Smedt (THO)
7	man	Hélder Alves (PTI)
8	xdsl	Bas Gerrits (TNO), Rob van den Brink (TNO), Mauro Tilocca (TI)
9	fibre	Andrzej Mosek (TP), Joachim Vathke (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 V13, and considered as the final version delivered by MUSE.

TABLE OF CONTENTS

DOCUMENT INFORMATION **2**
TABLE OF CONTENTS **4**
EXECUTIVE SUMMARY **7**
1 INTRODUCTION **8**
1.1 Scope 8
1.2 Objectives 8
1.3 Innovation – what is new? 10
1.4 History of the creation of this document 10
1.5 Summary per chapter 11
2 DEFINITIONS **14**
2.1 Terminology 14
2.2 Classification Framework 18
2.3 Abbreviations 18
3 QOS TESTING **26**
3.1 Introduction 26
3.2 Pre-conditions for testing QoS 27
3.2.1 Test scenarios *27*
3.2.2 Limiting other network internal pre-conditions *29*
3.2.3 Terminal related issues *30*
3.2.4 Determining traffic load regimes *31*
3.3 Voice-over-IP 33
3.3.1 Perceived QoS for VoIP *33*
3.3.2 Test methods *34*
3.3.3 Test specification at application layer *35*
3.3.4 Test specification at network layer *38*
3.4 Streaming Video 39
3.4.1 Perceived QoS for streaming Video *39*
3.4.2 Test methods *40*
3.4.3 Test specification at application layer *43*
3.4.4 Test specification at network layer *46*
3.5 Video conference 47
3.5.1 Perceived QoS for Video conferencing *47*
3.5.2 Test methods *48*
3.5.3 Test specification at application layer *48*
3.5.4 Test specification at network layer *51*
3.6 Web browsing and downloads 52
3.6.1 Perceived QoS for web browsing and downloads *52*
3.6.2 Test methods *53*
3.6.3 Test specification at application layer *54*
3.6.4 Test specification at network layer *57*
3.7 Interactive gaming 58
3.7.1 Perceived QoS for Interactive Gaming *58*
3.7.2 Test methods *59*
3.7.3 Test specification at application layer *59*
3.7.4 Test specification at network layer *59*
3.8 Annex to Chapter 3: Sending and capturing streaming video 61
3.8.1 Sending and receiving video *61*
3.9 Manual: iVQM_iptv HOWTO 63
3.9.1 Network architecture and hardware requirements *63*
3.9.2 Monitoring with iVQM_iptv *67*

3.10 References 70

4 SERVICE CONNECTIVITY TESTING 74
4.1 Introduction 74
4.2 Tools 74
4.3 High-speed Internet Service 74
4.3.1 Functional Tests 74
4.4 Performance Tests 75
4.5 Multicast Streaming Service 75
4.5.1 Functional Tests 75
4.5.2 Performance Tests 80
4.6 Voice over IP Service 82
4.6.1 Functional Tests 82
4.6.2 Performance Tests 88

5 NETWORK CONNECTIVITY TESTING 92
5.1 Introduction 92
5.2 MUSE Data Plane 92
5.2.1 Network layer 92
5.2.2 Link Layer Tests 95
5.3 MUSE Control Plane 108
5.3.1 Functional tests 108
5.3.2 Performance tests 110

6 CONNECTIVITY TESTING OF RESIDENTIAL GATEWAYS 122
6.1 Introduction 122
6.2 Multicast test methods 122
6.2.1 Testing IGMP-Proxy Requirements 126
6.2.2 Testing DSLForum Multicast Requirements for RGW 164
6.3 DHCP test methods 171
6.3.1 DHCP Client 179
6.4 VLAN test methods 203
6.4.1 Test: upstreamvlan 203
6.4.2 Test: vlantransparant 204

7 MANAGEMENT TESTING 205
7.1 Introduction 205
7.2 Test methodes for Muse Management tests 206
7.2.1 Test Methods for Fault Management 206
7.2.2 Test Methods for Configuration Management 218
7.2.3 Test Methods for Account Management 232
7.2.4 Test Methods for Performance Management 243
7.2.5 Test Methods for Security Management 251
7.3 References 260

8 XDSL SPECIFIC TESTING 262
8.1 Introduction 262
8.2 Test configurations 262
8.2.1 Set-ups 263
8.2.2 Test loops 267
8.2.3 Noise sources 268
8.2.4 System configuration profiles 271
8.3 Testing management capabilities 272
8.3.1 Configuration management tests 273
8.4 Testing Transceiver Signal Characteristics 291
8.4.1 Introduction 291
8.4.2 Measurement difficulties 292
8.4.3 Testing total transmit power 297
8.4.4 Power Spectral Density 299
8.4.5 Power Back Off 302
8.4.6 Power management 305

8.5 Testing performance under noisy stress conditions 311
8.5.1 Introduction 311
8.5.2 Reported line parameter verification tests 313
8.5.3 Testing margin 315
8.5.4 Testing bit rate 317
8.5.5 Testing resistance against slowly transmission impairments 319
8.5.6 Testing bit rate using INP_min and Delay_max configuration 322
8.5.7 Testing resistance against impulsive noise 323
8.5.8 Inter comparing test results 328
8.6 Example test configurations 331
8.6.1 Example test loops 331
8.6.2 Example noise profiles for stationary crosstalk noise 331
8.6.3 Example system configuration profiles 336
8.6.4 Example PSD specifications 347
8.7 References 348

9 FIBRE SPECIFIC TESTING 349
9.1 Introduction 349
9.2 Test configurations 349
9.3 Transceiver characteristic 352
9.3.1 Optical transmitter 353
9.3.2 Optical receiver 360
9.3.3 Optical power budget calculation 362
9.4 Testing performance under stress conditions 364
9.4.1 Determination of optical reach 364
9.4.2 Sensitivity to reflection (P2MP, no optical circulators) 366
9.4.3 Sensitivity to reflection (P2MP, with optical circulators) 368
9.4.4 Differential fibre distance 369
9.4.5 Sensitivity to crosstalk 370
9.5 Testing optical signal quality on different parts of optical path 371
9.5.2 Q-factor/BER estimation 373
9.5.3 Received optical power level 375
9.5.4 Optical path penalty 377
9.6 ODN characteristic 378
9.6.1 Insertion Loss 378
9.6.2 Optical Return Loss 379
9.6.3 Chromatic Dispersion 380
9.6.4 Polarization Mode Dispersion 382
9.6.5 Spectral Response 382
9.7 References 383

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 2 (the "test methods") gives guidance on "how to test", while the companion part 1 (the "test objectives") gives guidance on "what 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 2 of this test suite, is a comprehensive document, that provides a holistic *system* view on "how to test" for analyzing the capabilities of access systems. It describes a wide range of test methods 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 methods 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. The chapter related to fibre was fully rewritten (almost from scratch as well) 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 was extended with 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 2 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 creation 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 built-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 built-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 its vertical position and height are roughly indicative for the OSI layers being covered by that particular chapter.

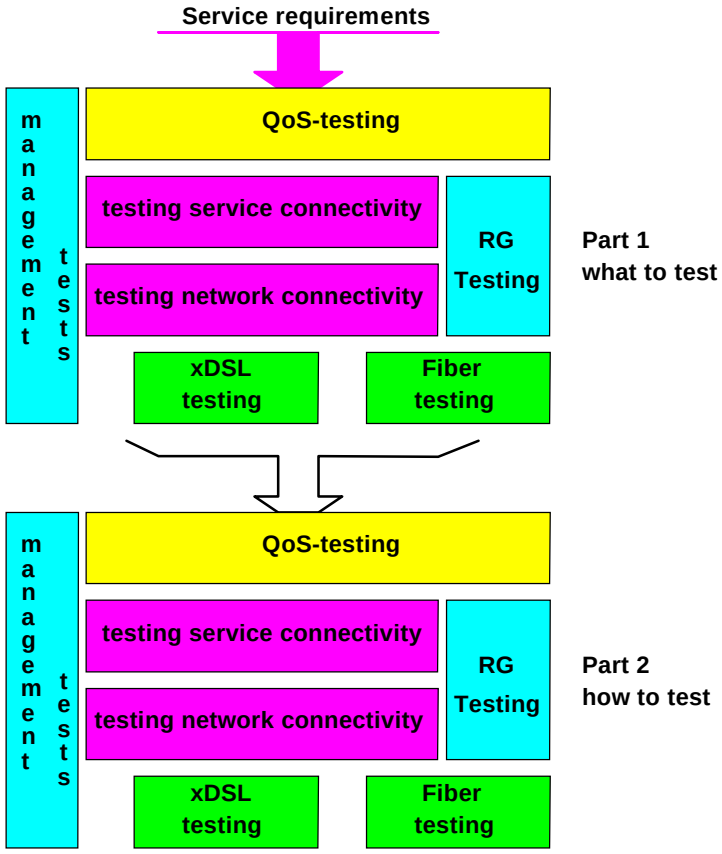


Figure 1-1: Schematic overview of various aspects of end-to-end testing

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 of 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 needs 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 analyses? 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 been 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. The chapter related to fibre was fully rewritten (almost from scratch as well) 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 was extended with 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.

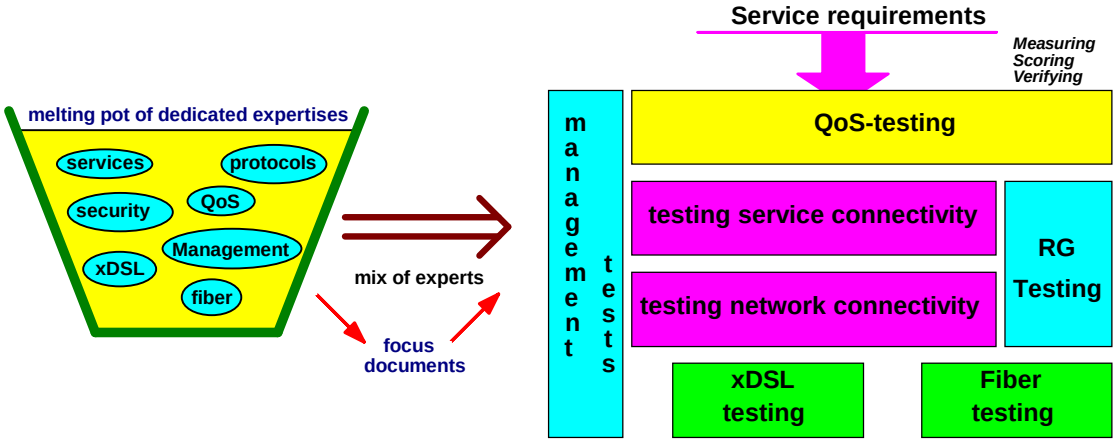


Figure 1-2: Schematic overview of the two-step approach being followed to create this part 1 of the test suite

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 2 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 frame work, 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.

1.5 Summary per chapter

A short summary per chapter is given next.

Chapter 2: Definitions

The objective of this chapter is to give a good and complete overview of the terminology and abbreviations used throughout this document.

Chapter 3: QoS testing

This chapter discusses in detail how to measure the perceived QoS for VoIP, streaming video, video conferencing, interactive gaming and web browsing.

Key words: perceived QoS, speech quality, video quality, gaming quality, browsing quality

Chapter 4: Service Connectivity testing

A top-down view on connectivity, starting from a service point of view. Multiple classes of services are described and for each class an example service (e.g. high speed internet, multicast streaming, VoIP) has been used to show how service testing can be done from the service down to the network layer. Of course, this chapter is not exhaustive on all services.

	Key words: session establishment, number of simultaneous sessions, maximum attainable throughput.
Chapter 5: Network Connectivity testing	A bottom-up view on connectivity, starting from the architecture. It describes relevant tests and standards for the network layer and upward. It concentrates on functionality and performance tests without detailing on specific test procedures; it excludes the physical layer. As it is focused specifically on the MUSE architecture, it is a lot more specific than the chapters on service connectivity. *Key words: network layer testing, link layer testing.*
Chapter 6: Connectivity testing RGWs	A reference for network and higher layer tests on residential gateways. It describes the test procedures in more detail for testing IGMP, IGMP proxy, DHCP and PPPoE functionality and conformance. The test procedures were formulated as they were used and verified while implementing an automatic test suite on residential gateways. *Key words: IGMP, IGMP proxy, DHCP, RGW multicast requirement testing.*
Chapter 7: Management testing	A detailed mapping of the TMN management functions described in ITU-T M.3400, into an exhaustive list of requirements. The readers are made familiar with the TMN model and its management functions, so that they can understand why MUSE has chosen TMN as its reference model for testing Management systems *Key words: management testing, TMN, ITU-T M.3400*
Chapter 8: XDSL specific testing	This chapter refers to existing standard tests and concentrates on describing missing details. Furthermore, it adds methods on recent topics, such as means for loop qualification (DELT/SELT), mitigating impulsive noise, and protecting legacy systems (PSD shaping). *Key words: xDSL testing, DELT/SELT, PSD shaping*

Chapter 9: Fibre specific testing

A top-down view on testing of generic system aspects that is characteristic to fibre-based access networks. It concentrates on optical signals and on the performance of an access *system* as a whole (leaving tests for underlying optical *components* out of scope). Systems are differentiated with respect to their interfaces (analogue, digital, framed digital) and topologies (point-to-point, point-to-multipoint). Test methodologies are identified for each of them. Specifically, it covers tools and procedures available to measure relevant physical layer parameters, referencing appropriate standards.

Key words: fibre optic system testing, P2P/P2MP network testing

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.

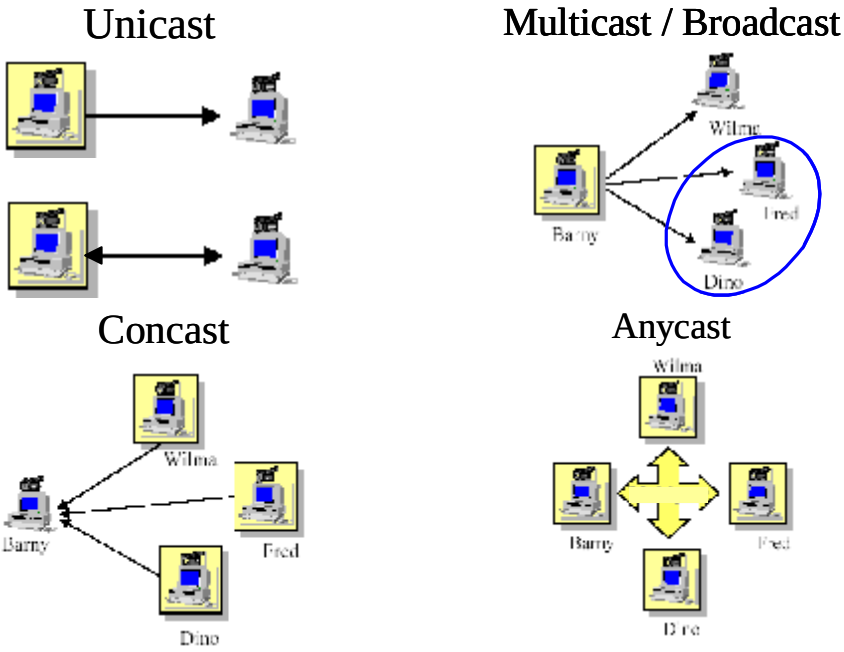
======= *Connectivity* =======

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).

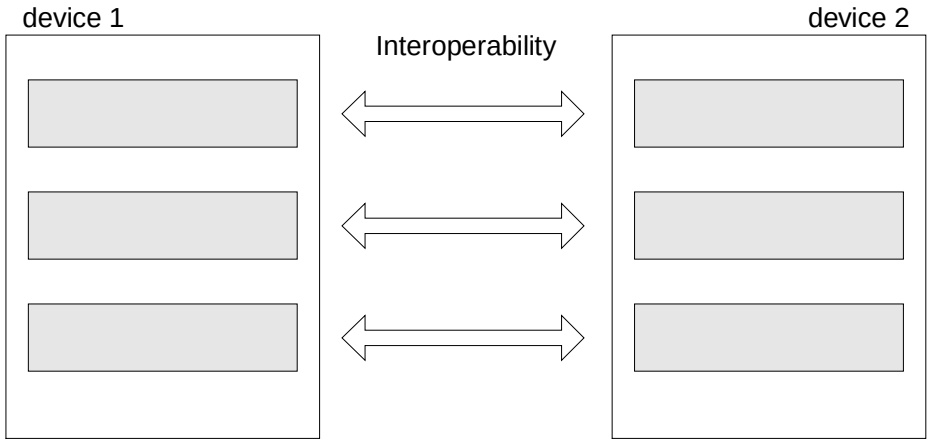
Multicast/Broadcast, means 1:n communication between one terminal and many terminals. The dataflow is unidirectional (e.g. Broadcast TV)

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

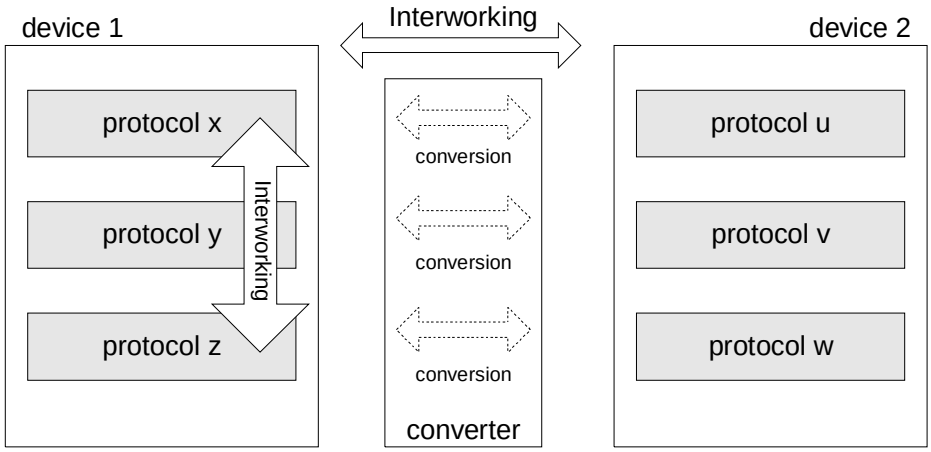
Anycast, means m:n communication between many terminals and one terminal. The dataflow is multidirectional (e.g. Video conference, Gaming).



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 Classification Framework

In this document, high-level descriptions are being used to classify key functionalities of an access system. Due to the wide range of functionalities being identified, a common model will not be applicable. Therefore various different classifications are being used in this document. A detailed summary of these classifications can be found in “part 1” of this test suite.

2.3 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
AN	Access Node
ANSI	American National Standards Institute
AON	Active optical network
APC	Angular physical contact
APD	Avalanche Photo-Diode
APON	ATM-based Passive Optical Network
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	Arrayed waveguides
BAP	Bluetooth Access Point
BER	Bit Error Ratio
BLES	Broadband Loop Emulated Service
BPDU	Bridge Protocol Data Unit
BPON	Broadband Passive Optical Networks
BRAS	Broadband Remote Access Server
CAC	Call Admission Control
CAP	Carrierless Amplitude/Phase modulation
CATV	Cable-TV
CCE	Call Control Element
CCS7	Common Channel Signalling #7
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

CO	Central Office
CoS	Class of Service
CPE	Customer Premises Equipment
CPG	Customer Premises Gateway
CPN	Customer Premises Network
CS	Complementary Services
CSO	Composite Second Order
CTB	Composite Triple Beat
CW	Continuous Wave
CWDM	Coarse WDM
CWMP	CPE WAN Management Protocol (aka TR-69)
DARPA	Defense Advanced Research Projects Agency
DCR	Degradation Category Rating
DCT	Discrete-Cosing Transform
DFB	Distributed Feedback
DHCP	Dynamic Host Configuration Protocol
DIAMETER	An AAA (authentication, authorization and accounting) protocol, the successor of RADIUS
DML	Directly Modulated Laser
DMT	Discrete Multitone modulation
DMZ	DeMilitarized Zone
DNS	Domain Name System
DOS	Denial Of Service
DoS	Denial of service
DRM	Digital Rights Management
DSA	Digital Signal Analyser
DSCP	Differentiated Services Code Point
DSCQS	Double Stimulus Continuous Quality Scale
DSF	Dispersion Shifted Fibre
DSIS	Double Stimulus Impairment Scale
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
DTMF	Dual Tone Multi Frequency
DUT	Device Under Test
DVD	Digital Versatile Disc
DVMRP	Distance Vector Multicast Routing Protocol
E2E	End-to-End
EAP	Extensible Authentication Protocol
EC	Echo Cancelled (see also under EC, in clause 3.1 on definitions)
EDC	Electronic Dispersion Compensation
EFM	Ethernet in the first Mile
EIA	Electronic Industries Alliance
EMC	Electromagnetic compatibility
EP	Enforcement Point
EPG	Electronic Programming Guide
EPON	Ethernet-based Passive Optical Network
ER	Extinction Ratio

ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standardisation Institute
FDD	Frequency Division Duplexing/Duplexed
FEC	Forward Error Correction
FHR	First Hop Router
FP	Fabry-Perot
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
FTTx	Fibre to the x={Home, Premises, Basement…}
GbE	Gigabit Ethernet
GDMF	Guidelines for the Definition of TMN Management Functions
GMPLS	Generalised MPLS
GDMF	Guidelines for the Definition of TMN Management Functions
GPON	Gigabit-capable Passive Optical Network
GPS	Global Positioning System
GSB	Global Solution for Broadband
H.264	MPEG-4 Part 10 or AVC
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
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
ICS	Implementation Conformance Statement
IEEE	Institution of Electrical and Electronics 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
IVR	Interactive Voice Response unit
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	Message Authentication Code
MAC	Medium Access Control
MAP	Metro Access Point
M-BGP	Multi-protocol extension to BGP
MDU	Multi-dwelling unit
MFA	Management Functional Area
MGCP	Media Gateway Control Protocol
MIDCOM	MIDdlebox COMmunications
MIME	Multipurpose Internet Mail Extension
MLD	Multicast Listener Discovery Protocol
MLP	Mean Lauch Power
MLM	Multi-Longitudinal Mode
MM	Multi Mediq
MMF	Multimode Fibre
MMS	Multimedia Message Service
MOS	Mean Opinion Scores
MPEG	Moving Pictures Experts Group
MPLS	Multi-protocol Label Switching
MP-to-MP	Multi-point to Multi-point
MSA	Multi-source Agreement
MSDP	Multicast Source Discovery Protocol
MSE	Mean Squared Error
MUX	Multiplexer
N-OSF	Operations System Function block of the Network Management Layer
NAP	Network Access Provider
NAPT	Network Address/Port Translator
NAT	Network Address Translation
NE	Network Element
NIDS	Network Intrusion Detection System
NOD	News On Demand
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
NZDSF	Non-zero dispersion shifted fibre
OAM	Operation, Administration and Maintenance
ODN	Optical Distribution Network
O/E	Optical/Electrical
OLT	Optical Line Termination
OMA	Optical Modulation Amplitude
ONT	Optical Network Termination
ONU	Optical Network Unit
OPP	Optical Path Penalty
ORL	Optical Return Loss
ORR	Optical Rejection Ratio
OSA	Optical Spectrum Analyser
OSI	Open Systems Interconnection
OSNR	Optical Signal-to-Noise Ratio
OTDR	Optical Time Domain Reflectometry / Reflectometer
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
PDL	Polarisation dependent loss
PDLA	Photonic Dispersion and Loss Analyser
PESQ	Perceptual Evaluation of Speech Quality
PHB	Per Hop Behaviour
PICS	Protocol Implementation Conformance Statement
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIN	Positive Intrinsic Negative (diode)
PIP	Picture In Picture
PLC	Power Line Communication
PM	Performance Monitoring (the TMN Management Function Set Group)
PMD	Physical Media Dependent
PMD	Polarisation mode dispersion

PON	Passive Optical Network
POP	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
PS-PON	Power-Splitting Passive Optical Network
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
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAS	Reliability, Availability and Survivability
RBS	Radio-basestation
RFC	Request For Comment
RIN	Relative Intensity Noise
RMS	Root Mean Square
RNP	Regional Network Provider
RPC	Remote Procedure Call
RPR	Resilient Packet Ring
RPT	Rendezvous Point Trees
RRNR-TV	Reduced Reference No Reference TV
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTT	Round-trip Time
Rx	Receiver
SB	Service Broker
SCM	Sub-Carrier Multiplexing
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 Definition TV
SEN	Service Edge Node
SFF	Small Form Factor
SFP	Small Form Factor Pluggable
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Single-Longitudinal Mode
SME	Small-Medium Enterprise
SMF	Single-Mode Fibre
SMS	Short Message Service

SMTP	Simple Mail Transfer Protocol
SMSR	Side Mode Suppression Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SOHO	Small Office – Home Office
SONET	Synchronous Optical NETwork
SpM	Spectral Management
SSCQE	Single Stimulus Continuous Quality Evaluation
SSH	Secure Shell
SSM	Single Source Multicast/Source Specific Multicast
SSMF	Standard Single-Mode Fibre
STB	Set Top Box
SUT	System Under Test
S-VID	Stacked VLAN ID
S-VLAN	Stacked VLAN
TCP	Transmission Control Protocol
TAP	Test Access Path
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TDP	Transmitter and Dispersion Penalty
TFF	Thin Film Filter
TIA	Telecommunications Industry Association
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
T&L	Terminate test and Leave
TMF	Tele Management Forum
TMN	Telecommunications Management Network
ToIP	Telephony over IP
ToS	Type of Service
TR	Technical Report (DSLForum)
TRx	Transceiver
TTC	Telecommunication Technology Committee (e.g. TS-1000 Technical Specs)
TTCN	Tree and Tabular Combined Notation
TTL	Time To Live
TVoIP	Television over IP
Tx	Transmitter
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UPE	User Profile Engine
URI	Unified Resource locator
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCR	Video Cassette Recorder
VCSEL	Vertical cavity surface emitting laser

VDSL	Very-high-speed Digital Subscriber Line
VGA	Video graphics array
VHE	Virtual Home Environment
VLAN	Virtual LAN
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
WDM	Wave Division Multiplexing
WDMA	Wave Division Multiple access
WINS	Windows Internet Naming Service
WMP	Windows Media Player
WT	Working Text (DSLForum)
xDSL	(all systems) Digital Subscriber Line
XFP	10 Gigabit Small Form Factor Pluggable (module)
XL-PON	Extra Large Passive Optical Network
xTU-C	xDSL Transceiver Unit – Central office side
xTU-R	xDSL Transceiver Unit – Remote side (customer premises)
xWDM	All types of WDM (e.g. CWDM, DWDM, ...)
ZWPF	Zero water-peak fibre

3 QOS TESTING

3.1 Introduction

The objective of chapter 3 is to specify and describe “how” the (perceived) QoS related items indicated in “test suite, part1” should be measured.

In this subsection we discuss the hierarchy of test methods for obtaining the perceived quality of service, which was already stated in “test suite, part 1”:

- objective measurement methodologies that are standardized, or in the process of being standardized, 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 that are standardized, or in the process of being standardized, must be used;
- if subjective measurement methodologies are non-existent, they must be invented or indicated as for further study. However, it should be noted that the subjective obtained score is highly dependent on the experimental context;
- whenever considered as relevant, tests at the network packet level 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 3-1.

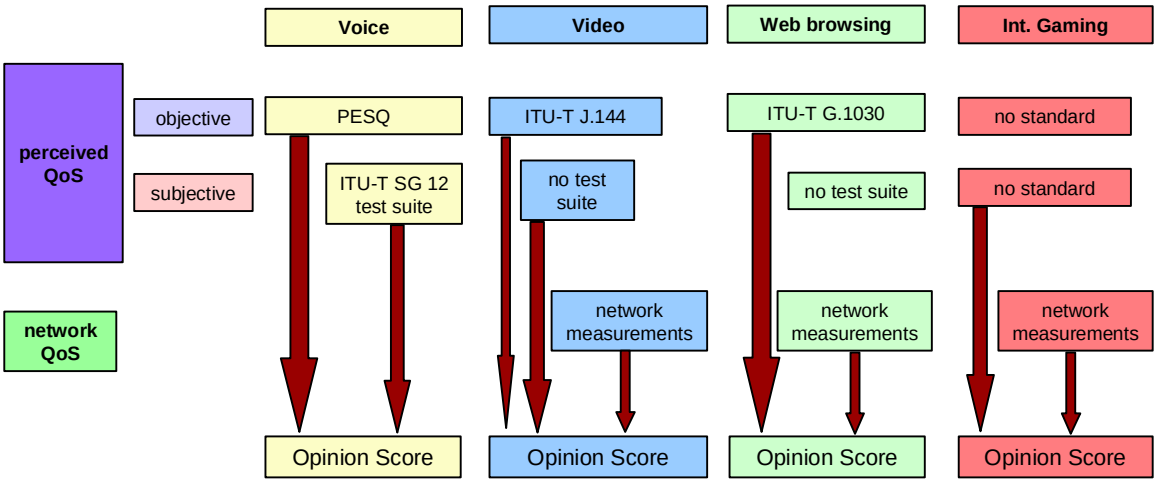


Figure 3-1 Hierachy of preferred test methods for perceived quality

ITU-T Rec. G.1030 [QoS1] is a recommendation to the ITU-T Study Group 12 which is still under construction.

In the subsequent sections we will work out the above steps for a number of applications including VoIP, Streaming Video, Videoconference, Web browsing/bulk data and Interactive Gaming. In fact we will start with a description of tests for characterising the network link quality. However, we will first list a number of pre-conditions for the tests.

3.2 Pre-conditions for testing QoS

The test of QoS related issues, even when restricted to its end-user perceived component, as it is the case in the scope of the present document is an exhaustive and endless task. Indeed, it is very difficult, if not impossible at all, if in addition to the above mentioned end-user perceived QoS, one might want to test the network performance, the target values of the associated parameters when applied to each of the selected applications, the adopted IP QoS control mechanisms, etc, as well as all the variants that can be performed when the use of terminals is considered.

If some sound results on QoS testing are intended to be achieved, and besides the above mentioned restriction related to the end-user perceived component, other limits must be defined in advance, in order to find a common understanding about the pre-conditions under which the tests will be performed.

In this section, a brief discussion on three aspects considered as fundamental is carried out, i.e., the definition of test scenarios that will be adopted, the identification of internal conditions that may affect the performance, followed by the selection of a specific one related to the traffic conditions that will be subject to variations, and finally the definition of some assumptions as pre-conditions related to the use of terminals.

3.2.1 Test scenarios

For end-to-end user perceived QoS, initially three basic scenarios can be envisaged:

§ peer-to-peer type of communication, i.e., inside the same AN domain, in terms of L2 technology, e.g. inside the same VLAN if Ethernet is considered

§ end-to-end type of communication, where the two end users are connected through the same AN, but belong to different domains
§ end-to-end type of communication, where the two end users are connected through two ANs by an Edge Node.

These three scenarios are depicted in the following two figures, where the first one can be used to represent the first cases, as only one AN is involved:

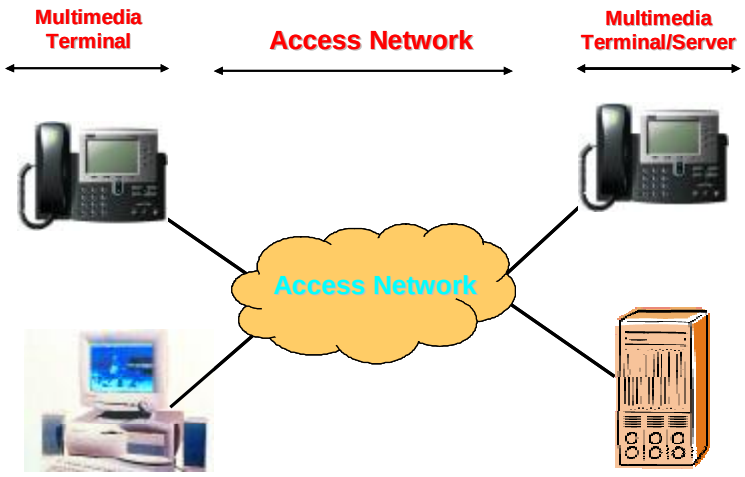


Figure 3-2: - Scenarios for peer-to-peer and end-to-end types of communication within just one AN

The second picture illustrates the third case, were two ANs are considered:

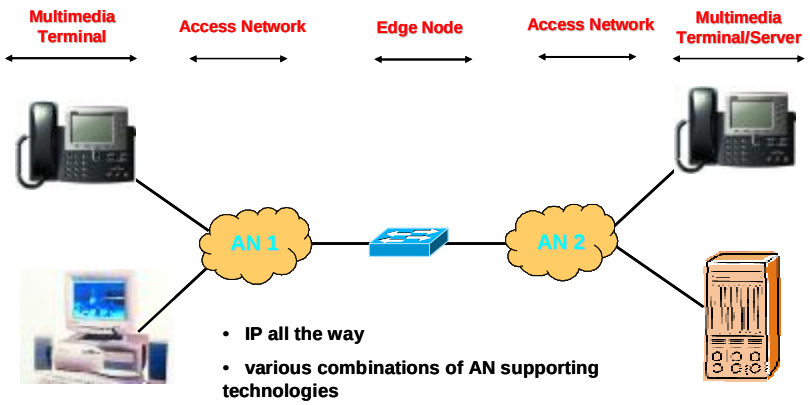


Figure 3-3: - Scenario for end-to-end type of communication involving two ANs

The choice of these scenarios was also influenced by the fact that it would be convenient to meet, as far as possible, the following pre-conditions:

§ to handle of peer-to-peer situations, since these type of communications can always happen whatever the dimension of the Access Networks may be

- to adopt an IP based configuration, with IP all the way, as it constitutes the final target of the MUSE connectivity
- to create an interworking situation, as close as possible to real scenarios where end-to-end communications between two Access Networks separated by a Core Network will be performed. With this scenario, the user can connect to other terminals or servers (video content, web documents, gaming server) through the edge node, which makes it possible to test multiple combinations of technologies, at least in the ANs.

Still related to the last scenario, and still considering the second phase of MUSE, each network may be supported by different types of technologies, e.g., in the access, xDSL, ATM, Eth, fibre, coax, or 3G, as well as DWDM, SDH, or ATM, in the core. Moreover, a particular case of utmost importance for network operators will be the possibility of testing interworking situations with the PSTN/ISDN, either between an IP based configuration and the PSTN/ISDN, or between an all IP based configuration, but where one or even the two end terminals are POTS connected to the AN through media gateways.

It might be considered that this is definitively a connectivity issue, however it is also a QoS matter, as the mapping of QoS parameters resulting from different transport interworking situations must be performed, and this can influence the e2e test results.

3.2.2 Limiting other network internal pre-conditions

Dimensioning and configuration are crucial aspects whose target is to find the proper relation between used resources, such as bandwidth, buffers, etc, and the performance at application level as experienced by users. As such, network designers of QoS enabled IP networks will have to be able to answer amongst others, to the following questions:

- to what load can links be loaded such that the end-to-end delay for voice remains small?
- what is the influence of best effort traffic on interactive traffic?
- what is the influence of packet sizes on end-to-end delay?
- how should buffer sizes be set such that end-to-end packet loss ratios remain small?
- what is the relation between access link capacity and WWW download times?

Apparently, there are no single and conclusive answers, mainly because the scarcity of resources-to-be-optimised may be different in various network parts and may shift over time. Moreover, the number and relative contribution of the different applications is not precisely known, and may also evolve over time towards an even larger number of different applications. As mentioned above, to carry out a complete set of tests would be an exhaustive and endless task.

In this context, and in order to keep the number of testing situations as simple as possible, it would be advisable to limit the pre-conditions that can be varied, beginning e.g. by the **traffic** factor as indicated below:

- the **traffic load** of the IP network, i.e., light, mild or heavy, denoted by L1, L2 and L3, where:
  - **light** can be defined as *"only one flow of the application under study",*
  - **mild**
  - **heavy**

- the **traffic mix**, i.e., single play, or multi play, :
  - **single play** can be defined as *"only the application under study"*
  - **for multi play** at least two applications are running over the access network simultaneously

In case of multi play it is left to the tester to choose the relative load of each of the applications. Note that this relative load is influenced by the bandwidth and number of users per application.
Obviously, in order to deliver multi play successfully the access network should support some form of QoS differentiation. With the perceived QoS tests one can validate whether the QoS mechanisms work properly.
When dealing with mild and heavy traffic loads, it has to be considered that on top of the flow of the application under study, additional traffic has to be generated. As an example, let us consider the case where the performance of VoIP is being studied and uses 100 kbps on a 10 Mbps access link. Let us assume the situation that heavy traffic corresponds to a load of 90%. Hence, there would be a real VoIP call set up, and in addition generated traffic corresponding to 89 VoIP calls.

On the other hand, when dealing with a combination for triple play including interactive gaming, the latter should both be treated as data traffic, i.e., with **lowest priority**, as well as in the same class as Voice, i.e., with **highest priority**.

As far as the **packet level** conditions are concerned, they will not be varied, as they can be obtained from the combination of the scenario under test and from the traffic load condition.

Finally, and where possible, **packet sizes** should be restricted to single values. For instance, for VoIP we will restrict ourselves to what ETSI calls the *"formation time"*, which corresponds to a **packetization delay** of 20 ms.

3.2.3 Terminal related issues

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 [QoS15], and ETSI TS 101 329-1 [QoS16]. Moreover, as indicated in DTF4.1 [QoS17] the performance tests for terminal equipment are beyond the scope of this test suite, and therefore will not be specified. However, their impact should definitely be taken into account when evaluating the results, and this is the reason why some assumptions and proposals are considered in below for their characteristics.

Voice over IP

The following objectives are proposed to be fulfilled by the voice terminal equipment:

- additional delay in the jitter buffer is at most 30 ms,
- packetisation delay is 20 ms
- coding and decoding delay is at most 10 ms
- packet loss due to the operation of the jitter buffer is at most 0,25%
- the G.711 codec is used.

Videoconference

A proposal for the objectives of the videoconferencing terminal equipment is:

- camera captures video at least at 25 frames/s.
- spatial resolution used is at least VGA (640 x 480 pixels)
- additional delay in the jitter buffer is at most 30 ms for the video stream
- video packetisation, coding and decoding delay is at most 30 ms

- video packet loss due to the operation of the jitter buffer is zero

Streaming Video

A proposal for the objectives of the streaming video terminal equipment is:

- camera captures video at least at 25 frames/s
- spatial resolution used is at least VGA (640 x 480) or SVGA (800 x 600)
- video packet loss due to the operation of the jitter buffer is zero
- the codecs MPEG-2 or MPEG-4 are used

Web browsing and bulk data

The terminal equipment aspects for information and data services are:

- Operating System (OS) parameters
- TCP/IP implementation
- data presentation.

For web browsing we assume HTTP 1.1 is used while for downloads the use of FTP is assumed.

Interactive Gaming

For the terminal equipment used for interactive gaming the following questions should be answered:

- what transport protocol is used?
- what mechanisms are implemented to deal with packet loss and excessive delay?

It is suggested that the above questions are answered for one application out of each of the following gaming families, where at least the first one should be considered:

- First Person Shooter,
- Massive Multiplayer On-line Role Playing Games.

3.2.4 Determining traffic load regimes

In this section it will be described how network related measurements can be used to characterize an end-to-end network path. We will also describe under which conditions the application specific measurements can be performed. These conditions will be characterized by the amount of background traffic load that is present along side the actual traffic of a application, and is split up into three regimes called light, mild and heavy background traffic load. These regimes were first introduced in the previous subsection.

When performing application specific testing there will be two different types of traffic load present in the network during the test, first the traffic generated by the application itself and second the traffic generated using a traffic generator, which emulates the background traffic load for the specific application type and/or QoS class. As stated above the amount background traffic load is split up into three regimes, and in order to resolve the light, mild and heavy regimes the basic end-to-end network path characterization test combined with a simple application specific test is performed over the end-to-end connection. This will resolve which amount of background traffic load gives rise to which level of application specific packet loss. These tests will give relevant background information for the analysis of the application specific tests later on, where it is important to decide under which conditions, or regime, one wants to perform the test. Furthermore, it gives a hint of the needed dimensioning of the system for certain traffic matrices. Worth noticing is the importance of choosing the right characteristic for the generated background traffic depending on the type of application that is being tested. For instance the packet size and transmission protocol (TCP, UDP, RTP etc.) will vary for different types of applications.

Depending on the application specific requirements it is possible to find traffic loads relating to light, mild and heavy background traffic load. The background traffic levels light, mild and heavy are exemplified in Figure 3.4. Note that the quality factor indicated in the figure is indeed the packet loss.

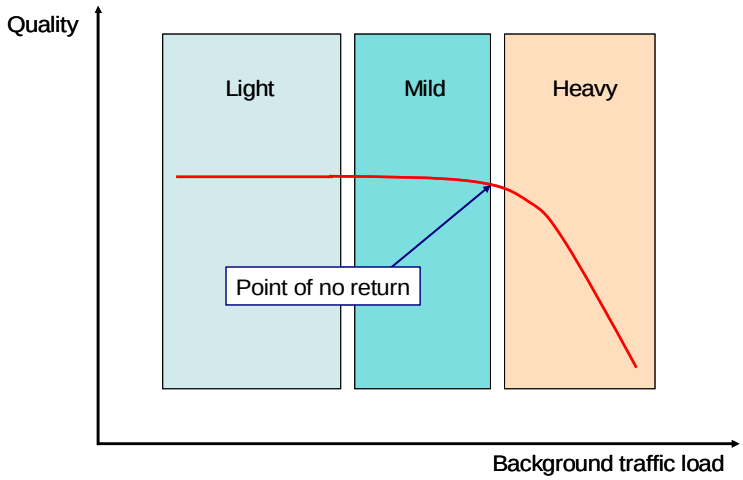


Figure 3-4: Definition of traffic load regimes

Application specific testing can be done in all of the regimes, and the regime chosen should reflect what one wants to measure. For example, if measurements with as little as possible influence of the network are done, the light regime should be used, where the application quality is expected to be excellent. Doing measurements to find where the background load affects the quality of the application to a level that is unacceptable is a very interesting test case in itself since it gives a pointer to how to dimension the system under a specified traffic matrix. Finding this point, the point of no return, can be quite time consuming since in the mild regime the network gives rise to application errors but on a fairly low error rate. For IP-TV, as an example, the error rate is often specified for a well working network as less than one visible error per hour on average. This gives an indication on how long it will take to find statistically verified errors in the part of the mild regime where the background traffic load is lower than at the point of no return, i.e. where the error rate is lower than one error per hour.

As an example, for the perceived QoS tests that will be conducted in MUSE we will take from the light traffic load regime the case with no background traffic at all, i.e. the only traffic then generated is from the application under study. From the mild regime we take a traffic load well before the point of no return while for the heavy load regime we choose a traffic load value sufficiently far beyond the point of no return.

For the single play scenario, background traffic is generated into the same QoS class as the application that is being tested. However, for the multi play scenario we will also take into account the case where background traffic is generated in other QoS classes. In principle this means that in the MUSE context we will test the case when priority handling takes care of the lower priority traffic and dimensioning takes care of the higher priority traffic, i.e. we test in-class influences under a limited bandwidth condition. In-class influences also means that the specific application under test will only be influenced by a background traffic type of that class.

In order to determine the point of no return one needs to use instruments like Agilent N2X platform[1], Ixia[2] etc. In fact such instruments can and will be used to determine the end-to-end network characteristics such as delay, jitter, packet loss and QoS differentiation. In fact, all subsequent sections will contain a subsection called “test specification at the network layer”. These subsections will contain more detail on the tests with respect to the network characteristics.

3.3 Voice-over-IP

3.3.1 Perceived QoS for VoIP

The aim of the test described in this section is to determine the perceived QoS of a VoIP call between a SIDE A and a SIDE B.

Before we describe the test in more detail we first recapitulate some relevant aspects related to perceived quality of VoIP, see also DTF4.4 [QoS17].

The overall quality of interactive speech is referred to as *conversational quality*.
The conversational quality is determined by three aspects: *listening quality* (“how well can the other person hear me?”), *talking quality* (“how well can I hear myself?”) and *interaction quality* (“how well is it possible to communicate interactively?”).

Each quality aspect is expressed as a Mean Opinion Score on a five point scale, as depicted in Table 3.1.

Mean Opinion Score	Absolute quality	Impairment
5	Excellent	Imperceptable
4	Good	Perceptable, not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

Table 3-1: Definition of MOS scale

[1] www.agilent.com
[2] www.ixia.com

Because the MOS can refer to different aspects we propose the following notation, which is currently also considered within ITU-T Study Group 12:

MOS-CQ = MOS overall conversational quality
MOS-LQ = MOS Listening Quality
MOS-TQ = MOS Talking Quality
MOS -IQ = MOS Interaction Quality

Because the overall conversational quality is determined by the other three aspects we have

MOS-CQ = min{ MOS-LQ, MOS-TQ, MOS-IQ}.

For MUSE we require that MOS-CQ ≥ 4.0. Note that this condition should be verified at both sides.

3.3.2 Test methods

The architecture for the test is depicted in Figure 3-5.

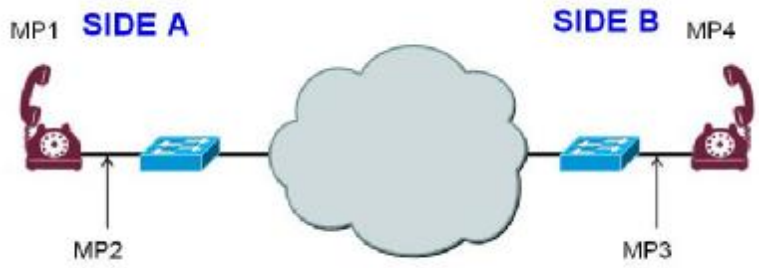


Figure 3-5: Architecture of VoIP test

In order to determine the conversational quality of a voice link we will use a combined objective/subjective tests battery as proposed by Beerends [QoS18]. We will denote the conversational quality at SIDE A and SIDE B by **A_MOS_CQ** and **B_MOS_CQ** respectively.

All tests described by Beerends [QoS18] are truly end-to-end tests, i.e. between measurement points MP1 and MP4 in Figure 3.5.

The test suite consists of the following six steps:

a) One-way listening, speech quality
b) One-way talking, side tone/echo quality
c) One-way talking, echo quality, maximum criticality
d) One-way talking, background noise quality
e) Two-way interaction, full/semi-full/half duplex quality
f) Two-way interaction, delay

The conversational quality is determined by the minimum MOS obtained tests A-F.
In the next section we describe all six steps in more detail.
In addition to the above test suite, one can also use the network quality to determine the conversational speech quality. This can be done through a mapping that is standardized as the E-model in ITU-T G.107, see [QoS19].

In this test we will use the E-model as a validation of the results obtained through the objective/subjective test suite. In order to apply the E-model we will have to determine the network quality between MP2 and MP3 in Figure 3.5 in terms of delay, delay variation and packet loss. Note that on the path between MP2 and MP3 the characteristics of the IP Phone are not taken into account so before we apply the E-model this has to be accounted for some how. More details about the network quality measurements are given in Section 3.4.4.

3.3.3 Test specification at application layer

In this section we describe in details the six steps in the objective/subjective test suite.
It is essential to have an additional phone connection available during the tests in order to communicate during the tests.

3.3.3.1 Test A: One-way listening, speech quality

This test uses the objective method PESQ, see [QoS20].
In order to apply this method a reference signal is used, call sample.wav.
This sample file contains 30 seconds of speech of both a female and male speaker, sampled at 16kHz. The file starts with a synchronization signal.
The speech file needs to be played by one party over the VoIP connection and be recorded by the other party, see Figure 3.6.

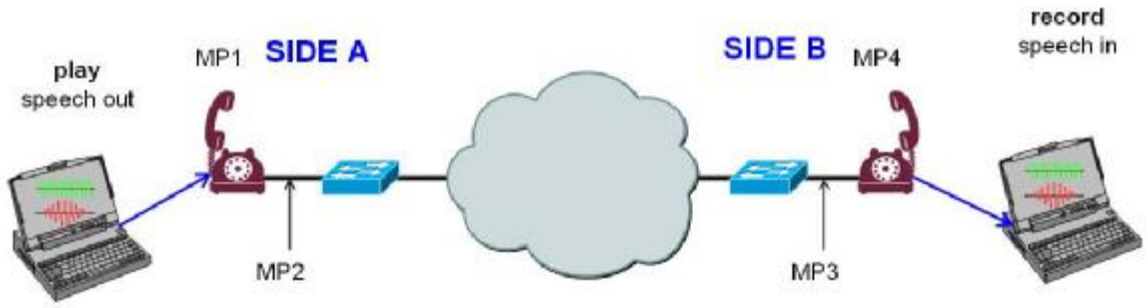


Figure 3-6: PESQ measurement architecture

The laptops should be connected to the IP phones through RJ-11 jacks. For playing and recording the file the freeware program audacity (http://audacity.sourceforge.net/) is recommended.

When playing sample.wav the loop function should be enabled such that it allows the recording party to make a recording from synchronization signal to synchronization signal.
In this test both SIDE A and SIDE B will have to make the recording. The resulting speech files will be called SIDE_A.wav and SIDE_B.wav respectively. They will be processed by TNO to determine the listening quality by means of PESQ. The resulting listening quality at SIDE A and SIDE B will be denoted by **A_MOS_A_LQ** and **B_MOS_A_LQ** respectively.

3.3.3.2 Test B: One-way talking, side tone/echo quality

This subjective test uses the set-up depicted in Figure 3-6.
After the VoIP connection is established the expert at SIDE A talks and listens for echo and side tone distortion. The reference is the natural side tone. Speech should be produced at two levels, normal and loud.
The expert rates the side tone/echo quality by using the ITU-T P.800 [QoS21] DCR opinion scale (Degradation Category Rating) which is anchored in the following way:

5 = no echo and/or side tone distortion audible
4 = audible but not annoying
3 = slightly annoying
2 = annoying
1 = very annoying

The resulting talking quality with respect to side tone and echo at SIDE A is denoted by **A_MOS_B_TQ**.
The test is also conducted by SIDE B and results in **B_MOS_B_TQ**.

3.3.3.3 Test C: One-way talking, echo quality, maximum criticality

This subjective test uses the set-up depicted in Figure 3-6.
After the VoIP connection is established the expert at SIDE A talks and listens for echo while at SIDE B the telephone horn position is changed from default to a hard surface with the loudspeaker facing this surface. Speech should be produced at two levels, normal and loud.
The ITU-T P.800 [QoS21] DCR opinion scale is used, but only the top three categories are allowed using relaxed scaling criteria:

5 = audible echo but not annoying
4 = slightly annoying
3 = annoying

The resulting talking quality with respect to maximum echo criticality at SIDE A is denoted by **A_MOS_C_TQ**.
The test is also conducted by SIDE B and results in **B_MOS_C_TQ**.

3.3.3.4 Test D: One-way talking, background noise quality

This subjective test uses the set-up depicted in Figure 3-6.
After the VoIP connection is established the expert at SIDE A talks while at SIDE B a set of background noise audio files (office, babble, car noise) is played. The recordings should contain a slowly decreasing and/or slowly increasing background noise level in order to assess the system under test under a wide range of background noise conditions. The rate of change should lie in the order of about 20 dB/s and have a duration of about 20 seconds. Speech should be produced at two levels, normal and loud.

Comments: Most important distortions that occur are time-clipping resulting in background noise switching and changes in noise suppression resulting in unnatural level and timbre variations especially during the starts/stop of a speech spurt at the SIDE A side.
The ITU-T P.800 [QoS21] DCR opinion scale (Degradation Category Rating) is used in the assessment with

5 = no suppression of the background noise and other annoying changes audible.
4 = audible but not annoying
3 = slightly annoying
2 = annoying
1 = very annoying

The resulting talking quality with respect to background noise at SIDE A is denoted by **A_MOS_D_TQ**.
The test is also conducted by SIDE B and results in **B_MOS_D_TQ**.

3.3.3.5 Test E: Two-way interaction, full/semi-full/half duplex quality

This subjective test uses the set-up depicted in Figure 3-6.

After the VoIP connection is established the expert at SIDE B counts fast and continuously : *1, 2, 3, 4, 5, 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, 1, 2, 3, 4, 5*…etc (note the two different speech levels). Simultaneously the expert at SIDE A speaks with pauses using single letters*: a, pause, b, pause, c, pause, …etc.* In the assessment the quality of the continuous counting voice from the B-side (*1, 2, 3, 4, 5*) is judged together with the quality with which the own voice is perceived. During double talk no distortion and echo from one's own voice should be audible. Speech should be produced at two levels, normal and loud.
The ITU-T P.800 [QoS21] DCR opinion scale (Degradation Category Rating) is used in the assessment with

5 = no semi-full/half duplex degradation audible
4 = audible but not annoying
3 = slightly annoying
2 = annoying
1 = very annoying

The resulting talking quality with respect to duplex quality at SIDE A is denoted by **A_MOS_E_IQ**.
The test is also conducted by SIDE B and results in **B_MOS_E_IQ**.

3.3.3.6 Test F: Two-way interaction, delay

This test first determines the one-way delay on the VoIP connection. Then this estimate is used to determine the two-way interaction quality with respect to delay. For this test a stop-watch is needed at SIDE A.
After the VoIP connection is established the expert at SIDE A starts the procedure with the counting word "one" while at the same time he starts the stopwatch. Next the expert at SIDE B counts "two" after receiving "one", etc until SIDE A has heard SIDE B counting "ten' after which SIDE A stops the timing. The elapsed time (expressed in ms) is denoted by $\mathbf{T_1}$. This procedure is repeated 4 times resulting in $\mathbf{T_2}$, $\mathbf{T_3}$, $\mathbf{T_4}$.and $\mathbf{T_5}$. If the average of the five measurements is denoted by **T** then the mean one-way delay **D** of the voice-link is estimated by **0.1*(T-4500) ms.**
The resulting two-way interaction quality with respect to delay is denoted by **MOS_F_IQ** and is given by **min{5, 7 – 0.02*D)**.

Ideally the procedure is calibrated face-to-face until the START-STOP time is about 4500 ms.
Remark: If it is possible to conduct end-to-end packet level measurements then it is possible to obtain a more accurate estimate of the mean one-way delay, see also Section 3.3.4.

3.3.3.7 Summary of tests at application layer

The ultimate result of this section is the completion of Table 3-2.

Name	Description	Determined by	Unit	Value
A_MOS_A_LQ	Listening quality at SIDE A	TNO	MOS	
B_MOS_A_LQ	Listening quality at SIDE B	TNO	MOS	
A_MOS_B_TQ	Talking quality: side tone/echo at SIDE A	SIDE A	MOS	
B_MOS_B_TQ	Talking quality: side tone/echo at SIDE B	SIDE B	MOS	
A_MOS_C_TQ	Talking quality: maximum echo at SIDE A	SIDE A	MOS	
B_MOS_C_TQ	Talking quality: maximum echo at SIDE B	SIDE B	MOS	
A_MOS_D_TQ	Talking quality: background noise, at SIDE A	SIDE A	MOS	
B_MOS_D_TQ	Talking quality: background noise, at SIDE B	SIDE B	MOS	
A_MOS_E_IQ	Two-way interaction at SIDE A	SIDE A	MOS	
B_MOS_E_IQ	Two-way interaction at SIDE B	SIDE B	MOS	
T_1	Elapsed time Test F 1	SIDE A	ms	
T_2	Elapsed time Test F 2	SIDE A	ms	
T_3	Elapsed time Test F 3	SIDE A	ms	
T_4	Elapsed time Test F 4	SIDE A	ms	
T_5	Elapsed time Test F 5	SIDE A	ms	
T	Mean Elapsed time Test F	SIDE A	ms	
D	Mean One-Way Delay	SIDE A	ms	
MOS_F_IQ	Two-way interaction quality, with respect to delay	SIDE A	MOS	
A_MOS_CQ	Conversational quality SIDE A	SIDE A	MOS	
B_MOS_CQ	Conversational quality SIDE B	SIDE B	MOS	

Table 3-2: Results of tests at application layer for VoIP

In Table 3-2 the conversational quality at SIDE A and SIDE B is obtained through
A_MOS_CQ = min{ A_MOS_A_LQ, A_MOS_B_TQ, A_MOS_C_TQ, A_MOS_D_TQ, A_MOS_E_TQ, MOS_F_IQ}
and
B_MOS_CQ = min{ B_MOS_A_LQ, B_MOS_B_TQ, B_MOS_C_TQ, B_MOS_D_TQ, B_MOS_E_TQ, MOS_F_IQ}

3.3.4 Test specification at network layer

The test described above gives a measure of the perceived QoS of a VoIP call between Side A and Side B using the IP phones. In addition to the above objective and subjective quality methods one also can perform a number of network measurements, for instance by using PTAnalyzer software/hardware from Prosilient[3]. The method relies on the injection of known packet streams into the IP network. These packet streams are analysed upon reception and the result is stored in a log file.

[3] www.prosilient.com

The test set-up is as depicted in Figure 3-5. For the measurement two IP-network probes from Prosilient will be used, one connected the router at Side A, one at Side B. Referring to Figure 3-5 this means that the measurements take place between MP2 and MP3.
Packet streams are pre-configured, e.g. VoIP streams using RTP. The stream parameters can be configured to mimic the VoIP-call. The measurement packet streams are injected into the network and mixed with the traffic of the real-life VoIP application.
The measurement can be configured to run for e.g. a week in order to deduce IP-rush hour and low load time. The probes are managed by a central Prosilient node. The result is automatically analysed and presented in graphs and reports. Parameters such as bandwidth, end-to-end delay, end-to-end jitter, packet loss and packet miss-order will be determined.

The network measurement should take place in parallel with the perception-related test, and a correlation between the two can be deduced. In fact, the PTAnalyzer maps the network quality directly to the MOS_CQ by means of the E-model [QoS19]. Again, this value should be determined in both directions, i.e. both at Side A and at Side B.

The ultimate result of this section is the completion of Table 3-3.

Name	Description	Determined by	Unit	Value
A_delay	Delay from Side B to Side A	Side A	ms	
B_delay	Delay from Side A to Side B	Side B	ms	
A_jitter	Jitter from Side B to Side A	SIDE A	ms	
B_jitter	Jitter from Side A to Side B	SIDE B	ms	
A_loss	Packet loss from Side B to Side A	SIDE A	%	
B_loss	Packet loss from Side A to Side B	SIDE B	%	
A_MOS_CQ_Emodel	Conversational quality Side A	TNO	MOS	
B_MOS_CQ_Emodel	Conversational quality Side B	TNO	MOS	

Table 3-3: Results of tests at network layer for VoIP

3.4 Streaming Video

3.4.1 Perceived QoS for streaming Video

Video is truly an audio-visual experience, where the quality of the audio and video contributes both separately and combined to the overall experience. Unfortunately, there is today no method, at least not standardised, that measures the audio-visual quality. What will be outlined here are series of measurements and tests in order to still get hold of the audio-visual quality, although it will not come in one combined quality score.
For audio only there is a well established standard i.e. PEAQ, see [QoS2], but for the visual information (which is what is meant here when we say video) the situation is not that clear.
Video quality measurements methods are often divided into three groups, depending on how much of the reference or the original is available or needed by the method. These are:

- Full reference
  Methods that use or require the whole reference video, often an undistorted high quality original, to compare with the distorted video. These methods are best suited for off-line measurements.
- Reduced reference

Methods that extracts a set of quality features of the reference and the distorted video and sends this reduced set of data to the measurement point. These methods could also be used for in-service monitoring.

- No reference.
  Methods that determine the quality of the video based on the distorted video only. These methods are targeted for In-service, but usually less accurate than reduced and full reference methods.

3.4.2 Test methods

3.4.2.1 Visual quality

There are today no standards for in-service monitoring of streaming video. The standard for video quality measurements by ITU ([QoS22], [QoS4]) covers full reference methods for standard definition TV. The unfortunate fact is that the standard covers four different methods. This means that it is possible to measure with standardised methods and still come to different results. Although, the difference was not statistically significant in the VQEG phase II test ([QoS23]), there was one method that was slightly better than the others i.e. the Video Quality Metric (VQM). Apart from its slight performance advantage from the other standardised methods, which could be debated on statistical grounds, VQM has a design benefit. It could be used for real time monitoring, since it is really a reduced reference video quality measurement method. It means that VQM does not need to have access to all the data of the reference at the measurement point, but rather small subset of extracted parameters, that could be transmitted at a much lower bandwidth than the original. We will, therefore, base the measurements of video quality on this method. There is a real time implementation of the VQM, called IVQM [QoS5]. The version of IVQM available from NTIA cannot currently handle streaming video in a broadband network. An IPTV interface has therefore been developed by Acreo and has now been integrated with IVQM. For short term test e.g. video that could easily be stored uncompressed on both sending and receiving end, VQM is still recommended to be used. For more long term tests the IVQM is a better choice. The method based on VQM will be described below and the IVQM will be described in the Annex.

The architecture of the test is similar to the voice test, see Figure 3-7 A test video sequence will be sent from side B to side A, using a computer at side B to generate a video stream. The stream will then be recorded at side B and then analysed off line using VQM. In this scenario, the measurement point MP4 will contain the undistorted uncoded reference video. At MP3, the outgoing encoded video stream will be found. The incoming video stream, without the influence of the display system, could be measured at MP2. However, in order to use VQM a decoding will have to be done and the specific choice of decoder will have an effect of the overall quality. Measurement point MP1 is the video at the display. We will thus measure the quality of the video between MP2 and MP3. This will correspond to the quality at MP1 if the display screen is of a very high quality. Recently, [QoS3] have suggested an objective/subjective measurement protocol that takes into account some aspects of the display such as the brightness.

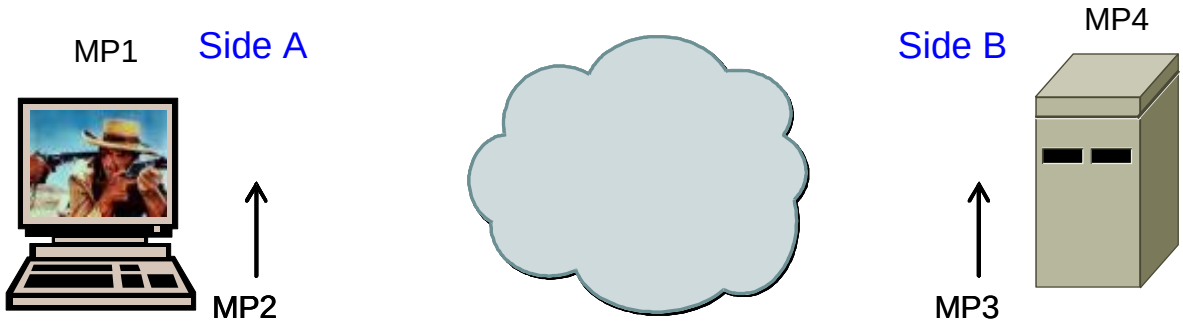


Figure 3-7: The VQM test set-up

3.4.2.2 Audio quality

Audio can be objectively measured with the PEAQ method, see [QoS2].

3.4.2.3 Combined audio-visual quality

Previous studies, such as [QoS7] and [QoS8] have shown that the overall audio-visual quality of video can be predicted accurately from stand-alone audio and video quality models. We will always use VQM as stand-alone video quality model. For streaming video we will use PEAQ as stand-alone audio quality model while for videoconference we will use PESQ.

Denoting the audio quality as MOS_A and the video as MOS_V then according to [QoS7] the audio-visual quality $MOSA_V$ is accurately predicted through:

$$MOS_{AV} = 0.87 + 0.2\ MOS_A * MOS_V\ . \qquad (1)$$

In [QoS7] only one sequence video was used. Recently [QoS8] showed that the form of the predictive model is content dependent. In fact [QoS8] studied both a high-motion video and a talking head video.

For Streaming Video we propose to use the mapping suggested in [QoS8] for high-motion sequences:

$$MOS_{AV} = 0.95 + 0.15\ MOS_A * MOS_V + 0.25\ MOS_V. \qquad (2)$$

We prefer to use (2) instead of (1) because in [QoS7] video dominated audio. This is probably due to the fact that [QoS7] used a very high-motion video sequence (a movie trailer, with many scene changes).

The area of measuring audio-visual quality is still very immature, so the computed qualities should be used with some caution.

3.4.2.4 Synchronization

The effect of asynchrony between audio and video may play an important role in low bit rate audiovisual services. Differences less than 200 ms can already lead to a clear perceived disturbing degradation. In order to have no significant influence the delay between audio and video has to be less than 150 ms if video advances audio and less than 70 ms if audio advances video (see Rihs [QoS9]). The findings of Rihs and related papers lead to ITU-R Rec. BT.1359 [QoS10], see also Figure 3-8.

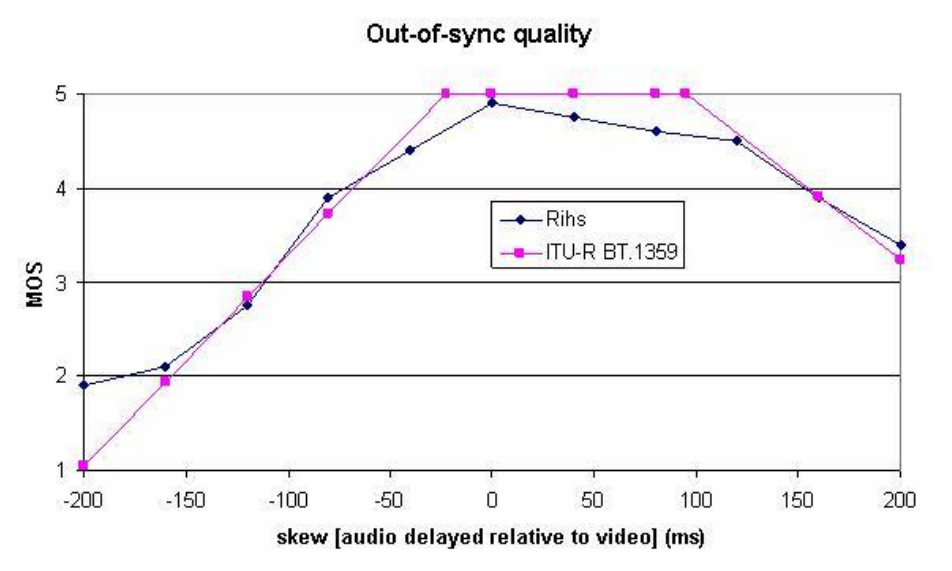


Figure: 3-8: Perceived QoS when audio and video signals are not played synchronously

In fact, the amount of acceptable skew also depends on the frame rates, see [QoS11]. However, within MUSE we always assume frame rates of at least 25 fps therefore we can use the results of [QoS10]. Based upon [QoS10] we get the following mapping between the skew (in ms) and the lip-synchronization (MOS_LS):

$$MOS_LS = \max\{1, \min\{\frac{Skew}{45} + 5.5, -\frac{Skew}{60} + 6.58, 5\}\},$$

where the skew is given in ms.

3.4.2.5 Zapping

The time it takes to change the TV-channel, often referred to as zapping, will also affect the overall experience of viewing TV. Zapping will also act stressful on the network. For example, during a short period the old channel will be on at the same time as the new channel, especially if the signalling is not done in a proper way, which means that it is useful to measure the zapping time for several reasons. However, the mapping between zapping time and MOS score is currently not well known. For this reason we have conducted our own subjective experiments which led to a relation between MOS and zapping time, see [QoS26].

3.4.3 Test specification at application layer

3.4.3.1 Visual quality

To measure the perceived quality through a network link, from Side B to Side A, using VQM (for a detailed description see [QoS6]) a test video should be sent through the network, stored on the receiving side and then evaluated against the video on the sending side using VQM. Depending on where the video is captured different comparisons are done i.e. MP1-MP4, see Figure 3-9. If the perceptual quality of the network link is of interest, the comparison should be done between MP2 and MP3, but if the end-to-end quality is of interest then MP1 and MP4 should be compared.
As mentioned before, we will here determine the visual quality between MP2 and MP3.
The video that should be sent should be coded by the codec that is typically used for the application of interest. For instance, IP-TV is typically coded using MPEG 2, whereas for Video-on-Demand (VOD) or multimedia this could also be WMV 9 or MPEG 4 part 10. The bitrates should typically be set in the range 4-6 MBit/s for IP-TV and VOD coded using MPEG 4 about 2 MBit/s or less.

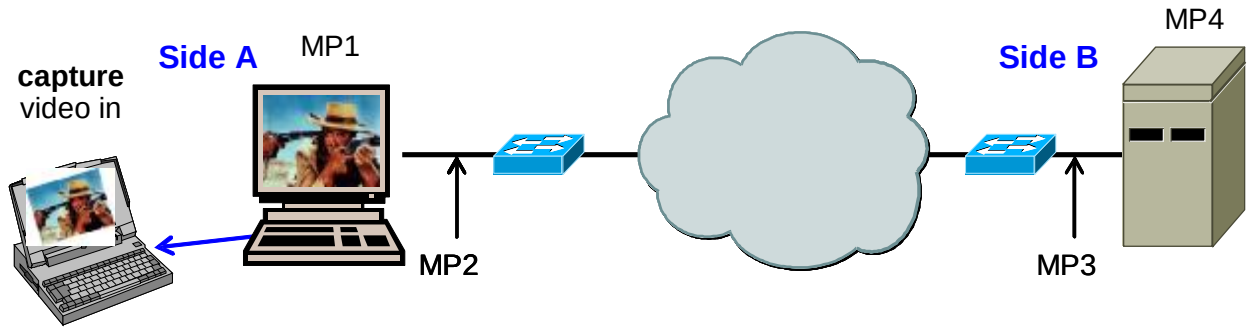


Figure 3-9: Streaming video measurement set-up.

VQM has more than one computational model implemented. For streaming video there is a model called the general model that is not optimised for any particular material or bandwidth. For TV i.e. the higher quality and bandwidth range there is an optimised model called Television. The result from VQM can be set to give the scores in the range of a few subjective scales. Choosing the Double Stimulus Impairment Scale gives a result similar to the MOS scale.

In order to apply this method a reference clip is used, called sample.avi which contains both audio and video. The audio and video signals of this reference clip can be separated and are called sampleA.wav and sampleV.avi respectively. This sample clip lasts 30 seconds, contains video coded at 2 Mbps (MPEG-4) or 4-6 Mbps (MPEG-2) while the audio is coded at 192 kbps. The clip starts with a synchronization signal.

There are no standardised set of test material to use. However, in [QoS24], [QoS25] there are discussions of ways to characterise the video content. What is important is to get a representative set of video clips for the application under test. The selection of picture size and frame rates should also be based on the picture size used in the application, which is investigated. For IP-TV the size and frame rate of a standard definition TV (SDTV) i.e. 720x576 25 fps interlaced is recommended. For multimedia where the target display is a small flat panel the size of VGA (640x480) 25 fps or 30 fps progressive, depending on frame rate of the source materials, could be used instead. At a later stage also HDTV will be considered.

The clip needs to be streamed over the IP connection and for the video quality test the video must be captured recorded by Side A, see Figure 3-10. The captured file will be denoted by recorded.avi.
When playing sample.avi a loop function of the video playing software should be enabled such that it allows the recording party to make a recording from synchronization signal to synchronization signal.
The visual quality will be determined by using the General Model provided in VQM with sampleV.avi and the video part of recorded.avi as input files. The resulting visual quality will be denoted by $\mathbf{MOS_V}$.

The Annex contains a description of how to capture a video stream.

3.4.3.2 Audio quality

This test uses the objective method PEAQ, see [QoS2].
In order to apply this method a reference clip is used, called sample.avi which contains both audio and video. The audio and video signals of this reference clip can be separated and are called sampleA.wav and sampleV.avi respectively. This sample clip lasts 30 seconds, contains video coded at 2 Mbps (MPEG-4) or 4-6 Mbps (MPEG-2) while the audio is coded at 192 kbps. The clip starts with a synchronization signal.
The clip needs to be streamed over the IP connection and for the audio quality test the audio must be recorded by Side A, see Figure 3-10.

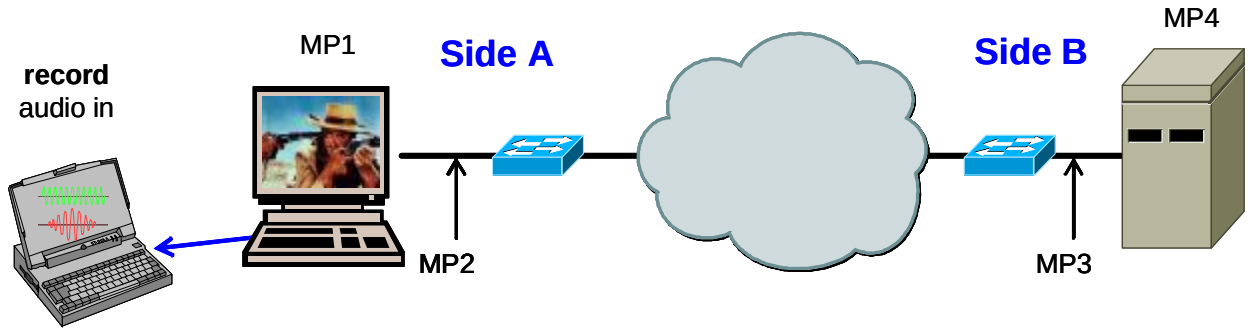


Figure 3-10: PEAQ measurement architecture

The laptop at Side A should be connected to the PC. For recording the audio the freeware program audacity (http://audacity.sourceforge.net/) is recommended.

When playing sample.avi a loop function of the video playing software should be enabled such that it allows the recording party to make a recording from synchronization signal to synchronization signal.
The resulting speech file will be called recorded.wav. The audio quality will be determined by feeding sampleA.wav and recorded.wav into PEAQ. The resulting audio quality will be denoted by $\mathbf{MOS_A}$.

3.4.3.3 Combined audio-visual quality

The audio and video MOS scores are measured independently with the methods described in the previous subsections. These values are weighted together as described in Section 3.5.2.3. If we denote the resulting audio-visual quality by $\mathbf{MOS_{AV}}$ then we have

$\mathbf{MOS_{AV}}$ = 0.95 + 0.15 $\mathbf{MOS_A}$ *$\mathbf{MOS_V}$ + 0.25 $\mathbf{MOS_V}$.

3.4.3.4 Synchronization

In order to measure the synchronisation we will use the reference clip sync_sample.avi that we have made ourselves. This clip is taken from a high quality video trailer and was cropped to a resolution of 720x576 at 25 fps. The length of the clip is 30 seconds. Starting at t = 2 seconds, every 3 seconds the clip contains both a visual marker and an audio marker. The visual marker is formed by 8 consecutive frames that are completely red. Hence the length of each visual marker is 320 ms. The audio marker consists of a beep that lasts 300 ms. The reference clip is streamed over the network and captured at the receiving Side A. For the captured file we compare the relative difference delay between the beginnings of the visual and audio markers. In this way we obtain 10 sample values for the skew. The average value will be denoted by **SKEW** (in ms). Finally, the MOS score with respect to audio-video synchronization, which will be denoted by $\mathbf{MOS_{LS}}$, can be obtained from Section 3.5.2.4:

$$MOS_{LS} = \max\{1, \min\{\frac{SKEW}{45} + 5.5, -\frac{SKEW}{60} + 6.58, 5\}\}$$

3.4.3.5 Zapping

The time it takes from pressing the channel changing button on the remote control and until the channel starts on the TV is measured with a stop watch. This is repeated 10 times. Finally, **T_ZAP**, defined as the average value of the 10 zapping times, will be determined.

Note that the relation between **T_ZAP** and MOS scores is explored in [QoS26] There the following relation is established between zapping time and MOS:

$\mathbf{MOS_{ZAP}}$ = max{min{5, -1.0225*ln(T_ZAP) + 2.6456}, 1}.

For the overall perceived QoS for Streaming Video, denoted by $\mathbf{MOS_{SV}}$ we have

$\mathbf{MOS_{SV}}$ = min{ $\mathbf{MOS_{AV}}$, $\mathbf{MOS_{LS}}$, $\mathbf{MOS_{ZAP}}$}

3.4.3.6 Summary of tests at application layer

The ultimate result of this section is the completion of Table 3-4.

Name	Description	Determined by	Unit	Value
MOS_V	Visual quality	TNO	MOS	
MOS_A	Audio quality	TNO	MOS	
MOS_{AV}	Audio-visual quality	SIDE A	MOS	
SKEW	Delay audio relative to video	SIDE A	ms	
MOS_{LS}	Synchronization quality	SIDE A	MOS	
T_ZAP	Zapping time	SIDE A	sec	
$MOSZ_{AP}$	Zapping quality	SIDE A	MOS	
MOS_{SV}	Overall perceived Streaming Video quality	SIDE A	MOS	

Table 3-4: Results of tests at application layer for Streaming Video

3.4.3.7 Limitations

The methods described above will lead to a sample value for the perceived quality for Streaming Video. Because the tests described above use sample clips of length 30 sec, one might wonder how reliable such a sample value is for predicting perceived quality of Streaming Video, especially because typical holding times of Streaming Video sessions can be in the order of at least one hour. For the time being, we recommend the use of our test method once for an initial assessment of the perceived quality of Streaming Video for a given network scenario. One could then use tests at the network layer over a longer time period (for instance several hours) and use those as an indication whether or not the network conditions are constant over that time period. If this is not the case then one can decide to repeat the objective measurement process a number of times. Note that it depends on the variability of the measured perceived quality; how often one should repeat the objective measurements in order to obtain a statistically reliable result. This issue is left for further study. IVQM is also an option for longer term monitoring, but the IPTV interface is still under evaluation and is currently not completely stable.

In Section 3.5.3.5 we have suggested the following relation between the overall perceived QoS for Streaming Video, denoted by $\mathbf{MOS_{SV}}$, and the audio-visual quality ($\mathbf{MOS_{AV}}$), the lip-synchronization quality ($\mathbf{MOS_{LS}}$) and the zapping quality ($\mathbf{MOS_{ZAP}}$):

$$\mathbf{MOS_{SV}} = \min\{\mathbf{MOS_{AV}}, \mathbf{MOS_{LS}}, \mathbf{MOS_{ZAP}}\}$$

However, to our knowledge, this relation has never been validated with subjective experiments. Validation of this assumption is also left for further study.

3.4.4 Test specification at network layer

The tests described above gives a measure of the perceived QoS of a Streaming Video call between Side A and Side B. In addition to the above objective and subjective quality methods one also needs to perform a number of network measurements, for instance by using PTAnalyzer software/hardware from Prosilient[4]. The method relies on the injection of known packet streams into the IP network. These packet streams are analysed upon reception and the result is stored in a log file.

The test set-up is as depicted in Figure 3-7. For the measurement two IP-network probes from Prosilient can be used, one connected the router at Side A, one at Side B. Referring to Figure 3-7 this means that the measurements take place between MP2 and MP3.
Packet streams are pre-configured, e.g. Video streams using RTP. The stream parameters can be configured to mimic the Streaming Video call. The measurement packet streams are injected into the network and mixed with the traffic of the real-life Streaming Video application.
The measurement can be configured to run for e.g. a week in order to deduce IP-rush hour and low load time. The probes are managed by a central Prosilient node. The result is automatically analysed and presented in graphs and reports. Parameters such as bandwidth, end-to-end delay, end-to-end jitter, packet loss and packet miss-order will be determined.

The network measurement should take place in parallel with the perception-related test, and a correlation between the two can be deduced. Note that there is no mapping known between network quality and perceived QoS for Streaming Video. Therefore the network quality parameters just serve as an indication for the perceived QoS.

[4] www.prosilient.com

Note that the selection of the measuring time is an important issue. On a lightly loaded network the mean time between failures could be very long, so in order to catch these the measuring time should also be very long, typically several hours or even a few days. In these cases this method in not very suited and a real time method should be used. For instance, the IVQM when there is a version that works on an IP-based network. Another possibility is to use a commercial no-reference method e.g. Agama (www.agama.tv). If the network is either medium or heavily loaded, the suggested method could be used. The limitation is storage space, since all data needs to be stored on disk. For instance, 10 minutes SDTV at 4 MBits/s would require about 0.8 GByte. Furthermore, the input to VQM needs decoded video clips, which will increase the size of the clip by a factor of about 40-50 times, but this needs only to be available at the analysis stage.

The ultimate result of this section is the completion of Table 3-5:

Name	Description	Determined by	Unit	Value
Delay	Delay from Side B to Side A	Side A	ms	
Jitter	Jitter from Side B to Side A	Side A	ms	
Loss	Packet loss from Side B to Side A	Side A	%	
Bandwidth	Bitrate of the Video Stream	Side A	Mbps	

Table 3-5: Results of tests at network layer for Streaming Video

3.5 Video conference

3.5.1 Perceived QoS for Video conferencing

Measurement of the quality of video conference could in principle be done by using what is described in the perceived quality of VoIP and streaming video tests. The difference with VoIP is the interaction effects of the quality of video on the voice quality and vice versa, as well as the effects of synchronization between voice and video (i.e the lips). These latter issues are also present in streaming video. The difference between video conference and streaming video is that it is a, at least, two ways communication situation, whereas streaming video is a one way broadcasting situation. The content of audio of video is much wider in streaming video, which in principal may contain just about anything. Video conference on the other hands contains mainly voice and talking heads. Another difference is that video conference usually uses other type codecs e.g. H.263, than streaming video and often also lower bandwidth, at least compared to TV. A further complication is that video conference systems tend to be an integrated solutions that could be difficult to get access to.

The explicit assumption in the remainder of this section is that we can actually get into the videoconferencing system under study, in the sense that we can send pre-recorded clips over the system. If this is NOT the case then we can only use subjective methods for obtaining the perceived quality. In that case, we suggest the use the test protocol for end-to-end perceived quality for videoconferencing described in [QoS31].

3.5.2 Test methods

3.5.2.1 Visual quality

The test method used for video conference will also be VQM, see section 3.5.2 and the Annex for a description, but using a different internal model i.e. video conference model. Currently and due the available implementations of IVQM, this method is not suited for video conference and will not be further described here. The test scenario is shown in Figure 3-11. Video conference is more than one way communication, which means that measuring the quality involves both looking at the quality degradation from side A to side B and vice versa.

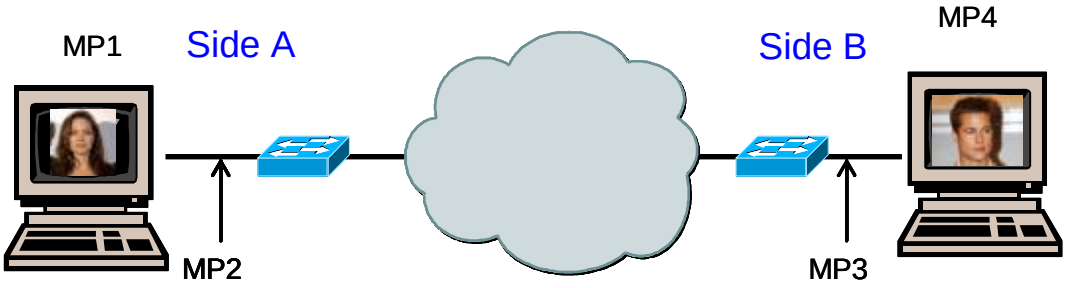


Figure 3-11: Videoconference test set-up

3.5.2.2 Audio quality

The audio quality is determined by using the objective/subjective test suite also used for VoIP, see Section 3.4.3.

3.5.2.3 Combined audio-visual quality

For Videoconference we propose to use the mapping suggested in [QoS8] for talking head sequences, see also section 3.5.2:

$$MOS_{AV} = 1.15 + 0.17\ MOS_A * MOS_V.$$

3.5.2.4 Synchronization

The synchronization is measured and MOS scores are estimated using the method presented in section 3.5.2.

3.5.3 Test specification at application layer

3.5.3.1 Visual quality

For measuring video quality of video conference VQM will be used just as for streaming video, see section 3.5.2. The difference here is that the measurements should be taken both ways, as mentioned above. Figure 3-12 shows a one way capturing of video, where video has been sent from side B to side A. The end-to-end perceived quality is measured between MP1 and MP4, whereas the quality of a network link is taken between MP2 and MP3.

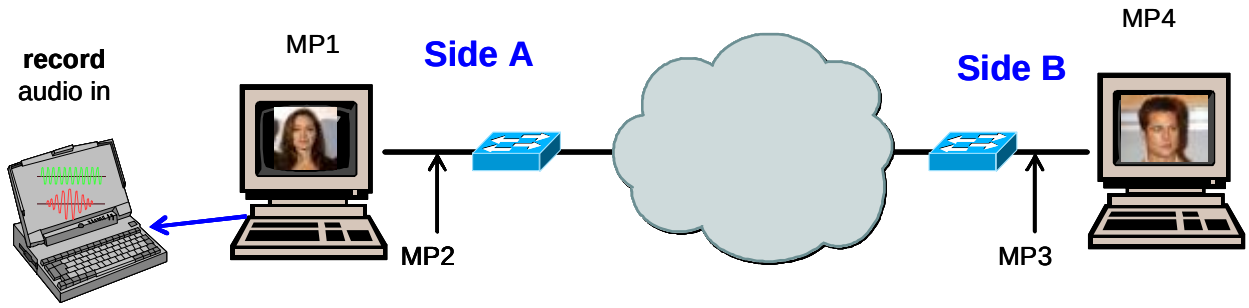


Figure 3-12: Videoconference measurement set-up

In order to apply this method a reference clip is used, called sample.avi which contains both audio and video. The content obviously needs to be a talking head. The audio and video signals of this reference clip can be separated and are called sampleA.wav and sampleV.avi respectively. This sample clip lasts 30 seconds, contains video coded at around 2 Mbps while the audio is coded at 192 kbps. The clip has is VGA (640x480) 25 fps or 30 fps progressive.

The clip needs to be streamed over the IP connection through the Videoconference application and for the video quality test the video must be captured recorded by Side A, see Figure 3-12. The captured file will be denoted by recorded.avi.
When playing sample.avi a loop function of the video playing software should be enabled such that it allows the recording party to make a recording from synchronization signal to synchronization signal.
The visual quality will be determined by using the General Model provided in VQM with sampleV.avi and the video part of recorded.avi as input files. The resulting visual quality will be denoted by $\mathbf{MOS_V}$. Because we need to assess the visual quality at Side A and at Side B, we actually need to determine $\mathbf{A_MOS_V}$ and $\mathbf{B_MOS_V}$, respectively.

3.5.3.2 Audio quality

The audio quality is measured in the same way as for VoIP, see section 3.4.3. The set-up for measuring the listening quality at Side A is depicted in Figure 3-13. Note that we will now use PESQ for determining the audio quality.

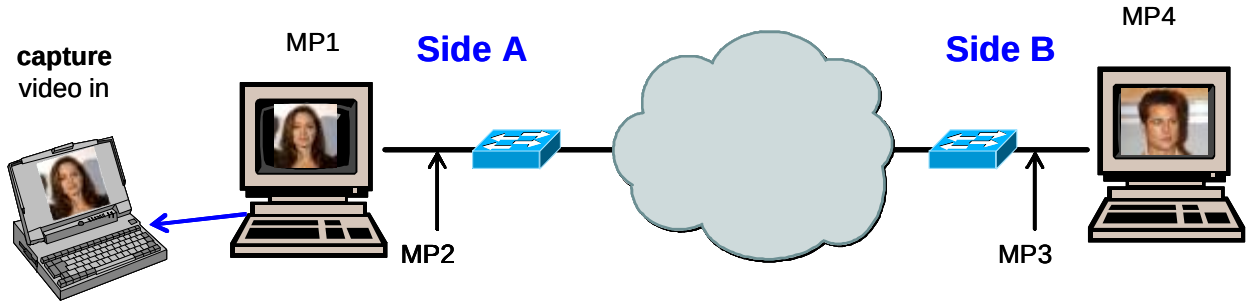


Figure 3-13: Measuring listening quality for Videoconferencing

The resulting audio quality will be denoted by $\mathbf{MOS_A}$. Because we need to assess the audio quality at Side A and at Side B, we actually need to determine $\mathbf{A_MOS_A}$ and $\mathbf{B_MOS_A}$, respectively.

3.5.3.3 Combined audio-visual quality

The audio and video MOS scores are measured independently with the methods described in the previous subsections. These values are weighted together as described in section 3.5.2. If we denote the resulting audio-visual quality by **MOS_{AV}** then we have

$$MOS_{AV} = 1.15 + 0.17\ MOS_A * MOS_V \ .$$

Because we need to assess the audio-visual quality at Side A and at Side B, we actually need to determine **A_MOS_{AV}** and **B_MOS_{AV}**, respectively.

3.5.3.4 Synchronization

In order to measure the synchronisation we will use the reference clip sync_sample.avi that we have made ourselves. This clip is taken from a high quality video trailer and was cropped to a resolution of 720x576 at 25 fps. The length of the clip is 30 seconds. Starting at t = 2 seconds, every 3 seconds the clip contains both a visual marker and an audio marker. The visual marker is formed by 8 consecutive frames that are completely red. Hence the length of each visual marker is 320 ms. The audio marker consists of a beep that lasts 300 ms. The reference clip is streamed over the network and captured at the receiving Side A. For the captured file we compare the relative difference delay between the beginnings of the visual and audio markers. In this way we obtain 10 sample values for the skew. The average value will be denoted by **SKEW** (in ms). Finally, the MOS score with respect to audio-video synchronization, which will be denoted by **MOS_{LS},** can be obtained from Section 3.5.2.4:

$$MOS_{LS} = \max\{1, \min\{\frac{SKEW}{45} + 5.5, -\frac{SKEW}{60} + 6.58, 5\}\}$$

Because we need to assess the synchronization quality at Side A and at Side B, we actually need to determine **A_MOS_{LS}** and **B_MOS_{LS}**, respectively.

For the overall perceived QoS for Videoconference, denoted by **MOS_{VC}** we have

$$MOS_{VC} = \min\{ MOS_{AV}, MOS_{LS}\}$$

Because we need to assess the overall perceived quality at Side A and at Side B, we actually need to determine **A_MOS_{VC}** and **B_MOS_{VC}**, respectively.

3.5.3.5 Summary of tests at application layer

The ultimate result of this section is the completion of Table 3-6.

Name	Description	Determined by	Unit	Value
A_MOS_V	Visual quality at Side A	TNO	MOS	
B_MOS_V	Visual quality at Side B	TNO	MOS	
A_MOS_A	Audio quality at Side A	TNO	MOS	
B_MOS_A	Audio quality at Side B	TNO	MOS	
A_MOS_{AV}	Audio-visual quality at Side A	SIDE A	MOS	
B_MOS_{AV}	Audio-visual quality at Side B	SIDE B	MOS	
SKEW_A	Delay audio relative to video at Side A	SIDE A	ms	
SKEW_B	Delay audio relative to video at Side B	SIDE B	ms	

Name	Description	Determined by	Unit	Value
A_MOS_{LS}	Synchronization quality at Side A	SIDE A	MOS	
B_MOS_{LS}	Synchronization quality at Side B	SIDE B	MOS	
A_MOS_{SV}	Overall perceived Videoconference quality at Side A	SIDE A	MOS	
B_MOS_{SV}	Overall perceived Videoconference quality at Side B	SIDE B	MOS	

Table 3-6: Results of tests at application layer for Videoconference

3.5.3.6 Limitations

The methods described above will lead to a sample value for the perceived quality for Videoconferencing. Because the tests described above use sample clips of length 30 sec, one might wonder how reliable such a sample value is for predicting perceived quality of Videoconferencing, especially because typical holding times of Videoconferencing sessions can be in the order of at least half an hour. For the time being, we recommend the use of our test method once for an initial assessment of the perceived quality of Videoconferencing for a given network scenario. One could then use tests at the network layer over a longer time period (for instance several hours) and use those as an indication whether or not the network conditions are constant over that time period. If this is not the case then one can decide to repeat the objective measurement process a number of times. Note that it depends on the variability of the measured perceived quality: how often one should repeat the objective measurements in order to obtain a statistically reliable result. This issue is left for further study.

In Section 3.6.3.4 we have suggested the following relation between the overall perceived QoS for Videoconferencing, denoted by $\mathbf{MOS_{VC}}$, and the audio-visual quality ($\mathbf{MOS_{AV}}$) and the lip-synchronization quality ($\mathbf{MOS_{LS}}$):

$$\mathbf{MOS_{VC}} = \min\{\mathbf{MOS_{AV}}, \mathbf{MOS_{LS}}\}$$

However, to our knowledge, this relation has never been validated with subjective experiments. Validation of this assumption is also left for further study.

3.5.4 Test specification at network layer

The tests described above give a measure of the perceived QoS of a Videoconference call between Side A and Side B and vice versa. In addition to the above objective and subjective quality methods one also needs to perform a number of network measurements, for instance by using PTAnalyzer software/hardware from Prosilient. The method relies on the injection of known packet streams into the IP network. These packet streams are analysed upon reception and the result is stored in a log file.

The test set-up is as depicted in Figure 3-11. For the measurement two IP-network probes from Prosilient can be used, one connected the router at Side A, one at Side B. Referring to Figure 3-11 this means that the measurements take place between MP2 and MP3.
Packet streams are pre-configured, e.g. Videoconference streams using RTP. The stream parameters can be configured to mimic the Videoconference call. The measurement packet streams are injected into the network and mixed with the traffic of the real-life Videoconference application.

The measurement can be configured to run for e.g. a week in order to deduce IP-rush hour and low load time. The probes are managed by a central Prosilient node. The result is automatically analysed and presented in graphs and reports. Parameters such as bandwidth, end-to-end delay, end-to-end jitter, packet loss and packet miss-order will be determined.

The network measurement should take place in parallel with the perception-related test, and a correlation between the two can be deduced. Note that there is no mapping known between network quality and perceived QoS for Videoconferencing. Therefore the network quality parameters just serve as an indication for the perceived QoS.

Note that the selection of the measuring time is an important issue. On a lightly loaded network the mean time between failures could be very long, so in order to catch these the measuring time should also be very long, typically several hours or even a few days. In these cases this method in not very suited and a real time method should be used. For instance, the IVQM when there is a version that works on an IP-based network. Another possibility is to use a commercial no-reference method e.g. Agama (www.agama.tv). If the network is either medium or heavily loaded, the suggested method could be used. The limitation is storage space, since all data needs to be stored on disk. For instance, 10 minutes SDTV at 4 MBits/s would require about 0.8 GByte. Furthermore, the input to VQM needs decoded video clips, which will increase the size of the clip by a factor of about 40-50 times, but this needs only to be available at the analysis stage.

The ultimate result of this section is the completion of Table 3-7.

Name	Description	Determined by	Unit	Value
A_Delay	Delay from Side B to Side A	Side A	ms	
B_Delay	Delay from Side A to Side B	Side B	ms	
A_Jitter	Jitter from Side B to Side A	Side A	ms	
B_Jitter	Jitter from Side A to Side B	Side B	ms	
A_Loss	Packet loss from Side B to Side A	Side A	%	
B_Loss	Packet loss from Side A to Side B	Side B	%	
A_Bandwidth	Bitrate of the Video Stream from Side B to Side A	Side A	Mbps	
B_Bandwidth	Bitrate of the Video Stream from Side A to Side B	Side B	Mbps	

Table 3-7: Results of tests at network layer for Videoconferencing

3.6 Web browsing and downloads

3.6.1 Perceived QoS for web browsing and downloads

The aim of the test described in this section is to determine the perceived QoS of a web browsing session. When browsing users interact with a webpage, e.g. by entering a URL and receiving a webpage, followed by inserting search text in a query box on this webpage, pushing a send button, and then retrieving another web page with the requested information from the server. This form of browsing is called interactive web browsing (IWB).

The perceived QoS for web browsing is affected by many parameters (web page layout and design, etc), but in the following only the objective parameter time is considered; the longer users have to wait for a webpage to download, the lower their quality perception will be. More specifically, for an interactive web session the perceived quality is determined by four time parameters: the response times and the download times of the initial and results web page. The response time (RT) is the time elapsing between the start of a web page retrieval upto the first appearance of some text or pictures. Typical response time values are characterised as follows:

- **0.1 second**. is about the limit for having the feel that the system is reacting instantaneously,
- **1.0 second** is about the limit for the user's flow of thought to stay uninterrupted, even though the user does lose the feeling that the service is operating directly, an important limit for interactive services
- **10 second** is about the limit for keeping the user's attention focused on the dialogue. For longer delays, users will want to perform other tasks while waiting for the computer to finish, so they should be given feedback indicating when the computer expects to be done. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what to expect

The time elapsing between the response time upto the moment that all text and pictures have been retrieved is known as the data transfer time. The sum of the response time and the data transfer time is called the download time. The sum of the download times is known as the session time for the web browsing session, see Figure 3-14.

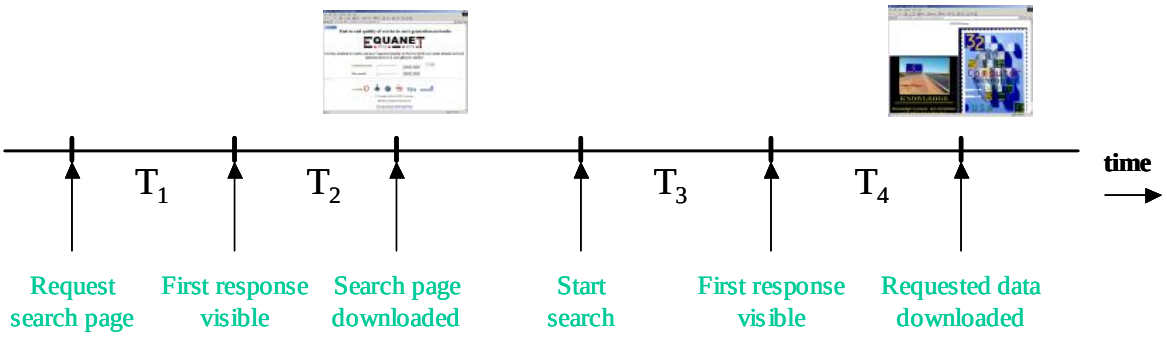


Figure 3-14: The objective time parameters in an interactive web browsing session. T1 and T2 are the response time and download time for the initial page. T3 and T4 are the equivalent for the results page. T1+T2+T3+T4 is the session time

For (large) downloads, that take at least minutes and possible even hours, to our knowledge, there is no mapping known between download times and perceived QoS. However, for this case it is obvious that the obtained throughput is an important indicator for quality to the user. Note that it is also important to users that the progress of the download is clearly indicated.
Because the overwhelming majority of IP applications use the reliable byte stream transfer services of TCP we will describe methods for estimating TCP throughput for (large) downloads, in addition to the method described above.

3.6.2 Test methods

The architecture for the test is depicted in Figure 3-15.

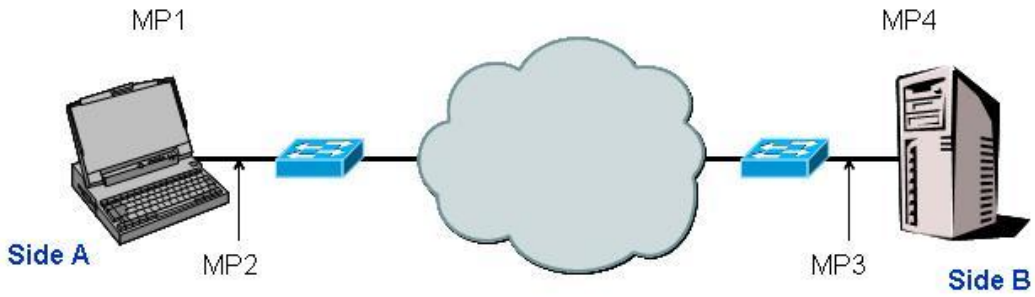


Figure 3-15: Architecture of web browsing and download test

In order to determine the perceived QoS for web browsing we will use the results of [QoS1] in which subjects were asked to assess the quality of web browsing with different settings of the parameters T1 to T4 and contextual conditions. These contextual conditions (e.g. web browsing over fast or slow networks, browser cache on or off, etc.) affected the maximum session time in which the same webpage was retrieved. Initial values were chosen to be 6s and 60s, indicating web browsing over a fast network and a slower network respectively. The outcome of the experiments showed clearly that the perceived quality goes down linearly with the logarithm of the session time, where the perceived quality is expressed in a Mean Opinion Score on an absolute five point scale, ranging from MOS 1 “bad”, … to MOS 5 “excellent”.
We will here consider high speed access and we will use the model from [QoS1] in the 6 s context. The result of the test is a MOS score for the perceived QoS of web browsing and will be denoted as **WEB_MOS**. It should be noted that this test is an end-to-end test, which takes into account the effects of processing time at the server side, the network latency and the processing time at the client side.

In order to determine throughput we will use two different approaches.
In the first approach we will use a network monitoring tool that can monitor directly the throughput of a TCP connection, such as Iperf, see [QoS12]. For the second approach we monitor network parameters and then, by also taking into account TCP parameters, calculate the throughput by means of the analytical TCP model of Padhye et al [QoS13].

The throughput will be determined in both uplink and downlink directions. The reason for also taking the uplink direction into account is the popularity of peer-to-peer applications. Because the throughputs are obtained in two ways we obtain four values which will be denoted by **T_up_monitor**, **T_up_model**, **T_down_monitor** and **T_down_model**.

3.6.3 Test specification at application layer

In this section we describe in more detail how to perform the measurements. We will start with the web browsing case. Before the measurements are done, it is essential to check the following settings in the browser application: cookies enabled/disabled, caching enabled/disabled, other network related aspects e.g. proxy server connection enabled/disabled. These settings, when enabled will allow for a much faster retrieval of the content than could be expected on the basis of the underlying network characteristics.

3.6.3.1 Web browsing

The architecture for the test consists of a client PC with a web browser connected to a web server, see Figure 3-15. The parameters that need to be measured are the time parameters T1, T2, T3, T4, which can then be mapped to the perceived browsing quality according to [QoS1]. All measurements are done at Side A.

The test specification starts by starting the browser and then typing a URL. After the URL is typed and the enter button or the "go" button is pressed two stopwatches are started: the first stopwatch measures T1 and the second measures T2. The latter time can be related to the text "done" appearing on the status bar of the browser. The same is done for the second page, measuring T3 and T4. In the test the second page may be obtained by clicking a link on the first page. This procedure is repeated ten times to be able to deal with variations in these times due to variability in network behaviour. The next step is to calculate the average values of T1..T4 which will be denoted as $\overline{T1}$ .. $\overline{T4}$. Then the weighted session time needs to be determined, which according to [QoS2] defines as

$$WST = 0.47 * \overline{T1} + 0.60\overline{T2} + 0.71 * \overline{T3} + 2.22\overline{T4}$$

Finally the perceived QoS for the web browsing session satisfies

$$WEB_MOS = 4.38 - 1.30 * \ln(WST) .$$

It should be noted that a method for automatically measuring T1 .. T4 is currently under construction.

3.6.3.2 Downloads

For (large) downloads we will conduct throughput measurements.
Iperf [QoS12] is a benchmarking tool for TCP/IP networks that can be used to measure various aspects of network performance. This tool was developed by the National Laboratory for Applied Network Research (NLANR). We will use Iperf to measure TCP bandwidth.

In order to run the test Iperf needs to be installed both at the client side and at the server side. In addition, we also install the front-end that can be downloaded with Iperf, the GUI Jperf.

A fundamental tuning parameter for TCP is the maximum TCP window size W_{max}. The theoretical value to use for this is the bandwidth delay product:

BD = bottleneck bandwidth * RTT

The bottleneck bandwidth is obtained through measurement reported in a previous section. The RTT will be estimated by the use of a PING.

Denoting the maximum window sizes of the client and the server by $W_{max,C}$ and $W_{max,S}$ respectively, we choose the following value

W_{max} = min{BD, $W_{max,C}$,$W_{max,S}$}.

For our experiment we measure the bandwidth for a TCP based download of a large file, say of size 100MByte.

The measurement is initialized through Jperf. For an example of this GUI see Figure 3-16.

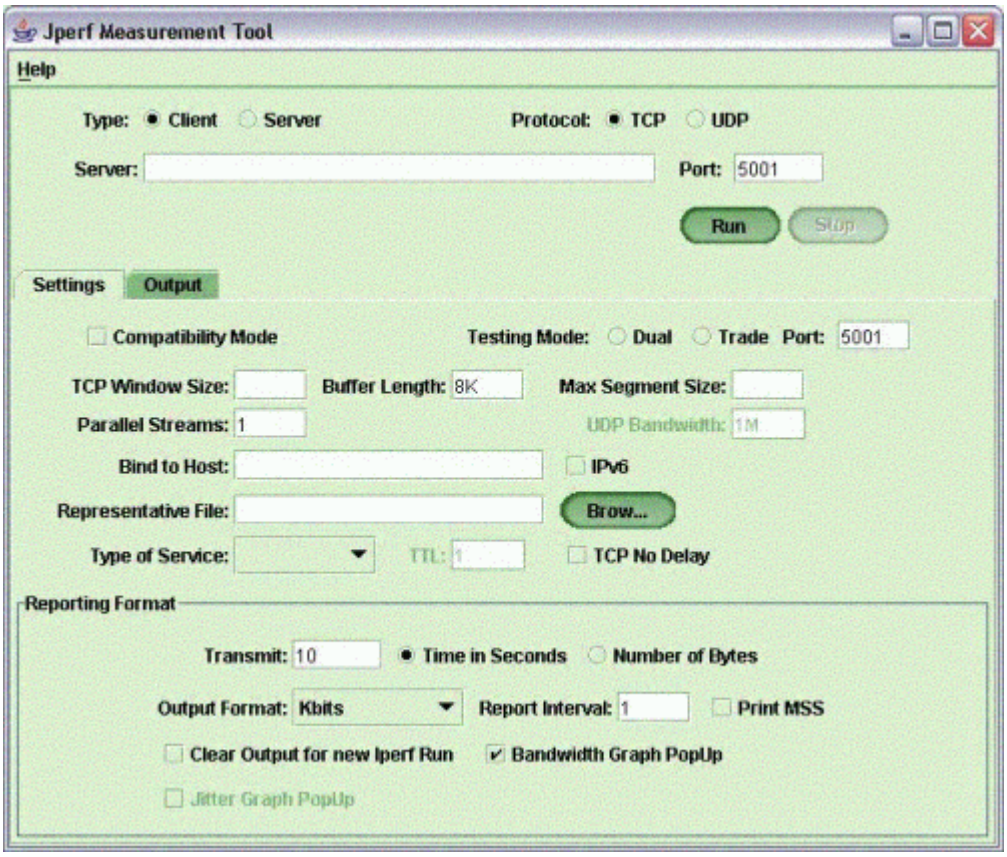


Figure 3-16: Jperf GUI

The exact settings that need to be chosen within Iperf is a subject that is still under study in WP C4. Anyhow, the outcome of the measurement is the measured downlink TCP throughput, which will be denoted as **T_down_monitor**.

Because we want to monitor the TCP bandwidth in both directions, we need to repeat the experiment where the role of client and server is exchanged. This will result in the measured uplink TCP throughput, which will be denoted as **T_up_monitor**.

3.6.3.3 Summary of tests at application layer

The ultimate result of this section is the completion of Table 3-8 and Table 3-9.

Name	Description	Unit	Value
T1	Response Time 1	sec	
T1 + T2	Download Time 1	sec	
T3	Response Time 2	sec	
T3 + T4	Download Time 2	sec	
$\overline{T1}$	Mean Response Time 1	sec	
$\overline{T2}$	Mean Data Transfer Time 1	sec	
$\overline{T3}$	Mean Response Time 2	sec	

Name	Description	Unit	Value
$\overline{T4}$	Mean Data Transfer Time 2	sec	
WST	Weighted Session Time	sec	
WEB_MOS	Perceived QoS web browsing	MOS	

Table 3-8: Results of tests at application layer for web browsing

Name	Description	Determined by	Unit	Value
Bb_down	Bottleneck bandwidth downlink	Side A	Mbps	
bb_up	Bottleneck bandwidth uplink	Side A	Mbps	
RTT	Round Trip Time	Side A	ms	
$W_{max,C}$	Max window Side A	Side A	KByte	
$W_{max,S}$	Max window Side B	Side B	KByte	
BD_down	Bandwidth delay product downlink	Side A	KByte	
BD_up	Bandwidth delay product uplink	Side A	KByte	
$W_{max,down}$	Max window downlink	Side A	KByte	
$W_{max,up}$	Max window uplink	Side B	KByte	
T_down_monitor	TCP throughput downlink	Side A	Mbps	
T_up_monitor	TCP throughput uplink	Side B	Mbps	

Table 3-9: Results of tests at application layer with respect to throughput

3.6.4 Test specification at network layer

At the network layer we will only conduct a test with respect to throughput. An alternative to the approach used in the previous section is by measuring the relevant network parameters and map those to the TCP throughput.

Padhye et. al. [QoS13] present a generic formula for TCP throughput. We propose to use a simplified approximation of this formula:

$$Throughput \approx \min\left\{\frac{W_{\max}}{RTT}, \frac{MSS}{RTT\sqrt{\frac{2bp}{3}} + T_0 \min\left(1,3\sqrt{\frac{3bp}{8}}\right) p\left(1+32p^2\right)}\right\}$$

where

W_{max} :the maximum TCP Window,
RTT: round trip time
MSS: maximum segment size
b: number of packets that are acknowledged by an ACK message,
T_0 :the period of time the sender waits before a packet is retransmitted,
p: packet loss probability.

It is shown in [QoS13] that the above formula is accurate for large file downloads.

In order to apply the throughput formula we have to obtain values for all six parameters. We again use Iperf for a TCP based download of a file of size 100MByte. The exact settings that need to be chosen within Iperf is a subject that is still under study in WP C4. The MSS can be set in the Jperf GUI, see also Figure 3.16. From the Iperf output we can obtain values for RTT and p. Using the method described in the previous subsection we can obtain W_{max}. The parameter b needs to be obtained from the TCP settings at the client. For the Retransmission Timer T_0 we use the heuristic suggested by [QoS14], i.e. $T_0 = 4$ RTT.

The experiment will be performed both in the downlink and the uplink direction. The throughputs thus obtained will be denoted as **T_down_model** and **T_up_model**, respectively.

3.6.4.1 Summary of tests at network layer

The ultimate result of this section is the completion of Table 3-10.

Name	Description	Determined by	Unit	Value
RTT	Round Trip Time	Side A	ms	
$W_{max,down}$	Max window downlink	Side A	KByte	
$W_{max,up}$	Max window uplink	Side B	KByte	
MSS	Maximum Segment Size	Side A	Byte	
p_{down}	Packet loss probability downlink	Side A	-	
p_{up}	Packet loss probability uplink	Side B	-	
b_A	# packets ack'd per ACK Side A	Side A	-	
b_B	# packets ack'd per ACK Side B	Side B	-	
T_down_model	TCP throughput downlink	Side A	Mbps	
T_up_model	TCP throughput uplink	Side B	Mbps	

Table 3-10: Results of tests at network layer

3.7 Interactive gaming

3.7.1 Perceived QoS for Interactive Gaming

Interactive Gaming has taken an enormous flight since the Internet enabled gamers to play over a globally accessible network. A number of factors contribute to this explosive growth of online gaming, of which the ongoing penetration of broadband connections and the expansion of online console platforms are only two [QoS27].
Increasingly, gaming looks to be one of the mainstay applications that help to strengthen retention and loyalty of high-speed Internet consumers. By providing a superior gaming experience that produces reliable performance, broadband operators can likely retain relationships for years with the next generations of customers [QoS28].

The main goal of this section is the description of an end-to-end quality measurement method that allows us to quantify the perceived quality of Interactive Gaming.
In this section we will only consider so-called First Person Shooter (FPS) games, in particular Quake IV. The reason that we only consider FPS games is that it is well-known that others gaming categories like Real Time Strategy and Massive Multiplayer Online Role Playing games pose less stringent requirements to the underlying network.

3.7.2 Test methods

Many papers investigate the impact of delay, jitter and packet loss on gameplay for FPS games, see [QoS29] and its references. Most of these works have focused on network performance metrics that game players can tolerate. However, some papers also deal with subjective experiments, and quantify the relation between network characteristics (i.e. delay and packet loss) and perceived QoS.
We have also conducted subjective experiments in order to assess user perceived quality as a function of the network parameters, see [QoS29]. Our approach is novel in the following respects; at first, we construct a model for the prediction of the experienced gameplay that depends on more than one network parameter simultaneously. Secondly, we introduce the approach of relating measured network impairment to perceived QoS, instead of using the a-priori impairment values of the configured network emulator. And last, we suggest an objective measurement method for determining the network impairment.

Based upon the data of the subjective experiments we have constructed a mapping between the perceived QoS (expressed as a Mean Opinion Score (MOS), see [QoS21]) and network parameters ping, jitter and packet loss.
We call the obtained model the G-model, analogous to the VoIP speech quality prediction model (E-model) [QoS19].

Our model was initially only based upon subjective measurements for Quake IV. We have chosen to use Quake IV for this user experiment, because it is one of the newest First Person Shooters on the market and has (by our knowledge) not yet been used for research purposes. However, afterwards, we have done additional subjective tests and double-checks with the literature, for additional FPS games such as Quake III, Unreal Tournament, Counter Strike, Halo etc. Our finding was that our G-model can be used to produce a well-founded lower limit of gaming quality. If our model predicts a certain MOS value then the quality of games other than Quake IV will likely be the same or better (again expressed in MOS).

We will describe our G-model in Section 3.8.4.

3.7.3 Test specification at application layer

The only tests available at the application layer are subjective tests. To assess the perceived quality one could ask a test panel to score the quality according to the ITU-T ACR scale, see [QoS21]: 5: *Excellent gaming quality*, 4: *Good gaming quality*, 3: *Fair gaming quality*, 2: *Poor gaming quality*, 1: *Bad gaming quality*. We recommend the use of this method in addition to the objective measurement that will be described in the following section.

3.7.4 Test specification at network layer

The architecture for the test is depicted in Figure 3-17.

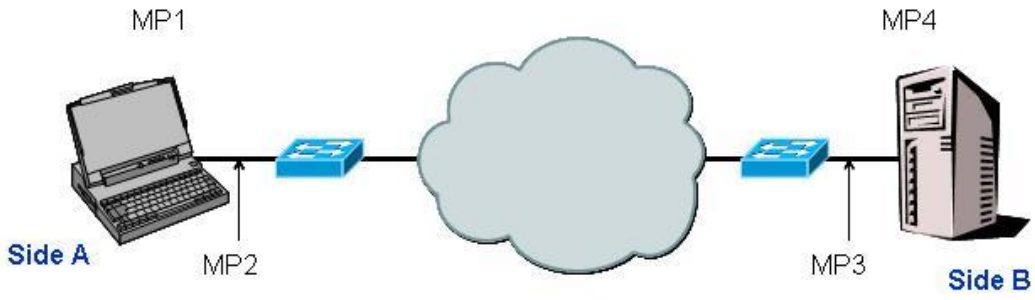


Figure 3-17: Architecture of Gaming test

Our method, which is described in detail in [QoS29], consists of a mapping relating network parameters to user perceived quality expressed as MOS.

In the first step we measure the network conditions by using a variant of the Chirp method [QoS30].

First 100 standard pings (ICMP Echo Request) are sent from the client (Side A) to server (Side B) and vice versa. The average value over these 200 pings gives the ping_average value in ms. Secondly, a series of 300 UDP packets is sent from client to server and vice versa. The UDP packet size including UDP and IP header is 100 bytes. Each UDP packet is sent 50 ms after the other. At the receiving side the transmission time of each UDP packet from sender to receiver is logged. The transmission time of the fastest UDP packet is shifted to 0 ms, after which all shifted transmission times are averaged. This is done for both directions and the average of these is called jitter_average.

Multi-dimensional regression analysis, see [QoS29], shows that the network impairment *X* is given by the following equation:

$$X = 0.104 * ping_average + jitter_average$$

Finally, the mapping for MOS values is given by:

$$MOS_{gaming} = 0.00000587\ X^3 + 0.00139\ X^2 - 0.114\ X + 4.37.$$

Note that the above mapping defines our G-model.

The ultimate result of this section is the completion of Table 3-11

Name	Description	Determined by	Unit	Value
ping_average	Round Trip Time	Side A/ Side B	ms	
jitter_average	Delay Variation	Side A/ Side B	ms	
X	Network Impairment	Side A	-	
MOS_{gaming}	Perceived QoS Gaming	Side A	-	

Table 3-11: Results of tests at network layer for Interactive Gaming

3.8 Annex to Chapter 3: Sending and capturing streaming video

This is a detailed step by step description on how to send and capture video over a network link. The selection of software is a specific choice, but there might be other software that could perform these steps equally well. The examples given are from a Windows environment, but Linux could also be used for most of these programs.

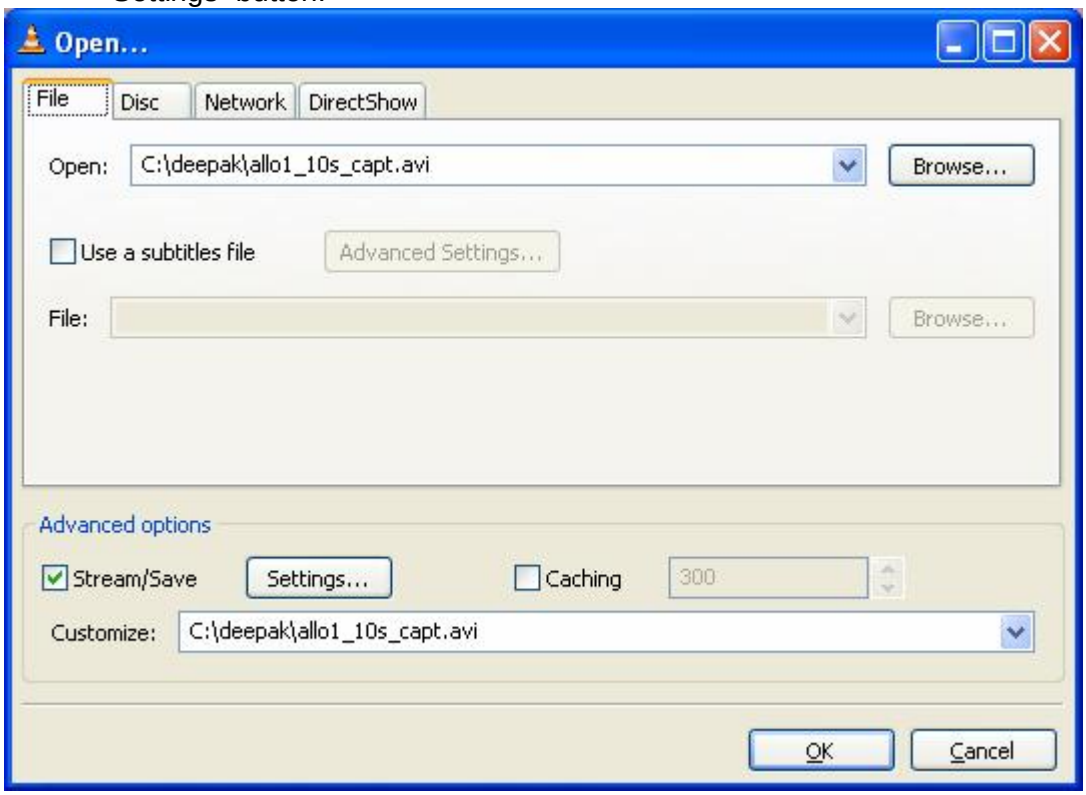
3.8.1 Sending and receiving video

Start VLC Media Player (www.videolan.org). You will get the following window.



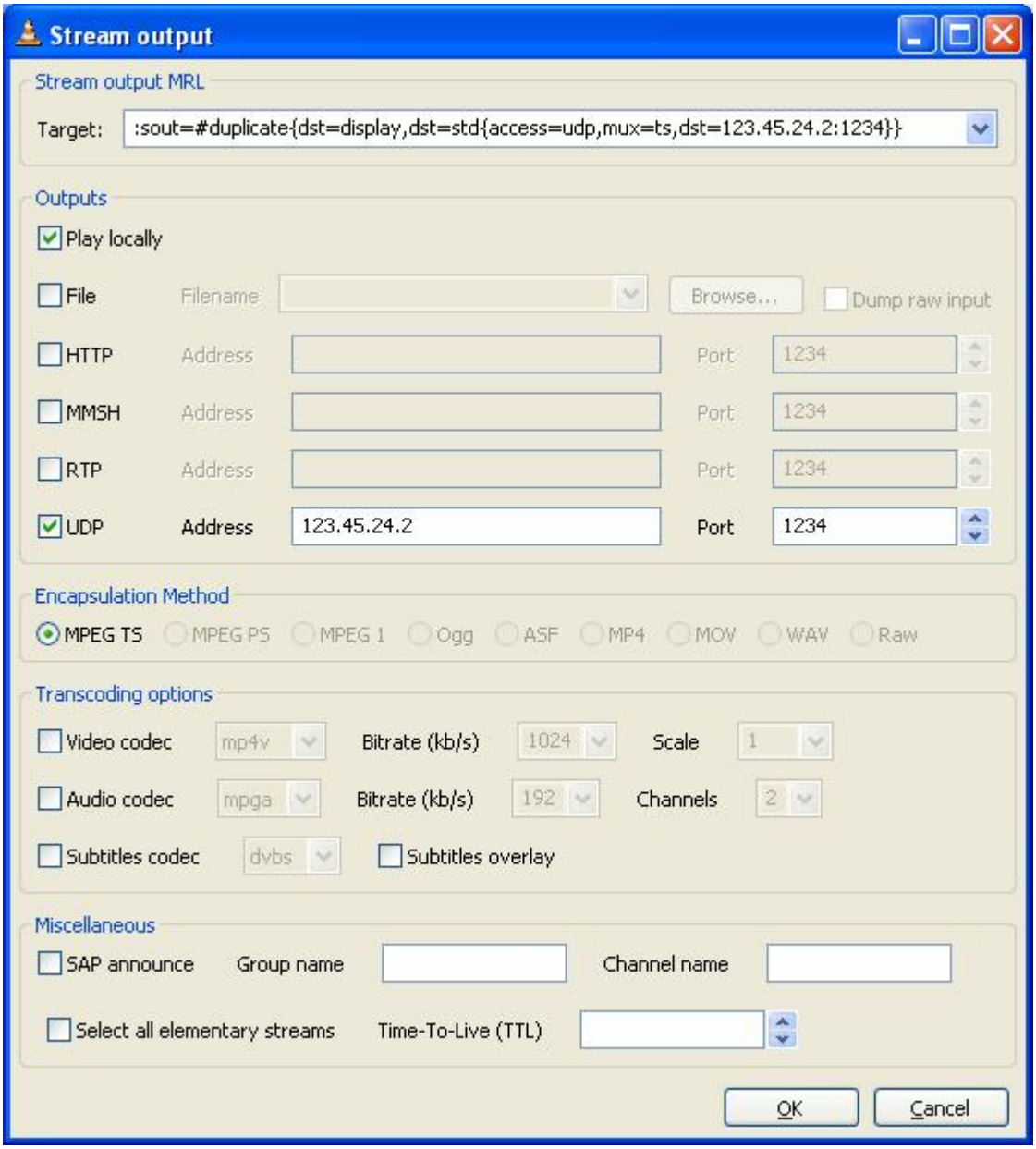
3.8.1.1 Sending

1. Open a video file by using “Open File” command in the “File” menu. (It is also possible to run directly from a DVD.
2. At the lower left in “Open file” dialog, check “Stream/Save” and then push the “Settings” button.



3. Mark UDP or RTP and set either an unicast (the IP address of the receiving system) or multicast address, as well as port number.
4. If the output should be saved, then the archive tick box should be checked and output file name given. This will store the sent video stream.

5. The container format should be selected. For IP-TV MPEG TS should be used. The video stream could be transcoded if needed



3.8.1.2 Receiving

1. For the receiver side start VLC.
2. In the “File” menu select “Open Network Stream” If it an unicast transmission then just select “UDP/RTP” and give the port number. For a multicast transmission the multicast address must be given as well.
3. Click “Stream output” then click “setting...”.
4. Tick File and select a file name. This will store the MPEG TS stream.

3.8.1.2.1 Analysing with VQM

To use VQM the stored video streams need to be decoded and stored in a suitable format that VQM could read. The decoding is here done with the freeware Mplayer (/www.mplayerhq.hu). VirtualDub (www.virtualdub.org), also freeware, is used to convert the data into avi-format, which VQM could read.

3.8.1.2.2 Decoding with Mplayer

MPlayer can store the images it is about to display in some formats, unfortunately not any format that VQM can read directly. The selected format here was chosen, so that there would be no colour space conversion when converting it to avi and that there is support for it in VirtualDub. The selected format is the Targa file format (tga) 24 bits rgb or bgr as it is specified for the Targa format. The steps are as follows:

1. The Mplayer works in DOS.
2. Type *mplayer –vo tga –vf format=bgr24 filename*
3. Filename is in our case the file that was stored by VLC. Note, that the output file from this operation will be much larger, than the input, also there will be one output file per frame, so it could be a good idea to create a directory for each sequence.
4. Read the output files into VirtualDub. It is enough to open the first frame in the sequence. Check that the frame rate will be correctly set.
5. Store it as avi.

3.8.1.2.3 Running VQM

VQM can be used for free for evaluation purposes. The software and a licence can be obtained from Institute of Telecommunication Science (ITS) of the National Telecommunications and Information Administration (NTIA) (www.its.bldrdoc.gov) in the U.S.A. The program would need two sequences as input one reference and one distorted in either in a 4:2:2 YUV (e.g. UYVY) format or avi containing rgb24 data i.e. each pixel has three bytes. Actually the avi format will be converted into YUV by VQM before the processing starts, which involves a colour conversion, so if the format before processing with VQM is in YUV it should not be converted to avi. For the actual use of VQM, please see the manual [QoS6].

3.9 Manual: iVQM_iptv HOWTO

This is a practical oriented how-to in using the iVQM for IPTV, for further information on usage of iVQM see [QoS5]. At the moment of writing of this document, the source code of iVQM can be obtained from www.Acreo.com.

3.9.1 Network architecture and hardware requirements

The iVQM_iptv monitoring system consists of two probes connected to the network, each on either side of the network link to monitor. One probe is connected close to the IPTV server, and is called the source probe. The other one is connected close to the end-user side of the network link, and is called the destination probe. The network architecture between the IPTV server and the end users is illustrated in Figure 3-18, with grey boxes symbolising routers and/or switches, and black arrows showing the flow of the IPTV stream. Blue arrows show the data exchange between the probes, taking place on the same network as the IPTV stream.

To ensure that the data exchange between the probes does not interfere with the IPTV service, it can be desirable to use a separate network link, for example using a VLAN with a lower priority or a physically separate link, as illustrated in Figure 3-19. In this HOWTO, we will consider that each probe has two network interface cards (NICs).

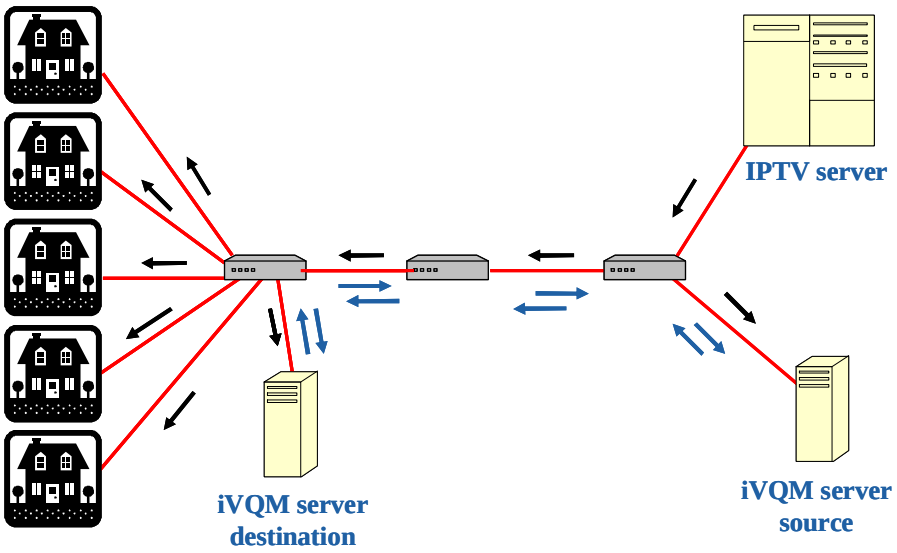


Figure 3-18: Network architecture of an IPTV delivery service, with service monitoring by two iVQM_IPTV probes. Data is exchanged between the probes using the same network link as the IPTV stream.

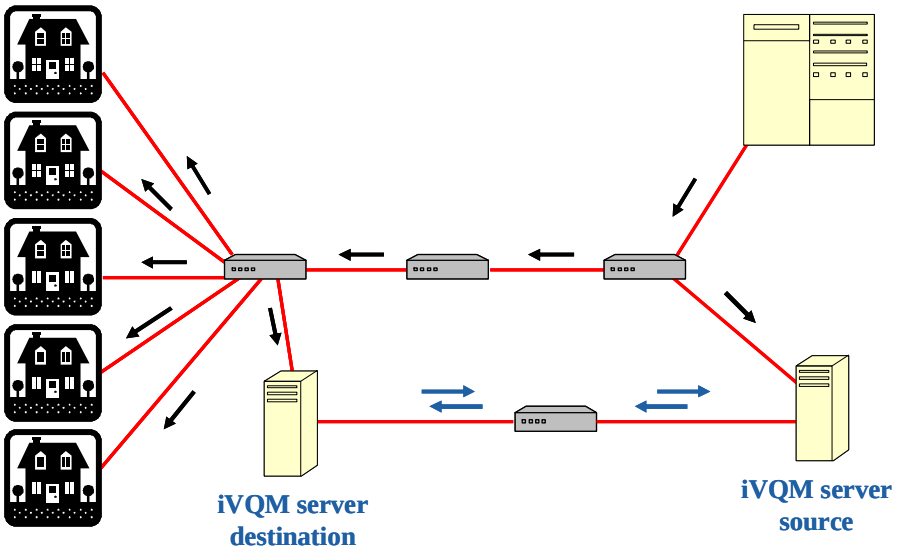


Figure 3-19: Network architecture of an IPTV delivery service, with service monitoring by two iVQM_IPTV probes. Black arrows show the IPTV stream Data is exchanged between the probes using a separate network link.

Each probe is a PC-compatible computer with the following characteristics:

- Operating system: **Windows 2000** or **Windows XP** (not tested with NT4 or Vista), fully patched but with automatic updates tuned off (Automatic updates install automatically, then reboot your computer, terminating the service).
- **2 NICs** (or one with VLAN support).

- At least **2GB** of memory
- At least **1GB** of free space on the hard disk drive.

3.9.1.1 System configuration

Configuring an iVQM_IPTV probe consists in setting up the network configuration properly, setting up shared space to allow the probes to exchange data, and installing the required software. iVQM can share data through two means: accessing to a shared Windows folder, or using an ftp server. In this HOWTO, we describe how to share a folder from one of the probes. If access to a shared folder on another computer or to an ftp server already exists, no folder needs to be shared on the probes.

3.9.1.2 Network configuration

We consider in this HOWTO that each probe contains two separate NICs, one for the IPTV stream and one for direct communication between the probes. We suggest the following configuration (should be adapted to the specifics of the network):

- The primary NIC is set-up according to the requirements of the network (dynamic IP address from a DHCP server or static IP address) and is used to access the IPTV stream.
- The secondary NIC should use a static IP address within a subnet **that is not used by the primary NIC**. Also, both probes should have their secondary NIC use the same subnet, so they can see each other. For example, if the subnet 192.168.17.x is does not exist fron the primary NIC's perspective, it can be used for the secondary NIC, with for example IP addresses **192.168.17.2** and **192.168.17.3** for the probes, and a netmask of **255.255.255.0**.
- To ensure that the multicast requests (for an IPTV channel) go out through the primary NIC, the secondary link should have a lower priority that the primary one. This can be achieved by using a slower link for the secondary NIC (by connecting the NIC to a slower switch than the primary NIC), or by changing the metric for the specific route. The metric is a value describing the penalty caused by using a given interface to access a network. The higher the metric, the larger the penalty. Metrics can be checked by using the *route* command at a command prompt, to list all locally-known destination networks, their netmasks, corresponding gateways, which local IP address they are accessed through, and what metric they have been affected:
  C:\> route print
  The metric for the destination network corresponding to the secondary NIC can be increased with the command route. For example, if we want to change the metric to 50 for the network accessed through NIC 192.168.17.2, we will use the command line:
  route change destination_address mask mask_address gateway_address metric new_metric
  C:\> route change 192.168.17.0 mask 255.255.255.0 192.168.17.2 metric 50
  Please note that this configuration disappears when the computer is restarted!

If the shared data is accessed though the same NIC as the IPTV stream, only one NIC needs configuring and there are no issues with network metrics. If, instead, two separate networks are accessed through the same NIC using VLANs, the same procedure as for two separate NICs is used to set the metric, one the VLANs are configured. VLAN configuration is outside the scope of this document.

Once the Network is configured for both probes, it is time to choose a way to share data between the probes. If no access to an external ftp server of shared Windows folder exists, one of the probes has to share a folder. This is done by choosing a folder to share on one of the probes, or creating a new one. Let us call this folder *iVQM_share*. With a right mouse-click on the folder, a menu appears. Choose the entry “sharing”, as shown on Figure 3-20 (left). A property window appears, as shown on Figure 3-20 (centre). Sharing is activated there, by choosing “Share this folder”. Clicking on the “Permissions” button opens the window shown in Figure 3-20 (right), where the “Read” and “Change” properties should be chosen.

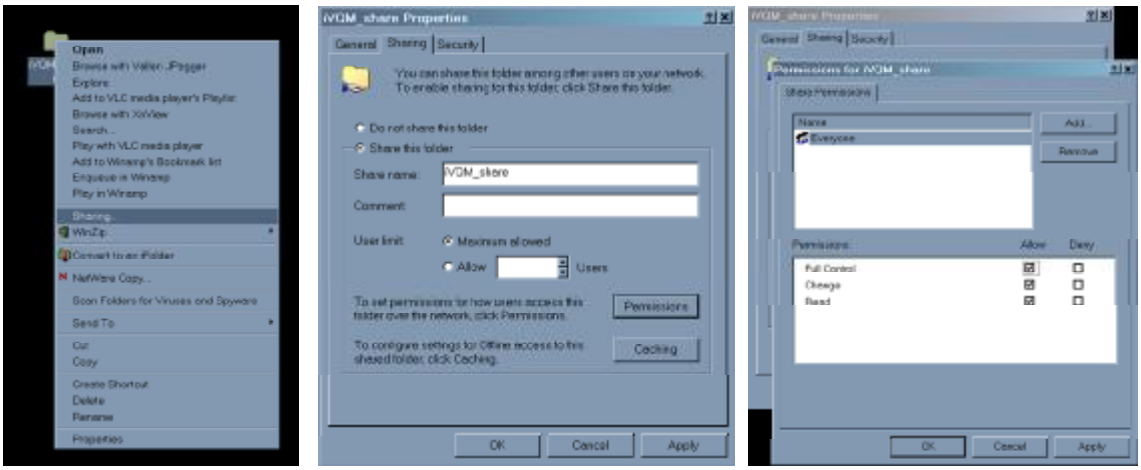


Figure 3-20: left: Menu appearing after a right click on a folder, showing that the entry "sharing" should be chosen; Centre: Folder sharing window, in which the folder sharing should be activated; Right: Window showing the permisssion settings for the shared folder.

3.9.1.3 Software installation

The Elecard MPEG player version 4.5 has to be installed on each probe. Some of the codecs from this player are used by the IPTVinterface module to handle IPTV streams. The player can be found at www.elecard.com. Note that the player has to be activated by purchasing a key. If run without activation, it adds artefacts to the video that will prevent iVQM_iptv from working properly.

The iVQM_iptv package comes as a zip file containing documentation (text and pdf files), the Matlab runtime environment (MCRinstaller.exe), the ivqm.exe executable and its archive file, ivqm.ctf.

If an older version of the Matlab Runtime environment is already installed on the system, it should be removed prior to any other action. Then, the Matlab Runtime environment provided with iVQM_iptv should be installed (by double-clicking on MCRinstaller.exe).

Installing iVQM_iptv itself is just a matter of copying the relevant file (ivqm.exe, ivqm.ctf and the documentation files) to the appropriate folder (for example: C:\Program Files\Services\ivqm_iptv).

3.9.2 Monitoring with iVQM_iptv

3.9.2.1 Starting iVQM_iptv

To start ivqm, double click on ivqm.exe. The window shown in Figure 3-21 appears. The user provides the probe location (source or destination of the IPTV stream) and defines one probe as master an the other one as slave. It is recommended to choose the more powerful computer as master.



Figure 3-21: Start window of iVQM_iptv, in which the user selects 1) the probe location (source or destination) and 2) whether the probe is master or slave.

After the user has clicked on “Start”, the configuration window appears. It is not identical for the master and slave probes (the master probe requires more information). The configuration window for the master probe is shown in Figure 3-22. The data exchange scheme between the probes is chosen in the “end-to-end communication medium” area, where “Shared directory” and “ftp server” can be chosen. In the figure, a shared directory named *IVQM_share* on computer named *IVQM_source* was chosen.

The “Video source” is the place where the IPTV interface module of a computer-connected TV card can be selected. Using IPTV, the IP address and port of the TV stream are required, in the form *IPaddress:port*.

In the calibration area, the expected delay between the source and destination streams can be adjusted. If iVQM_iptv complains about the delay being close to the range limit during monitoring, increase the “combine temporal registration uncertainty.

Finally, the video quality model has to be chosen. To find out the differences between the proposed models, please refer to the iVQM manual. A video sequence length of 10 seconds is chosen by default. It may be needed to decrease it if the memory consumption is too high (resulting in iVQM_iptv failing to record sequences and stopping monitoring). The maximum sequence length depends on the amount of memory in the probe and the bandwidth of the **uncompressed** stream.

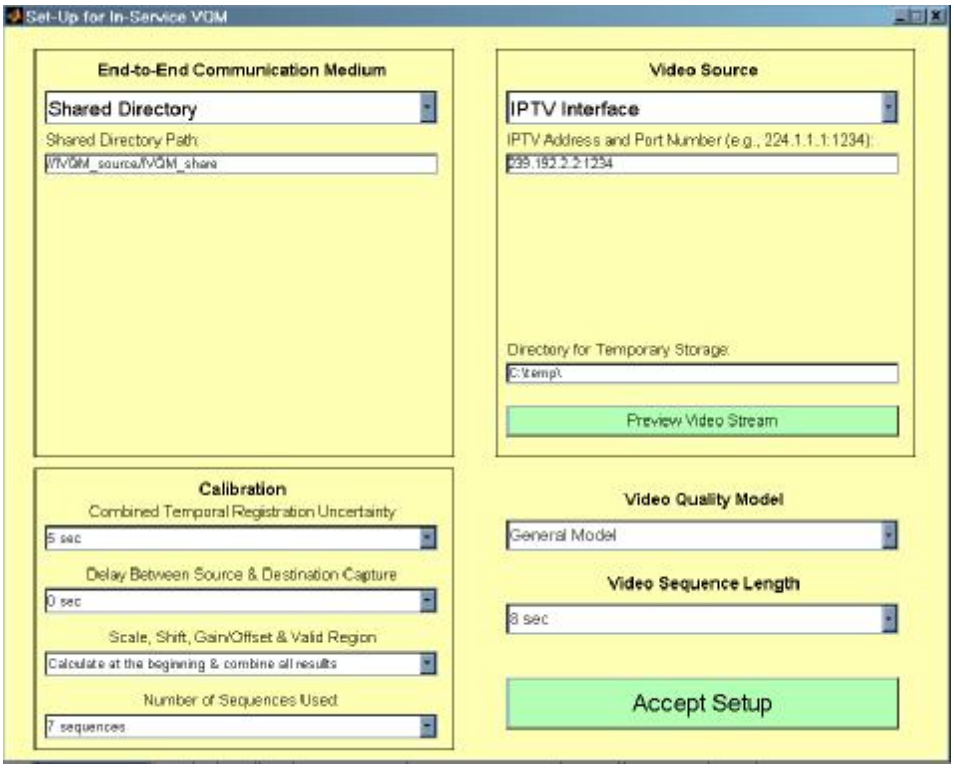


Figure 3-22: Configuration window for the master probe.

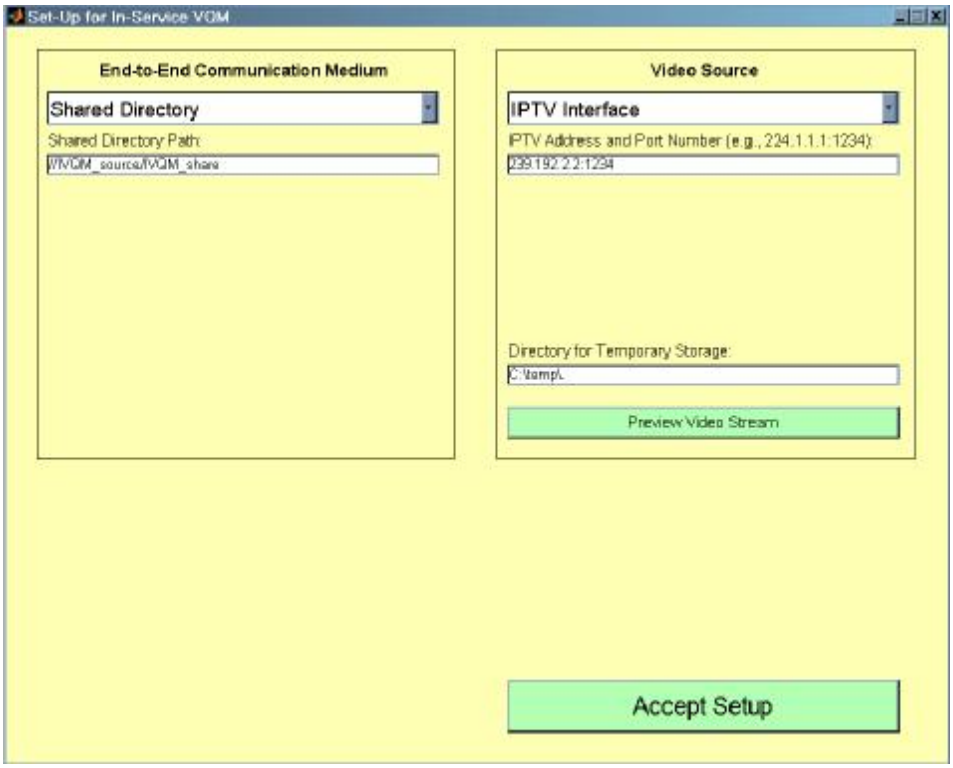


Figure 3-23: Configuration window for the slave probe.

The configuration window for the slave probe is shown in Figure 3-23. It contains only communication parameters. Once the configuration window is filled properly, press “Accept setup”. The probe then shows the monitoring window, initialises the IPTVinterface module and checks that the IPTV stream is available. Monitoring windows for the master and slave probes are shown in Figure 3-24 and Figure 3-25 respectively.

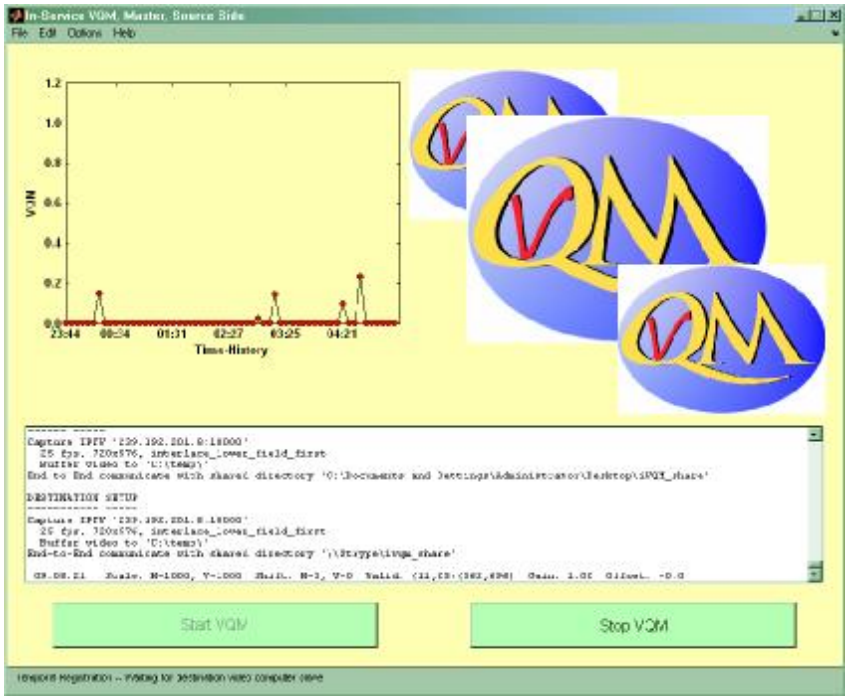


Figure 3-24: iVQM_iptv monitoring window for the master probe.

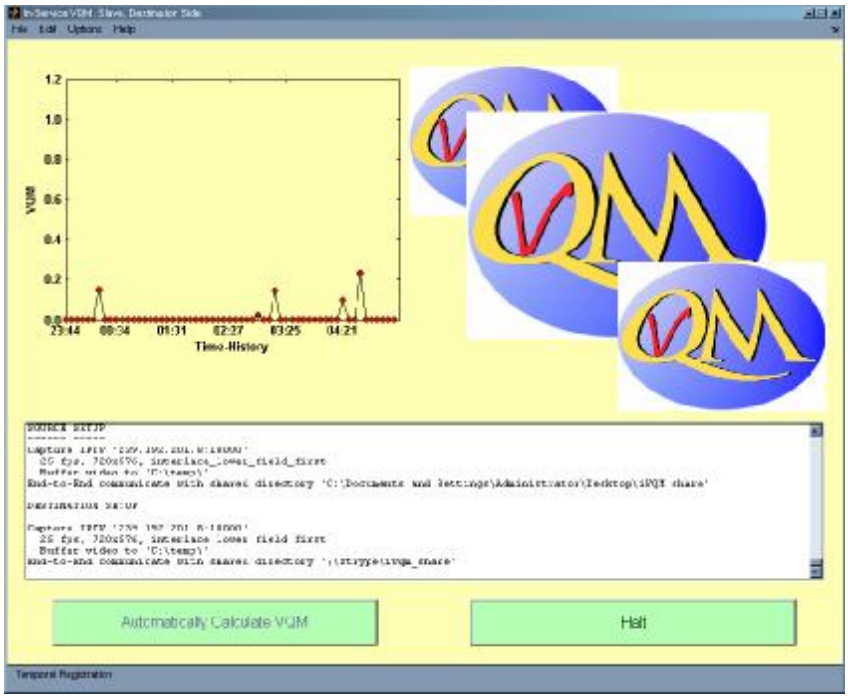


Figure 3-25: iVQM_iptv monitoring window for the slave probe.

Both probes are now configured. To start monitoring, press “Start VQM” on the master probe, and “Automatically calculate VQM” on the slave probe. When both probes are started, they synchronize and monitoring begins. Each probe outputs logs in the log-area of the window, and the VQM value is plotted as a function of time. During frame-grabbing, a separate window on each probe displays the sequence being grabbed.

3.9.2.2 Troubleshooting

Here is the description of some common error situations that can be encountered when using iVQM_iptv, how to identify and solve them.

- If a configuration parameter is wrong in the configuration window, iVQM will complain about it, and tell you what the problem is (for example, if the shared directory path cannot be found, or if the IPTV address and port entry is not in the right form). For more information, you can refer to the iVQM manual.
- If, after pressing “Accept Setup”, nothing happens in the configuration window and the console window shows complains that it is *unable to open VQM_video.avi*, then the IPTV stream could not be found. The reason for the failure can generally be found by looking at the logfile of the IPTVinterface module, named *iptvdebug.txt* and located in the same directory as the ivqm executable. The most common errors are:
  - IPTVERROR_PINOUT_SYNC, which means that the IPTV stream could not be found. This can be due to your firewall forbidding iVQM_iptv from accessing the stream, because the stream is not available at all, or because the multicast stream is not requested to the right NIC (see paragraph on network configuration in this document)
  - IPTVERROR_FILTER_NETWORK, which means that the video codecs could not be found: the Elecard MPEG video player is not installed properly on the computer.
  - A memory allocation error (unlikely during initialisation, but more likely during monitoring): the IPTV module could not allocate the memory buffer necessary to store the uncompressed sequence. Add more memory to the probe, or close all other programs running on that computer.
- It can happen that the probes start monitoring, and after some time one of them stops with and “Out of memory error” in the log area of the monitoring window. It can be due to a failure of iVQM_iptv to allocate memory during the sequence analysis, but it is usually the sign that the recording of an IPTV sequence failed. The reason for the failure can be found by looking at the *iptvdebug.txt* logfile, as described in the previous point. It will usually be due to one of the two reasons:
  - The IPTV link was unavailable at some point in time (the IPTVERROR_PINOUT_SYNC error), in which case it is usually sufficient to push the “Start VQM” or “Automatically calculate VQM” button to resume monitoring, provided that the IPTV stream is available again;
  - The memory allocation failed. Resuming monitoring will usually work without having to reboot the probe (Windows sometimes needs a laps of time after memory has been released by a process, before it is available to another one), but if the problem happens too often, you might want to consider:
    - Increasing the amount of memory in the probe; or
    - Decreasing the memory need, by recording shorter sequences (see the configuration window of the master probe).

3.10 References

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

[QoS1] ITU-T Rec. G.1030, “Estimating end-to-end performance in IP networks for data applications”, prepublished recommendation, November 2005.

[QoS2] ITU-R Rec. BS.1387, “Method for Objective Measurements of Perceived Audio Quality,” International Telecommunication Union, Geneva, Switzerland, 1998.

[QoS3] 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”, Com 12-C19 –E, Contribution to ITU-T SG12, July 2005.

[QoS4] 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.

[QoS5] 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.

[QoS6] 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.

[QoS7] 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

[QoS8] D. S. Hands, “A basic Multimedia quality model”. IEEE Transactions on multimedia, Vol. 6, No. 6, December 2004, pp. 806-816

[QoS9] 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.

[QoS10] ITU-R Rec. BT.1359-1: Relative timing of sound and vision for broadcasting

[QoS11] 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.

[QoS12] Iperf Version 2.0.2, http://dast.nlanr.net/projects/Iperf/

[QoS13] 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

[QoS14] V.Paxson, M.Allman, Computing TCP’s Retransmission Timer, Internet Archives RFC 2988, November 2000

[QoS15] ITU-T Y.1541, “Network performance objectives for IP-based services”, 2001

[QoS16] 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)”

[QoS17] MUSE Deliverable DTF4.4, “Test Suite, part 1: Test objectives, Test Suite for Full-Service End-toEnd Analysis of Access Solutions”, Edited by R.F.M van den Brink, December 2006.

[QoS18] 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

[QoS19] ITU-T G.107, “The E-model, a computational tool for use in transmission planning”, March 2003 (revised version)

[QoS20] 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)

[QoS21] ITU-T Rec. P.800, "Methods for Subjective Determination of Transmission Quality", International Telecommunication Union, Telecommunication standardization sector, (1996)

[QoS22] 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)

[QoS23] 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)

[QoS24] ITU-R BT.500-11, "Methodology for the Subjective Assessment of the Quality of Television Pictures", International Telecommunication Union - Radiocommunication Sector, (2002)

[QoS25] ITU-T Rec. P.910, "Subjective Video Quality Assessment Methods for Multimedia Applications", International Telecommunication Union, Telecommunication standardization sector, (1999)

[QoS26] R.E. Kooij, O.K. Ahmed, K. Brunnström, “Perceived quality of channel zapping", Proc. Of Int. Conf. On Comm. Systems and Networks, August 26-28, Mallorca, Spain, 2006.

[QoS27] N. Shah, C. Haigh, “The video game industry, An Industry Analysis, from a VC perspective ", Hanover (NH), U.S.A., 2005.

[QoS28] Camiant, http//www.camiant.com/perspectives/gaming.htm

[QoS29] 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”, Proc. NetGames’06, Singapore, 30-31 October, 2006.

[QoS30] J.G. Beerends, J. M. van Vugt, “A data chirp measurement method for assessing end-to- end quality of data links”, Com 12-C11 –E, Contribution to ITU-T SG12, July 2005.

[QoS31] J.G. Beerends, J. M. van Vugt, “A combined subjective/objective test protocol for determining the end-to-end perceived quality of videophone links”, Com 12-C8 –E, Contribution to ITU-T SG12, June 2005.

4 SERVICE CONNECTIVITY TESTING

4.1 Introduction

In chapter 4 we will describe the E2E Connectivity Test Methods for the different E2E Connectivity Test Objectives that have been identified in the first part of this test suite (DTF4.1). Some of the Test Objectives have been grouped into one Test Method because they required the same setup, prerequisites and (almost) the same procedures.

In this document we continue to use the split-view approach for E2E connectivity testing as was introduced in DTF4.1.

The Test methods described in this section will focus on Functional and Performance tests of the access network. Many of the tests are described for an environment with some MUSE-specific elements. However, it is a simple task to adapt these tests to other networks with slightly different prerequisites.

Conformance tests are out of the scope of this part of the document. If the reader requires Conformance tests, he is referred to the standardization organizations who typically implement/describe some Conformance tests for the protocols/systems they standardize.

4.2 Tools

Many of the tests require several simultaneous data streams to be generated or consumed through the access network. One can use multiple PCs with a number of real users or simulated users. But the most efficient way to perform tests of this type is to use network traffic generation and measurement equipment that can simulate multiple users over multiple ports (individual or aggregated) and which is capable of emulating a part of a complex network (e.g. a whole PIM-SM domain). The tests presume the availability of such equipment although the tests are described in terms of individual testing elements (e.g. Host, Server, Background traffic, …)

4.3 High-speed Internet Service

For background information about the different services and why they were selected in the first place can be found in the E2E Connectivity chapter in DTF4.1.

4.3.1 Functional Tests

4.3.1.1 Auto-configuration Test

Objective: Verify the correct operation of the auto configuration of the High-Speed Internet Service.

See “Chapter 5” for details

4.3.1.2 Basic reachability Test

Objective: Verify that a basic form of connectivity can be established through the MUSE access network.

See “Chapter 5” for details.

4.3.1.3 Advanced reachability Test

Objective: Verify that the Access network is capable of giving access to higher layer services like web access.

See “Chapter 5” for details.

4.4 Performance Tests

Given that the High-Speed Internet Service only offers a best-effort service, we do not describe in this document any HSI specific performance tests.

For generic performance tests see the “Chapter 5” tests in this document.

4.5 Multicast Streaming Service

4.5.1 Functional Tests

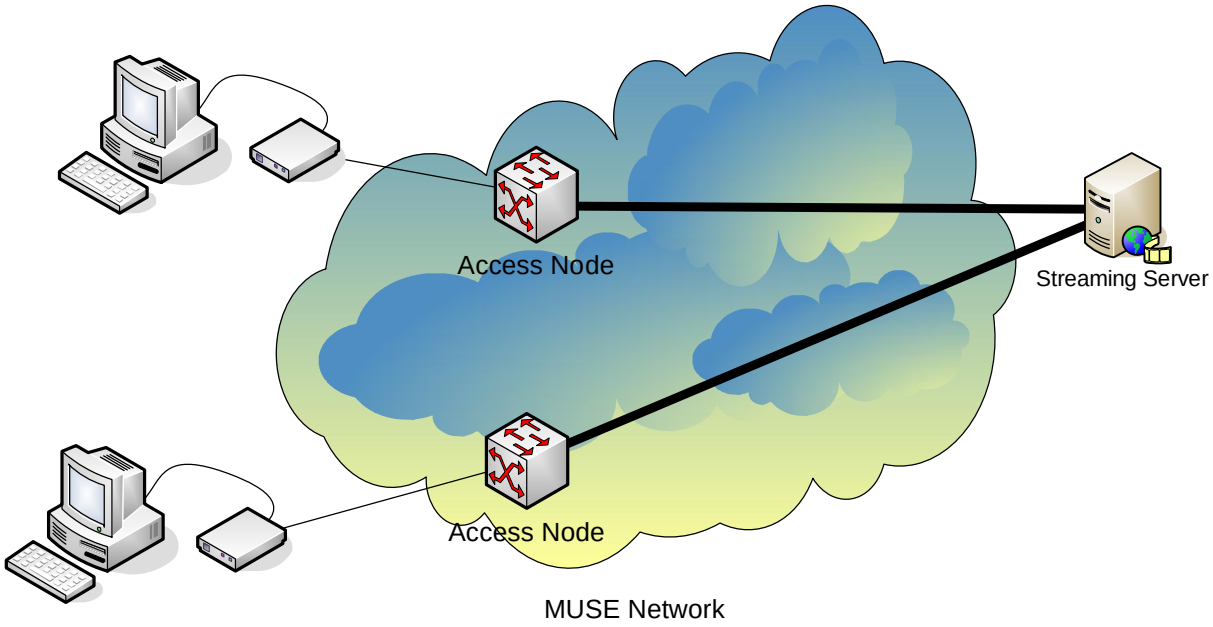


Figure 4-1: IP Multicast Streaming with content injection at the access node

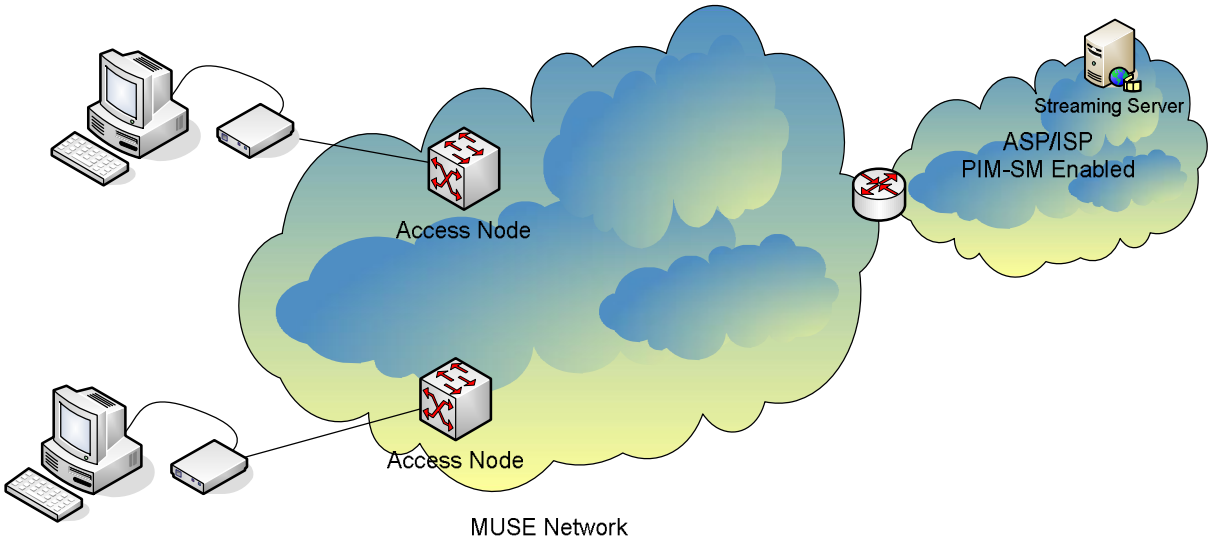


Figure 4-2: IP Multicast Streaming with content injection at the ASP or ISP which is PIM-SM enabled

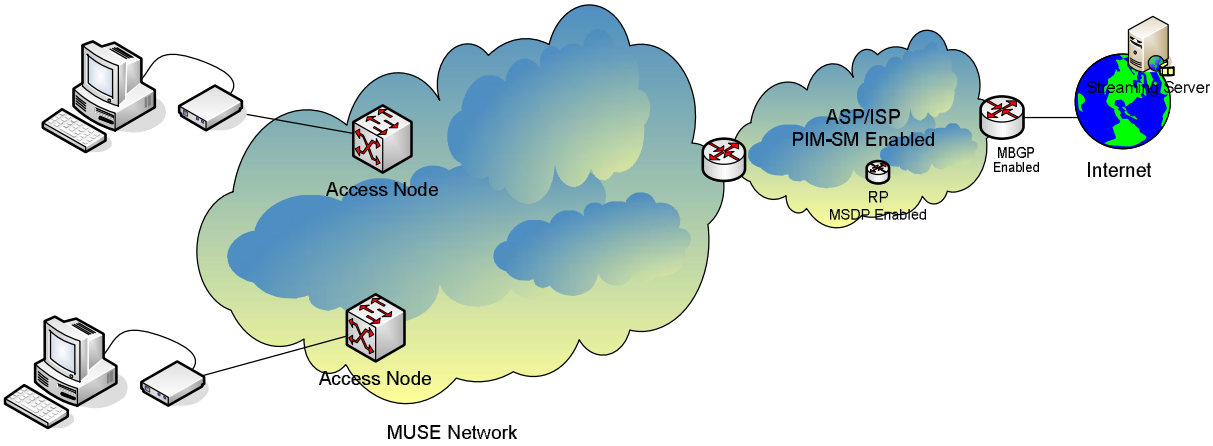


Figure 4-3: IP Multicast Streaming with content sourced from the Internet. This presumes an operational inter-domain multicast infrastructure

4.5.1.1 IP Multicast reception

Objective: Verify the reception of IP Multicast traffic originating form either the access network, ISP/ASP network or the Internet.

Setup: See Figure 4-1, 4-2 or 4-3 depending on the case one wants to test.

Prerequisites: The MUSE access network is optimized for the delivery of IP Multicast and supports ASM and/or SSM style of IP Multicast. Depending on the case one wants to test, the multicast RTP content is being injected either at the access/edge node(s), the ASP/ISP network or the Internet. The last two cases presume that the ASP/ISP network is routed and that they deploy PIM-SM. The case of content injected somewhere on the Internet presumes that the RP of the ISP/ASP was configured with MSDP and the BGP routers optionally have the multicast functionality of MBGP turned on. At each of the possible origination locations one has a Streaming Server (or equivalent emulation device) which is configured to stream in multicast to a fixed multicast channel. An associated media player application is installed and configured on the end-user machine.

Procedure: Launch the media application and provide it with the URL or parameters for it to join the multicast channel. Verify that the access networks delivers the stream using a protocol analyzer and verify that the application receives the stream and that it is capable of rendering the media stream. Verify that in the case of ASM where the host uses IGMPv3 with an include source list that only data for the specified sources is delivered. In the case of SSM verify that the delivered IP Multicast datagrams are only originating from the specific source.

Results: One should be able to watch/listen to the streamed content.

4.5.1.2 Packet loss and out-of-order delivery test

Objective: 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.

Setup: See Figure 4-1, 4-2 or 4-3 depending on the case one wants to test.

Prerequisites: The same prerequisites as in test 4.5.1.1.

Procedure: For this one can inspect at the receiving side the RTP sequence numbers of the received RTP packets that belong to the same Synchronization Source (SSRC). The latter assures that one inspects only packets that originate from the same source and that belong to either the audio or video stream when both are not multiplexed onto the same channel. A channel in this context is uniquely identified by the destination group address and destination port number of the packets. In order to receive IP multicast traffic one can use some media player like QuickTime or VLC. The streaming server needs to send out in RTP.

Results: For streams originating from within the MUSE access network and/or ISP network there should not be any packet loss and out-of order packet delivery.

4.5.1.3 NAT/Firewall traversal

Objective: assess the traversal of IGMP and IP Multicast datagrams through a NAT/Firewall if the access network/home network contains such functionalities.

Setup:

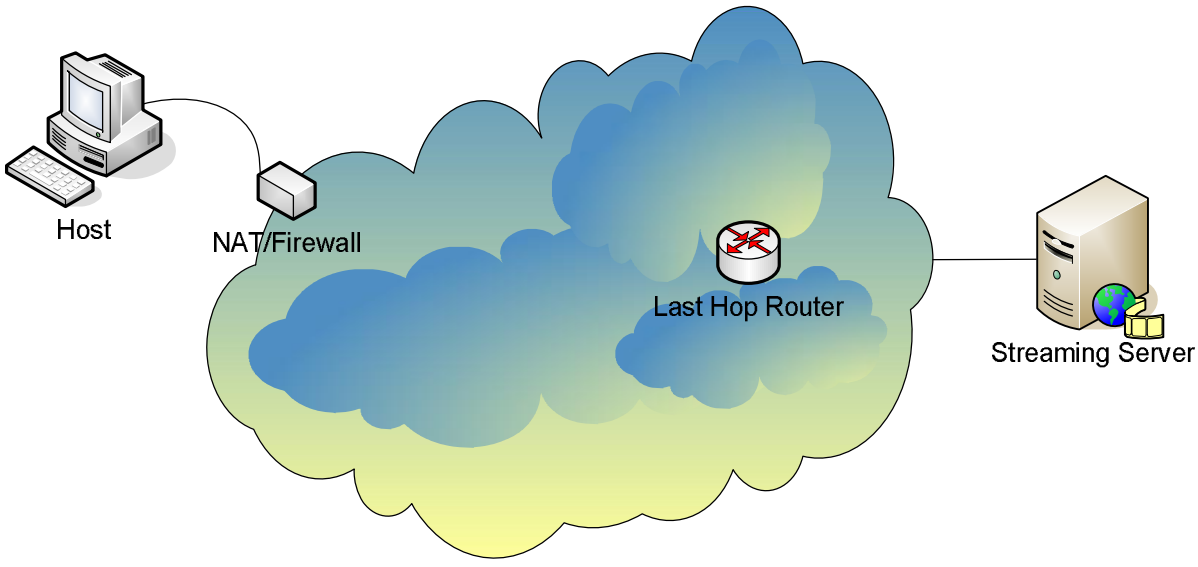


Figure 4-4: NAT/Firewall functional test

Prerequisites: The NAT/Firewall is configured for IP Multicast/IGMP traversal. The MUSE access and aggregation network is Multicast enabled (IGMP snooping/Multicast routing). There should be at least a Last Hop router in order to "terminate" the IGMP sessions. The streaming server (or traffic generator) can be configured to stream multiple RTP streams on different multicast channels. The host is fully (auto) configured.

Procedure: Use a testing application or a media application (QuickTime, VideoLan client, …) to join a sub set of the multicast channels being streamed. Additionally source from the host some IP multicast data (TTL > 1) on a different multicast channel.

Results: Verify that IP multicast traffic is received by the host and that the traffic is only from/for the joined channels. Verify that the data sourced at the Host is receivable at the streaming server or last hop router.

4.5.1.4 IGMP/MLD snooping test

Objective: Verify correct operation of the IGMP/MLDvx snooping functionality. I.e. Verify that only on the ports with hosts that joined a group address one sees IP Multicast traffic destined for that group address.

Setup:

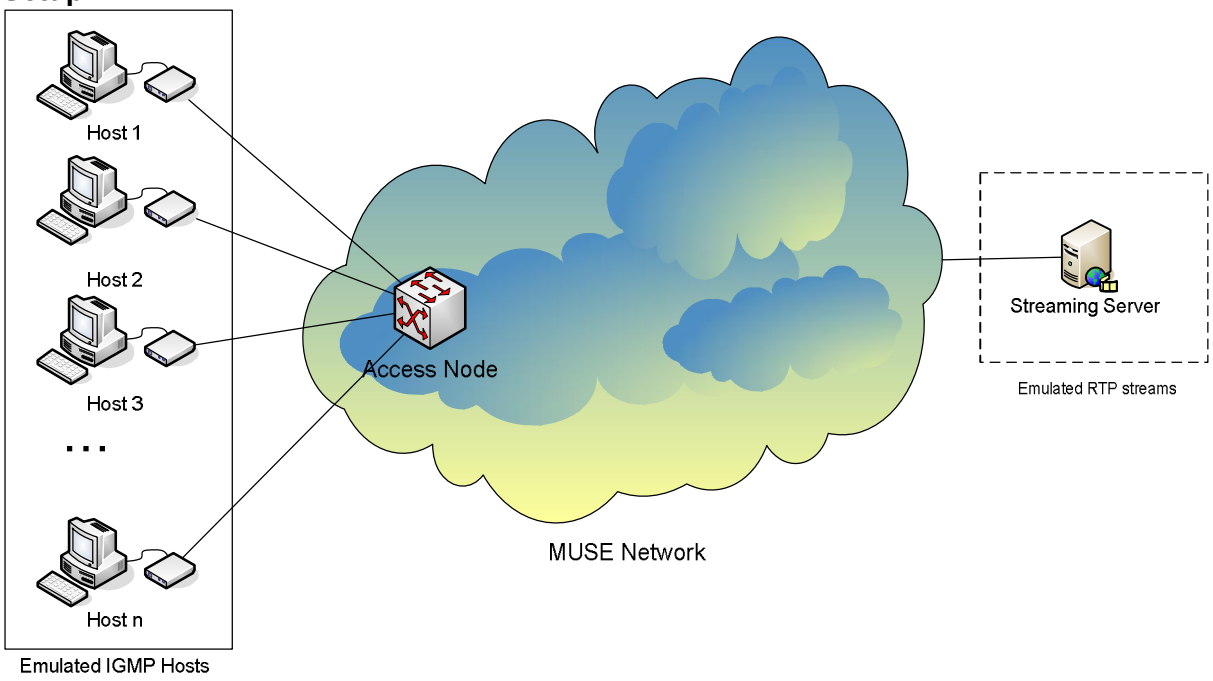


Figure 4-5: IGMP/MLD snooping test

Prerequisites: The MUSE access network is optimized and configured for IP Multicast operation. The access network and the host support the same version(s) of IGMP/MLD. The Streaming server sends multiple IP Multicast streams out.

Procedure:

Case 1: The Host 1 joins one channel and the hosts on all other ports do not join any multicast.

Case 2: The Host 1 joins one channel and the other hosts join a mix of other channels.

Results:
Besides the regular unicast and IGMP/MLD related multicast traffic one should only see the following traffic on the ports in each of the above mentioned test cases.

Case 1: The ports other then the one on which Host 1 is connected should not see any IP packets with destination address equal to the group address of the channel joined by Host 1.

Case 2: On each port one should only see IP Multicast traffic destined for the group address of the joined channel(s). Depending on the implementation in the Ethernet switches it is possible that due to the 32 to 1 mapping of IP Multicast addresses onto Ethernet Multicast MAC addresses that IP Multicast streams on consecutive addresses (within the same mapping) are all forwarded. Depending on the deployment scenario this can represent an issue.

4.5.1.5 IGMP version mix test

Objective: Verify that Hosts with different versions of IGMP can coexist on the same access network and that the Hosts are not switched back to the lowest IGMP version present on the access network.

Setup: See Figure 4-5.

Prerequisites: The MUSE access network is configured and optimized for IP Multicast. The Hosts 1, 2 and 3 respectively support IGMPv1, IGMPv2 and IGMPv3. The IP Multicast router (or BRAS) should be configured to use on all ports IGMPv3.

Procedure: Boot all the hosts and observe the IGMP interaction.

Results: verify that there is only an IGMP version fall-back on those ports where there is a host present with an IGMP version lower then the version of the IGMP querier (router). This fall-back should not go any further then the IGMP version of the Host.

4.5.1.6 IGMP/VLAN Scalability test

Objective: 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?

Setup: See Figure 4-5.

Prerequisites: The MUSE access network is Ethernet based and uses VLAN ids (Cross-connect or S-VLAN). The access network is additionally configured and optimized for IP Multicast (IGMP Snooping). De streaming server(s) are able to generate streams in accordance with the number of channels joined by the different hosts.

Procedure: Let each of the hosts use different VLAN-IDs and join as many multicast groups as possible. Measure the number of groups that were joined when the forwarding of datagrams no longer works. Make this measurement with an increasing number of VLANs.

Results: From the measurements it becomes possible to make extrapolations (presuming linear properties) for different numbers of VLANs.

4.5.2 Performance Tests

4.5.2.1 NAT/Firewall traversal

Objective: Measure the attainable throughput for fragmented UDP traffic through a NAT/Firewall.

Setup:

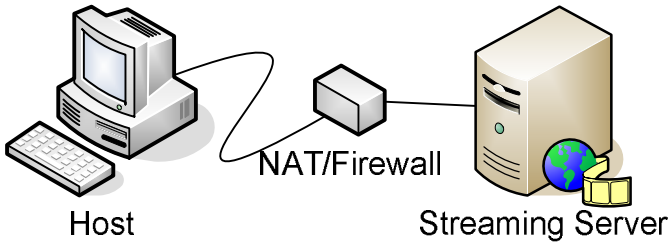


Figure 4-6: NAT/Firewall traversal test

Prerequisites: The MUSE Access network is optimized for multicast and the NAT is configured for IP Multicast/IGMP traversal. The streaming server can be configured with different RTP payload lengths for each of the measurement runs. The average bandwidth of the stream should be configurable from a few Kbps up to the theoretic maximum attainable throughput of the access network in which the NAT/Firewall will be deployed.

Procedure: For each of the payload sizes (<1500 Bytes, 2000 Bytes, 16KB) send out an RTP stream with an increasing bandwidth. At the receiving end observe the number of packets lost for each of the test runs.

Results: The maximal obtainable throughput is the highest bandwidth which did not cause any packet loss and this for each of the payload sizes. In the ideal case this should be in all the runs close to the theoretic maximum attainable throughput of the access network in the case of no additional load on the port.

4.5.2.2 IPv4 multicast benchmarking test

Objective: evaluate the performance of an IP multicast enabled SUT using RFC 3918 [Con72], “Methodology for IP Multicast Benchmarking”. The document describes the following tests which are relevant in the context of this document:

1. Forwarding and Throughput
    - Mixed Class Throughput
    - Scaled Group Forwarding Matrix
    - Aggregated Multicast Throughput
2. Forwarding Latency
    - Multicast Latency
    - Min/Max Multicast Latency
3. Overhead
    - Group Join Delay
    - Group Leave Delay

4. Capacity
   - o Multicast Group Capacity
5. Interaction
   - o Forwarding Burdened Multicast Latency
   - o Forwarding Burdened Group Join Delay

Setup: See also RFC 3918: Chapter 3. “Test set up”.

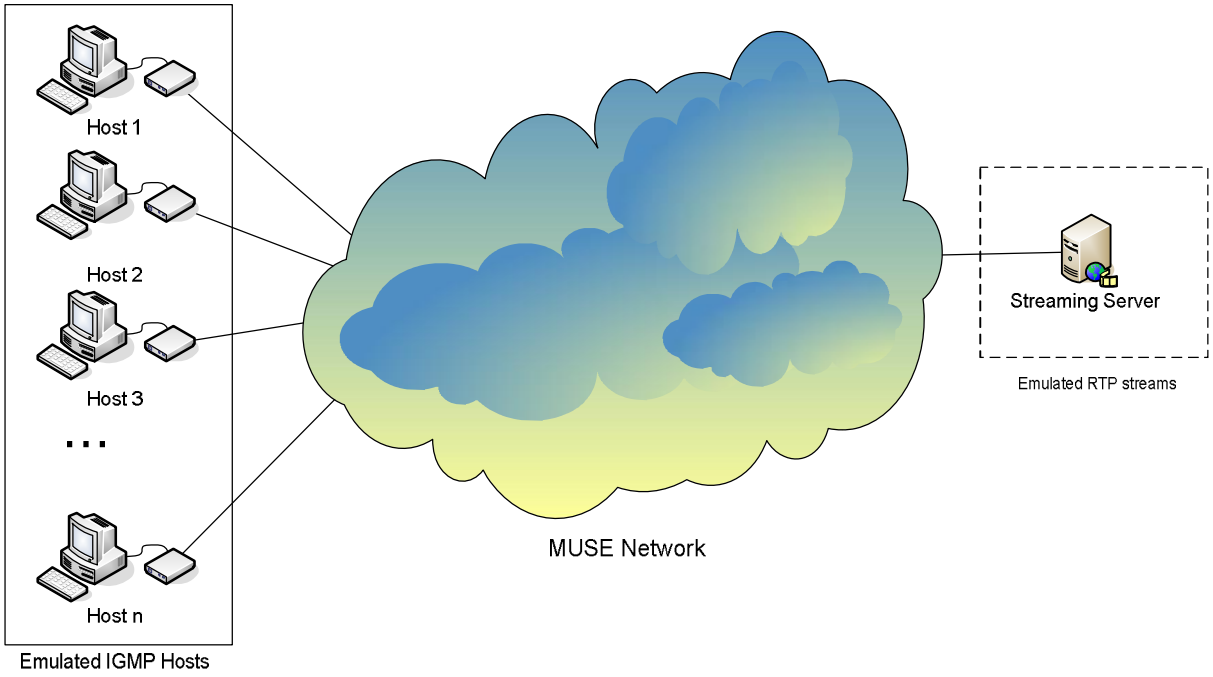


Figure 4-7: Multicast Performance testing/Benchmarking according to RFC 3918

Prerequisites: See RFC 3918: Section 3.1. “Test Considerations”.

Procedure: See RFC 3918: Chapters 4, 5, 6 and 7.

Results: Results according RFC 3918.

4.5.2.3 Zapping time under load

Objective: evaluate the time taken for a CPE device to join/leave multicast streams while the edge node is fully loaded with incoming streams and subscribers.

Setup: The same setup as in 4-7.

Prerequisites: When performing any measurement, it is important to have both accuracy and repeatability, so you can be confident that your measurement truly reflects the performance of the SUT. In order to achieve this one will need to time synchronize the sender and the receiver’s clocks.

Procedure:

- **Measure channel zapping time on a per-subscriber or per-channel basis**

It is important to measure the SUT's contribution to the zap time for each subscriber and each channel, not just the aggregate performance of the SUT. IGMP join, IGMP leave, and IGMP leave to join delay (channel zapping) measurements for each (simulated) subscriber (IGMP host) and for each channel should be performed.

- **Channel "flapping" per subscriber**
  In a realistic situation, each user will change channels with different patterns. It is important to be able to test according to different subscriber profiles and to test under different conditions of network load. For example, what if a large number of subscribers all change to the same channel, such as at the beginning of a popular show?
- **Subscriber scaling**
  To adequately characterize the channel zapping performance of your SUT, it is important to test under scaled conditions. Scaling the number of subscribers as well as the number of channels in the network are both critical factors. Service providers can then be confident that as more subscribers or channels are added to the network, channel zapping delays will not be adversely impacted.
- **Traffic Mix**
  Today's converged networks are not used for a single service as in the past. The norm is becoming "triple-play", where IPTV, VoIP and High-speed Internet services are all offered on the same subscriber connection. For this reason, it is important to have background traffic in the test scenario to determine the impact of this traffic on the channel zapping performance of your DUT. Run background unicast traffic and other protocols such as PPPoE/ DHCP, to realistically determine the performance of your system with mixed services.

Results: Gives an insight in the zapping performance under different network conditions and under different usage scenarios.

4.6 Voice over IP Service

4.6.1 Functional Tests

4.6.1.1 SIP implementation testing in the edge node

Objective: Check if an edge node handling the SIP protocol is responding to the standard described in the RFC 3261.

Setup:

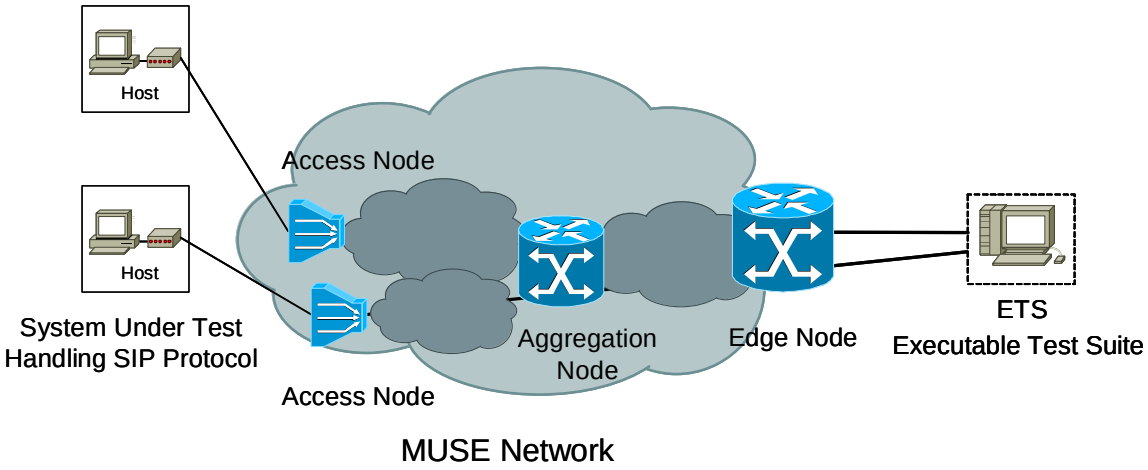


Figure 4-8: SIP implementation test

Prerequisites: The Executable Test Suite (E.T.S.) has to be configured with all the necessary parameters to create a SIP communication (test cases) between the E.T.S. and the System Under Test (S.U.T.). The system under test is up and running, and contains in its data base at least two SIP UA, one for the called and the other one for the caller. The connectivity between the executable test suite and the system under test is active.

Procedure: To establish a session between two SIP UA in order to check the implementation of the SIP protocol in the SIP UA (e.g. edge node) and the behavior of the SIP UA according to RFC 3261, a test tool generating a functional test suite is used. Such tool, which is composed of many scripts written in the standardized TTCN-3 test language, executes the test cases, analyzes the test results and verifies the received message according to the SIP syntax.

Results: Verify if the SIP messages are according to the SIP syntax. The software based SIP testing environment is able to produce a report which can be used to analyze the compliance with RFC 3261. If a script has for result a failure, we can check what was expected in the message, and what is missing and why.

4.6.1.2 SIP registration functional test

Objective: To be able to access the services, verify that a SIP endpoint or a SIP UA can register to the service node through the MUSE access network.

Setup:

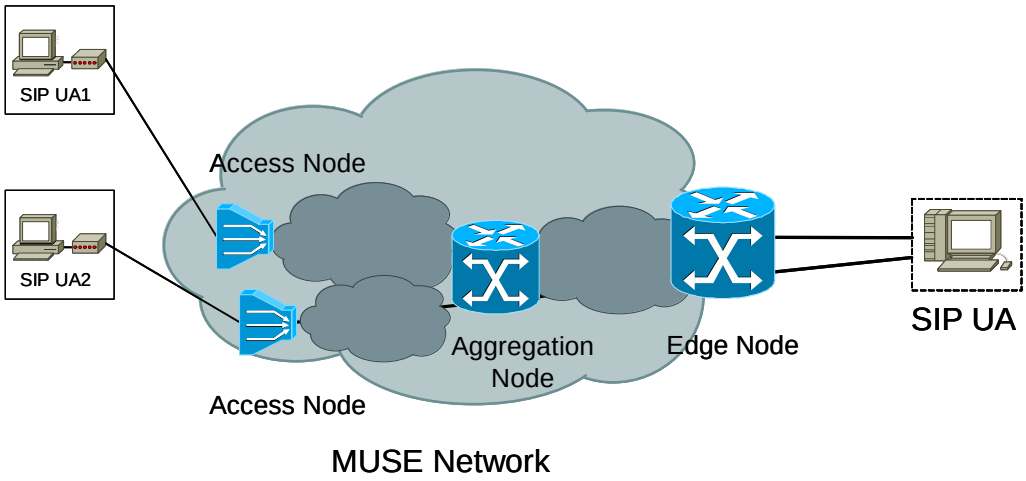


Figure 4-9: VoIP test configuration

Prerequisites: The SIP UA should be activated and obtained all suitable network parameters either statically or by auto-configuration. It is assumed that the functional entities (SIP UA, edge node …) are connected to an IP network and know each other's IP address.

Procedure: The SIP UA1 generates a SIP "Register" method towards a service node through the MUSE access network via the edge node.
Check the procedure during the registration session by parsing the end-to-end call flows showing the sequencing of the messages between all the functional entities by using a protocol analyzer.

Results: When the registration procedure for the SIP UA1 has succeeded, the service node sends in the SIP "200 OK" response to the edge node (the P-Associated-URI header will list the SIP URI associated to the SIP UA1 in the edge node). In fact, the Edge node should maintain a context of registrations (P-Associated URI, expiration timer, service node address …) for each SIP UA. Then in order to guarantee the identification of the SIP UA1 for execution rights for the services provided by the service node, the edge node includes the P-Asserted-Identity header within the SIP session request (i.e. Invite) which takes the value of the SIP URI of the SIP UA1 previously returned in P-Associated-URI.

4.6.1.3 VoIP services in a SIP environment

Objective: Verify that a SIP UA can initiate, maintain and tear down a session when calling another SIP UA through the MUSE access network.

Setup: See 4-9

Prerequisites: The MUSE access network is configured and dimensioned to support all the VoIP flows generated by the SIP user agents. In the MUSE network, voice traffic needs to be prioritized over data traffic to ensure real-time performance. The two SIP user agents (SIP UA1 and SIP UA2) are active and have obtained all suitable network parameters either statically or by auto-configuration. It is assumed that the functional entities are connected to an IP network and know each other's IP address.

Procedure: The SIP UA1 initiates the session establishment procedure with another SIP UA on the same access network by a SIP "INVITE" message which contains the media type and other capabilities of the client. The two SIP UA participating in the session negotiate the characteristics of the media (number of media flows, codec …) for the session. The MUSE network reserves the resources necessary for the session according to the characteristics of the media that are negotiated. If the stage of resource reservation in the MUSE network is successful, the called SIP UA2 may accept the invitation, acknowledging it with a response of "200 OK". The media flows can then be exchanged between the two SIP UA. Finally, the calling SIP UA1 will "close the loop" with the called SIP UA2 by sending an acknowledgment (SIP "ACK" method). The SIP UA1 tears down the session with SIP UA2 by a SIP "BYE" message.

Results: To analyze (by means of a protocol analyzer) the procedure during the session establishment by parsing the end-to-end call flows showing the sequencing of the SIP messages between all the functional entities. (SIP request messages: Invite, Ack, Bye – SIP response messages: 180 Ringing, 200 OK)

4.6.1.4 VoIP services interworking testing

Objective: Verify that a SIP UA can initiate, maintain and tear down a session when calling another client in a different access network (PSTN, H.323, MGCP …).

Setup:

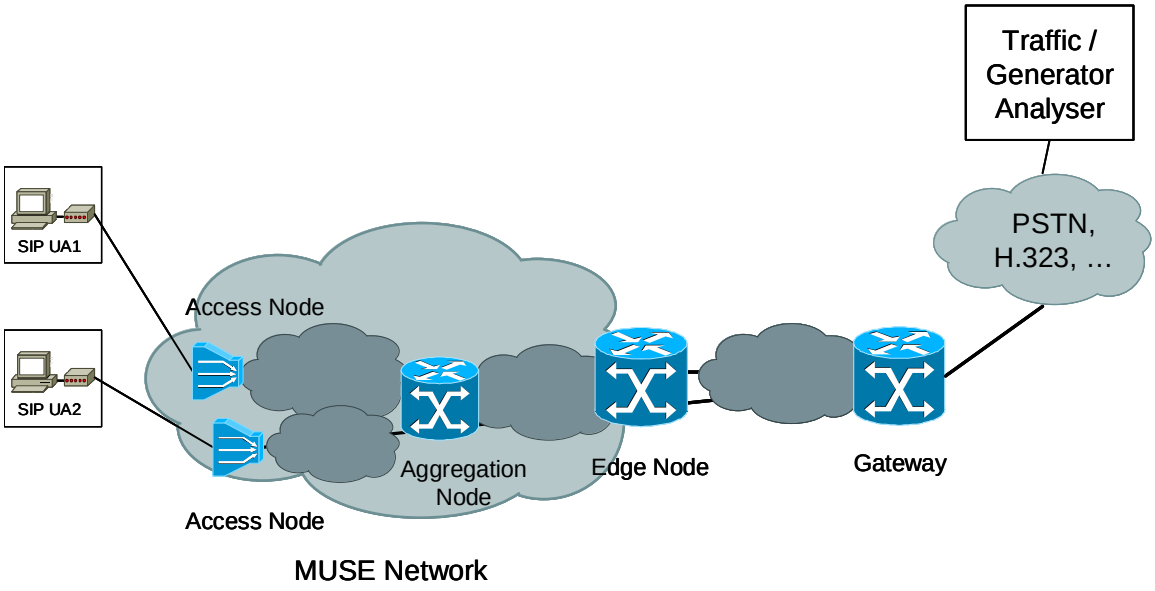


Figure 4-10: VoIP test configuration

Prerequisites: The MUSE access network is configured and dimensioned to support all the VoIP flows generated by the SIP user agents. The SIP user agent SIP UA1 is active and has obtained all suitable network parameters either statically or by auto-configuration. It is assumed that the functional entities are connected to an IP network and know each other's IP address.
The gateway, that connects networks using different protocols so that the voice data can be exchanged seamlessly between endpoints, is configured in terms of codecs, echo cancelling, packetization period, voice activity detection, silence suppression, jitter control …

Procedure: The SIP UA1 generates messages that establish a session and terminates transactions with another client in a different access network (PSTN, H.323 …). The gateway terminates the media streams from the packet network (RTP streams) and the bearer channels from the circuit network (e.g. PSTN).

Results: Verify that a call is established using only the media capabilities that can be supported by the endpoints or released between the two endpoints. Check that the media streams are established between the endpoints.
To analyze (by means of a protocol analyzer) the procedure during the session establishment by parsing the end-to-end call flows showing the sequencing of the SIP messages between all the functional entities. (SIP request messages: Invite, Ack, Bye – SIP response messages: 180 Ringing, 200 OK).

4.6.1.5 VoIP supplementary services testing

Objective: Verify the correct operation of a SIP UA in terms of supplementary services implementation (Call forward, calling line identification, …) through the MUSE access network via the edge node.

Setup: See 4-10.

Prerequisites: The SIP UA should be activated and has obtained all suitable network parameters either statically or by auto-configuration. It is assumed that the functional entities (SIP UA, edge node …) are connected to an IP network and know each other's IP address. The SIP UA should be registered in the edge and service node.

Procedure: The SIP UA1 generates a SIP "Invite" method to SIP UA2 towards a service node through the MUSE access network via the edge node.
Check the procedure during the session establishment by parsing the end-to-end call flows showing the sequencing of the messages between all the functional entities by using a protocol analyzer.

Results: The SIP session request is well managed by the originating Edge node (ie associated to SIP UA1) and terminating edge node (ie associated to SIP UA2). The Edge node must support Call flow association for each supplementary service.

4.6.1.6 DTMF code transmission test

Objective: Verify the correct transmission of DTMF code between two SIP endpoints or SIP UA through the MUSE access network via the edge node.

Setup: See Figure 4-10.

Prerequisites: The SIP UA should be activated and has obtained all suitable network parameters either statically or by auto-configuration. It is assumed that the functional entities (SIP UA, edge node …) are connected to an IP network and know each other's IP address. The SIP UA should be registered in the edge and service node.

Procedure: The SIP UA1 generates a SIP "Info" method towards a service node (e.g. Interactive Voice Response platform) through the MUSE access network via the edge node.

Check the procedure during the session establishment by parsing the end-to-end call flows showing the sequencing of the messages between all the functional entities by using a protocol analyzer.

Results: To analyze (by means of a protocol analyzer) the procedure during the session establishment by parsing the end-to-end call flows showing the sequencing of the SIP messages between all the functional entities.

4.6.1.7 Packet Loss and out-of-order delivery test

Objective: 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 a RTP stream

Setup: See Figure 4-10.

Prerequisites: The same prerequisites as in test 4.6.1.3

Procedure: For this, the objective is to inspect at the receiving side the RTP sequence numbers of the received RTP packets that belong to the same Synchronization Source (SSRC). The latter assures that one inspects only packets that originate from the same source and that belong to either the audio or video stream when both are not multiplexed onto the same channel. A channel in this context is uniquely identified by the destination group address and destination port number of the packets.

Results: For VoIP streams originating from within the MUSE access network and/or service provider network there should not be any packet loss and out-of-order packet delivery.

4.6.1.8 VoIP flows through NAT/PAT - Firewall test

Objective: When the architecture contains NAT/PAT features, verify that the NAT/PAT supports the traversal of VoIP flows at the access network/home Network..

Setup: See Figure 4-10.

Prerequisites: The NAT/PAT - Firewall function at the edge node/home level is configured for VoIP traversal. The SIP UA is fully (either auto-configured or statically) configured. The Access network/Home Network nodes may be configured with firewall function and NAT/PAT table to convert (either statically or dynamically) private addresses and/or port numbers to public addresses and/or port numbers. The service node (or traffic generator) can be configured to stream multiple RTP streams on different port numbers.

Procedure: Use a testing application or a media application (QuickTime, VideoLan client …) with multi-port traffic emulation capabilities to join a sub set of the udp ports being streamed.

Results: Verify that VoIP traffic is received by the SIP UA and the edge node and that the authorized VoIP traffic is only from/for the couple address/port number. Verify that the VoIP traffic sourced at the SIP UA is receivable at the edge node.

4.6.1.9 Shaping functional test

Objective: Ensure that unfriendly traffic is shaped and policed at the access node and edge node level.

Given that the voice flow is notably characterized by the bandwidth related to the payload type, codec, … the shaping function will be applied to this authorized bandwidth for voice session at the edge node.

See "Chapter 5" for shaping functional tests.

4.6.1.10 Flows prioritization test

Objective: To check if the edge node or access network/home network can prioritize voice flows with regard to the data flows

According to the prioritization of the voice stream with regard to the data flows, the edge node should manage the voice traffic with a higher priority then data traffic.

See "Chapter 5" for flow prioritization tests.

4.6.2 Performance Tests

4.6.2.1 Robustness and security level of a SIP implementation in the edge node

Objective: Check the ability of a SIP element (edge node) to identify invalid messages and to take appropriate action in order to assess the robustness and the security level of a SIP implementation.

Setup: See Figure 4-8 except that the executable test suite (E.T.S.) is a computer running a JAVA based test suite. See http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/ for background information on such a tool.

Prerequisites: The JAVA run-time environment is installed on the E.T.S. Two SIP endpoints or SIP UA are needed and are known by the SIP equipment (edge node) which has to be assessed. Then an application which is able to sniff the traffic between the two SIP UA (e.g. ethereal) is necessary.

Procedure: The test suite is composed of 4527 test cases. Several approaches are possible to execute the test suite: test case by test case, or set of test case (one packet correspond to a tested-header), or all the test-suite.

- The execution of the test suite requires the activation of the SIP UA or a prompt in windows shell and enter the following command lines: java –jar c07-sip-r2.jar –touri bob@biloxi.com from uri alice@biloxi.com

- Many options can be added to this line just enter: java –jar c07-sip-r2.jar –help
  For example: java –jar c07-sip-r2.jar –touri bob@biloxi.com -fromuri alice@biloxi.com -start 2 –stop 59.

This command will start the test at test case number 2 and stop at the 59th test case. Additional information can be obtained from the following URL: http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

Results: During the test cases, two points require to be checked, firstly the state of the SIP UA if it is up or down and secondly on the protocol analyzer if the "ICMP destination Unreachable" response is received from the IP address of the SIP UA.

4.6.2.2 Number of VoIP session establishments per second at the edge node level

Objective: Measure the number of VoIP session establishments per second at the edge node level while the edge node is fully loaded with incoming streams. Determine the performance limits of the edge node.

Setup:

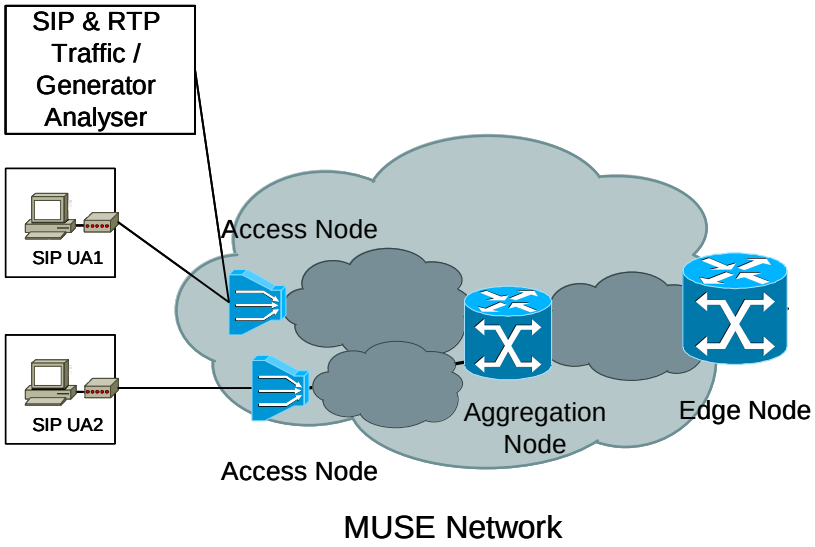


Figure 4-11: SIP performance test

Prerequisites: It is assumed that the functional entities (SIP UA, edge node, …) are connected to an IP network and know each other's IP address. The key question is the number of VoIP calls that can be established per second at the edge node level while maintaining adequate response times and throughput for the application provided by the edge node.

Procedure: Generate SIP "Invite" methods towards the edge node through the MUSE access network.
VoIP sessions traffic will be generated smoothly through the edge node till the limit of the Edge Node capacity. Analyze the quality of service through the measurement of the following parameters: response time, one way delay, jitter, packet loss.

Results: The maximum number of VoIP calls per second at the edge node level will be determined. The maximum number of VoIP calls will level at a certain point as the edge node's processing capacity becomes saturated. This metric is important to determine so that customers who are implementing a VoIP network can adequately design and provision their networks.

4.6.2.3 Number of simultaneous VoIP sessions at the edge node level

Objective: Measure the number of simultaneous VoIP sessions at the edge node level while the edge node is fully loaded with incoming streams. Determine the performance limits of the edge node.

Setup: See Figure 4-11

Prerequisites: The same prerequisites as those specified in the 4.6.2.2 section.

Procedure: VoIP sessions traffic will be generated smoothly through the edge node to have a maximum of simultaneous sessions till the limit of the Edge Node capacity.

Results: The maximum number of simultaneous active VoIP calls at the edge node level will be determined. The maximum number of VoIP calls will level at a certain point as the edge node's processing capacity becomes saturated.

4.6.2.4 Setup time to establish VoIP session at the edge node level

Objective: Measure the setup time to establish a session between the SIP UA and the Edge Node under various conditions of traffic load.

Setup: See Figure 4-11

Prerequisites: The same prerequisites as those specified in the 4.6.2.2 section.

Procedure: generate a session from the SIP UA1 towards the edge node and measure the delay between the message send by the SIP UA till the message send by the Edge Node to the Service Node.

Results: the average setup time to establish VoIP session.

4.6.2.5 Number of registration per second and the number of simultaneous registrations at the edge node level

Objective: Measure the number of registration per second and the number of simultaneous registrations at the edge node level under various conditions of traffic load. Determine the performance limits of the edge node for the registration procedure.

Setup: See Figure 4-11

Prerequisites: The same prerequisites as those specified in the 4.6.2.2 section.

Procedure: SIP "Register" method traffic will be generated smoothly through the edge node to have a maximum of registrations per second or simultaneous registrations till the limit of the Edge Node capacities through the MUSE access network.

Results: The maximum number of registrations per second and the maximum number of simultaneous registrations that can be established at the edge node level will be determined.

4.6.2.6 NAT/Firewall Traversal

Objective: Measure the attainable throughput for fragmented RTP traffic through a NAT.

Setup: See Figure 4-8

Prerequisites: It is assumed that the functional entities (SIP UA, edge node …) are connected to an IP network and know each other's IP address. The NAT function is configured for VoIP traversal. The executable test suite can be configured with different RTP payload lengths for each of the measurement runs. The average bandwidth of the SIP media stream should be configurable from a few Kbps up to the theoretic maximum attainable throughput of the access network in which the NAT/firewall will be deployed.

Procedure: For each of the payload sizes (<1500 Bytes, 2000 Bytes, 16KB) send out an RTP stream with an increasing bandwidth. At the receiving end observe the number of packets lost for each of the test runs.

Result: The maximal obtainable throughput is the highest bandwidth which didn't cause any packet loss and this for each of the payload sizes. In the ideal case this should be in all the cases be close to the theoretic maximum attainable throughput of the access network in the case of no additional load on the port.

4.6.2.7 Generic performance tests

For generic performance tests, see also "Chapter 5" for details.

5 NETWORK CONNECTIVITY TESTING

5.1 Introduction

This chapter 5 describes relevant tests and standards for testing the specific Muse architectures bottom-up to the network layer and excluding the physical layer. It is focused to an even greater extent on the MUSE models than the service connectivity chapter.

When applied to another network based on other models, this part of the test suite should be seen as a guideline and source of inspiration for necessary tests to implement in order to secure the network connectivity.

5.2 MUSE Data Plane

5.2.1 Network layer

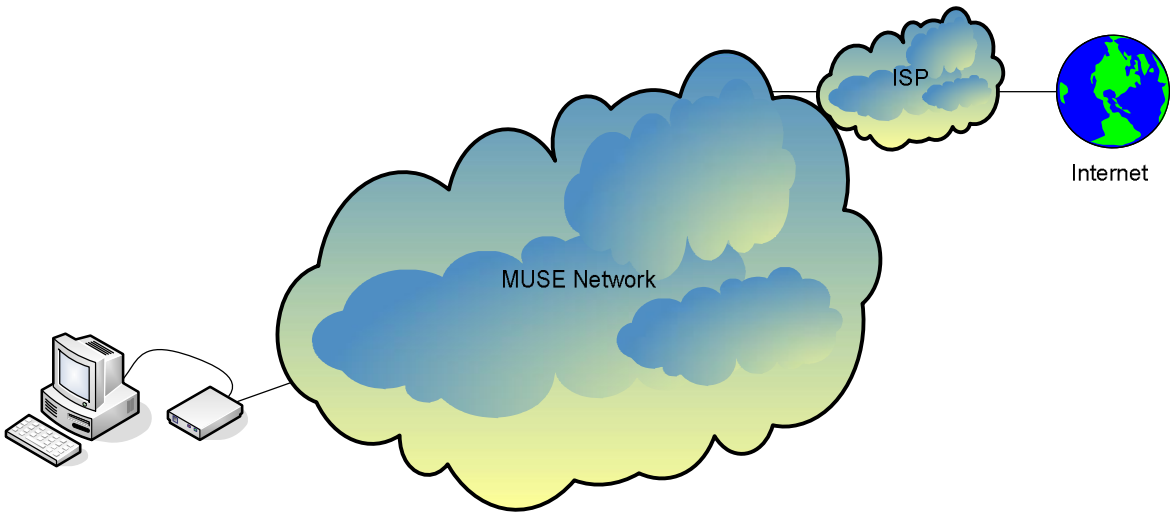


Figure 5-1: Network Connectivity test setup

5.2.1.1 Basic reachability test

Objective: Verify that a basic form of connectivity can be established through the MUSE access network.

Setup: See Figure 5-1.

Prerequisites: The host should be started and obtained all relevant network parameters either statically or through auto-configuration.

Procedure:

We will use the **ping** command which implements the ICMP Echo Request and Reply processing part of the ICMP specification. This command can be used to verify multiple aspects of the basic reachability.

1. Local

Here we can verify whether the TCP/IP stack of the host system is operational and that the auto-configuration parameters were correctly configured in the TCP/IP stack.

ping a.b.c.d

Here a.b.c.d corresponds to the ip address that was assigned through auto-configuration.

An example of the output on MS Window is given below.

```
$>ping 157.193.214.250

Pinging 157.193.214.250 with 32 bytes of data:

Reply from 157.193.214.250: bytes=32 time<1ms TTL=128
Reply from 157.193.214.250: bytes=32 time<1ms TTL=128
Reply from 157.193.214.250: bytes=32 time<1ms TTL=128
Reply from 157.193.214.250: bytes=32 time<1ms TTL=128

Ping statistics for 157.193.214.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Router

Here we verify whether the access network is capable of forwarding packets between the Host and the first router. In the case of a MUSE style of access network this represents a elementary test of the access network itself.

ping a.b.c.d

Here a.b.c.d corresponds to the IP address of the gateway/router that was assigned through auto-configuration.

2. Remote

To verify the forwarding of packets between the Access Network and the rest of the network one can “ping” a host located somewhere on the ISPs network (e.g. web server of ISP) or on the Internet (e.g. 66.249.93.99 = www.google.com).

```
$>ping 66.249.93.99

Pinging 66.249.93.99 with 32 bytes of data:

Reply from 66.249.93.99: bytes=32 time=9ms TTL=246
Reply from 66.249.93.99: bytes=32 time=9ms TTL=246
Reply from 66.249.93.99: bytes=32 time=10ms TTL=246
Reply from 66.249.93.99: bytes=32 time=9ms TTL=246
```

```
Ping statistics for 66.249.93.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
```

Results: The ping command should in the case of the local ping test indicate that there is no packet loss and that the Round-Trip time should be smaller then 1ms. The results in the case of a router ping should under normal load conditions present no packet losses and the delay (RTT/2) should be lower then or equal to the targeted value for the specific MUSE architecture under test.
The ping test towards a remote host on the Internet should indicate that there is basic connectivity (at least one reply) but given that the Internet is best-effort there can be packet losses and the delay is unconstrained.

5.2.1.2 Advanced Reachability test

Objective: Verify that the Access network is capable of giving access to higher layer services like web access.

Setup: See Figure 5-1.

Prerequisites: The host should have obtained a valid network layer configuration and the access network should be interconnected with the Internet.

Procedure: On the Host a web browser should be launched and an URL should be entered. Prior to entering the URL one should clear the local cache in order to prevent the loading of the page from the cache. If the access network implements some (transparent) web caching system then this cache should also be cleared prior to running the tests. In a first test, one could open a web page located on a server located in the ISPs network. As a second test one can open a web page on a server on the Internet.

Results: The web page of the ISP should be loaded immediately under normal conditions of load on the access network. The pages from a server on the Internet should load but given that Internet access is best-effort there is no guarantee on the timeliness of the delivery of the pages.

5.2.1.3 Connectivity tests with background noise

Objective: Verify that the Access network is capable of giving basic connectivity and advanced connectivity when background noise is present.

See DSLForum TR-48 “9.3 PPPoE End-to-End Connectivity Test” section for details.

5.2.1.4 Throughput, Frame loss, E2E delay, E2E Jitter (Delay Variation), Packet sequence test

Objectives: Measure Network Layer Throughput, Frame loss, E2E delay, E2E Jitter (Delay Variation), Packet sequencing according the IETF IP Performance Metrics (IPPM) specifications.

Setup: A basic IPPM measurement setup consists of minimally two active measurement probes and a data collection station as depicted in Figure. The IETF draft draft-ietf-ippm-implement-*.txt gives an overview of the currently available commercial and open source implementations.

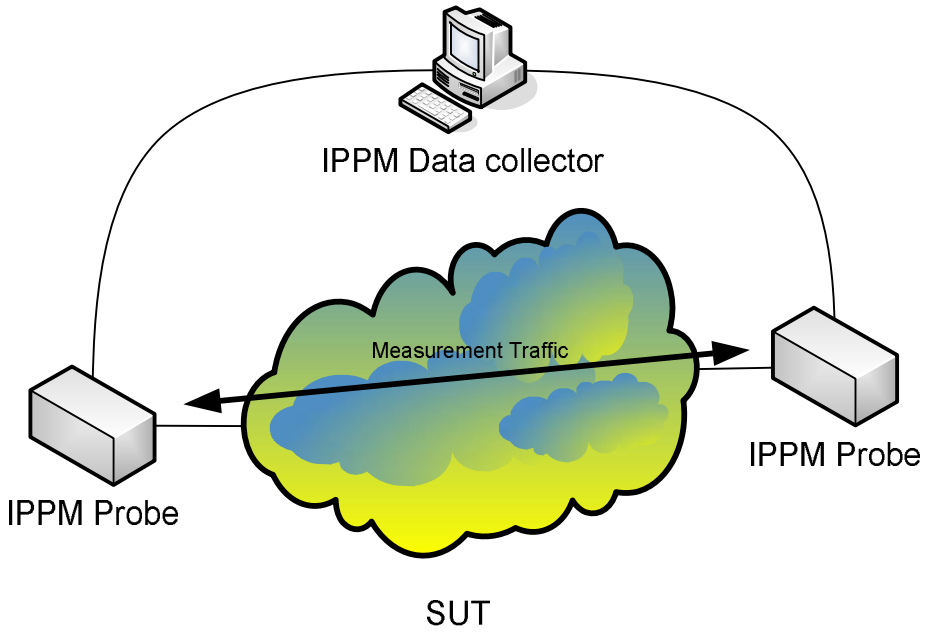


Figure 5-2: IPPM measurement setup

Prerequisites: The IPPM Probes have IP connectivity and are time synchronized (NTP, GPS, …). The IPPM Data collector station has connectivity with the probes.

Results: Depending on the IPPM Metrics implemented by the probes different performance indicators can be obtained.

5.2.2 Link Layer Tests

5.2.2.1 Support of standardized Ethernet traffic

Objectives:

- 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

Setup: The test set-up is depicted in Figure 5-3.

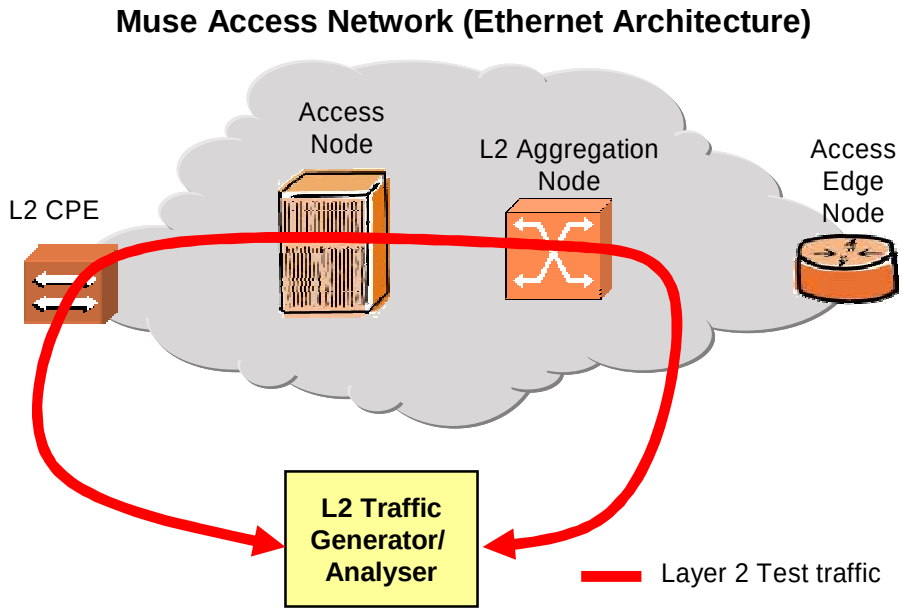


Figure 5-3: One-to-One Link layer tests between CPN and EN

Prerequisites:

- Transparent Ethernet connection is required, meaning there is no Ethernet termination within CPE, Access and Aggregation Nodes.

Procedure:

- Connect a Traffic Generator/Analyzer and/or protocol analyzer to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-3.
- Conformance tests:
  - Set-up Ethernet unicast streams (downstream and upstream) conform to IEEE 802 standards.
  - Set-up Ethernet broadcast streams (downstream and upstream) conform to IEEE 802 standards.
  - Set-up Ethernet multicast streams (downstream and upstream) conform to IEEE 802 standards.

Option:

- Conformance tests:
  - Set-up Ethernet unicast streams (downstream and upstream) conform to relevant IEEE 802 standards (802.3, 802.1D/Q and 802.1ad)
  - Set-up Ethernet broadcast streams (downstream and upstream) conform to relevant IEEE 802 standards (802.3, 802.1D/Q and 802.1ad)
  - Set-up Ethernet multicast streams (downstream and upstream) conform to relevant IEEE 802 standards (802.3, 802.1D/Q and 802.1ad)

Expected Results:

- The system under test is able to forward standardized Ethernet traffic specified by IEEE-802 with unicast, multicast and broadcast MAC addresses.

5.2.2.2 Customer and Service separation: Conformance

Objectives:

- 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 using of MPLS in the aggregation network to solve the VLAN scalability restriction, verify that the MPLS mechanisms are conform to IETF specifications.

Setup: The test set-up is depicted in Figure 5-3.

Prerequisites:

- Transparent Ethernet connection is required that means there is no Ethernet termination within CPE, Access and Aggregation Nodes.

Procedure:

- Connect a Traffic Generator/ Analyzer and/or protocol analyzer to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-3.
- Set-up Ethernet streams (downstream and upstream)
  - Downstream: Generate VLAN tagged traffic conform to IEEE 802
  - Upstream: Analyze the VLAN Tag conformance using a protocol Analyzer
  - In case of using of MPLS: Analyze the MPLS label conformance using a protocol Analyzer

Expected Results:

- The system under test supports VLAN tagging specified by IEEE 802.1D and IEEE 802.1ad (Provider Bridges) in order to separate customers and services.
- In case of using of MPLS in the aggregation network the system under test supports MPLS mechanisms conform to the IETF specifications.

5.2.2.3 Customer and Service separation: Functionality

Objectives:

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

Setup: The test set-up is depicted in.

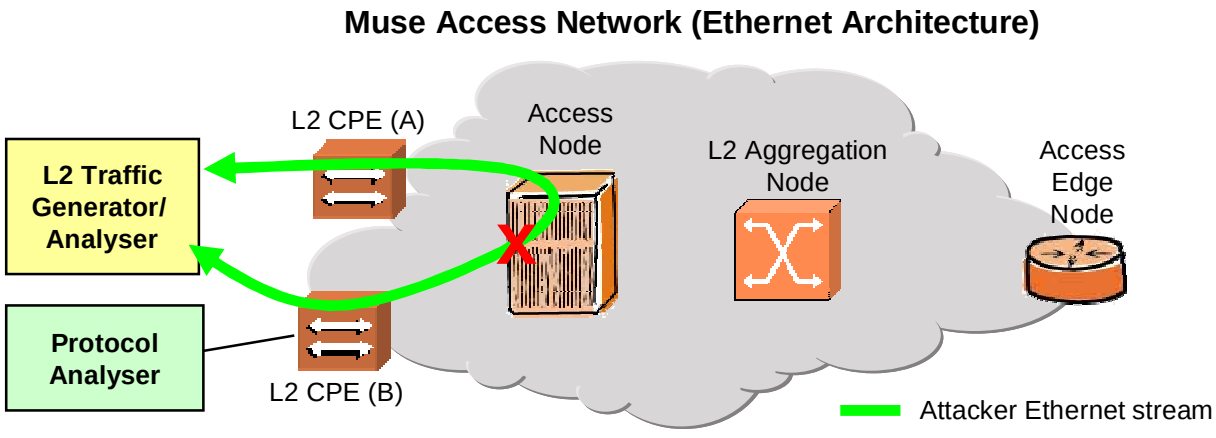


Figure 5-4: Test set-up to verify Customer and Service separation

Prerequisites:

- Transparent Ethernet connection is required that means there is no Ethernet termination within CPE, Access and Aggregation Nodes.

Procedure:

- Generate an attacker Ethernet steam that tries to set-up an Ethernet stream from CPE A to CPE B
- Check that no attacker traffic is received at CPE B using a Protocol Analyzer

Expected Results:

- Attacker traffic is not received at CPE B
- traffic and services of different customers are strictly separated

5.2.2.4 Link layer Redundancy

Objectives:

- Verify that reconfiguration is performed in case of link layer failure.
- Verify that Link layer protection is supported 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
- 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

Setup: The schematic test set-up is depicted in Figure 5-11.

Prerequisites: At least one protected link must be set-up

Procedure:

- Connect a Traffic Generator/ Analyser to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-11.
- Generate an Ethernet test stream
- Interrupt a protected link and check that link layer reconfiguration is performed
- Use a protocol analyzer to check the protocol conformance
- Generate Spanning Tree Protocol BPDUs using a traffic generator

Expected Results:

- Link layer protection is supported.
- Link layer protection is standards conforming
- Spanning Tree Protocol BPDU (Bridge Protocol Data Unit) generated by the CPN does not start a reconfiguration process in the Access network

5.2.2.5 Topology aspects

Objectives:

- Verify if star, tree, ring or mesh topologies are supported in the Network without packet loops (e.g. using Spanning Tree Protocol)
- Verify that Spanning Tree (native), Rapid spanning tree, Multiple spanning tree Protocol conform to the IEEE specifications can be used to enable ring or mesh topologies without packet loops in the network

Setup: One possible ring topology test set-up is depicted in Figure 5-5.

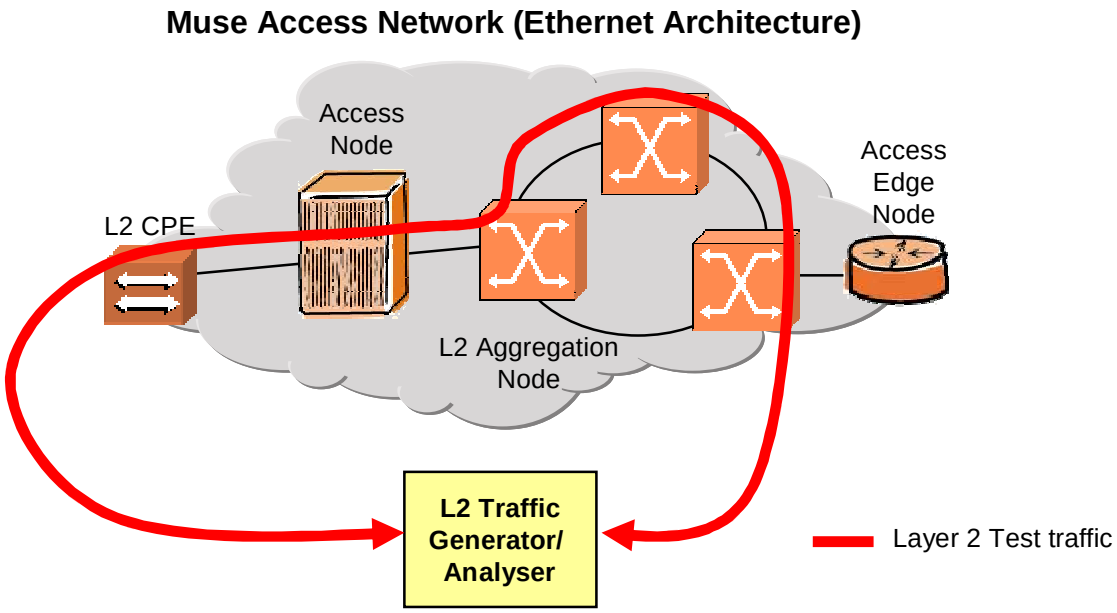


Figure 5-5: Ring topology test set-up

Prerequisites:

- This test scenario requires an adequate number of nodes that allows to set-up star, tree, ring or mesh topologies. That means it is not possible to set-up a ring topology on the basis of only one Aggregation Node and Access Node.

Procedure:

- Set-up a ring or mesh topology on the basis of Spanning Tree (native), Rapid spanning tree, Multiple spanning tree Protocol conform to the IEEE specifications
- Generate Ethernet traffic using a Traffic Generator
- Check up on packet loops using a Traffic Analyzer
- Check the protocol conformance using a protocol analyzer

Expected Results:

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

5.2.2.6 Connectivity characteristics: P-to-P between CPN and EN

Objectives:

- Verify that Ethernet P-to-P connections are supported between CPN and EN

Setup: The test set-up is depicted in Figure 5-3

Prerequisites:

- Transparent Ethernet connection is required that means there is no Ethernet termination within CPE, Access and Aggregation Nodes.

Procedure:

- Connect a Traffic Generator/ Analyzer and/or protocol analyzer to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-3.
- Set-up a P-t-P connection
- Generate an Ethernet stream

Expected Results:

- The system under test supports P-t-P connections

5.2.2.7 Connectivity characteristics: P-to-MP between EN and CPN

Objectives:

- Verify if Ethernet P-to-MP connections are supported between EN and CPN (e.g. using one or multiple Multicast Service VLANs)

Setup: Test set-up is depicted in Figure 5-6

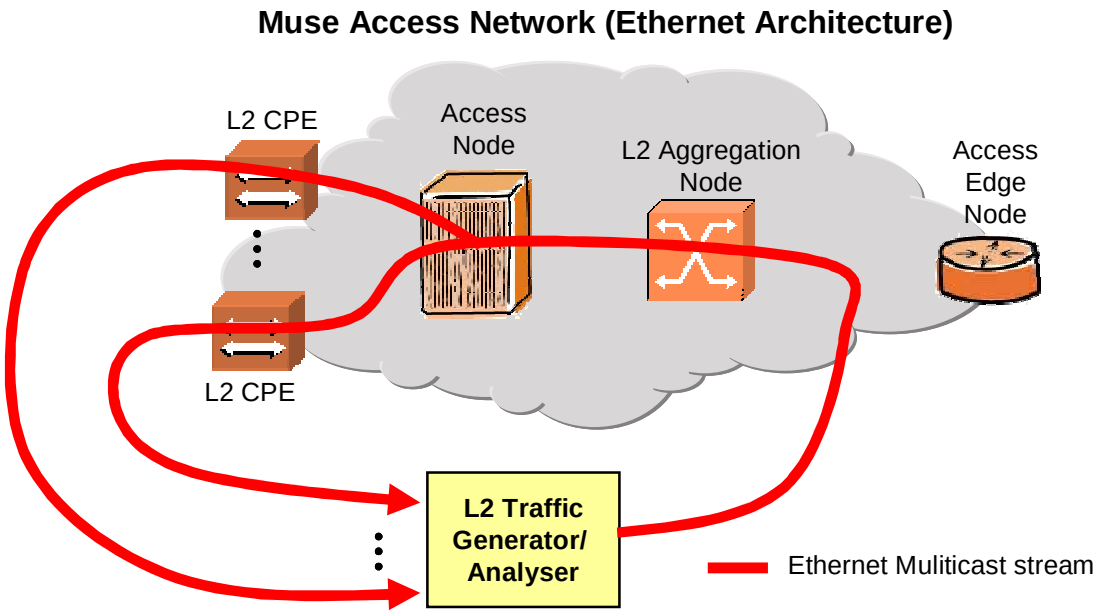


Figure 5-6: Test set-up P-to-MP between EN and CPN

Prerequisites:

- Transparent Ethernet connection is required that means there is no Ethernet termination within CPE, Access and Aggregation Nodes.

Procedure:

- Set-up an Ethernet P-t-MP connection between the Aggregation Node uplink and two or multiple CPEs (e.g. on the basis of a Mulitcast VLAN)
- Generate a downstream Ethernet Multicast stream using a Traffic Generator
- Analyze the Multicast traffic using a Traffic Analyzer

Expected Results:

- Ethernet P-to-MP connections are supported between EN and CPN

5.2.2.8 Connectivity characteristics: Peer-to-Peer between two CPEs

Objectives:

- Check that Peer-to-Peer C-VLAN transparent Ethernet connections are supported between two CPEs

Setup: Test set-up is depicted in Figure 5-7.

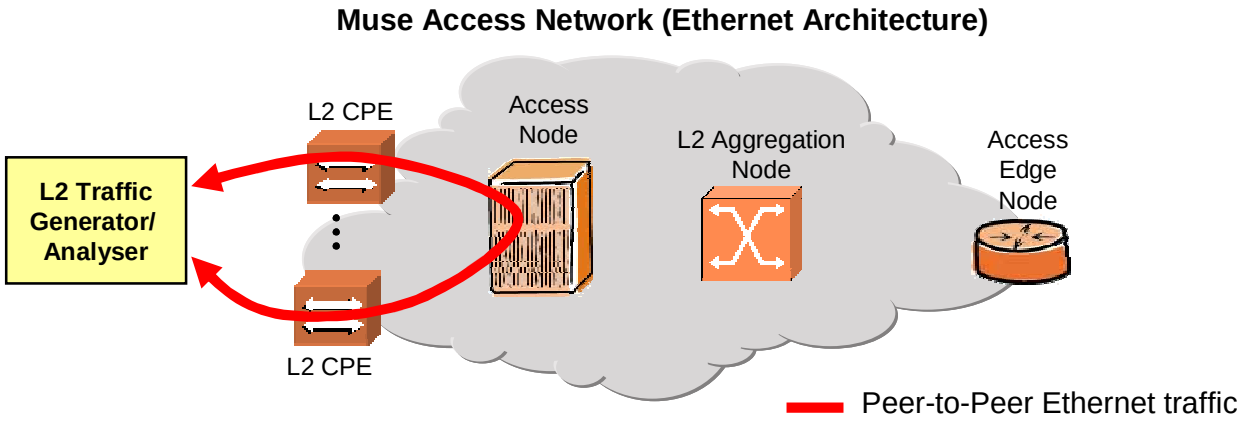


Figure 5-7: Test set-up Peer-to-Peer connectivity

Prerequisites:

- Peer-to-Peer connections must be supported by the Access Node, for example on the basis of S-VLANs.

Procedure:

- Set-up a Peer-to-Peer connections between two CPEs
- Generate C-VLAN tagged and untagged Ethernet traffic using a Traffic Generator
- Analyze the Ethernet Traffic using a Traffic Analyzer

Expected Results:

- The Access Node forwards Peer-to-Peer Ethernet Frames between two CPEs
- In addition, C-VLAN transparent Ethernet connections are supported that means Customers can use C-VLAN tagging for CPN configurations

5.2.2.9 Connectivity characteristics: MP-to-MP connectivity

Objectives:

- Verify that Ethernet MP-to-MP connections are supported between multiple CPEs

Setup:

- Figure 5-8 shows an example for a MP-t-MP test set-up using three Access Nodes.
- For the case that only one Access Node is available Figure 5-10 offers an optional solution.

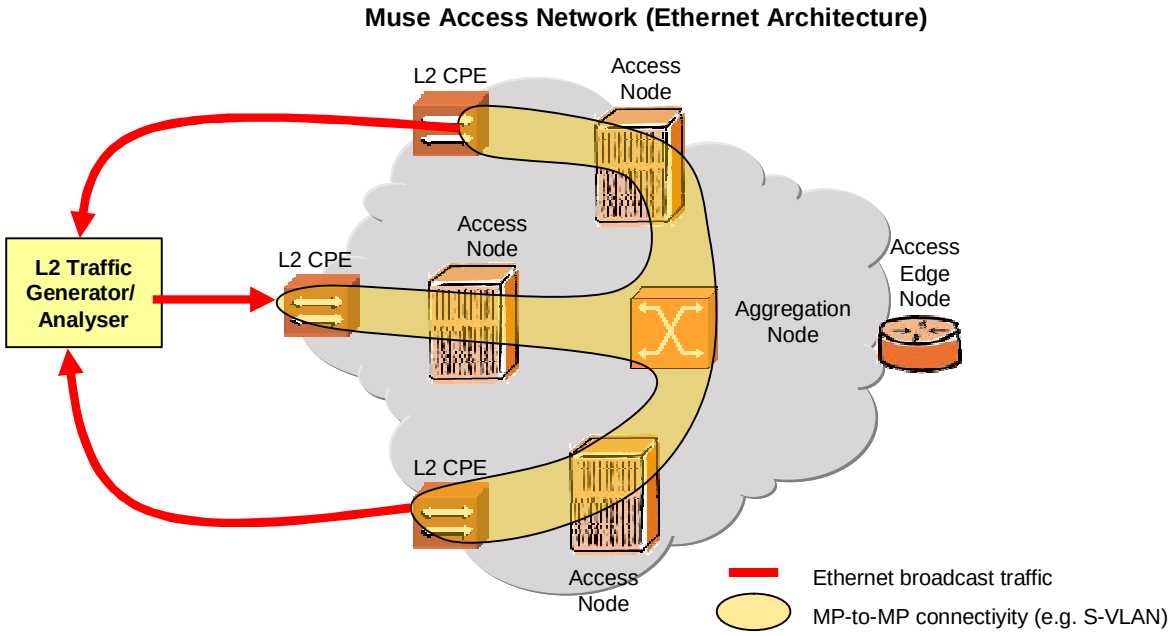


Figure 5-8: Example for a MP-t-MP test set-up

Prerequisites:

A more realistic MP-t-MP test scenario requires a set-up using multiple Access Nodes, e.g. depicted in Figure 5-8.

Procedure:

- Set-up a MP-t-MP connectivity between multiple CPEs on the basis of one or more Access Nodes
- Generate a broadcast Ethernet steam using a Traffic Generator
- Analyze the correct broadcast procedure using a Traffic Analyzer

Expected Results:

- The Ethernet Switching layer duplicates and forwards the broadcast Ethernet frames to all CPEs
- MP-to-MP connections are supported between multiple CPEs

5.2.2.10 Performance Tests

This section describes test methods to perform Link layer performance tests.
Following Requests for Comments (RFC) are the basis of the described test methods:

RFC 1242 [Con07]: Benchmarking Technology for Network Interconnection Device

- This memorandum discusses and defines a number of terms that are used to describe performance benchmarking tests and its results.

RFC 2544 [Con25]: Benchmarking Methodology for Network Interconnect Device

- This memo discusses and defines a number of tests that may be used to describe the performance characteristics of a network interconnecting device and it describes specific formats for reporting the results of the tests.

RFC 2285 [Con19]: Benchmarking Methodology for LAN Switching Devices

- This document defines the terminology for the benchmarking of local area network (LAN) switching devices. It defines terms like forwarding performance, congestion control, latency, address handling, and filtering.

These RFCs can be seen as the quasi standard for performance tests that were developed by the "The Internet Society" and the Internet Engineering Task Force (IETF).
Table 5-1 lists some important definitions of the RFCs 1242, 2544 and 2285.

Table 5-1: Definitions of the RFCs 1242, 2544 and 2285

RFC	Term	Description
1242/2544	Throughput	"The maximum rate at which none of the offered frames are dropped by the device." (RFC-1242)
1242/2544	Latency	Total delay of a device or system. "For store and forward devices: The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port. For bit forwarding devices: The time interval starting when the end of the first bit of the input frame reaches the input port and ending when the start of the first bit of the output frame is seen on the output port." (RFC-1242)
1242/2544	Frame Loss rate	"Percentage of frames that should have been forwarded by a network device under steady state (constant) load that were not forwarded due to lack of resources." (RFC-1242)
2544	Frame sizes	"All of the described tests SHOULD be performed at a number of frame sizes."…" Frame sizes to be used on Ethernet: 64, 128, 256, 512, 1024, 1280, 1518" (RFC-2544)
2544	Trial duration	"The duration of the test portion of each trial SHOULD be at least 60 seconds." (RFC-2544)

The performance parameter Jitter was not defined by the RFCs described above but MUSE (MA2.10) defines Jitter as follows:

The Jitter is defined as (max delay – min delay). It is only valid together with the associated quantile.

5.2.2.11 One-to-One Ethernet performance tests between CPN and EN

Objective:

- Verify the Ethernet performance parameters Throughput, Latency, Frame loss rate and Jitter for a MUSE Ethernet Architecture One-to-One set-up between CPN and EN.

Setup: The test set-up is depicted in Figure 5-3.

Prerequisites:

- A Layer-2 connection must be established between a L2 CPE and the uplink interface (interface to the Access Edge Node) of the L2 Aggregation Node.

Procedure:

- Connect a Traffic Generator/ Analyser to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-3.
- Set-up Ethernet test streams using the L2 Traffic Generator/ Analyser
- Analyse Throughput, Latency, Frame loss rate and Jitter for the Ethernet Frame sizes 64, 128, 256, 512, 1024, 1280, 1518 Bytes and different link load rates (10% to 100% with 10% steps) and a trial duration of at least 60 seconds

Expected Results:

- Throughput: Theoretical max data rate of the link with the lowest link rate (First mile) on the path independent of the Ethernet Frame size.
- Latency: For further studies (first assumption: less than 10ms)
- Frame loss rate: at least 10^{-10} per node
- Jitter: at most 1 ms per node

5.2.2.12 Ethernet performance tests between two or multiple CPN and EN (Many-to-One/ One-to-Many)

Objective:

- Verify the Ethernet performance parameters Throughput, Latency, Frame loss rate and Jitter for a MUSE Ethernet Architecture Many-to-One/ One-to-Many set-up between CPN and EN. In contrast to the test described before this experiment evaluates the system performance for the case of processing multiple Layer-2 streams simultaneously.

Setup The test set-up is depicted in Figure 5-9.

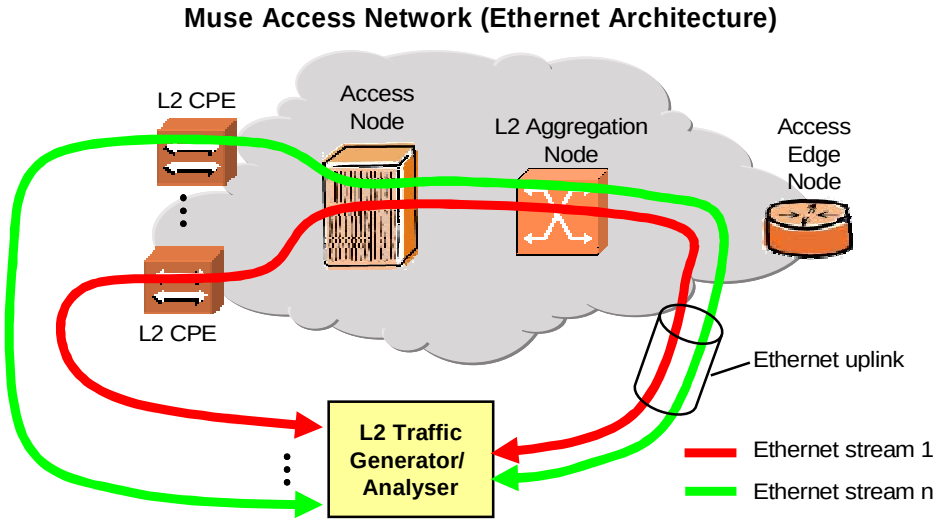


Figure 5-9: Ethernet performance tests between two or multiple CPN and EN (Many-to-One/ One-to-Many)

Prerequisites:

- Multiple connections must be established between several L2 CPEs and the uplink interface (interface to the Access Edge Node) of the L2 Aggregation Node.

Procedure:

- Connect a Traffic Generator/ Analyser to the test system (multiple L2 CPEs and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-9.
- Set-up Ethernet test streams (downstream/ One-to-Many) using a Traffic Generator
- Analyse One-to-Many Throughput, Latency, Frame loss rate and Jitter for the Ethernet Frame sizes 64, 128, 256, 512, 1024, 1280, 1518 Bytes and different link load rates (10% to 100% with 10% steps) and a trial duration of at least 60 seconds
- Set-up Ethernet test streams (upstream/ Many-to-One) using a Traffic Generator
- Analyse Many-to-One Throughput, Latency, Frame loss rate and Jitter for the Ethernet Frame sizes 64, 128, 256, 512, 1024, 1280, 1518 Bytes and different link load rates (10% to 100% with 10% steps) and a trial duration of at least 60 seconds

Expected Results:

- Throughput: Theoretical max data rate of the link with the lowest link rate (First mile) on the path independent of the Ethernet Frame size.
- Latency: For further studies (first assumption: less than 10ms)
- Frame loss rate: at least 10^{-10} per node
- Jitter: at most 1 ms per node

5.2.2.13 Ethernet performance tests between two or multiple CPNs (One-to-One, Many-to-One/ One-to-Many and Many-to-Many)

Objective:

- Verify the Ethernet performance parameters Throughput, Latency, Frame loss rate and Jitter for a MUSE Ethernet Architecture set-up between multiple CPNs. This scenario represents, for example, a business multipoint-to-multipoint VPN connectivity service using S-VLANs.

Setup

- The test set-up is depicted in Figure 5-10 for the case that only one Access Node is available
- Figure 5-8 shows a test set-up using multiple Access Nodes that is a more realistic test scenario.

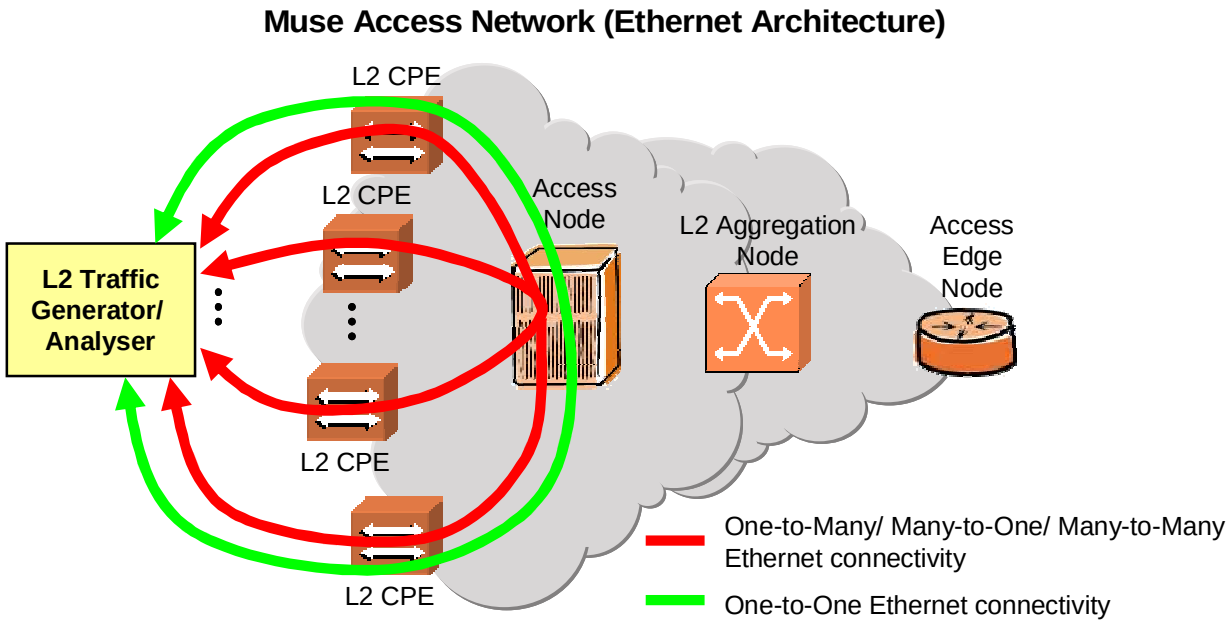


Figure 5-10: Ethernet performance tests between two or multiple CPNs (One-to-One, Many-to-One/ One-to-Many and Many-to-Many)

Prerequisites: Multiple connections must be established between several L2 CPEs passing one or more Access Nodes or Aggregation Nodes. All CPEs are members within the same VPN (S-VLAN) with a multipoint-to-multipoint connectivity.

Procedure:

- Connect a Traffic Generator/ Analyser to the test system (multiple L2 CPEs) depicted in Figure 5-10.
- Set-up Ethernet test streams using the L2 Traffic Generator/ Analyser
- Analyse Throughput, Latency, Frame loss rate and Jitter for the Ethernet Frame sizes 64, 128, 256, 512, 1024, 1280, 1518 Bytes and different link load rates (10% to 100% with 10% steps) and a trial duration of at least 60 seconds

Expected Results:

- Throughput: Theoretical max data rate of the link with the lowest link rate (First mile) on the path independent of the Ethernet Frame size.
- Latency: For further studies (first assumption: less than 10ms)
- Frame loss rate: at most 10^{-10} per node
- Jitter: at most 1 ms per node

5.2.2.14 Link layer Redundancy aspects

Objective: Verify the reconfiguration time in case of link layer failure.

Setup The schematic test set-up is depicted in Figure 5-11.

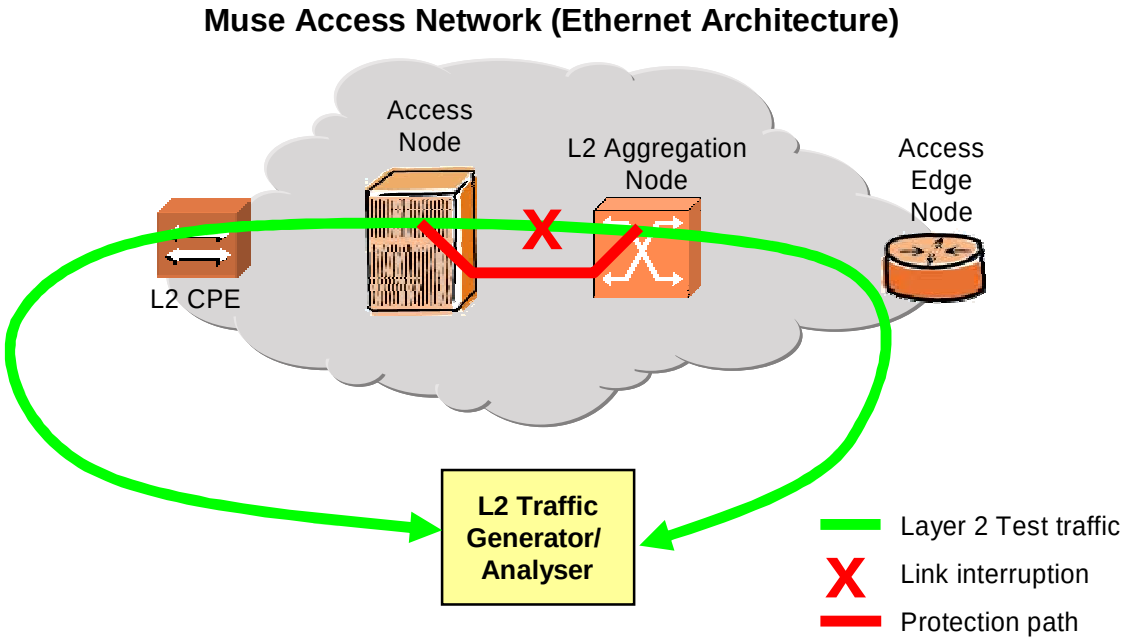


Figure 5-11: Test set-up to verify the reconfiguration time

Prerequisites:
The system under test must provide link layer protection and restoration mechanisms, e.g.:.

- 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

In addition, one or more protected links must be set-up.

Procedure:

- Connect a Traffic Generator/ Analyser to the test system (L2 CPE and the Aggregation Node uplink interface to the Access Edge Node) depicted in Figure 5-11.
- Generate an Ethernet test stream
- Interrupt a protected link and analyze the reconfiguration time using a traffic analyzer.

Expected Results:
MUSE (Phase I) does not define reconfiguration parameters but the system under test should provide protection and restoration mechanisms.
The Metro Ethernet Forum specification MEF 2 defines some requirements for Ethernet service protection including following restoration-time categories.

- Sub 50ms restoration time.
- Sub 200ms restoration time.
- Sub 2 seconds restoration time.
- Sub 5 seconds restoration time.

These categories can be used as reference to evaluate the reconfiguration performance.

5.3 MUSE Control Plane

5.3.1 Functional tests

5.3.1.1 Single host L3 auto-configuration test

Objective: Verify the correct operation of the auto configuration service. In this case only a single host/service needs to be auto-configured.

Setup:

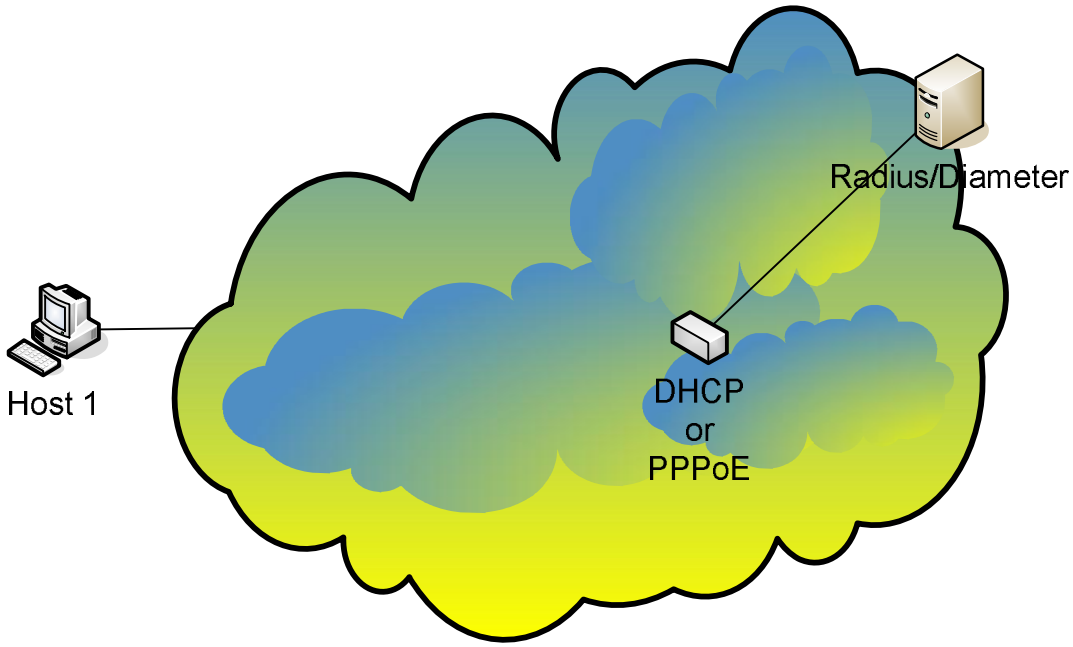


Figure 5-12: Single Host auto-configuration test

Prerequisites: The Host/device is configured for the auto-configuration mechanism used by the MUSE access network (e.g. DHCP, PPPoE, …). The Host/device is configured with a valid login and password for access to the required service. The Host/device is powered off. The edge node or the DHCP server has been correctly configured.

Procedure: The Host/device is turned on. Depending on the host/device the user has to log in. Through some status menu/command one should verify the correct auto-configuration.

On a host one can verify the result of the auto-configuration by using the following command:

- MS Windows.

  The ***ipconfig /all*** command gives details about all the network parameters that have been configured in the host. The output of the command is illustrated below in the case of DHCP.

```
$>ipconfig /all

Windows IP Configuration
```

```
        Host Name . . . . . . . . . . . . : pc235
        Primary Dns Suffix  . . . . . . . : intec.ugent.be
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : intec.ugent.be


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : intec.ugent.be
        Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
        Physical Address. . . . . . . . . : 00-14-38-0C-42-97
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 157.193.214.250
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 157.193.214.1
        DHCP Server . . . . . . . . . . . : 157.193.214.12
        DNS Servers . . . . . . . . . . . : 157.193.214.2
                                            157.193.214.4
        Primary WINS Server . . . . . . . : 157.193.214.5
        Lease Obtained. . . . . . . . . . : donderdag 11 augustus 2005 10:36:21
        Lease Expires . . . . . . . . . . : donderdag 11 augustus 2005 10:46:21
```

- UNIX/Linux systems

  The **ifconfig** command on linux systems give similar output as is shown below.

```
# ifconfig -a
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
          RX packets:302 errors:0 dropped:0 overruns:0 frame:0
          TX packets:302 errors:0 dropped:0 overruns:0 carrier:0 coll:0

eth0      Link encap:Ethernet  HWaddr 00:20:AF:EE:05:45
          inet addr:24.128.53.102  Bcast:24.128.53.255  Mask:255.255.254.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24783 errors:1 dropped:1 overruns:0 frame:1
          TX packets:11598 errors:0 dropped:0 overruns:0 carrier:0 coll:96
  Interrupt:10 Base address:0x300
```

Results: The host//device should indicate it obtained an IP address in the public address space, that there was a correct subnet mask being assigned and a correct gateway/router address was configured. Additionally a list of DNS servers can get configured.

5.3.1.2 L3 auto-configuration mix test

Objective: Verify the correct operation of the auto configuration when using different devices which use different configuration mechanisms (PPPoE, DHCP).

Setup: (see next page)

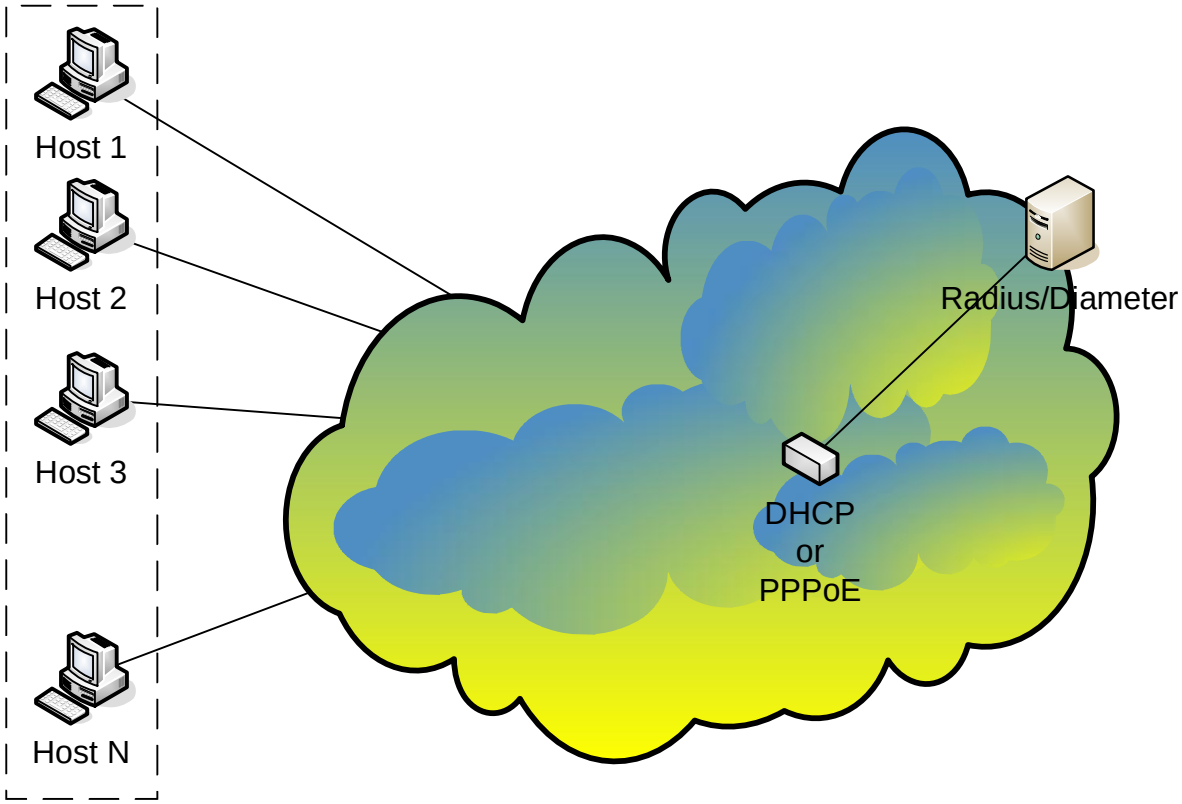


Figure 5-13: Auto-configuration test-setup

Procedure & Results:
See 5.3.1.1 Single host L3 auto-configuration test, for the procedure and the expected output for each of the individual devices.

5.3.2 Performance tests

5.3.2.1 L3 auto-configuration duration test

Objective: Measure the time it takes before a device is fully auto-configured.

Setup: Same as in Figure 5-12.

Prerequisites: The Host/device is configured for the auto-configuration mechanism used by the MUSE access network (e.g. DHCP, PPPoE, …). The Host/device is configured with a valid login and password for access to the required service. The edge node (PPPoE) or the DHCP server has been correctly configured.

Procedure: The auto-configuration is restarted (i.e. using ***ipconfig /renew*** on Windows). After the restart measure the time it takes for the ***ipconfig*** command to return.

Results: The action should take at most a couple of seconds.

5.3.2.2 L3 auto-configuration scalability test

Objective: Measure the time it takes before a device is fully auto-configured when other devices perform auto-configuration at the same time.

Setup: Same as in Figure 5-13.

Prerequisites: The Hosts/devices are configured for the auto-configuration mechanism used by the MUSE access network (e.g. DHCP, PPPoE). The Hosts/devices are configured with valid logins and passwords for access to the required service. The edge node (PPPoE) or the DHCP server has been correctly configured.

Procedure: The auto-configuration is restarted/initiated and the auto-configuration duration is measured for Host 1. This measurement is repeated multiple times. After each run an extra Host is added which performs an auto-configuration at the same time.

Results: The results will show the relation ship between the auto-configuration duration and the number of simultaneous auto-configuration requests.

5.3.2.3 DHCP auto-configuration failover test

Objective: Verify the correct operation of the auto-configuration mechanism after the main DHCP server becomes unavailable (Shutdown, network connectivity failure, server crash).

Setup: The basic setup containing a main DHCP server and a backup sever is depicted in the figure below.

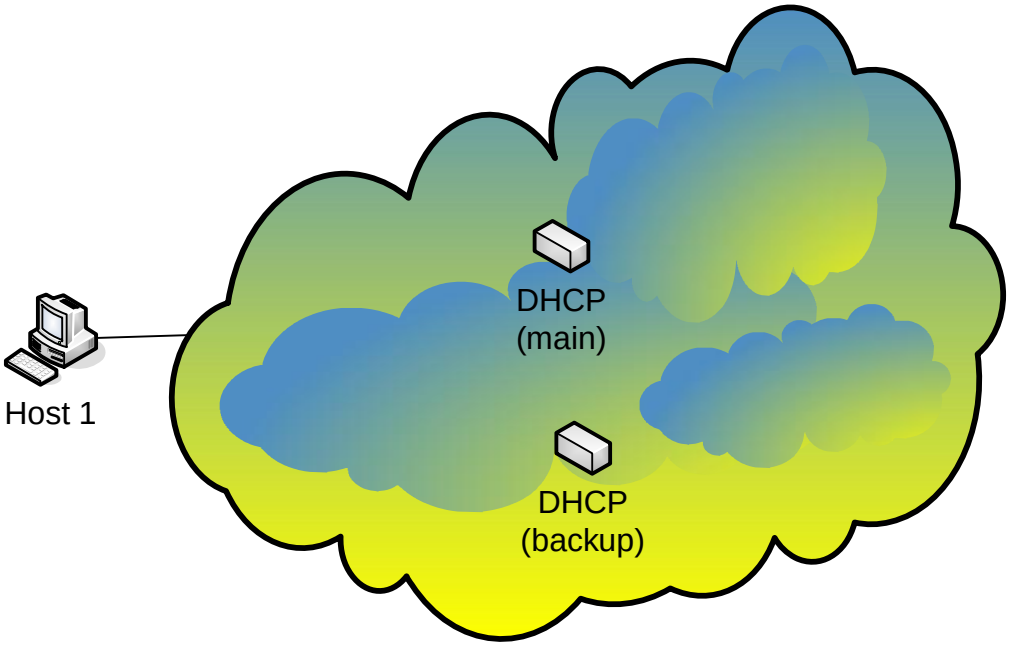


Figure 5-14: DHCP auto-configuration fail-over test setup

Prerequisites: The Host is configured for DHCP auto-configuration. If DHCP is combined with authentication (DHCP Option 90) there is the additional requirement for an out-of-band authentication mechanism like 802.1x or PANA. The main and backup DHCP servers are configured to synchronize with each other.

Procedure: The Host obtained a lease. Near lease expiration (+/-1/2 lease time) the main DHCP server is disconnected from the network.

Results: The Host should continue to obtain the same configuration parameters as before, without any manual intervention. All running applications and connections should not be affected.

5.3.2.4 Traffic shaper/policer baseline throughput test

Objective: Establish a baseline throughput measurement of stateful traffic through the SUT without enabling any traffic prioritization policies.

Setup:

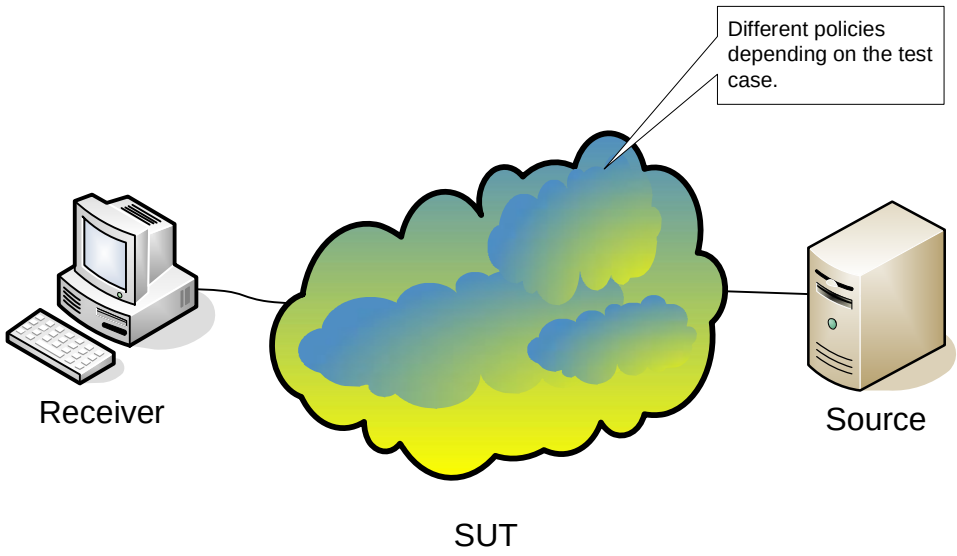


Figure 5-15: Traffic shaping and policing test setup

Prerequisites: The data plane is configured and operational. The traffic shaper/policer has no prioritization or bandwidth shaping policies active.

Procedure: Establish a connection and send a large amount of data to the requester. i.e. establish a TCP connection and issue a HTTP GET requests for a 10MB file. Measure the time it takes to transfer the file and calculate the obtainable goodput (=file size/time). This measurement should be repeated a number of time.

NOTE: Since we are using one single TCP connection to measure the throughput/goodput it is possible that in cases where the device has high throughput capabilities that due to limited TCP window scaling a lower measurement is obtained than would have been obtained if the window scaling function would have been enabled in the measurement host/device.

Results: An average obtainable goodput value should be obtained. This is then information used to assess the impact of different policies on the obtainable goodput.

5.3.2.5 Bandwidth policing test

Objective: Test traffic-shaping functionality and performance of the SUT based on different flow characteristics (i.e. HTTP request payload). These flow characteristics can be present in the ingress and/or egress direction. Each type of flow has a corresponding policy defining the maximum bandwidth.

Setup: See Figure 5-15.

Prerequisites: The data plane is configured and operational. For each of flow types (i.e. part of the URI) different bandwidth policies have been defined.

Procedure: Establish a connection for each of the chosen flow types. Measure for each of the flows the time it takes to transfer a given amount of data and calculate the obtained goodput. This measurement should be repeated a number of times. This test should also be performed with multiple instances of the different flow types.

Results: The goodput obtained by each of the flows should be in line with the defined policies as long as the total bandwidth is not exceeded.

5.3.2.6 Prioritization policing test

Objective: Test traffic-shaping functionality and performance of the SUT based on different flow characteristics. Each flow type has a corresponding policy defining the flow's priority relative to other flow types running through the SUT.

Setup: See Figure 5-15.

Prerequisites: The data plane is configured and operational. For each of the chosen flow types different prioritization policies are defined.

Procedure: Establish flows for each of the selected flow types. Measure for each of the flows the instantaneous goodput over the time of the experiment. This measurement should be repeated a number of times. This test should also be performed with multiple instances of the same flow type.

Results: The relative instantaneous goodput should be in line with the defined prioritization policy. The aggregated goodput should be ideally close to the baseline goodput.

5.3.2.7 Mixed traffic policing test

Objective: 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).

Setup: See Figure 5-15.

Prerequisites: The data plane is configured and operational. Define in the SUT, for some flows appropriate policies (e.g. bandwidth shaping). Define a policy to limit stateless traffic (i.e. reduce impact of ping flood attack) and some bandwidth shaping policies for a number of flow types.

Procedure: Send background traffic for example based on IMIX, through the SUT. Send multiple instances of the flow types through the SUT and additionally add stateless traffic (i.e. ping floods) up to the maximum attainable throughput of the SUT.

Results: The SUT should limit the stateless traffic in such a way that the other flows obtain the bandwidth/throughput as defined by the policy.

5.3.2.8 QoS verification

5.3.2.8.1.1 Introduction

Traditional performance tests (described in 5.2.2) focus on a per-port basis, addressing the evaluation of the performance of each port such as the maximum throughput, the packet loss and the average latency of the network device.
To evaluate the QoS functionality some additional aspects must be considered.

Flow-based measuring
Usually different applications are multiplexed onto a single device port, combining different QoS traffic classes. In order to evaluate the QoS feasibility of a network the test have to address individual traffic flows. A flow-based measuring is the foundation of the QoS testing. The measuring equipment has to be able to provide flow-based measuring procedures.

QoS metrics
QoS can be characterized by a set of network performance metrics including:

- End-to-End Throughput
- End-to-End Delay
- Frame Loss rate
- Delay variation or jitter
- Max. burst size
- Packet sequence – the ability of the network to deliver packets in proper sequence
- Service availability – the ability to gain access to the network
- Connection availability – the ability of the network to complete the required connections (i.e., TCP) with the requested performance characteristics

Jitter

The end-to-end jitter is relevant for streaming audio or video applications, where the receiver must compensate the maximum delay in the play-out buffer. For other applications such as web browsing or remote computing the end-to-end mean delay is relevant. The user experiences the mean delay when waiting for response. For remote computing also the maximum delay must be kept below the timeout value of handshake protocols.

The jitter is defined as (max delay – min delay). It is only valid together with the associated quantile.

5.3.2.8.1.2 QoS approach and resources reservation

Objective:

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

- Verify that the system is able to reserve resources end-to-end using Tight QoS control and/or
- Verify that the system is able to reserve resources on links with congestion risk (First Mile) using Loose QoS control

Setup:

- Figure 5-16 shows the test set-up.

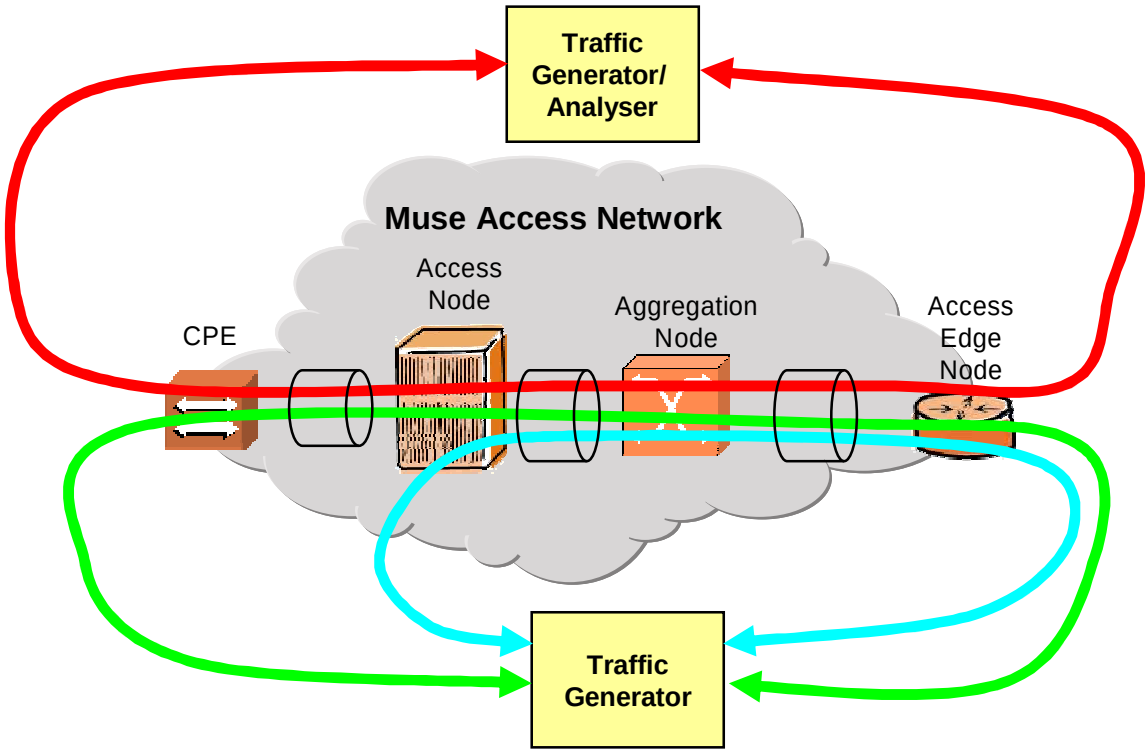


Figure 5-16: Test set-up to verify QoS approach and resources reservation

Prerequisites:

- Bandwidth broker and Call Admission control functionalities

Procedure:

- Generate a high quality flow (Low latency or Real time) that represents a Voice or Video session
- Generate an additional First Mile background traffic stream with the same QoS class that fills the whole capacity of the First Mile link.
- Analyze the QoS metrics of the high quality flow
- Generate an additional Aggregation Network background traffic stream (e.g. Best Effort traffic) that fills the whole capacity of the Aggregation Network links.
- Analyze the QoS metrics of the high quality flow again

Expected Results:

- In the case of First Mile background traffic good QoS metric values for Tight- or Loose- or Mixed- QoS approach
- In the case of Aggregation Network background traffic good QoS metric values for Tight QoS control only

5.3.2.8.1.3 Low rate Link restriction aspects

Objective:

- Verify the Bandwidth broker and Call Admission control functionalities considering the link restrictions described in the Test objectives document, section “Bottom-up solution for QoS “.

Setup:

- Figure 5-17 shows two possible test set-ups to verify Bandwidth broker and Call Admission control functionalities

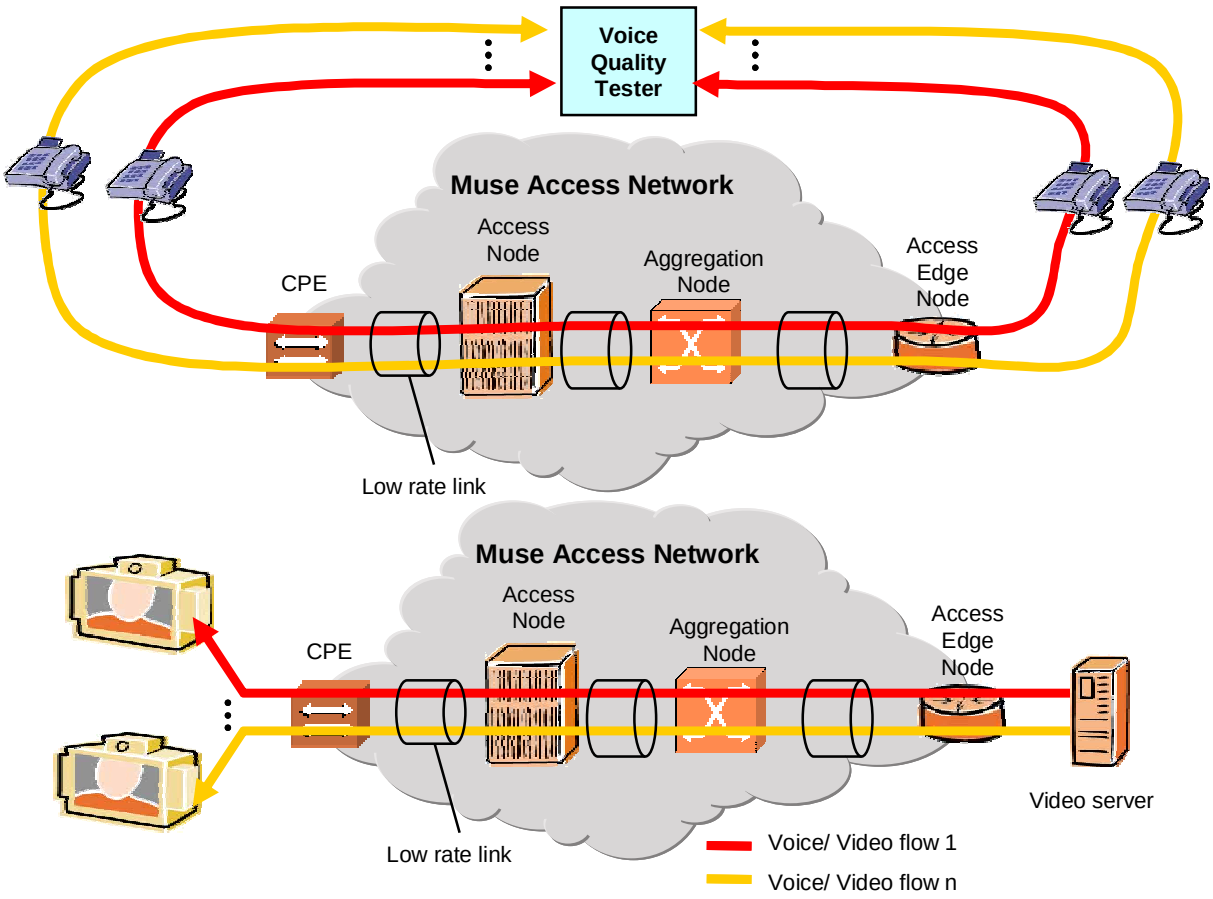


Figure 5-17: Test set-up Low rate link restrictions

Prerequisites:

- The system under test must provide Low rate links as described in Table 5-2.

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 5-2: Parameters for low rate links

Procedure:

- Set-up a Low rate link according to Table 5-2 (Link rate: 0.5M, 1M, 2M, 5M or 10M)
- Start one or more QoS class flows according to Table 5-2
- Try to set-up more flows than allowed.

Expected Results:

- It is not possible to set-up more flows than allowed
- Bandwidth broker and Call Admission control functionalities consider the link restrictions

5.3.2.8.1.4 Specific Loose QoS control aspects

Objective:

- Verify the system behavior using Loose QoS control in case of congestion.
- Verify if a switching from Loose to Tight QoS control is supported

Setup:

- The set-up is depicted in Figure 5-16.

Prerequisites:

- The Loose control implementation must support mechanisms to act in case of congestion. Two mechanisms are described in MA2.10:
  - An additional central QoS control unit should instruct to use more restrict policing profiles
  - The system switches from Loose to Tight QoS control

Procedure:

- Generate a congestion situation at the Access Node uplink using a Traffic generator
- Try to set-up some additional service flows
- In the case of successful set-up of additional service flows check if Tight QoS control is enabled

Expected Results:

- In case of congestion the system under test uses more restrict policing profiles, or
- the system under test switches from Loose to Tight QoS control

5.3.2.8.1.5 Priority queuing

Objective:

- 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
- Verify the queuing behavior of the system under test considering all supported queuing mechanisms but at least strict priority queuing

Setup: The test set-up is depicted in Figure 5-18.

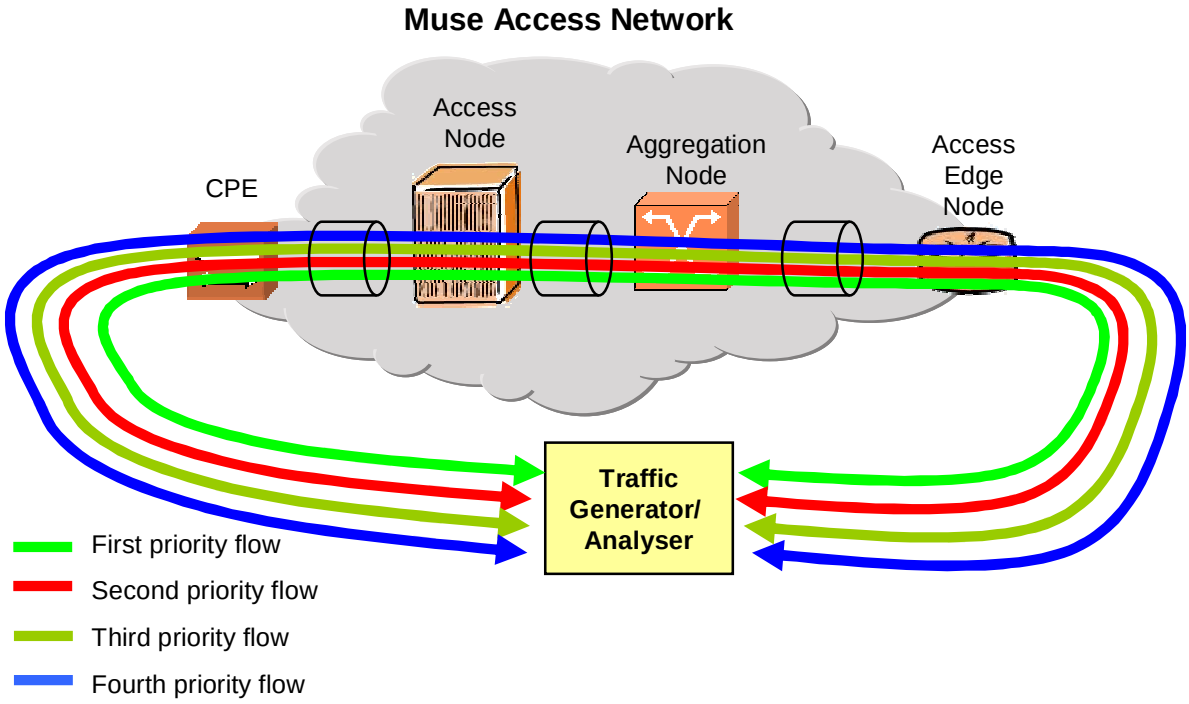


Figure 5-18: Test set-up for Priority queuing

Prerequisites:

- 4 QoS classes must be supported

Procedure:

- Strict priority set-up
  - Set-up and generate 4 QoS class IP flows (First, Second, Third and Fourth priority flow) using a Traffic Generator
  - Increase the traffic load for all flows up to the max link rate. (e.g. for the case of a max link rate of 20 Mbps each QoS class flow must be increased up to 20 Mbps)
  - Analyze the strict priority queuing behavior using a Traffic Analyzer
- Set-up on the basis of other queuing mechanisms
  - Analyze the priority queuing behavior considering the queuing mechanism characteristics

Expected Results:

- The system under test supports at least 4 QoS classes conform to the MUSE bottom-up approach for QoS
- Strict priority set-up
  - In case of congestion at first the Fourth priority packets are dropped, then the Second priority packets and at last the Third priority packets. First priority packets are never dropped.
- Other queuing mechanisms
  - The dropping behavior depends on the bandwidth weighting per QoS class

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

Objective:

- Verify the end-to-end throughput, the end-to-end delay, the Packet loss rate, the end-to-end Jitter, the max. burst size and the packet sequence of a Low latency QoS class stream.

Setup: The test set-up is depicted in Figure 5-19.

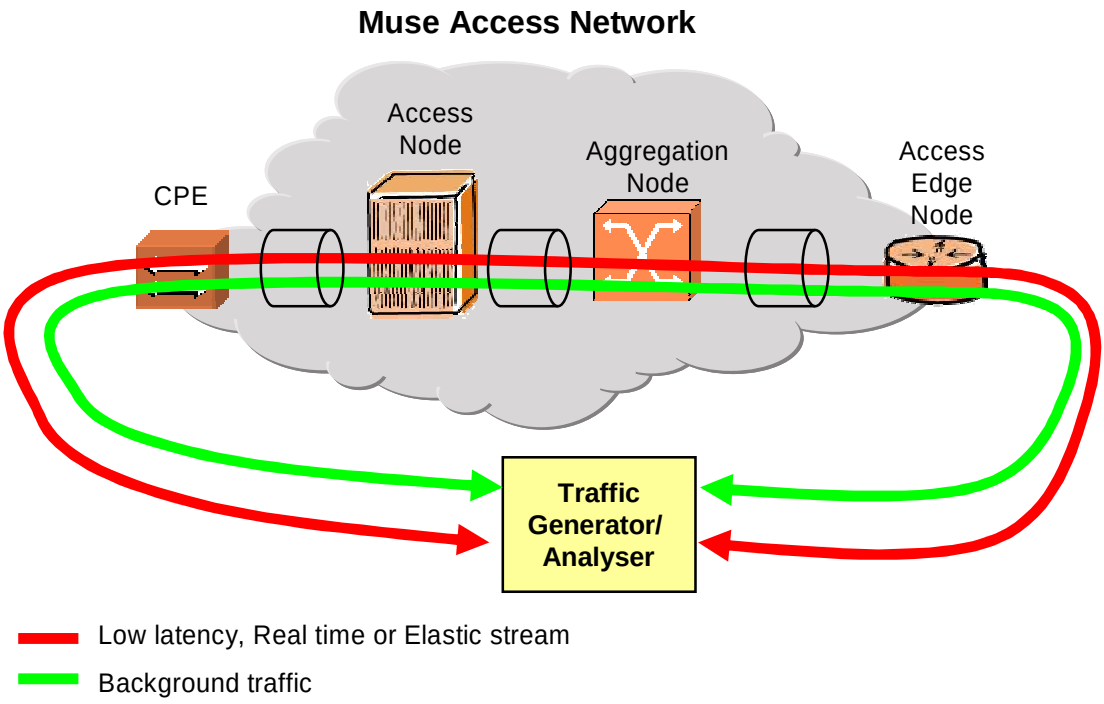


Figure 5-19: Test set-up QoS class performance tests

Prerequisites: -

Procedure:

- Set-up a Layer-3 (IP) end-to-end Low latency QoS class stream (downstream) with the Max. burst size using a Traffic Generator
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the packet sequence of the system under test without congestion situation using a Traffic Analyzer

- Set-up an additional background traffic stream (e.g. Best Effort traffic) that fills the whole capacity of the link.
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the packet sequence of the Low latency stream with congestion situation using a Traffic Analyzer
- Repeat the test procedure for upstream traffic

Expected Results:
- End-to-end Throughput: Committed Information Rate (CIR)
- End-to-End Delay was not specified by MUSE so far (for further studies)
- Max. jitter target per node: 1 ms
- Max. Packet loss rate per node: 10-10
- Max. burst size: 200 byte
- Packet sequence: No sequence failures (Note: Not specified by MUSE)

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

Objective:
- Verify the end-to-end Throughput, the end-to-end delay, the Packet loss rate, the end-to-end Jitter, the max. burst size and the packet sequence of a Real time QoS class stream.

Setup: The test set-up is depicted in Figure 5-19.

Procedure:
- Set-up a Layer-3 (IP) end-to-end Real time QoS class stream (downstream) with the Max. burst size using a Traffic Generator
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the packet sequence of the system under test without congestion situation using a Traffic Analyzer
- Set-up an additional background traffic stream (e.g. Best Effort traffic) that fills the whole capacity of the link.
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the packet sequence of the Real time stream with congestion situation using a Traffic Analyzer
- Repeat the test procedure for upstream traffic

Expected Results:
- End-to-end Throughput: Committed Information Rate (CIR)
- End-to-End Delay was not specified by MUSE so far (for further studies)
- Max. jitter target per node: 30 ms
- Max. Packet loss rate per node: 10^{-10}
- Max. burst size: 1500 byte
- Packet sequence: No sequence failures(Note: Not specified by MUSE)

5.3.2.8.1.8 Elastic QoS class stream with full link capacity background traffic

Objective:
- Verify the end-to-end Throughput, the end-to-end delay, the Packet loss rate, the end-to-end Jitter, the max. burst size and the Packet sequence of a Elastic QoS class stream (AF low drop precedence).

Setup: The test set-up is depicted in Figure 5-19.

Procedure:

- Set-up a Layer-3 (IP) end-to-end Elastic QoS class downstream (AF low drop precedence) with the Max. burst size using a Traffic Generator
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the Packet sequence of the system under test without congestion situation using a Traffic Analyzer
- Set-up an additional background traffic stream (e.g. Best Effort traffic) that fills the whole capacity of the link.
- Analyze end-to-end Throughput, the end-to-end delay, the end-to-end Packet loss rate, the end-to-end Jitter and the Packet sequence of the Elastic stream with congestion situation using a Traffic Analyzer
- Repeat the test procedure for upstream traffic

Expected Results:

- End-to-end Throughput: Committed Information Rate (CIR)
- End-to-End Delay was not specified by MUSE so far (for further studies)
- Max. jitter target per node: 900 ms
- Max. Packet loss rate per node: 10^{-10}
- Max. burst size: 9000 byte
- Packet sequence: No sequence failures (Note: Not specified by MUSE)

6 CONNECTIVITY TESTING OF RESIDENTIAL GATEWAYS

6.1 Introduction

This chapter describes the test procedures for higher layer residential gateway testing in deep detail. In fact, the chapters on residential gateway testing were described while implementing an automatic test suite. As such, only IGMP, IGMP proxy, DHCP and part of PPPoE are tested.

6.2 Multicast test methods

The test objectives specified for the RGW testing result in a couple of test methods which are defined in this section. First, we start with two tables which define the relation between the test objectives and the test methods.

Test method	Test objective/requirement
igmpproxyv3.mhost.mhost-01	I 1, I 2, I 3, I 5
igmpproxyv3.mhost.mhost-02	I 25
igmpproxyv3.mhost.mhost-03	I 7
igmpproxyv3.mhost.mhost-04	I 8
igmpproxyv3.mhost.mhost-05	IP 3
igmpproxyv3.mhost.mhost-06	I 9
igmpproxyv3.mhost.mhost-07	I 34
igmpproxyv3.mhost.mhost-08	I 23
igmpproxyv3.mhost.interopv2-01	I 26, I 27, IP 7
igmpproxyv3.mhost.interopv2-02	I 11, I 12, I 13, I 14
igmpproxyv3.mhost.interopv2-03	I 29
igmpproxyv3.mhost.interopv1-01	I 15, I 16
igmpproxyv3.mrouter.mrouter-01	I 1, I 2, I 3, I 4, I 36
igmpproxyv3.mrouter.mrouter-02	I 35
igmpproxyv3.mrouter.mrouter-03	I 37
igmpproxyv3.mrouter.mrouter-04	I 7
igmpproxyv3.mrouter.mrouter-05	I 8
igmpproxyv3.mrouter.mrouter-06	I 6
igmpproxyv3.mrouter.mrouter-08	I 45
igmpproxyv3.mrouter.mrouter-09	I 10
igmpproxyv3.mrouter.mrouter-10	I 33
igmpproxyv3.mrouter.query-01	
igmpproxyv3.mrouter.query-02	
igmpproxyv3.mrouter.interop-01	I 46
igmpproxyv3.igmpv3.*	I 18, I 19, I 21, I 38, I 40, I 41, I 44, IP 4, IP 5
igmpproxyv3.hosttracking.*	I 18, I 19, I 21, I 38, I 40, I 41, I 44, IP 4, IP 5, RG 9
igmpproxyv3.interopv2.*	I 18, I 19, I 21, I 38, I 40, I 41, I 44, IP 4, IP 5, I 49, I 50

State transition (Interop. IGMPv2 + HT)	I 18, I 19, I 21, I 38, I 40, I 41, I 44, IP 4, IP 5, I 49, I 50, RG 9
State transition tests (interop. IGMPv1)	I 18, I 19, I 21, I 38, I 40, I 41, I 44, IP 4, IP 5, I 49, I 51
igmpproxyv3.forward.forward	I 39, IP 6, RG 2, RG 4
igmpproxyv3.specific.testrg47	RG 6
igmpproxyv3.specific.testrg48	RG 7
igmpproxyv3.specific.testrg49	RG 8
igmpproxyv3.specific.testrg56	RG 5
igmpproxyv3.igmpv3.fastleave-01	
igmpproxyv3.igmpv3.fastleave-02	
igmpproxyv3.igmpv3.fastleave-03	
igmpproxyv3.igmpv3.fastleave-04	
igmpproxyv3.igmpv3.fastleave-05	
igmpproxyv3.specific.performance-01	RG 10
igmpproxyv3.specific.noip-01	RG 12
igmpproxyv3.specific.noip-02	RG 13
igmpproxyv3.specific.multi-01	RG 15
igmpproxyv3.specific.multi-02	RG 16
igmpproxyv3.specific.multi-03	RG 14
igmpproxyv3.specific.testrg201	RG 21
igmpproxyv3.specific.testrg43	RG 23
Fast-Leave tests	RG 9
Query tests	I 1, I 2, I 3, I 5

Test objective/requirement	**Test method**
I 1	igmpproxyv3.mhost.mhost-01, igmpproxyv3.mrouter.mrouter-01
I 2	igmpproxyv3.mhost.mhost-01, igmpproxyv3.mrouter.mrouter-01
I 3	igmpproxyv3.mhost.mhost-01, igmpproxyv3.mrouter.mrouter-01
I 4	igmpproxyv3.mrouter.mrouter-01
I 5	igmpproxyv3.mhost.mhost-01
I 6	igmpproxyv3.mrouter.mrouter-06
I 7	igmpproxyv3.mhost.mhost-03, igmpproxyv3.mrouter.mrouter-04
I 8	igmpproxyv3.mhost.mhost-04, igmpproxyv3.mrouter.mrouter-05
I 9	igmpproxyv3.mhost.mhost-06
I 10	igmpproxyv3.mrouter.mrouter-09
I 11	igmpproxyv3.mhost.interopv2-02
I 12	igmpproxyv3.mhost.interopv2-02
I 13	igmpproxyv3.mhost.interopv2-02
I 14	igmpproxyv3.mhost.interopv2-02
I 15	igmpproxyv3.mhost.interopv1-01
I 16	igmpproxyv3.mhost.interopv1-01
I 17	n/a (igmpv1 router only)
I 18	igmpproxyv3.igmpv3.*,

	igmpproxyv3.interopv2.*
I 19	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 20	Not yet available: empty ALLOW/BLOCK
I 21	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 22	Not yet available: merging reports
I 23	igmpproxyv3.mrouter.mrouter-07
I 24	Not yet available: combined responses
I 25	igmpproxyv3.mhost.mhost-02
I 26	igmpproxyv3.mhost.interopv2-01
I 27	igmpproxyv3.mhost.interopv2-01
I 28	n/a
I 29	igmpproxyv3.mhost.interopv2-03
I 30	Not yet available: suppress IGMPv3 Report
I 31	n/a (igmpv1 router only)
I 32	n/a (igmpv2 router only)
I 33	igmpproxyv3.mrouter.mrouter-10
I 34	igmpproxyv3.mhost.mhost-07
I 35	igmpproxyv3.mrouter.mrouter-02
I 36	igmpproxyv3.mrouter.mrouter-01
I 37	igmpproxyv3.mrouter.mrouter-03
I 38	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 39	igmpproxyv3.forward.forward
I 40	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 41	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 42	Not yet available: router side process flag
I 43	Not yet available: router side process flag
I 44	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
I 45	igmpproxyv3.mrouter.mrouter-08
I 46	igmpproxyv3.mrouter.interop-01
I 47	n/a (IGMPv1 router only)
I 48	n/a (IGMPv2 router only)
I 49	igmpproxyv3.interopv1.*, igmpproxyv3.interopv2.*
I 50	igmpproxyv3.interopv2.*
I 51	igmpproxyv3.interopv1.*
IP 1	This is implied by the other tests.
IP 2	[Testing IGMP-Proxy Requirements]
IP 3	igmpproxyv3.mhost.mhost-05
IP 4	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
IP 5	igmpproxyv3.igmpv3.*, igmpproxyv3.interopv2.*
IP 6	igmpproxyv3.forward.forward
IP 7	igmpproxyv3.mhost.interopv2-01
RG 1	[Testing IGMP-Proxy Requirements]

RG 2	igmpproxyv3.forward.forward
RG 3	Ok, if all tests are performed on all ports.
RG 4	igmpproxyv3.forward.forward
RG 5	igmpproxyv3.specific.testrg56
RG 6	igmpproxyv3.specific.testrg47
RG 7	igmpproxyv3.specific.testrg48
RG 8	igmpproxyv3.specific.testrg49
RG 9	State transition (IGMPv3+HT, Interop. IGMPv2+HT)
RG 10	igmpproxyv3.specific.performance-01
RG 11	**SETUP 4**
RG 12	igmpproxyv3.specific.noip-01
RG 13	igmpproxyv3.specific.noip-02
RG 14	igmpproxyv3.specific.multi-03
RG 15	igmpproxyv3.specific.multi-01
RG 16	igmpproxyv3.specific.multi-02
RG 17	
RG 18	Not yet available: filter
RG 19	Not yet available: filter
RG 20	Not yet available: filter
RG 21	igmpproxyv3.specific.testrg201
RG 22	igmpproxyv3.specific.testrg42
RG 23	igmpproxyv3.specific.testrg43

Not all tests can be executed on all possible configuration setups. As such, some setups are defined and for tests which can be run only on a subset of these configuration setups, the setup number is listed in the test method.

SETUP 1: PPPoE with IGMP-Proxy and switch

The RGW initiates a PPPoE session on its WAN interface. IGMP-Proxy is enabled with one upstream interface (WAN) and one downstream interface (LAN). If the device has multiple LAN interfaces they are Ethernet switched. All LAN interfaces are thus connected to the same downstream interface of the IGMP-Proxy.

SETUP 2: IPoE with IGMP-Proxy and switch

Similar as **SETUP 1** but with IPoE encapsulation on the WAN interface (e.g. static IP address or automatic IP address configuration with DHCP).

SETUP 3: IGMP-Proxy with a downstream interface for every port (IPoE)

IGMP-Proxy configuration with IPoE encapsulation on the upstream interface (WAN) and a downstream interface for each LAN port. This setup assumes that the RGW has multiple LAN ports.

SETUP 4: IPoE upstream interface with ip address 0.0.0.0.

Identical to **SETUP 2** but the upstream interface MUST be configured to have the IP address 0.0.0.0 (either give up no IP address or set it explicitly to 0.0.0.0).

SETUP 5: IPoE and PPPoE interface over one PVC with IGMP-Proxy

IGMP-Proxy configuration with two upstream interfaces and one (or more) downstream interface(s). The first upstream interface uses IPoE encapsulation and the second PPPoE encapsulation.
There are different possibilities to configure this:
1. Both upstream interfaces over one PVC (the one proposed here)
2. Two IP upstream interfaces over the same Ethernet upstream interface. Might be used in ATM empty configurations.

SETUP 6: IPoE and PPPoE interfaces with IGMP-Proxy on one upstream interface

The RGW is configured with two WAN interfaces (IPoE and PPPoE encapsulation), but the IGMP-Proxy functionality is only enabled on the IPoE interface.

SETUP 7: IPoE and PPPoE interfaces with IGMP-Proxy and forwarding only on IPoE

RGW configuration with two upstream interfaces; an IPoE interface and a PPPoE interface. Multicast forwarding in the upstream direction must only be enabled on the IPoE interface, but IGMP Proxy reporting must be enabled on both interfaces.

SETUP 8: IGMP-Proxy with a custom multicast range blocked

SETUP 9: IGMP-Proxy with an IPoE upstream interface and switch (fast leave)

IGMP-Proxy configuration with fast leave (or host tracking) functionality enabled.

SETUP 10: IGMP-Proxy with limit on simultaneous multicast streams enabled

6.2.1 Testing IGMP-Proxy Requirements

6.2.1.1 Introduction

The test cases related to upstream interfaces and downstream interfaces will be described next.

6.2.1.1.1 Upstream Interfaces: Multicast Host Requirements

6.2.1.1.1.1 Test: igmpproxyv3.mhost.mhost-01 (packet format requirements)

Setup: **SETUP 1**, **SETUP 2**

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 5 IGMPv3 reports are sent with IP Destination of 224.0.0.22.

Procedure:
1. Reset device.
   State: empty state

2. Send an IGMPv3 Report with an ALLOW(G, {a}) record.
   State: INCLUDE(G, {a})
3. Wait for an IGMPv3 report on the upstream interface.
4. Verify that the value of the Time-to-Live field in the IP Header is set to 1.
5. Verify that the value of Type of Service in the IP Header is set to 0xC0.
6. Verify that the Destination IP Address is set to 224.0.0.22.
7. Verify that the IP Headers contains an IP Router Alert option.

6.2.1.1.1.2 Test: igmpproxyv3.mhost.mhost-02a,b,c (reply to a query)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
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.

6.2.1.1.1.2.1 Test: igmpproxyv3.mhost.mhost-02a (reply to an IGMPv3 General Query)

1. Reset device.
   State: empty state
2. Send an IGMPv3 Report with an ALLOW(G, {a}) record .
   State: INCLUDE(G, {a})
3. Send an IGMPv3 General Query with destination IP address 224.0.0.0.1.
4. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {a}) record.
5. Send an IGMPv3 General Query on the upstream interface with destination IP address set to (one of) its public ip address(es).
6. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {a}) record.

6.2.1.1.1.2.2 Test: igmpproxyv3.mhost.mhost-02b (reply to an IGMPv3 Group-Specific Query)

1. Reset device.
   State: empty state
2. Send an IGMPv3 Report with an ALLOW(G, {a, b}) record
   State: INCLUDE(G, {a})
3. Send an IGMPv3 Group-Specific Query Q(G) with destination IP address G.
4. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {a, b}) record.
5. Send an IGMPv3 Group-Specific Query Q(G) with destination IP address 224.0.0.1.
6. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {a, b}) record.
7. Send an IGMPv3 General Query Q(G) on the upstream interface with destination IP address set to (one of) its public ip address(es).
8. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {a, b}) record.

6.2.1.1.1.2.3 Test: igmpproxyv3.mhost.mhost-02c (reply to an IGMPv3 Group-and-Source-Specific Query)

1. Reset device.
   State: empty state
2. Send an IGMPv3 Report with an ALLOW(G, {a, b}) record

State: INCLUDE(G, {a, b})
3. Send an IGMPv3 Group-and-Source-Specific Query Q(G, {b, c}) with destination IP address G.
4. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {b}) record.
5. Send an IGMPv3 Group-and-Source-Specific Query Q(G, {b, c}) with destination IP address 224.0.0.1.
6. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {b}) record.
7. Send an IGMPv3 Group-and-Source-Specific Query Q(G, {b, c}) on the upstream interface with destination IP address set to (one of) its public ip address(es).
8. The proxy MUST send one IGMPv3 Report containing an IS_IN(G, {b}) record.

6.2.1.1.1.3 Test: igmpproxyv3.mhost.mhost-03 (future extensions)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
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.

Procedure:
1. Reset device.
2. Send a Current-State Report on a downstream interface: IS_IN(G1, {a, b}), IS_IN(G2, {b, c})
3. Send a General Query Q on the upstream interface with some extra data appended after the empty Source Address fields, this extra data must be included in the checksum calculation.
4. The proxy MUST send an IS_IN(G1, {a, b}) and an IS_IN(G2, {b, c}) record.
5. Send a Group-Specific Query Q(G1) on the upstream interface with some extra data appended after the empty Source Address fields.
6. The proxy MUST send an IS_IN(G1, {a, b}) record.
7. Send a Group-and-Source-Specific Query Q(G1, {a, c}) on upstream with some extra data appended after the Source Address fields.
8. The proxy MUST send an IS_IN(G1, {a}) record.

6.2.1.1.1.4 Test: igmpproxyv3.mhost.mhost-04 (checksum)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
I 8 The checksum field in Query and Report messages MUST be verified before processing a message.

Procedure:
1. Reset device.
2. Send a Current-State Report on a downstream interface: IS_EX(G1, {}), IS_EX(G2, {})
3. Send a Group-Specific Query for group G1 on upstream with an invalid IGMP checksum.
4. The device MUST NOT respond and send an report with IS_EX(G1, {})

6.2.1.1.1.5 Test: igmpproxyv3.mhost.mhost-05 (upstream interface is not an igmp router)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
IP 3 The igmp proxy device MUST NOT perform the router portion of IGMP on its upstream interface.

Procedure:
1. Reset device.
   State: empty state
2. The proxy device MUST NOT send a General Query on its upstream interface. (verify this for an interval of at least [Other Querier Present Interval])

Default value:
Other Querier Present Interval = (Robustness Variable * Query Interval) + (Query Response Interval)/2 = 2 * 125 + 10/2 = 255

6.2.1.1.1.6 Test: igmpproxyv3.mhost.mhost-06 (membership report size)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
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.

We assume a MTU of 1500:
Headers: 8 (preamble) + 14 (eth) + 2 (crc) + 20 (ip) + 4 (router alert) + 8 (igmp) = 56
Record: IS_IN(G, 16 Sources): 8 + 4*16=72
Maximum 20 records per IGMPv3 Report.

Procedure:
1. Reset device.
   State: empty state
2. Send IS_IN(Gx, Sx,y) with x:1..10 and y:1..16 on downstream interface
   Send IS_IN(Gx, Sx,y) with x:11..20 and y:1..16 on downstream interface
   Send IS_IN(Gx, Sx,y) with x:21..30 and y:1..16 on downstream interface
3. Send a General Query on upstream interface
4. Verify that there are no IMGP Reports sent with size greater them the MTU (fragmentation) and that for all groups (Gx x:1..30) the correct sources are reported.

Problem:
Testing splitting of IS_EX records: for a MTU of 1500 we would need to send an IS_EX record with 349 sources, do we change the MTU ?

6.2.1.1.1.7 Test: igmpproxyv3.mhost.mhost-07 (no igmp packets for 224.0.0.1)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
I 34 No IGMP messages are ever sent regarding the all-systems multicast address (224.0.0.1).

Procedure:
1. Reset device.
   State: empty state
2. Send an ALLOW(G, {a}) report on downstream interface
3. Give the device some time to send State-Change records on upstream
4. Send an IGMPv3 General Query on upstream
5. Wait for a report and verify that there is no record with a multicast group field set to 224.0.0.1.
6. Send TO_EX(224.0.0.1, {}) on downstream interface.
7. Send TO_IN(224.0.0.1, {a}) on downstream interface.
8. Verify that no reports or queries are sent regarding multicast group 224.0.0.1.

6.2.1.1.1.8 Test: igmpproxyv3.mhost.mhost-08 (burstiness of responses to queries)

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.

Future work: Make test procedure, delay depends nonlinearly on the Max Resp Code.

6.2.1.1.1.9 Test: igmpproxyv3.mhost.interopv2-01 (IGMPv3 to IGMPv2 transition on upstream interface)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
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.
I 27 The version of IGMP a host uses MUST be equal to its Compatibility Mode.
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.

Procedure:
1. Reset device and initialize the device into its startup state.
   State: [Host=1] IN(G1, {a})
   [Host=2] IN(G2, {b})
   INCLUDE(G1, {a}), INCLUDE(G2, {b})
2. Send an IGMPv3 General Query on the upstream interface
3. The device MUST send a report with IS_IN(G1, {a, b}), IS_IN(G2, {b}) records.
4. Send an IGMPv2 General Query on the upstream interface forcing the device to go into IGMPv2 Host Compatibility Mode.
5. The device MUST send a REPORTv2(G1) and a REPORTv2(G2) message.
6. Send an IGMPv2 Group-Specific Query Qv2(G1)
7. The device MUST send a REPORTv2(G1) message.

6.2.1.1.1.10 Test: igmpproxyv3.mhost.interopv2-02 (IGMPv2 packet requirements)

Setup: **SETUP 1**, **SETUP 2**

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.

Procedure:
1. Reset device and initialize the device into its startup state.
   State: [Host=1] EX(G:T, {})
   EXCLUDE(G:T1, ({}, {}))
2. Send an IGMPv2 General Query on the upstream interface.
3. Wait for a report from the device on the upstream interface.
4. Verify that the Time-to-Live field of the IP Header is set to 1.
5. Verify that the IP Header contains an IP Router Alert options.
6. Verify that the IP Destination Address and the Group Address field of the Report is set to G.
7. Group Timer G expires at T1+GMI
8. Receive a IGMPv2 Leave message on upstream interface
9. Verify that the Time-to-Live field of the IP Header is set to 1.
10. Verify that the IP Header contains an IP Router Alert options.
11. Verify that the IP Destination Address is set to 224.0.0.0.2.

6.2.1.1.1.11 Test: igmpproxyv3.mhost.interopv2-03 (handling IGMPv3 queries in IGMPv2 mode)

Setup: **SETUP 1**, **SETUP 2**

Requirements:
I 29 IGMP Queries are designed to be backwards compatible, IGMPv3 Group-Specific and IGMPv3 Group-and-Source-Specific Queries are interpreted, as IGMPv2 Group-Specific Queries by IGMPv2 devices and as IGMPv1 General Queries by IGMPv1 Hosts.

Procedure:
1. Reset device and initialize the device into its startup state.
   State: [Host=1] IN(G1, {a})
   [Host=2] IN(G2, {b})
   INCLUDE(G1, {a}), INCLUDE(G2, {b})
2. Send an IGMPv2 General Query on the upstream interface
3. Give the device some time to respond (QRI seconds).
4. Send an IGMPv3 General Query (an IGMPv2 host must interpret this as an IGMPv2 General Query)
5. The device MUST send a REPORTv2(G1) and a REPORTv2(G2) message.
6. Send an IGMPv3 Group-Specific Query Qv3(G1) (an IGMPv2 host must interpret this as an IGMPv2 Group-Specific Query)
7. The device MUST send a REPORTv2(G1) message.

8. Send an IGMPv3 Group-and-Source-Specific Query Qv3(G1, {b, c}) (an IGMPv2 host must interpret this as an IGMPv2 Group-Specific Query)
9. The device MUST send a REPORTv2(G1) message.

6.2.1.1.1.12 Test: igmpproxyv3.mhost.interopv1-01 (IGMPv1 packet requirements)

Setup: **SETUP 1**, **SETUP 2**

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.

Procedure:
1. Reset device and initialize the device into its startup state.
   State: [Host=1] EX(G, { })
   INCLUDE(G, { })
2. Send an IGMPv1 General Query on the upstream interface
3. Wait for a report from the device on the upstream interface.
4. Verify that the Time-to-Live field of the IP Header is set to 1.
5. Verify that the IP Destination Address and the Group Address field of the Report is set to G

6.2.1.1.2 Downstream interface: Multicast Router Requirements

6.2.1.1.2.1 Test: igmpproxyv3.mrouter.mrouter-01 (packet format requirements)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

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 36 Multicast Routers send General Queries periodically to request group membership information from an attached network.

Procedure:
1. Reset device
   State: empty state
2. Wait for two subsequent IGMPv3 General Query on a downstream interface.
3. Verify that the interval between two General Queries is [Query Interval]
4. Verify that the value of the IP Time-to-Live field in the IP Header is set to 1
5. Verify that the Type of Service field in the IP Header is set to 0xC0.
6. Verify that the IP Destination Address is set to 224.0.0.1.
7. Verify that the IP Header contains an IP Router Alert option.

6.2.1.1.2.2 Test: igmpproxyv3.mrouter.mrouter-02 (report group 224.0.0.22 on downstream interface)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 35 A Multicast Router MUST perform the group membership part of IGMPv3 for the multicast address 224.0.0.22.

Procedure:
1. Reset device.
   State: empty state
2. Wait for an IGMPv3 General Query on a downstream interface.
3. An IGMPv3 Report with an IS_EX(224.0.0.22, {}) record MUST be sent from the proxy device and this in within an interval of [Query Response Interval] after the IGMPv3 General Query arrived.

Default value:
Query Response Interval = 10 sec

6.2.1.1.2.3 Test: igmpproxyv3.mrouter.mrouter-03 (accept a report from 0.0.0.0)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 37 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.

Procedure:
1. Reset device.
   State: empty state
2. Send an IGMPv3 Report with an ALLOW(G, {a}) record with source IP 0.0.0.0.
   State: INCLUDE(G, {a})
3. Send an IGMPv3 General Query on the upstream interface
4. The device MUST send an report with an IS_IN(G, {a}) record.

Note: Using a General Query to request the current status of the upstream interface is more robust then listening for State-Change Reports.

6.2.1.1.2.4 Test: igmpproxyv3.mrouter.mrouter-04 (future extensions)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
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.

Procedure:
1. Reset device.
   State: empty state

2. Send a report with two records, e.g. ALLOW(G1, {a}) and TO_EX(G2, {b}), with extra data after its source addresses and the group records. Make sure the checksum is valid.
   State: G1 -> INCLUDE({a})
   G2 -> EXCLUDE({}, {b})
3. Send a Genral Query on the upstream interface
4. Verify that an IGMPv3 Report is sent with IS_IN(G1, {a}), IS_EX(G2, {b})

6.2.1.1.3 Test: igmpproxyv3.mrouter.mrouter-05 (checksum verification)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 8 The checksum field in Query and Report messages MUST be verified before processing a message.

Procedure:
1. Reset device.
   State: empty state
2. Send an ALLOW(G, {a }) report
   State: INCLUDE(G, {a})
3. Send an ALLOW(G, {b}) report with an invalid IGMP checksum
   State: INCLUDE(G, {a})
4. Send a General Query on upstream
5. The device MUST send a report with an IS_IN(G, {a}) record.

6.2.1.1.3.1 Test: igmpproxyv3.mrouter.mrouter-06 (Destination IP Address of Specific Queries)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
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.

Procedure:
1. Reset and initialize device in the startup state
   State: [Source=1] EX(G, {a,b,c,d}) -> T1
   [Source=2] IN(G, {c, d}) -> T1*
   EXCLUDE({c:T1*, d:T1*}, {a, b}:T1)
2. T2: Send [Source=3] TO_IN(G, {c}) on downstream interface
   State: [Source=1] EX(G, {a,b,c,d})
   [Source=2] IN(G, {c, d})
   [Source=3] IN(G, {c})
   EXCLUDE({c:T2, d:T1*}, {a, b}:T1)
3. Receive Group-and-Source-Specific Query Q(G, {d}) on downstream interface
4. Verify that this query has an IP destination address equal to G
5. Receive Group-Specific Query Q(G) on upstream interface
6. Verify that this query has an IP destination address equal to G

6.2.1.1.3.2 Test: igmpproxyv3.mrouter.mrouter-08 (querier election)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 45 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.

Procedure:
1. Reset device.
   State: empty state
2. Wait for a General Query on a downstream interface, record the source IP address (IP_IGMPPROXY)
3. Send a General Query on the same downstream interface with a lower source IP address and in the same subnet.
4. Wait for the next General Query sent with source IP address set to IP_IGMPPROXY.
5. Verify that [Other Querier Present Interval] seconds have passed since step 3, if not the General Query was sent to soon and the device fails this test.

6.2.1.1.3.3 Test: igmpproxyv3.mrouter.mrouter-09 (ignore unrecognized record type)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 10 Unrecognized Record Type values MUST be silently ignored.

Procedure:
1. Start: reset device
2. Send IS_IN(G1, {a, b}) on a downstream interface
3. Send an IGMPv3 Report with IS_IN(G2, {d, e}) and an unknown record type (e.g. 7) for group G1 and source list {b, c}.
4. Send a General Query on the upstream interface
5. Receive IS_IN(G1, {a, b}), IS_IN(G2, {d, e}) on the upstream interface.
6. Verify that no specific queries are sent on the downstream interface.

6.2.1.1.3.4 Test: igmpproxyv3.mrouter.mrouter-10 (igmp router must respond to queries)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 33 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.

Procedure:
1. Reset device.
   State: empty state
2. Send an IS_IN(G, {a}) report on the downstream0 interface.
   State: INCLUDE(G, {a})
3. Send a General Query on the downstream1 interface.

4. Verify if an IS_IN(G, {a}) report is received from the igmp proxy device on downstream1.

6.2.1.1.3.5 Test: igmpproxyv3.mrouter.interop-01 (IGMP version misconfiguration warning)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
I 46 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.

Procedure:
1. Reset device.
2. Send a IGMPv2 General Query on downstream interface
3. Login the device and verify if a warning is logged.
4. Reset device.
5. Send an IGMPv1 Query on downstream interface.
6. Login the device and verify if a warning is logged.

6.2.1.1.3.6 Test: igmpproxyv3.mrouter.query-01 (Group-and-Source-Specific Query)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Objective:
This test verifies if the downstream interfaces handle correctly group-and-source-specific queries.

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1, c:T1})
   INCLUDE(G, {a:T1, b:T1, c:T1})
2. T2: Send [Host=1,2] BLOCK(G, {b, c}) on downstream interface
   State: INCLUDE(G, {a:T1, b:T1, c:T1})
3. (RV x) Receive a Group-and-Source-Specific Query Q(G, {b, c}) on downstream interface
   State: INCLUDE(G, {a:T1, b:T2+LMQT, c:T2+LMQT})
4. T3: Send [Host=1,2,3] IS_IN(G, {c}) on downstream interface
   State: INCLUDE(G, {a:T1, b:T2+LMQT, c:T3})
5. Source Timer for {b} will expire at T2+LMQT
   State: INCLUDE(G, {a:T1, c:T3})
6. (RV x) Receive a BLOCK(G, {b}) on upstream interface
7. Source Timer for {a} will expire at T1+GMI
   State: INCLUDE(G, {c:T3})
8. (RV x) Receive a BLOCK(G, {a}) on upstream interface
9. Source Timer for {c} will expire at T3+GMI
   State: INCLUDE(G, {})
10. (RV x) Receive a BLOCK(G, {c}) on upstream interface

6.2.1.1.3.7 Test: igmpproxyv3.mrouter.query-02 (Group-Specific Query)

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Objective:
This test verifies if the downstream interfaces handle correctly group-specific queries.

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b }):T1
   EXCLUDE(G:T1, ({}, {a, b }))
2. T2: Send [Host=1,2,3] TO_IN(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T1, ({b:T2, c:T2 }, {a}))
3. (RV x) Receive ALLOW(G, {b}) on upstream
4. (RV x) Receive Group-Specific Query Q(G) on downstream interface
   State: EXCLUDE(G:T2+LMQT, ({b:T2, c:T2 }, {a}))
5. T3: Send [Host=1,2,3,4] IS_EX(G, {a, b}) on downstream interface
   State: EXCLUDE(G:T3, ({b:T2}, {a}))
6. Source Timer for {b} expires at T2+GMI
   State: EXCLUDE(G:T3, ({}, {a, b}))
7. (RV x) Receive BLOCK(G, {b}) on upstream interface
8. Group Timer G expires at T3+GMI
   State: empty state
9. Receive TO_IN(G, {}) on upstream interface

6.2.1.2 State transition testing

Objective: An IGMP Proxy device must hold state per downstream interface to be able to decide where multicast packets must be forwarded to. The state is built from IGMP protocol messages received on downstream interfaces. The interface states are merged and reported on the upstream interface. This test will verify if the device is able to capture every possible state and report them correctly to the igmp router attached on the upstream interface.

The state verification system has to take into account:
1. Filter Mode (INCLUDE vs. EXCLUDE)
2. Source Addresses
3. Timers (Group Timer, Source Timers, IGMP version timer, …)
4. Queries sent on the downstream interfaces.

Procedure: We push the device into a start state and then send one of the possible IGMP messages forcing the start state to change into a new state. We listen on the upstream interface for State-Change reports and verify if the reported state is correct. To measure the timers we wait until they expire, when this happens the igmp proxy device updates its state and sends state-change reports to announce its new state. We also test if the reports and queries are retransmitted sufficient times.

The transition tests are divided into 5 parts.
1. Standard IGMPv3 state transition tests
2. IGMPv3 state transition tests with Host Tracking
3. IGMPv2 Interoperation state transition tests
4. IGMPv2 Interoperation state transition tests with Host Tracking
5. IGMPv1 Interoperation state transition tests

6.2.1.2.1 Standard IGMPv3 state transition tests

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**
Objective: Test IGMPv3 only state transitions for a standard IGMPv3 implementation.
Requirements: I 18, I 19, I 21, I 38, I 40, I 41, I 44
Summary:

Router State	Report Received	New State	Downstream Actions	Upstream Actions
NONE	IS_IN(A)	INCLUDE(A)	(A)=GMI	ALLOW(A)
NONE	IS_EX(A)	EXCLUDE({}, A)	(A)=0 Group Timer=GMI	TO_EX(A)
NONE	ALLOW(A)	INCLUDE(A)	(A)=GMI	ALLOW(A)
NONE	BLOCK(A)	n/a	n/a	n/a
NONE	TO_IN(A)	INCLUDE(A)	(A)=GMI ~~Send Q(G, {})~~	ALLOW(A)
NONE	TO_EX(A)	EXCLUDE({}, A)	(A)=0 ~~Send Q(G, {})~~ Group Timer=GMI	TO_EX(A)
INCLUDE(A)	IS_IN(B)	INCLUDE(A+B)	(B)=GMI	ALLOW(B-A)
INCLUDE(A)	IS_EX(B)	EXLUDE(A*B,B-A)	(B-A)=0 Delete (A-B) Group Timer=GMI	TO_EX(B-A)
INCLUDE(A)	ALLOW(B)	INCLUDE(A+B)	(B)=GMI	ALLOW(B-A)
INCLUDE(A)	BLOCK(B)	INCLUDE(A)	Send Q(G,A*B)	n/a
INCLUDE(A)	TO_IN(B)	INCLUDE(A+B)	(B)=GMI Send Q(G,A-B)	ALLOW(B-A)
INCLUDE(A)	TO_EX(B)	EXCLUDE(A*B,B-A)	(B-A)=0 Delete (A-B) Send Q(G,A*B) Group Timer=GMI	TO_EX(B-A)
EXCLUDE(X, Y)	IS_IN(A)	EXCLUDE(X+A, Y-A)	(A)=GMI	ALLOW(A*Y)
EXCLUDE(X, Y)	IS_EX(A)	EXCLUDE(A-Y, Y*A)	(A-X-Y)=GMI Delete (X-A) Delete (Y-A) Group Timer=GMI	ALLOW(Y-A)
EXCLUDE(X, Y)	ALLOW(A)	EXCLUDE(X+A, Y-A)	(A)=GMI	ALLOW(A*Y) / TO_IN()
EXCLUDE(X, Y)	BLOCK(A)	EXCLUDE(X+(A-Y), Y)	(A-X-Y)=Group Timer Send Q(G, A-Y)	n/a
EXCLUDE(X, Y)	TO_IN(A)	EXCLUDE(X+A, Y-A)	(A)=GMI Send Q(G,X-A) Send Q(G)	ALLOW(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	ALLOW(Y-A)

6.2.1.2.1.1 IGMPv3 - Empty State

6.2.1.2.1.1.1 Test: igmpproxyv3.igmpv3.emptytest-01

1. Reset device

State: empty state
2. T1: Send [Host=1] IS_IN(G, {a}) on downstream interface
State: INCLUDE(G, {a})
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {a} expires at T1+GMI:
State: empty state
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.1.2 Test: igmpproxyv3.igmpv3.emptytest-02

1. Reset device
State: empty state
2. T1: Send [Host=1] IS_EX(G, {a}) on downstream interface
State: EXCLUDE(G, ({}, {a}))
3. (RV x) Receive TO_EX(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
State: empty state
6. (RV x) Receive TO_IN(G, {}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.1.3 Test: igmpproxyv3.igmpv3.emptytest-03

1. Reset device
State: empty state
2. T1: Send [Host=1] ALLOW(G, {a}) on downstream interface
State: INCLUDE(G, {a})
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {a} expires at T1+GMI
State: empty state
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.1.4 Test: igmpproxyv3.igmpv3.emptytest-04

1. Reset device
State: empty state
2. T1: Send [Host=1] BLOCK(G, {a}) on downstream interface
State: empty state
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.1.5 Test: igmpproxyv3.igmpv3.emptytest-05

1. Reset device
State: empty state
2. T1: Send [Host=1] TO_IN(G, {a}) on downstream interface
State: INCLUDE(G, {a})

3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {a} expires at T1+GMI:
   State: empty state
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.1.6 Test: igmpproxyv3.igmpv3.emptytest-06

1. Reset device
   State: empty state
2. T1: Send [Host=1] TO_EX(G, {a}) on downstream interface
   State: EXCLUDE(G, ({}, {a}))
3. (RV x) Receive TO_EX(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer for G expires:
   State: empty state
6. (RV x) Receive TO_IN(G, {}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.2 IGMPv3 - Include State

6.2.1.2.1.2.1 Test: igmpproxyv3.igmpv3.includetest-01

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a, b }) -> T1
   INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1,2] IS_IN(G, {b, c }) on downstream interface
   State: INCLUDE(G, {a:T1, b:T2, c:T2 })
3. (RV x) Receive ALLOW(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {a} expires at T1+GMI
   State: INCLUDE({b:T2, c:T2})
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {b, c} expires at T2+GMI
   State: empty state
9. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.2.2 Test: igmpproxyv3.igmpv3.includetest-02

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a, b }) -> T1
   INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1,2] IS_EX(G, {b, c }) on downstream interface
   State: EXCLUDE(G:T2, ({b:T1}, {c}))
3. (RV x) Receive TO_EX(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {b} expires at T1+GMI
   State: EXCLUDE(G:T2, ({}, {b, c}))

6. (RV x) Receive BLOCK(G, {b}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer for G expires at T2+GMI
   State: empty state
9. (RV x) Receive a TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: the source {a} was removed from the include-source-timer list because its timer will always expire before the Group Timer does. If a downstream devices wants to receive multicast traffic from this source when the group timer expires and the device jumps into the INCLUDE state, it has to request this source again so it can be added to the list.

6.2.1.2.1.2.3 Test: igmpproxyv3.igmpv3.includetest-03

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1 })
   INCLUDE(G, {a:T1, b:T2})
2. T2: Send [Host=1,2] ALLOW(G, {b, c }) on downstream interface
   State: INCLUDE(G, {a:T1, b:T2, c:T2})
3. (RV x) Receive ALLOW(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {a} expires at T1+GMI
   State: INCLUDE(G, {b:T2, c:T2})
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {b, c} expires at T2+GMI
   State: empty state
9. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.2.4 Test: igmpproxyv3.igmpv3.includetest-04

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1 })
   INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1,2] BLOCK(G, {b, c }) on downstream interface
   State: INCLUDE(G, {a:T1, b:T1})
3. (RV x) Receive a Group-and-Source-Specific Query Q(G, {b}) on downstream interface
   State: INCLUDE(G, {A:T1, b:T2+LMQT})
4. Source Timer for {b} will expire at T2+LMQT
   State: INCLUDE(G, {a:T1})
5. (RV x) Receive a BLOCK(G, {b}) on upstream interface
6. Verify that no specific queries are sent on the downstream interface
7. Source Timer for {a} will expire at T1+GMI
   State: empty state
8. (RV x) Receive a BLOCK(G, {a}) on upstream interface
9. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: someone is blocking an unregistered source

6.2.1.2.1.2.5 Test: igmpproxyv3.igmpv3.includetest-05

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1 })
   INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1,2] TO_IN(G, {b, c }) on downstream interface
   State: INCLUDE(G, {a:T1, b:T2, c:T2})
3. (RV x) Receive ALLOW(G, {c}) on upstream interface
4. (RV x) Receive a Group-and-Source-Specific Query Q(G, {a}) on the downstream interface
   State: INCLUDE(G, {a:T2+LMQT, b:T2, c:T2})
5. Source Timer for {a} will expire at T2+LMQT
   State: INCLUDE(G, {b:T2, c:T2})
6. (RV x) Receive a BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {b, c} will expire at T2+GMI
   State: empty state
9. (RV x) Receive a BLOCK(G, {b, c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.2.6 Test: igmpproxyv3.igmpv3.includetest-06

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1 })
   INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1,2] TO_EX(G, {b, c }) on downstream interface
   State: EXCLUDE(G:T2, ({b:T1}, {c}))
3. (RV x) Receive TO_EX(G, {c}) on upstream interface
4. (RV x) Receive a Group-and-Source-Specific Query Q(G, {b}) on the downstream interface
   State: EXCLUDE(G:T2, ({b:T2+LMQT}, {c}))
5. Source Timer for {b} expires at T2+LMQT
   State: EXCLUDE(G:T2, ({}, {b, c}))
6. (RV x) Receive a BLOCK(G, {b}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer for G expires at T2+GMI
   State: empty state
9. (RV x) Receive a TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: source {a} has been removed from the include-source-timer list.

6.2.1.2.1.3 IGMPv3 - Exclude State

6.2.1.2.1.3.1 Test: igmpproxyv3.igmpv3.excludetest-01

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] IS_IN(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T2, c:T2, d:T1*, e:T2}, {b}))

3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
   State: INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {d} expires at T1*+GMI
   State: INCLUDE(G, {a:T2, c:T2, e:T2})
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Source Timer for {a, c, e} expires at T2+GMI
    State: empty state
12. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

Note: we assume that T1* > T1 -> this is ok, we only have to check the transition states. It is not the intention to test every possible path from here.

6.2.1.2.1.3.2 Test: igmpproxyv3.igmpv3.excludetest-02

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] IS_EX(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T2, ({c:T1*, e:T2}, {a}))
3. (RV x) Receive ALLOW(G, {b}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer {c} expires at T1*+GMI
   State: EXCLUDE(G:T2, ({e:T2}, {a, c}))
6. (RV x) Receive BLOCK(G, {c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer expires for G on T2+GMI
   State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: source {d} has been removed from the include-source-timer list.

6.2.1.2.1.3.3 Test: igmpproxyv3.igmpv3.excludetest-03

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] ALLOW(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T2, c:T2, d:T1*, e:T2}, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
   State: INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface

7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {d} expires at T1*+GMI
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Source Timer for {a, c, e} expires at T2+GMI
    State: empty state
12. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.3.4 Test: igmpproxyv3.igmpv3.excludetest-04

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d }):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] BLOCK(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T1, ({c:T1*, d:T1*, e:T1}, {a, b}))
3. Verify that no reports are sent on the upstream interface
4. (RV x) Receive Group-and-Source-Specific Query Q(G, {c, e}) on downstream interface
   State: EXCLUDE(G:T1, ({c:T2+LMQT, d:T1*, e:T2+LMQT}, {a, b}))
   Case T1* > T1
5. Source Timer for {c, e} expires at T2+LMQT
   State: EXCLUDE(G:T1, ({d:T1* }, {a, b, c, e}))
6. (RV x) Receive BLOCK(G, {c, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer G expires at T1+GMI
   State: INCLUDE(G, {d:T1* })
9. (RV x) Receive TO_IN(G, {d:T1*}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Source Timer for {d} expires at T1*+GMI
    State: empty state
12. (RV x) Receive BLOCK(G, {d}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: blocking source { e } who wasn't requested before.

6.2.1.2.1.3.5 Test: igmpproxyv3.igmpv3.excludetest-05

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] TO_IN(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T2, c:T2, d:T1*, e:T2}, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream
4. (RV x) Receive Group-Specific Query Q(G) on downstream interface
   State: EXCLUDE(G:T2+LMQT , ({a:T2, c:T2, d:T1*, e:T2}, {b}))
5. (RV x) Receive Group-and-Source-Specific Query Q(G, {d}) on downstream interface
   State: EXCLUDE(G:T2+LMQT , ({a:T2, c:T2, d:T2+LMQT, e:T2}, {b}))
6. Source Timer for {d} and Group Timer G will expire at T2+LMQT
   State: INCLUDE(G, {a:T2, c:T2, e:T2})

7. (RV x) Receive TO_IN(G, {a, c, e})
8. Verify that no specific queries are sent on the downstream interface
9. Source Timer for {a, c, e}) will expire at T2+GMI
   State: empty state
10. (RV x) Receive BLOCK(G, {a, c, e})
11. Verify that no specific queries are sent on the downstream interface

6.2.1.2.1.3.6 Test: igmpproxyv3.igmpv3.excludetest-06

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1,2,3] TO_EX(G, {a, c, e}) on downstream interface
   State: EXCLUDE(G:T2, ({c:T1*, e:T1}, {a}))
3. (RV x) Receive ALLOW(G, {b}) on upstream interface
4. (RV x) Receive Group-and-Source-Specific Query Q(G, {c, e}) on downstream interface
   State: EXCLUDE(G:T2, ({c:T2+LMQT, e:T2+LMQT},{a}))
5. Source Timer for {c, e} will expire at T2+LMQT
   State: EXCLUDE(G:T2, ({}, {a, c, e}))
6. (RV x) Receive BLOCK(G, {c, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer G expires at T2+GMI
   State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: source {e} has been removed from the include-source-timer list.

6.2.1.2.2 Host Tracking IGMPv3 state transition tests

Setup: **SETUP 9**
Objective: Test IGMPv3 only state transitions for a standard IGMPv3 implementation.
Requirements: I 18, I 19, I 21, I 38, I 40, I 41, I 44, RG 9

6.2.1.2.2.1 Empty state

These tests are identical to the ones described in igmpproxyv3.igmpv3.empty*.

6.2.1.2.2.2 Include state

6.2.1.2.2.2.1 Test: igmpproxyv3.hosttracking.includetest-01

This test is identical to igmpproxyv3.igmpv3.includetest-01.

6.2.1.2.2.2.2 Test: igmpproxyv3.hosttracking.includetest-02

Source1
1. Reset and initialize the device into its startup state

State: [Host=1] IN(G, {a:T1, b:T1 })
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1] IS_EX(G, {b, c }) on downstream interface
State: [Host=1] EX(G, {b, c}):T2
EXCLUDE(G:T2, ({}, {b, c}))
3. (RV x) Receive TO_EX(G, {b, c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T2+GMI
State: empty state
6. (RV x) Receive a TO_IN(G, {})
7. Verify that no specific queries are sent on the downstream interface

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] IN(G, {a:T1, b:T1 })
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=2] IS_EX(G, {b, c }) on downstream interface
State: [Host=1] IN(G, {a:T1, b:T1})
[Host=2] EX(G, {b, c}):T2
EXCLUDE(G:T2, ({b:T1}, {c}))
3. (RV x) Receive TO_EX(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Source Timer for {b} expires at T1+GMI
State: [Host=2] EX(G, {b, c}):T2
EXCLUDE(G:T2, ({}, {b, c}))
6. (RV x) Receive BLOCK(G, {b}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Group Timer G expires at T2+GMI
State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.2.3 Test: igmpproxyv3.hosttracking.includetest-03

This test is identical to igmpproxyv3.igmpv3.includetest-03.

6.2.1.2.2.2.4 Test: igmpproxyv3.hosttracking.includetest-04

Source 1
1. Reset and initialize the device into its startup state
State: [Host=1] IN(G, {a:T1, b:T1})
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1] BLOCK(G, {b, c }) on downstream interface
State: [Host=1] IN(G, {a}):T2
INCLUDE(G, {a:T1})
3. (RV x) Receive BLOCK(G, {b}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 expires at T1+GMI or Source Timer for {a} expires at T1+GMI
State: empty state
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: blocking source {c} that was previously not requested.

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] IN(G, {a:T1, b:T1 })
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=2] BLOCK(G, {b, c }) on downstream interface
State: [Host=1] IN(G, {a, b }):T1
[Host=2] ??
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface

Weird behavious expected: unknown host is blocking sources {b, c} and {c} has never been requested before. (send query to host ?)

6.2.1.2.2.2.5 Test: igmpproxyv3.hosttracking.includetest-05

Source 1
1. Reset and initialize the device into its startup state
State: [Host=1] IN(G, {a:T1, b:T1 })
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=1] TO_IN(G, {b, c }) on downstream interface
State: [Host=1] IN(G, {b, c}):T2
INCLUDE(G, {b:T2, c:T2})
3. (RV x) Receive ALLOW(G, {c}), BLOCK(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {b, c} expires at T2+GMI
State: empty state
6. (RV x) Receive a BLOCK(G, {b, c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

Warning: unconventional way of leaving and joining other channels.

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] IN(G, {a:T1, b:T1 })
INCLUDE(G, {a:T1, b:T1})
2. T2: Send [Host=2] TO_IN(G, {b, c }) on downstream interface
State: [Host=1] IN(G, {a:T1, b:T1})
[Host=2] IN(G, {b:T2, c:T2})
INCLUDE(G, {a:T1, b:T2, c:T2})
3. (RV x) Receive ALLOW(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Source Timer for {a} expires at T1+GMI
State: [Host=2] IN(G, {b:T2, c:T2})
INCLUDE(G, {b:T2, c:T2})
6. (RV x) Receive BLOCK(G, {a}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Source Timer for {b, c} expires at T2+GMI
State: empty state
9. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.6 Test: igmpproxyv3.hosttracking.includetest-06

Source 1

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1 })
   INCLUDE({a:T1, b:T1})
2. T2: Send [Host=1] TO_EX(G, {b, c }) on downstream interface
   State: [Host=1] EX(G, {b:T2, c:T2})
   EXCLUDE(G:T2, ({}, {b, c}))
3. (RV x) Receive TO_EX(G, {b, c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 2 will expire at T2+GMI
   State: empty state
6. (RV x) Receive TO_IN(G, {}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

Source 2

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1, b:T1})
   INCLUDE({a:T1, b:T1})
2. T2: Send [Host=2] TO_EX(G, {b, c }) on downstream interface
   State: [Host=1] IN(G, {a:T1, b:T1})
   [Host=2] EX(G, {b, c}):T2
   EXCLUDE(G:T2, ({b:T1}, {c}))
3. (RV x) Receive TO_EX(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Source Timer for {b} expires at T1+GMI
   State: [Host=2] EX(G, {b, c}):T2
   EXCLUDE(G:T2, ({}, {b, c}))
6. (RV) Receive BLOCK(G, {b}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Group Timer G expires at T2+GMI
   State: empty state
9. (RV x) Receive a TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.3 Exclude state

6.2.1.2.2.3.1 Test: igmpproxyv3.hosttracking.excludetest-01

Source 1

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1] IS_IN(G, {a, c, e}) on downstream interface
   State: [Host=1] IN(G, {a:T2, c:T2, e:T2})
   [Host=2] IN(G, {c, d}):T1*
   INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
3. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Source Timer for {d} expires at T1*+GMI
   State: [Host=1] IN(G, {a:T2, c:T2, e:T2})

INCLUDE(G, {a:T2, c:T2, e:T2})
6. (RV x) Receive BLOCK(G, {d}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer for {a, c, e} expires on T2+GMI
   State: empty state
9. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Warning: somehow a TO_IN report has been dropped.

Source 2
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=2] IS_IN(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {a:T2, c:T2, e:T2})
   EXCLUDE(G:T1, ({a:T2, c:T2, e:T2}, {b, d}))
3. (RV x) Receive ALLOW(G, {a}), BLOCK(G, {d}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer G expires at T1+GMI
   State: [Host=2] IN(G, {a, c, e}):T2
   INCLUDE(G, {a:T2, c:T2, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
   State: empty state
9. (RV x) Receive BLOCK({a, c, e}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Warning: somehow an ALLOW/BLOCK report has been dropped.

Source 3
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=3] IS_IN(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   [Host=3] IN(G, {a:T2, c:T2, e:T2})
   EXCLUDE(G:T1, ({a:T2, c:T2, d:T1*, e:T2}, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer expires at T11+GMI
   State: [Host=2] IN(G, {c:T1*, d:T1*})
   [Host=3] IN(G, {a:T2, c:T2, e:T2})
   INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {d} expires at T1*+GMI
   State: [Host=3] IN(G, {a, c, e}):T2

INCLUDE(G, {a:T2, c:T2, e:T2})
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
State: empty state
12. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.3.2 Test: igmpproxyv3.hosttracking.excludetest-02

Source 1
1. Reset and initialize the device into its startup state
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1] IS_EX(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, c, e}):T2
[Host=2] IN(G, {c, d}):T1*
EXCLUDE(G:T2, ({c:T1*}, {a, e}))
3. (RV x) Receive ALLOW(G, {b}), BLOCK(G, {e}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1* or Source Timer for {c} expires at T1*+GMI
State: [Host=1] EX(G, {a, c, e}):T2
EXCLUDE(G:T2, ({}, {a, c, e}))
6. (RV x) Receive BLOCK(G, {c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 expires at T2+GMI
State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=2] IS_EX(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] EX(G, {a, c, e}):T2
EXCLUDE(G:T2, ({}, {a, c}))
3. (RV x) Receive ALLOW(G, {b}), BLOCK(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 expires at T1+GMI
State: [Host=2] EX(G, {a, c, e}):T2
EXCLUDE(G:T2, ({}, {a, c, e}))
6. (RV x) Receive BLOCK(G, {e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 expires at T2+GMI
State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Source 3

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=3] IS_EX(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c, d}):T1*
   [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({c:T1*, d:T1*}, {a}))
3. (RV x) Receive ALLOW(G, {b}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 expires at T1+GMI
   State: [Host=2] IN(G, {c, d}):T1*
   [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({c:T1*}, {a, e}))
6. (RV x) Receive BLOCK(G, {e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {c} expires at T1*+GMI
   State: [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({}, {a, c, e}))
9. (RV x) Receive BLOCK(G, {c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Host Timer 2 or Group Timer G expires at T2+GMI
    State: empty state
12. (RV x) Receive TO_IN(G, {}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.3.3 Test: igmpproxyv3.hosttracking.excludetest-03

Source 1

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1] ALLOW(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {b, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({d:T1*}, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer G expires at T1+GMI
   State: [Host=2] IN(G, {c:T1*, d:T1*})
   INCLUDE(G, {c, d})
6. (RV x) Receive TO_IN(G, {c, d}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* expires at T1*+GMI
   State: empty state
9. (RV x) Receive BLOCK(G, {c, d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: allowing source { e } who wasn't excluded before.
TODO: Is this correct? BLOCK doesnt update the timer of an EX record.

Source 2
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE({c:T1*, d:T1*}, {a, b}:T1)
2. T2: Send [Host=2] ALLOW(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {a, c, d, e}):T2
   EXCLUDE(G:T1, ({a:T2, c:T2, d:T2, e:T2 }, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Host Timer 1 or Group Timer G expires at T1+GMI
   State: [Host=2] IN(G, {a, c, d, e}):T2
   INCLUDE({a:T2, c:T2, d:T2, e:T2})
5. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
6. Verify that no specific queries are sent on the downstream interface
7. Host Timer 2 expires at T2+GMI
   State: empty state
8. (RV x) Receive BLOCK(G, {a, c, d, e}) on upstream interface

Source 3
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE({c:T1*, d:T1*}, {a, b}:T1)
2. T2: Send [Host=3] ALLOW(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c, d}):T1*
   [Host=3] IN(G, {a, c, e}):T2
   EXCLUDE({a:T2, c:T2, d:T1*, e:T2}, {b})
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer expires at T1+GMI
   State: [Host=2] IN(G, {c, d}):T1*
   [Host=3] IN(G, {a, c, e}):T2
   INCLUDE({a:T2, c:T2, d:T1*, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {c} expires at T1*+GMI
   State: [Host=3] IN(G, {a, c, e}):T2
   INCLUDE({a:T2, c:T2, e:T2})
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
    State: empty state
12. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.3.4 Test: igmpproxyv3.hosttracking.excludetest-04

Source 1
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})

EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1] BLOCK(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, b, c, d, e}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b, e}))
3. (RV x) Receive BLOCK(G, {e}) on upstream interface.
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 of Group Timer G expires at T1+GMI
State: [Host=2] IN(G, {c:T1*, d:T1*})
INCLUDE(G, {c:T1*, d:T1*})
6. (RV x) Receive TO_IN(G, {c, d}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {c, d} expires at T1*+GMI
State: empty state
9. (RV x) Receive BLOCK(G, {c, d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: excluding source { a, c } who where previously excluded.

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c, d}):T1*
State: EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=2] BLOCK(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {d}):T1*
EXCLUDE(G:T1, ({d:T1*}, {a, b, c}))
3. (RV x) Receive BLOCK(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer expires at T1+GMI
State: [Host=2] IN(G, {d}):T1*
INCLUDE(G, {d:T1*})
6. (RV x) Receive TO_IN(G, {d}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {d} expires at T1*+GMI
State: empty state
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Weird behavior expected: unexpected blocking of sources { a, e }.

Source 3
1. Reset and initialize the device into its startup state
Start: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c, d}):T1*
EXCLUDE({c:T1*, d:T1*}, {a, b}:T1)
2. Send [Host=3] BLOCK(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
[Host=3] ?
EXCLUDE({c:T1*, d:T1*}, {a, b}:T1)
3. Host Timer 1 or Group Timer expires at T1+GMI

State: [Host=2] IN(G, {c:T1*, d:T1*})
INCLUDE({c:T1*, d:T1*})
4. (RV x) Receive TO_IN(G, {c, d}) on upstream interface
5. Verify that no specific queries are sent on the downstream interface
6. Host Timer 1* or Source Timer for {c, d} expires at T1*+GMI
State: empty state
7. (RV x) Receive BLOCK(G, {c, d}) on upstream interface
8. Verify that no specific queries are sent on the downstream interface

Weird behaviour expected: unknown source is blocking sources. (sent query to host ?)

6.2.1.2.2.3.5 Test: igmpproxyv3.hosttracking.excludetest-05

Source 1
1. Reset and initialize the device into its startup state
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=1] TO_IN(G, {a, c, e}) on downstream interface
State: [Host=1] IN(G, {a, c, e}):T2
[Host=2] IN(G, {c, d}):T1*
INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
3. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1* or Source Timer for {d} will expire at T1*+GMI
State: [Host=1] IN(G, {a, c, e}):T2
INCLUDE(G, {a:T2, c:T2, e:T2})
6. (RV x) Receive BLOCK(G, {d}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
State: empty state
9. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Source 2
1. Reset and initialize the device into its startup state
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {c:T1*, d:T1*})
EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. T2: Send [Host=2] TO_IN(G, {a, c, e}) on downstream interface
State: [Host=1] EX(G, {a, b, c, d}):T1
[Host=2] IN(G, {a:T2, c:T2, e:T2})
EXCLUDE(G:T1, ({a:T2, c:T2, e:T2}, {b, d}))
3. (RV x) Receive ALLOW(G, {a}), BLOCK(G, {d}) on upstream
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 or Group Timer G expires at T1+GMI
State: [Host=2] IN(G, {a:T2, c:T2, e:T2})
INCLUDE(G, {a:T2, c:T2, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
State: empty state
9. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Source 3
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. Send [Host=3] TO_IN(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   [Host=3] IN(G, {a:T2, c:T2, e:T2})
   EXCLUDE(G:T1, ({a:T2, c:T2, d:T1*, e:T2}, {b}))
3. (RV x) Receive ALLOW(G, {a}) on upstream
4. Verify that no specific queries are sent on the downstream interface
   Case T1* > T1
5. Host Timer 1 or Group Timer G expires at T1+GMI
   State: [Host=2] IN(G, {c, d}):T1*
   [Host=3] IN(G, {a, c, e}):T2
   INCLUDE(G, {a:T2, c:T2, d:T1*, e:T2})
6. (RV x) Receive TO_IN(G, {a, c, d, e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {d} expires at T1*+GMI
   State: [Host=3] IN(G, {a, c, e}):T2
   INCLUDE(G, {a:T2, c:T2, e:T2})
9. (RV x) Receive BLOCK(G, {d}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Host Timer 2 or Source Timer for {a, c, e} expires at T2+GMI
    State: empty state
12. (RV x) Receive BLOCK(G, {a, c, e}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.2.3.6 Test: igmpproxyv3.hosttracking.excludetest-06

Source 1
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. Send [Host=1] TO_EX(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, c, e}):T2
   [Host=2] IN(G, {c, d}):T1*
   EXCLUDE(G:T2, ({c:T1*}, {a, e}))
3. (RV x) Receive ALLOW(G, {b}), BLOCK(G, {e}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1* or Source Timer for {c} expires at T1*+GMI
   State: [Host=1] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({}, {a, c, e}))
6. (RV x) Receive BLOCK(G, {c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 or Group Timer G expires at T2+GMI
   State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Warning: weird way to change your state.

Source 2

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. Send [Host=2] TO_EX(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({}, {a, c}))
3. (RV x) Receive ALLOW(G, {b}), BLOCK(G, {c}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Host Timer 1 expires at T1+GMI
   State: [Host=2] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({}, {a, c, e}))
6. (RV x) Receive BLOCK(G, {e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 2 expires at T2+GMI
   State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Source 3

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   EXCLUDE(G:T1, ({c:T1*, d:T1*}, {a, b}))
2. Send [Host=3] TO_EX(G, {a, c, e}) on downstream interface
   State: [Host=1] EX(G, {a, b, c, d}):T1
   [Host=2] IN(G, {c:T1*, d:T1*})
   [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({c:T1*}, {a}))
3. (RV x) Receive ALLOW(G, {b}) on upstream interface
4. Verify that no specific queries are sent on the downstream interface
   Case T1* > T1
5. Host Timer 1or Source Timer for {c} expires at T1+GMI
   State: [Host=2] IN(G, {c, d}):T1*
   [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({c:T1*}, {a, e}))
6. (RV x) Receive BLOCK(G, {e}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Host Timer 1* or Source Timer for {c} expires at T1*+GMI
   State: [Host=3] EX(G, {a, c, e}):T2
   EXCLUDE(G:T2, ({}, {a, c, e}))
9. (RV x) Receive BLOCK(G, {c}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Host Timer 2 or Group Timer G expires at T2+GMI
    State: empty state
12. (RV x) Receive TO_IN(G, {}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.3 IGMPv2 interoperation state transition tests

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**
Objective: Test IGMPv2 interoperation state transitions for a standard IGMPv3 implementation.
Requirements:I 18, I 19, I 21, I 38, I 40, I 41, I 44, I 49, I 50
Summary:

Router State	Report Received	New State	Downstream Actions	Upstream Actions
NONE	REPORTv2	INCLUDEv2	Group Timer=GMI IGMPv2Present=OVHPT	TO_EX({})
NONE	LEAVE	n/a	n/a	n/a
INCLUDE(A)	REPORTv2	INCLUDEv2	Delete (A) Group Timer=GMI IGMPv2Present=OVHPT	TO_EX({})
INCLUDE(A)	LEAVE	INCLUDE(A)	Send Q(G, A)	n/a
EXCLUDE(X, Y)	REPORTv2	INCLUDEv2	Delete (A) Group Timer=GMI IGMPv2Present=OVHPT	ALLOW(Y)
EXCLUDE(X, Y)	LEAVE	EXCLUDE(X, Y)	Send Q(G, X) Send Q(G)	n/a
INCLUDEv2(X)	REPORTv2	INCLUDEv2(X)	Group Timer=GMI IGMPv2Present=OVHPT	n/a
INCLUDEv2(X)	LEAVE	INCLUDEv2(X)	Send Q(G) Send Q(G, X)	n/a
INCLUDEv2(X)	IS_IN(A)	INCLUDEv2(X+A)	(A)=GMI	n/a
INCLUDEv2(X)	IS_EX(A)	INCLUDEv2(A)	(A-X)=GMI Delete (X-A) Group Timer=GMI	n/a
INCLUDEv2(X)	ALLOW(A)	INCLUDEv2(X+A)	(A)=GMI	n/a
INCLUDEv2(X)	BLOCK(A)	INCLUDEv2(X)	n/a	n/a
INCLUDEv2(X)	TO_IN(A)	INCLUDEv2(X+A)	(A)=GMI Send Q(G, X-A) Send Q(G)	n/a
INCLUDEv2(X)	TO_EX(A)	INCLUDEv2({})	Delete (X) Group Timer=GMI	n/a

6.2.1.2.3.1 Empty State

6.2.1.2.3.1.1 Test: igmpproxyv3.interopv2.empty-01

1. Reset and initialize the device into its startup state
   State: empty state
2. T1: Send [Host=1] REPORTv2(G) on downstream interface
   State: INCLUDEv2, this is equivalent to EXCLUDE(G, ({}, {}))
3. Receive TO_EX(G, {}) on upstream interface
4. Group Timer G expires at T1+GMI
   State: empty state
5. Receive TO_IN(G, {}) on upstream interface

6.2.1.2.3.1.2 Test: igmpproxyv3.interopv2.empty-02

1. Reset and initialize the device into its startup state
   State: empty state
2. Send [Host=1] LEAVEv2(G) on downstream interface
   State: empty state

6.2.1.2.3.2 Include State

6.2.1.2.3.2.1 Test: igmpproxyv3.interopv2.include-01

1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1})
   INCLUDE(G, {a:T1})
2. T2: Send [Host=1,2] REPORTv2(G) on downstream interface
   State: INCLUDEv2(G:T2)
3. Receive TO_EX(G, {}) on upstream interface
4. Group Timer G expires at T2+GMI
   State: empty state
5. Receive TO_IN(G, {}) on upstream interface

6.2.1.2.3.2.2 Test: igmpproxyv3.interopv2.include-02

1. Reset and initialize the device into its startup state
   Start: [Host=1] IN(G, {a:T1})
   INCLUDE(G, {a:T1})
2. T2: Send [Host=1,2] LEAVEv2(G) on downstream interface
   State: INCLUDE({a})
3. (RV x) Receive a Group-and-Source-Specific Query Qv3(G, {a}) on the downstream interface
   State: INCLUDE(G, {a:T2+LMQT})
4. Source Timer {a} expires at T2+LMQT
   State: empty state
5. (RV x) Receive BLOCK(G, {a}) on upstream interface

Note: this IGMPv3 Group-and-Source-Specific Query is backwards compatible with IGMPv2 Hosts, who MUST recognize it as an IGMPv2 Group-Specific Query

6.2.1.2.3.3 Exclude State

6.2.1.2.3.3.1 Test: igmpproxyv3.interopv2.exclude-01

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b}:T1)
   [Host=2] IN(G, { b}:T1*)
   EXCLUDE(G, ({b:T1*}, {a}:T1))
2. T2: Send [Host=1,2,3] REPORTv2(G) on downstream interface
   State: INCLUDEv2(G:T2)
3. (RV x) Receive ALLOW(G, {a}) on upstream interface
4. Group Timer G expires at T2+GMI
   State: empty state

5. (RV x) Receive TO_IN(G, {}) on upstream interface

6.2.1.2.3.3.2 Test: igmpproxyv3.interopv2.exclude-02

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a, b}:T1)
   [Host=2] IN(G, { b}:T1*)
   EXCLUDE(G, ({b:T1*}, {a}:T1))
2. T2: Send [Host=1,2,3] LEAVEv2(G) on downstream interface
   State: EXCLUDE(G, ({b:T1*}, {a}:T1))
3. Receive a Group-Specific Query Qv3(G) on the downstream interface
   State: EXCLUDE(G, ({b:T1*}, {a}:T2+LMQT))
4. Receive a Group-and-Source-Specific Query Qv3(G, {b}) on the downstream interface
   State: EXCLUDE(G, ({b: T2+LMQT }, {a}:T2+LMQT))
5. Group Timer G expires at T2+LMQT
   State: empty state
6. (RV x) Receive TO_IN(G, {}) on upstream interface

Note: this IGMPv3 Group-Specific Query is backwards compatible with IGMPv2 Hosts, who MUST recognize it as an IGMPv2 Group-Specific Query

6.2.1.2.3.4 Includev2 State

6.2.1.2.3.4.1 Test: igmpproxyv3.interopv2.includev2-01

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a}:T1*)
   EXCLUDE(G:T1, ({a:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] REPORTv2(G) on downstream interface
   State: EXCLUDE(G:T2, ({}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T2+GMI
   State: empty state
6. (RV x) Receive TO_IN(G, {}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface

6.2.1.2.3.4.2 Test: igmpproxyv3.interopv2.includev2-02

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a}:T1*)
   EXCLUDE(G:T1, ({a:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] LEAVEv2(G) on downstream interface
   State: EXCLUDE(G:T1, ({}, {}), IGMPv2:T1)
3. No reports are sent on the upstream interface
4. (RV x) Receive a Group-Specific Query Qv3(G) on the downstream interface
   State: EXCLUDE(G:T2+LMQT, ({a:T1*}, {}), IGMPv2:T1)

5. (RV x) Receive a Group-and-Source-Specific Query Qv3(G, {a}) on the downstream interface
   State: EXCLUDE(G:T2+LMQT, ({a:T2+LMQT}, {}), IGMPv2:T1)
6. Group Timer G expires at T2+LMQT
   State: empty state
7. (RV x) Receive TO_IN(G, {}) on upstream interface
8. Verify that no specific queries are sent on the downstream interface

6.2.1.2.3.4.3 Test: igmpproxyv3.interopv2.includev2-03

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] IS_IN(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T1*, b:T2, c:T2}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
   State: INCLUDE(G, {a:T1*, b:T2, c:T2})
6. (RV x) Receive TO_IN(G, {a, b, c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer {a} expires at T1*+GMI
   State: INCLUDE(G, {b:T2, c:T2})
9. (RV x) Receive BLOCK(G, {a}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Source Timer {b, c} expires at T2+GMI
12. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.3.4.4 Test: igmpproxyv3.interopv2.includev2-04

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*,b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] IS_EX(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T2, ({b:T1*, c:T2}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. IGMPv2 Host Present Timer expires at T1+OHPI
   State: EXCLUDE(G:T2, ({b:T1*, c:T2}, {}))
6. Verify that no reports are sent on the upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer {b} expires at T1*+GMI
   State: EXCLUDE(G:T2, ({c:T2}, {b}))
9. (RV x) Receive BLOCK(G, {b}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Group Timer G expires at T2+GMI
    State: empty state
12. (RV x) Receive TO_IN(G, { }) on upstream interface
13. Verify that no specific queries are sent on the downstream interface

6.2.1.2.3.4.5 Test: igmpproxyv3.interopv2.includev2-05

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] ALLOW(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T1*, b:T2, c:T2}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
   State: INCLUDE(G, {a:T1*, b:T2, c:T2})
6. (RV x) Receive TO_IN(G, {a, b, c}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer {a} expires at T1*+GMI
   State: INCLUDE(G, {b:T2, c:T2})
9. (RV x) Receive BLOCK(G, {a}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface
11. Source Timer {b, c} expires at T2+GMI
12. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
    Verify that no specific queries are sent on the downstream interface

6.2.1.2.3.4.6 Test: igmpproxyv3.interopv2.includev2-06

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] BLOCK(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. Group Timer G expires at T1+GMI
6. (RV x) Receive TO_IN(G, {a, b}) on upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Source Timer {a, b} expires at T1*+GMI
9. (RV x) Receive BLOCK(G, {a, b}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: When a multicast group is in IGMPv2 compatibility mode BLOCK records for that multicast address must be ignored.

6.2.1.2.3.4.7 Test: igmpproxyv3.interopv2.includev2-07

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] TO_IN(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T1, ({a:T1*, b:T2, c:T2}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface

4. (RV x) Receive a Group-Specific Query Qv3(G) on the downstream interface
   State: EXCLUDE(G:T2+LMQT, ({a:T1*, b:T2, c:T2}, {}), IGMPv2:T1)
5. (RV x) Receive a Group-and-Source-Specific Query Qv3(G, {a}) on the downstream I nterface
   State: EXCLUDE(G:T2+LMQT, ({a:T2+LMQT, b:T2, c:T2}, {}), IGMPv2:T1)
6. Group Timer G and Source Timer {a} expires at T2+LMQT
   State: INCLUDE(G, {b:T2, c:T2}, IGMPv2:T1)
7. (RV x) Receive TO_IN(G, {b, c}) on upstream interface
8. Verify that no specific queries are sent on the downstream interface
9. Source Timer {b, c} expires at T2+GMI
10. (RV x) Receive BLOCK(G, {b, c}) on upstream interface
11. Verify that no specific queries are sent on the downstream interface

Note: The IGMPv2 Host Present Timer is cleared before it expires! (is this correct ?)

6.2.1.2.3.4.8 Test: igmpproxyv3.interopv2.includev2-08

1. Reset and initialize the device into its startup state
   State: [Host=1] REPORTv2(G:T1)
   [Host=2] IN(G, {a, b}:T1*)
   EXCLUDE(G:T1, ({a:T1*, b:T1*}, {}), IGMPv2:T1)
2. T2: Send [Host=1,2] TO_EX(G, {b, c}) on downstream interface
   State: EXCLUDE(G:T2, ({}, {}), IGMPv2:T1)
3. Verify that no reports are sent on the upstream interface
4. Verify that no specific queries are sent on the downstream interface
5. IGMPv2 Host Present Timer expires at T1+OHPI
   State: EXCLUDE(G:T2, ({}, {}))
6. Verify that no reports are sent on the upstream interface
7. Verify that no specific queries are sent on the downstream interface
8. Group Timer G expires at T2+GMI
   State: empty state
9. (RV x) Receive TO_IN(G, {}) on upstream interface
10. Verify that no specific queries are sent on the downstream interface

Note: expiration of IGMPv2 Host Present Timer could be tested by sending BLOCK records.

6.2.1.2.4 Fast Leave IGMPv2 interoperation state transition tests

Setup: **SETUP 9**
Objective: Test IGMPv2 interoperation state transitions with Host Tracking.
Requirements: I 18, I 19, I 21, I 38, I 40, I 41, I 44, I 49, I 50, RG 9

6.2.1.2.5 IGMPv1 interoperation state transition tests

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**
Objective: Test IGMPv1 interoperation state transitions for a standard IGMPv3 implementation.
Requirements: I 18, I 19, I 21, I 38, I 40, I 41, I 44, I 49, I 51
Summary:

Router State	Report Received	New State	Downstream Actions	Upstream Actions
NONE	REPORTv1	INCLUDEv1	Group Timer=GMI IGMPv1Present=OVHPT	TO_EX({})
INCLUDE(A)	REPORTv1	INCLUDEv1	Group Timer=GMI IGMPv1Present=OVHPT	TO_EX({})
EXCLUDE(X, Y)	REPORTv1	INCLUDEv1	Group Timer=GMI IGMPv1Present=OVHPT	TO_EX({})
INCLUDEv2	REPORTv1	INCLUDEv1	Group Timer=GMI IGMPv1Present=OVHPT	n/a
INCLUDEv1	REPORTv2	INCLUDEv1	Group Timer=GMI IGMPv2Present=OVHPT	n/a
INCLUDEv1	IS_IN(A)	INCLUDEv1	(A)=GMI	n/a
INCLUDEv1	IS_EX(A)	INCLUDEv1	(A-X)=GMI Delete (X-A)	n/a
INCLUDEv1	ALLOW(A)	INCLUDEv1	(A)=GMI	n/a
INCLUDEv1	BLOCK(A)	INCLUDEv1	(A-X)=Group Timer Send Q(G, A)	n/a
INCLUDEv1	TO_IN(A)	INCLUDEv1	(A)=GMI Send Q(G, X-A) Send Q(G)	n/a
INCLUDEv1	TO_EX(A)	INCLUDEv1	(A-X)=Group Timer Delete (X-A) Send Q(G, A) Group Timer=GMI	n/a

6.2.1.3 Test: igmpproxyv3.forward.forward (Packet forwarding test)

Setup: **SETUP 3**

Objective: This test forces the igmp proxy device into different states and investigates if multicast packets are forwarded to the correct interfaces.

Requirements:

I 39 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.

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.

RG 2 The RGW 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). [TR-101 R-193] [TR-124 R-44]

RG 4 The RGW MUST be capable of supporting LAN to LAN multicast on the same LAN interface and across multiple different LAN interfaces. [TR-124 R-55]

Procedure:

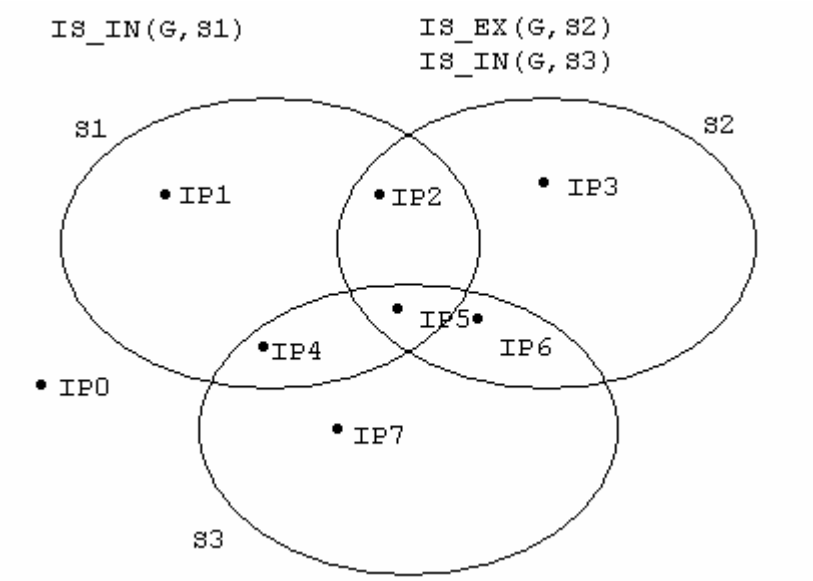
- Attach the upstream interface and all downstream interfaces to the test system
- Initialize the device in every possible internal state for which a downstream interface can be in the following modes:

1. Empty state: no reports received
2. INCLUDE state: one or more hosts reported an IS_IN state.
   We send one report with an IS_IN(G, S) record.
3. EXCLUDE state: at least one host reported an IS_EX state.
   We send one report with an IS_EX(G, S1) record, followed by another one with an IS_IN(G, S2) record.
4. INCLUDEv2 state: at least one host answered with an Igmpv2 Report.
5. (Future work: INCLUDEv1)

This means that an igmp proxy device with 4 downstream interfaces has to be tested in 4^4=256 different states.

- For every source ip address (further explanation below) we transmit a multicast packet on the upstream interface and one on every downstream interface.
- Verify if the multicast packets are forwarded to the correct interfaces.

The test system informs the current state of an interface by transmitting Current-State Reports holding IS_IN or IS_EX records. These records contain sets of source ip addresses. The igmp proxy device merges these sets using elemental set operations into the membership database for its upstream interface. We have to chose these sets carefully to hold enough elements so we can conclude if the right calculating was applied. The following figure should clarify this; we send on downstream0 an IS_IN(G, S1) report and on downstream1 an IS_EX(G, S2) report and an IS_IN(G, S3) report.



The state of the upstream interface must be EXCLUDE(G, S2-S1-S2) or EXCLUDE(G, {IP3}). Note that IP0 represents the set of ip addresses who are not reported in any transmitted report.

6.2.2 Testing DSLForum Multicast Requirements for RGW

6.2.2.1 General requirements

6.2.2.1.1 Test: igmpproxyv3.specific.testrg47

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 6 The RGW MUST support a minimum of 32 multicast groups. [TR-124 R-47]

Procedure:
1. Reset device
2. Send an IGMPv3 Report with 32 IS_EX(Gx, {}) records with Gx one of the 32 different multicast groups.
3. Wait some time to give the device time to send Status-Change reports.
4. Send a General Query on the upstream interface
5. Verify that all 32 registered multicast groups (Gx) are reported as EX(Gx, {}).

6.2.2.1.2 Test: igmpproxyv3.specific.restrg48

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 7 The RGW SHOULD support a minimum of 64 multicast groups. [TR-124 R-48]

Procedure:
1. Reset device
2. Send an IGMPv3 Report with 64 IS_EX(Gx, {}) records with Gx one of the 64 different multicast groups.
3. Wait some time to give the device time to send Status-Change reports.
4. Send a General Query on the upstream interface.
5. Verify that all 64 registered multicast groups (Gx) are reported as EX(Gx, {}).

6.2.2.1.3 Test: igmpproxyv3.specific.testrg49

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 8 The RGW 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. [TR-124 R-49]

Procedure:
1. Reset device
2. Send an IGMPv3 Report with an IS_IN(G, {a1, .., a64}) record, the source list for this record must contain 64 different source addresses.
3. Wait some time to give the device time to send Status-Change reports.
4. Send a General Query on the upstream interface
5. Verify that the multicast group G is in an include state and that all 64 source addresses are reported.

6.2.2.1.4 Test: igmpproxyv3.specific.testrg56

Setup: **SETUP 10**

Requirements:
RG 5 The RGW MUST be configurable as to how many simultaneous multicast streams are allowed from WAN to LAN. [TR-124 R-56]

Procedure:
1. Reset device
   State: empty state
2. Send IS_IN(G1, {a}) on downstream interface
3. Give the device some time to respond.
4. Send a General Query on upstream interface
5. Verify if an IS_IN(G1, {a}) record is reported.
6. Send a multicast udp packet with Source IP Address set to a and Destionation IP Address set to G1 on the upstream interface.
7. Verify if the udp packet is forwarden on the downstream interface.
8. Send IS_IN(G2, {b}) on downstream interface
9. Verify that no State-Change Report is sent on upstream interface.
10. Send a General Query on upstream interface.
11. Wait for a Current-State report and verify that only G1 is reported and not G2.
12. Send a multicast udp packet with Source IP Address set to a and Destionation IP Address set to G1.
13. Send a multicast udp packet with Source IP Address set to b and Destionation IP Address set to G2.
14. Verify that only the multicast ip packet for multicast group G1 is forwarded.

Problem: We assume that the second connection doesn't replace the first.

6.2.2.2 Immediate Leave

6.2.2.2.1 Test: igmpproxyv3.igmpv3.fastleave-01 (Fast Leave from an INCLUDE State with BLOCK)

Setup: **SETUP 9**

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1})
   INCLUDE(G, {a:T1})
2. Send [Host=1] BLOCK(G, {a}) on downstream interface
   State: empty state
3. (RV x) Receive on BLOCK(G, {a}) on upstream interface

Note: This will only work if the device implements Host Tracking ?

6.2.2.2.2 Test: igmpproxyv3.igmpv3.fastleave-02 (Fast Leave from an INCLUDE State with TO_IN)

Setup: **SETUP 9**

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1})
   INCLUDE(G, {a:T1})
2. Send [Host=1] TO_IN(G, { }) on downstream interface
   State: empty state
3. (RV x) Receive on BLOCK(G, {a}) on upstream interface

6.2.2.2.3 Test: igmpproxyv3.igmpv3.fastleave-03 (Fast Leave from an INCLUDE State with IS_IN)

Setup: **SETUP 9**

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] IN(G, {a:T1})
   INCLUDE(G, {a:T1})
2. Send [Host=1] IS_IN(G, { }) on downstream interface
   State: empty state
3. (RV x) Receive on BLOCK(G, {a}) on upstream interface

Note: This will only work if the device implements Host Tracking ?

6.2.2.2.4 Test: igmpproxyv3.igmpv3.fastleave-04 (Fast Leave from an EXCLUDE State with TO_IN)

Setup: **SETUP 9**

Procedure:
1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a}):T1
   EXCLUDE(G:T1, ({}, {a }))
2. Send [Host=1] TO_IN(G, { }) on downstream interface
   State: empty state
3. (RV x) Receive TO_IN(G, {}) on upstream interface

6.2.2.2.5 Test: igmpproxyv3.igmpv3.fastleave-05 (Fast Leave from an EXCLUDE State with IS_IN)

1. Reset and initialize the device into its startup state
   State: [Host=1] EX(G, {a}):T1
   EXCLUDE(G:T1, ({}, {a }))
2. Send [Host=1] IS_IN(G, {a }) on downstream interface
   State: empty state
3. (RV x) Receive TO_IN(G, {a}) on upstream interface

Note: This will only work if the device implements Host Tracking ?

6.2.2.2.6 Test: igmpproxyv3.specific.performance-01

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 10 The RGW MUST have a join and leave latency less then 20 ms. [TR-124 R-45]

Procedure:
1. Reset device.
2. Send multicast packets with source a and destination G on upstream interface

3. Verify that the multicast packets are not forwarded on the upstream interface
4. Send [Host = 1] IS_EX(G, {a}) on upstream interface
5. Measure how long it takes before the device starts forwarding the packets, this must be less then 20 ms.
6. Send [Host = 1] TO_IN(G, { }) on upstream interface
7. Measure how long it takes before the device stops forwarding the packets, this must be less than 20 ms.

Note:
- Future work: add a hybrid test (leave and join another channel with only one igmp report)?
- The Agilent N2X Multi-services test solution is able to test IGMP performance.

6.2.2.3 Upstream interface without an IP Address

6.2.2.3.1 Test: igmpproxyv3.specific.noip-01

Setup: **SETUP 4**

Requirements:
RG 12 The RGW 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. [TR-101 R-234]

Procedure:
1. Reset device.
   State: empty state
2. Send a TO_EX(G, {}) report on downstream interface
   State: EXCLUDE(G, ({}, {}))
3. Send a multicast packet with destination ip address G on the upstream interface
4. Verify if the packet is forwarded on the downstream interface

6.2.2.3.2 Test: igmpproxyv3.specific.noip-02

Setup: **SETUP 4**

Requirements:
RG 13 The RGW 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. [TR-101 R-235]

Procedure:
1. Reset device.
   State: empty state
2. Send a multicast packet with destination ip address G and a source ip address within the private ip address range on the downstream interface
3. Verify if the multicast packet is forwarded to the upstream interface and that its source ip is set to 0.0.0.0.

6.2.2.4 Multiple upstream interfaces

6.2.2.4.1 Test: igmpproxyv3.specific.multi-01

Setup: **SETUP 5**

Requirements:
RG 15 The default behavior MUST be to forward messages to all provisioned interfaces. [TR-101 R-195]

Procedure:
1. Reset device.
   State: empty state
2. Send an IS_IN(G, {a}) Report on the downstream interface.
   State: INCLUDE(G, {a})
3. (RV x) Receive ALLOW(G, {a}) on upstream IPoE interface
4. (RV x) Receive ALLOW(G, {a}) on upstream PPPoE interface

6.2.2.4.2 Test: igmpproxyv3.specific.multi-02

Setup: **SETUP 5**

Requirements:
RG 16 When the RGW 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. [TR-101 R-196]

Procedure:
1. Reset device.
   State: empty state
2. Send an IS_IN(G, {a}) Report on the downstream interface.
   State: INCLUDE(G, {a})
3. Send a IGMPv3 General Query on the IPoE upstream interface
4. Verify that the device responds with an IS_IN(G, {a}) report only on that interface
5. Send a IGMPv3 General Query on the PPPoE upstream interface
6. Verify that the device responds with an IS_IN(G, {a}) report only on that interface

6.2.2.4.3 Test: igmpproxyv3.specific.multi-03

Setup: **SETUP 6**

Requirements:
RG 14 When the RGW 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. [TR-101 R-194]

Procedure:
1. Reset device
   State: empty state
2. Send IS_EX(G, {}) on downstream interface
3. Verify that the device sends TO_EX(G, {}) only on the IPoE interface
4. Send a multicast packet on the downstream interface

5. Verify that the multicast packet is only forwarded on the IPoE interface.

6.2.2.5 Forwarding

6.2.2.5.1 Test: igmpproxyv3.specific.testrg201

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 21 The RGW MUST NOT forward UPNP multicast messages to its WAN interface. [TR-101 R-201]

UPNP uses the Simple Service Discovery Protocol (SSDP) to query and report services to clients and control points, SSDP packets are send to the IP multicast address 239.255.255.250.

Procedure:
1. Reset device.
   State: empty state
2. Send a multicast packet on a downstream interface with destination IP address 239.255.255.250.
3. Verify that the device doesn't forward it on the upstream interface.

6.2.2.5.2 Test: igmpproxyv3.specific.testrg42

Setup: **SETUP 8**

Requirements:
RG 22 The RGW 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). [TR-124 R-42]

Procedure:
1. Reset device.
   State: empty state
2. Pick a number of different random multicast groups in the specified range.
3. For every multicast group G:
   a. Send IS_EX(G, {}) on downstream interface
   b. Verify that no State-Change Report is sent regarding the multicast group G
4. Send a General Query on upstream interface
5. Verify that no Current-State report is sent with records for a multicast group in the predefined range.

6.2.2.5.3 Test: igmpproxyv3.specific.testrg43

Setup: **SETUP 1**, **SETUP 2**, **SETUP 3**

Requirements:
RG 23 The RGW MUST default to not sending IGMP messages for 239.0.0.0 through 239.255.255.255 to the WAN interfaces. [TR-124 R-43]

Procedure:
1. Reset device.
   State: empty state
2. Pick a number of different random multicast groups in the range 239.0.0.0 though 239.255.255.255.
3. For every multicast group G:
   a. Send IS_EX(G, {}) on downstream interface
   b. Verify that no State-Change Report is sent regarding the multicast group G
4. Send a General Query on upstream interface
5. Verify that no Current-State report is sent with records for a multicast group in the predefined range.

6.3 DHCP test methods

What to test ?
1. Allocation of a new network address, renewing the current lease and reallocating a previously used network address.
2. Verify that the different state transitions in the Client State Transition Diagram are working/implemented.
3. Networks with multiple DHCP servers attached.
4. Robustness to packet loss by testing the retransmission algorithms.
5. Silently ignoring corrupted packets.
6. DHCP client and server must still work when a DHCP relay agent forwards messages between them.
7. Implementation of (the most) important DHCP options.

Table of the relation between the test requirements and the test methods.

Requirement	**Test + remarks**
R 1	Function: CheckDhcpDiscover, Function: CheckDhcpOffer, Function: CheckDhcpRequestStateSelecting, Function: CheckDhcpRequestStateInitReboot, Function: CheckDhcpRequestStatRenewing, Function: CheckDhcpRequestStateRebinding, Function: CheckDhcpDecline, Function: CheckDhcpAck, Function: CheckDhcpAckInform, Function: CheckDhcpNak, Function: CheckDhcpRelease
R 2	dhcp.client.CorruptedOffer, dhcp.client.CorruptedAck, dhcp.server.CorruptedDiscover, dhcp.server.CorruptedRequest
R 3	TODO – minimum size DHCP frame
R 4	Function: CheckDhcp*
R 5	Future work
R 6	R 38, R 110, R 130, R 137
R 7	R 111, R 131
R 8	R 39, R 112
R 9	R 40, R 113
R 10	Function: CheckDhcp*

R 11	Function: CheckDhcp*
R 12	TODO – sname and file fields
R 13	Function: ParseDhcpMessage
R 14	Future work
R 15	Function: parseOptions
R 16	dhcp.client.OptionConcatenation, dhcp.server.OptionConcatenation
R 17	dhcp.client.OptionsOptionOverload
R 18	Not to be tested
R 19	TODO – parsing of sname and file fields for options
R 20	TODO – parsing of sname and file fields for options
R 21	TODO – new test (concatenation + overloading)
R 22	Function: CheckDhcpDiscover
R 23	Function: CheckDhcpDiscover
R 24	TODO – secs field
R 25	Function: CheckDhcpDiscover
R 26	Function: CheckDhcpDiscover
R 27	Function: CheckDhcpDiscover
R 28	dhcp.client.RandomXid
R 29	Function: CheckDhcpDiscover
R 30	MAY include “IP Address Lease Time” option
R 31	Function: CheckDhcpDiscover
R 32	MAY include “Vendor Class Identifier” option
R 33	Function: CheckDhcpDiscover
R 34	MAY include “Parameter Request List” option
R 35	MAY include “Maximum Message Size” option
R 36	Function: CheckDhcpDiscover
R 37	Future work – other configuration options
R 38	dhcp.server.RelayAgent, Function: CheckDhcpOffer
R 39	dhcp.server.AllocateAddressBroadcastFlag, Function: CheckDhcpOffer
R 40	Function: CheckDhcpOffer
R 41	Function: CheckDhcpOffer
R 42	Function: CheckDhcpOffer
R 43	Function: CheckDhcpOffer
R 44	Function: CheckDhcpOffer
R 45	Function: CheckDhcpOffer
R 46	Function: CheckDhcpOffer
R 47	Function: CheckDhcpOffer
R 48	Function: CheckDhcpOffer
R 49	Function: CheckDhcpOffer
R 50	Function: CheckDhcpOffer
R 51	Function: CheckDhcpOffer
R 52	MAY include “Vendor Class Identifier” option
R 53	Function: CheckDhcpOffer
R 54	Function: CheckDhcpOffer
R 55	Future work – other configuration options

R 56	Function: CheckDhcpRequestStateSelecting
R 57	Function: CheckDhcpRequestStateSelecting
R 58	Function: CheckDhcpRequestStateSelecting
R 59	Function: CheckDhcpRequestStateSelecting
R 60	Future work
R 61	Function: CheckDhcpRequestStateSelecting
R 62	Function: CheckDhcpRequestStateSelecting
R 63	Function: CheckDhcpRequestStateSelecting
R 64	Function: CheckDhcpRequestStateSelecting
R 65	Function: CheckDhcpRequestStateSelecting
R 66	Function: CheckDhcpRequestStateSelecting
R 67	MAY include “IP Address Lease Time” option
R 68	Function: CheckDhcpRequestStateSelecting
R 69	MAY include “Vendor Class Identifier” option
R 70	Function: CheckDhcpRequestStateSelecting
R 71	MAY include “Maximum Message Size” option
R 72	Function: CheckDhcpRequestStateSelecting
R 73	Function: CheckDhcpRequestInitReboot
R 74	Function: CheckDhcpRequestInitReboot
R 75	Function: CheckDhcpRequestInitReboot
R 76	Function: CheckDhcpRequestInitReboot
R 77	Future work – randomization of ‘xid’ field in INIT-REBOOT
R 78	TODO – secs field
R 79	Function: CheckDhcpRequestInitReboot
R 80	Function: CheckDhcpRequestInitReboot
R 81	Function: CheckDhcpRequestInitReboot
R 82	Function: CheckDhcpRequestInitReboot
R 83	Function: CheckDhcpRequestInitReboot
R 84	MAY include “Vendor Class Identifier” option
R 85	MAY include “Maximum Message Size” option
R 86	Function: CheckDhcpRequestInitReboot
R 87	Future work – other configuration options
R 88	Function: CheckDhcpRequestStateRenewing
R 89	Function: CheckDhcpRequestStateRenewing
R 90	Function: CheckDhcpRequestStateRenewing
R 91	Function: CheckDhcpRequestStateRenewing
R 92	Function: CheckDhcpRequestStateRenewing
R 93	Function: CheckDhcpRequestStateRenewing
R 94	Function: CheckDhcpRequestStateRenewing
R 95	Function: CheckDhcpRequestStateRenewing
R 96	Function: CheckDhcpRequestStateRenewing
R 97	Function: CheckDhcpRequestStateRenewing
R 98	Function: CheckDhcpRequestStateRenewing
R 99	Function: CheckDhcpRequestStateRebinding
R 100	Function: CheckDhcpRequestStateRebinding
R 101	Function: CheckDhcpRequestStateRebinding
R 102	Function: CheckDhcpRequestStateRebinding
R 103	Function: CheckDhcpRequestStateRebinding

R 104	Function: CheckDhcpRequestStateRebinding
R 105	Function: CheckDhcpRequestStateRebinding
R 106	Function: CheckDhcpRequestStateRebinding
R 107	Function: CheckDhcpRequestStateRebinding
R 108	Function: CheckDhcpRequestStateRebinding
R 109	Function: CheckDhcpRequestStateRebinding
R 110	dhcp.server.RelayAgent, Function: CheckDhcpAck
R 111	dhcp.server.RelayAgent , Function: CheckDhcpAck
R 112	dhcp.server.AllocateAddressBroadcastFlag , Function: CheckDhcpAck
R 113	Function: CheckDhcpAck
R 114	Function: CheckDhcpAck
R 115	Function: CheckDhcpAck
R 116	Function: CheckDhcpAck
R 117	TODO – yiaddr field
R 118	TODO – ciaddr, flags, giaddr, chaddr fields
R 119	Function: CheckDhcpAck
R 120	Function: CheckDhcpAck
R 121	Function: CheckDhcpAck
R 122	Function: CheckDhcpAck
R 123	Function: CheckDhcpAck
R 124	Future work – MUST NOT “Client Identifier” (could change to MAY)
R 125	MAY include “Vendor Class Identifier” option
R 126	Function: CheckDhcpAck
R 127	Function: CheckDhcpAck
R 128	Future work – other configuration options
R 129	Future work – other configuration options
R 130	Future work – DHCPINFORM
R 131	Future work – DHCPINFORM
R 132	Future work – DHCPINFORM
R 133	Future work – DHCPINFORM
R 134	Future work – DHCPINFORM
R 135	Future work – DHCPINFORM
R 136	Future work – DHCPINFORM
R 137	Function: CheckDhcpNak
R 138	Function: CheckDhcpNak
R 139	Function: CheckDhcpNak
R 140	Function: CheckDhcpNak
R 141	TODO – ‘flags’, ‘giaddr’, ‘chaddr’ fields
R 142	Function: CheckDhcpNak
R 143	Function: CheckDhcpNak
R 144	Function: CheckDhcpNak
R 145	Function: CheckDhcpNak
R 146	Function: CheckDhcpNak
R 147	MAY include “Client Identifier” option
R 148	MAY include “Vendor Class Identifier” option

R 149	Function: CheckDhcpNak
R 150	Function: CheckDhcpNak
R 151	TODO – MUST NOT other options
R 152	Function: CheckDhcpDecline
R 153	Future work – randomization of ‘xid’ in DHCPDECLINE
R 154	Function: CheckDhcpDecline
R 155	Function: CheckDhcpDecline
R 156	Function: CheckDhcpDecline
R 157	Function: CheckDhcpDecline
R 158	Function: CheckDhcpDecline
R 159	Function: CheckDhcpDecline
R 160	Function: CheckDhcpDecline
R 161	Function: CheckDhcpDecline
R 162	Function: CheckDhcpDecline
R 163	Function: CheckDhcpDecline
R 164	Function: CheckDhcpDecline
R 165	Function: CheckDhcpDecline
R 166	TODO – MUST NOT other options
R 167	Function: CheckDhcpRelease
R 168	Future work – xid field requirement could change
R 169	Function: CheckDhcpRelease
R 170	Function: CheckDhcpRelease
R 171	Function: CheckDhcpRelease
R 172	Function: CheckDhcpRelease
R 173	Function: CheckDhcpRelease
R 174	Function: CheckDhcpRelease
R 175	Function: CheckDhcpRelease
R 176	Function: CheckDhcpRelease
R 177	Function: CheckDhcpRelease
R 178	Function: CheckDhcpRelease
R 179	Function: CheckDhcpRelease
R 180	Function: CheckDhcpRelease
R 181	Function: CheckDhcpRelease
R 182	TODO – MUST NOT other options
R 183	Future work – DHCPINFORM
R 184	Future work – DHCPINFORM
R 185	Future work – DHCPINFORM
R 186	Future work – DHCPINFORM
R 187	Future work – DHCPINFORM
R 188	Future work – DHCPINFORM
R 189	Future work – DHCPINFORM
R 190	Future work – DHCPINFORM
R 191	Future work – DHCPINFORM
R 192	Future work – DHCPINFORM
R 193	Future work – DHCPINFORM
R 194	Future work – DHCPINFORM
R 195	Future work – DHCPINFORM
R 196	Future work – DHCPINFORM

R 197	Future work – DHCPINFORM
R 198	Future work – DHCPINFORM
R 199	Future work – DHCPINFORM
R 200	Future work – DHCPINFORM
R 201	Future work – DHCPINFORM
R 202	dhcp.client.RebindAddress, dhcp.client.TimeoutLease, dhcp.client.TimeoutRequestSelecting, dhcp.client.TimeoutReallocateAddress
R 203	No test required
R 204	dhcp.client.Desynchronization
R 205	dhcp.client.RandomXid
R 206	dhcp.client.TimeoutLease
R 207	dhcp.client.AllocateAddress
R 208	dhcp.client.TimeoutOffer
R 209	dhcp.client.MultipleServers
R 210	dhcp.client.ReallocateAddressNak
R 211	dhcp.client.AllocateAddress, dhcp.client.MultipleServers, dhcp.server.MultipleServers
R 212	dhcp.client.SelectingDiscardAck
R 213	dhcp.client.AllocateAddress
R 214	dhcp.client.AllocateAddress, dhcp.client.AllocateAddressNak
R 215	dhcp.client.AllocateAddressUseAckOptions
R 216	dhcp.client.TimeoutRequestSelecting
R 217	dhcp.client.AllocateAddress
R 218	dhcp.client.AllocateAddressNak
R 219	dhcp.client.TimeoutLease, dhcp.client.StopUsingIP
R 220	dhcp.client.AllocateAddress, dhcp.client.AllocateAddressInUse, dhcp.client.ReallocateAddress
R 221	dhcp.client.AllocateAddress, dhcp.client.AllocateAddressInUse, dhcp.client.ReallocateAddress
R 222	dhcp.client.AllocateAddressInUse
R 223	dhcp.client.AllocateAddress, dhcp.client.ReallocateAddress
R 224	Future work – desynchronization in INIT-REBOOT
R 225	Future work – lease expiration in INIT-REBOOT
R 226	Future work – randomization of ‘xid’ in INIT-REBOOT
R 227	dhcp.client.ReallocateAddress, dhcp.client.ReallocateAddressNak
R 228	dhcp.client.ReallocateAddress
R 229	Future work – what should the client check for ?
R 230	Future work – use parameters in DHCPACK (INIT-REBOOT)
R 231	Future work – lease expiration in INIT-REBOOT
R 232	dhcp.client.ReallocateAddressNak
R 233	dhcp.client.TimeoutReallocateAddress

R 234	dhcp.client.RenewAddress, dhcp.client.RenewAddressNak, dhcp.client.RebindAddress
R 235	dhcp.client.RebindAddress, dhcp.client.RebindAddressNak
R 236	dhcp.server.OptionRenewalRebindingLeaseTime
R 237	TODO – check default values for T1,T2
R 238	Future work – random “fuzz” around T1 and T2 to avoid synchronization
R 239	dhcp.client.RenewAddress
R 240	dhcp.client.RenewAddress
R 241	dhcp.client.RenewAddress
R 242	Future work – lease expiration in RENEWING
R 243	Future work – discard non matching DHCPACK (RENEWING)
R 244	dhcp.client.RenewAddress
R 245	dhcp.client.RenewAddressNak
R 246	dhcp.client.RebindAddress, dhcp.client.TimeoutLease
R 247	dhcp.client.RebindAddress
R 248	dhcp.client.RebindAddress
R 249	Future work – lease expiration in REBINDING
R 250	Future work – discard non matching DHCPACK (REBINDING)
R 251	dhcp.client.RebindAddress
R 252	dhcp.client.TimeoutLease
R 253	dhcp.client.RebindAddressNak
R 254	dhcp.client.TimeoutLease, dhcp.client.StopUsingIP
R 255	Future work – DHCPRELEASE
R 256	Future work – DHCPRELEASE
R 257	Future work – DHCPINFORM
R 258	Future work – DHCPINFORM
R 259	Future work – DHCPINFORM
R 260	Future work – DHCPINFORM
R 261	Future work – DHCPINFORM
R 262	dhcp.server.OptionClientIdentifier
R 263	dhcp.server.AllocateSameAddress, dhcp.server.ReallocateAddress
R 264	dhcp.server.AllocateAddress
R 265	dhcp.server.AllocateAddress, dhcp.server.AllocateAddressPingReply
R 266	dhcp.server.OptimizedOffer
R 267	Not to be tested
R 268	Future work – Vendor Class Identifer and Vendor Specific Information
R 269	Function: CheckDhcpOffer
R 270	TODO – options prepared to deliver with “Parameter Request List” in DHCPOFFER (NEW TEST)
R 271	dhcp.server.RenewAddress, dhcp.server.ReallocateWithDiscover
R 272	dhcp.server.AllocateSameAddress, dhcp.server.ReallocateAddress, dhcp.server.OptionClientIdentifier
R 273	dhcp.server.RequestAddress

R 274	dhcp.server.AllocateAddress
R 275	dhcp.server.DontReuseAddress
R 276	dhcp.server.ReuseExpiredAddress
R 277	Not to be tested
R 278	Not to be tested
R 279	Future work – what does this?
R 280	Not to be tested
R 281	Not to be tested
R 282	Future work – included configuration parameters
R 283	Future work – included configuration parameters
R 284	Future work – included configuration parameters
R 285	Future work – included configuration parameters
R 286	dhcp.server.AllocateAddress
R 287	Future work – DHCP server with multiple subnets
R 288	Not to be tested - echo request at wrong time (DHCP protocol wouldn't work if it wasn't implemented correctly)
R 289	dhcp.server.MultipleServers
R 290	TODO – lease time in DHCPACK must be at least as long as in DHCPOFFER
R 291	dhcp.client.AllocateAddressUseAckOptions
R 292	Future work – INCONSISTENCY with other requirements
R 293	dhcp.server.ReallocateAddressUnknown
R 294	Future work – DHCP server with multiple subnets
R 295	dhcp.server.ReallocateWrongAddress
R 296	dhcp.server.ReallocateAddress
R 297	dhcp.server.RenewAddress
R 298	Future work
R 299	dhcp.server.RebindAddress
R 300	dhcp.server.DeclineAddress
R 301	dhcp.server.ReuseReleasedAddress1, dhcp.server.ReuseReleasedAddress2
R 302	dhcp.server.Inform
R 303	dhcp.server.Inform
R 304	Future work – DHCPINFORM
R 305	Future work – DHCPINFORM
R 306	dhcp.client.OptionPad, dhcp.server.OptionPad
R 307	TODO – end option
R 308	dhcp.server.RequestAddress
R 309	dhcp.server.OptionRenewalRebindingLeaseTime
R 310	dhcp.client.OptionsOptionOverload
R 311	Function: CheckDhcp*
R 312	Function: CheckDhcp*
R 313	Function: CheckDhcp*
R 314	TODO – Maximum DHCP Message Size
R 315	dhcp.server.OptionRenewalRebindingLeaseTime
R 316	dhcp.server.OptionRenewalRebindingLeaseTime
R 317	Function: CheckDhcp*
R 318	TODO – Maximum DHCP Message Size
R 319	dhcp.client.OptionConcatenation
R 320	Future work – uniqueness of client identifier

R 321	Function: CheckDhcp*
R 322	Future work – Client Identifier format
R 323	Future work – Client Identifier format
R 324	dhcp.client.Options
R 325	dhcp.client.Options
R 326	dhcp.client.Options
R 327	dhcp.client.Options
R 328	TODO – Static Route option MUST NOT be used
R 329	dhcp.client.Options
R 330	TODO – Subnet Mask option before Router option
R 331	Future work – Interface MTU option
R 332	dhcp.client.Options
R 333	dhcp.client.Options
R 334	dhcp.client.Options
R 335	Future work – Vendor Class Identifer and Vendor Specific Information
R 336	Not to be tested
R 337	Future work – Vendor Class Identifer and Vendor Specific Information
R 338	dhcp.server.OptionRelayAgentInformation
R 339	Future work – Vendor Class Identifer and Vendor Specific Information
R 340	Future work – Vendor Class Identifer and Vendor Specific Information
R 341	Future work – Vendor Class Identifer and Vendor Specific Information
R 342	Future work – Vendor Class Identifer and Vendor Specific Information
R 343	Future work – Vendor Class Identifer and Vendor Specific Information
R 344	Future work – Vendor Class Identifer and Vendor Specific Information
R 345	dhcp.server.OptionRelayAgentInformation
R 346	TODO – Relay Agent Information not in sname or file field
R 347	Not to be tested
R 348	Future work – Network Time Protocol Servers
R 349	Future work – TFTP Server Name
R 350	Future work – Bootfile Name
R 351	Future work – SMTP Server
R 352	Future work – POP3 Server
R 353	Future work – NNTP Server

6.3.1 DHCP Client

6.3.1.1 Allocating a new network address

6.3.1.1.1 Test: dhcp.client.AllocateAddress

Test description:
Test if the client is able to allocate a new network address.

Requirements:
R 207 The client forms and sends a DHCPDISCOVER message as specified in 1.2.2.4.1.
R 211 The client extracts the server address from the ‘server identifier’ option in the selected DHCPOFFER message.

R 213 The client broadcasts a DHCPREQUEST message as specified in 1.2.2.4.3.1 (DHCPREQUEST generated in SELECTING state).
R 214 The client waits for a DCHPACK or DHCPNAK message from the server before proceeding.
R 217 Once the DHCPACK message from the server arrives, the client is initialized and moves to BOUND state.
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 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.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message
4. Wait for a DHCPREQUEST message
5. Send a DHCPACK message
6. Verify that the client sends an ARP request for the suggested address to ensure that the address is not already in use.
7. Verify that the client announces its new IP address by broadcasting an ARP reply.
8. Check if the client doesn't reject the configuration.
9. Verify that the client uses the allocated IP address by sending an ARP request and waiting for the reply.

6.3.1.1.2 Test: dhcp.client.AllocateAddressUseAckOptions

Test description:
Test if the client uses the DHCP options from the DHCPACK message.

Requirements:
R 215 The client SHOULD use the parameters in the DHCPACK message for configuration.
R 291 The options delivered in a DHCPACK message MAY differ from those in a DHCPOFFER message.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message with only an 'IP lease time option' and 'Server Identifier' option
4. Wait for a DHCPREQUEST message
5. Send a DHCPACK message with an additional 'Subnet Mask', 'Router' and 'Domain Name Server' option.
6. Check if the client doesn't reject the configuration.
7. Operator of test suite should check if client configured the DNS servers, the subnet mask and the gateway.

Note: Configuration of DNS server, subnetmask and the gateway can be checked by a script (e.g. expect script) that logs in with telnet or ssh.

6.3.1.1.3 Test: dhcp.client.RelayAgent

Test description:
Test if the client can work together with a relay agent to allocate a new network address.

Requirements:
R 211 The client extracts the server address from the 'server identifier' option in the selected DHCPOFFER message.
R 319 DHCP clients use the contents of the 'server identifier' field as the destination address for any DHCP messages unicast to the DHCP server.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message with source mac and source IP address set to the relay agents values.
4. Wait for a DHCPREQUEST message
5. Check if the client doesn't reject the configuration.
6. Wait for the renewal timer to expire
7. Wait for a DHCPREQUEST message and verify that it is send to the server and not to the relay agent

6.3.1.1.4 Test: dhcp.client.AllocateAddressNak

Test description:
Test if the client jumps to the INIT state when it receives a DHCPNAK message while waiting for a DHCPACK in the REQUESTING state.

Requirements:
R 214 The client waits for a DCHPACK or DHCPNAK message from the server before proceeding.
R 218 If the client receives a DHCPNAK message, the client restarts the configuration process and jumps to the INIT state.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message
4. Wait for a DHCPREQUEST message
5. Send a DHCPNAK message
6. Wait for a DHCPDISCOVER message

6.3.1.1.5 Test: dhcp.client.AllocateAddressInUse

Test description:
The client must verify if the offered IP address is not already in use. If it is used by someone else the client must reject the configuration and send a DHCPDECLINE message.

Requirements:
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.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message
4. Wait for a DHCPREQUEST message
5. Send a DHCPACK message
6. Wait for an ARP request from the client querying its received IP address.
7. Send an ARP reply from a different hardware address indicating that the IP is being used
8. Wait for a DHCPDECLINE message
9. Wait for a DHCPDISCOVER message

6.3.1.1.6 Test: dhcp.client.SelectingDiscardAck

Test description:
Test if the client discards DHCPACK messages in received in the SELECTING state.

Requirements:
R 212 Any arriving DHCPACK message MUST be silently discarded.

Procedure:
1. Reset the DHCP client
2. Measure the time between successive DHCPDISCOVER messages, continue when this time exceeds 16 seconds
3. Send a DHCPACK message
4. Verify that the client doesn't respond to the DHCPACK message and retransmits the

DHCPDISCOVER message (retransmission time should be larger than 16 seconds).

6.3.1.1.7 Test: dhcp.client.RandomXid

Test description:
Test if the client generates random Xid values.

Requirements:
R 28 The client inserts a random transaction identifier into the 'xid' field.
R 205 The client generates and records a random transaction identifier and inserts that identifier into the 'xid' field.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress and record the Xid value used.
2. Wait until the lease expires and the client jumps back to the INIT state
3. Wait for a DHCPDISCOVER message and record the Xid value.

4. Verify that the two Xid values are different.

6.3.1.1.8 Test: dhcp.client.Desynchronization

Test description:
Test if the device waits a random time after booting before starting the DHCP configuration process.

Requirements:
R 204 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)

Procedure:
1. Reboot the device a number of times (e.g. 5 times) and measure the time till the first DHCPDISCOVER message is sent.
2. Calculate the standard deviation, it should be larger then 1 (maybe 2 ?) seconds.

6.3.1.2 Renewing or rebinding current lease

6.3.1.2.1 Test: dhcp.client.RenewAddress

Test description:
Test if the client tries to renew its lease by unicasting DHCPREQUEST messages when the renewal timer has expired.

Requirements:
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 239 At T1 the client moves to RENEWING state.
R 240 A client MAY choose to renew or extend its lease prior to T1.
R 241 The client sends (via unicast) a DHCPREQUEST message to the server to extend its lease. (1.2.2.4.3.3)
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.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the renewal timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPACK message
5. Verify that the client doesn't reject the extended lease

6.3.1.2.2 Test: dhcp.client.RenewAddressNak

Test description:
Test if the client jumps to the INIT state when it receives a DHCPNAK message while trying to renew its lease in the RENEWING state.

Requirements:
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 245 If the client is in the RENEWING state and receives a DHCPNAK message in response to its DHCPREQUEST message it moves to the INIT state.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the renewal timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPNAK message
5. Wait for a DHCPDISCOVER message

6.3.1.2.3 Test: dhcp.client.RebindAddress

Test description:
Test if the client tries to renew its lease by broadcasting DHCPREQUEST messages when the rebinding timer has expired.

Requirements:
R 202 The client MUST adopt a retransmission strategy that incorporates a randomized exponential back off algorithm to determine the delay between retransmissions.
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 246 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 247 If no DHCPACK arrives before time T2, the client moves to REBINDING state.
R 248 The client sends (via broadcast) a DHCPREQUEST to extend its lease. (1.2.2.4.3.4)
R 251 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.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the rebinding timer to expire and verify that the client retransmits DHCPREQUEST messages in the RENEWING state
3. Wait for a DHCPREQUEST message
4. Send a DHCPACK message
5. Verify that the client doesn't reject the extended lease

6.3.1.2.4 Test: dhcp.client.RebindAddressNak

Test description:
Test if the client jumps to the INIT state when it receives a DHCPNAK message while trying to renew its lease in the REBINDING state.

Requirements:

R 235 T2 is the time at which the client enters the REBINDING state and attempts to contact any server.
R 253 If the client is in the REBINDING state and receives a DHCPNAK message in response to its DHCPREQUEST message it moves to the INIT state.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the rebinding timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPNAK message
5. Wait for a DHCPDISCOVER message

6.3.1.2.5 Test: dhcp.client.TimeoutLease

Test description:
1. Test if the client stops using its allocated IP address when the lease period has expired and jumps to the INIT state.
2. Test if the client implements the randomized exponential back off algorithm.

Requirements:
R 202 The client MUST adopt a retransmission strategy that incorporates a randomized exponential back off algorithm to determine the delay between retransmissions.
R 206 The client records its own local time for later use in computing the lease expiration.
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.
R 246 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 252 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 254 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.

Procedure:
1. Let the client allocate a new address as using the procedure described in dhcp.client.AllocateAddress.
2. Wait for the renewal timer, rebinding timer to expire and verify that the client sends DHCPREQUEST messages using the randomized exponential back off algorithm
3. Wait for the rebinding timer, rebinding timer to expire and verify that the client broadcasts DHCPREQUEST messages using the randomized exponential back off algorithm
4. Wait for the lease to expire.
5. Verify by waiting for a DHCPDISCOVER message that the client moved to the INIT state.

6.3.1.2.6 Test: dhcp.client.StopUsingIP

Test description:
Verify that the client immediately stops using the IP address when the lease expires.

Requirements:
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.
R 254 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.

Procedure:
1. Let the client acquire an IP address as described in dhcp.client.AllocateAddress
2. Wait for the lease to expire
3. Send an ARP Request for its IP and verify that the client does not send a reply

6.3.1.3 Reallocating a network address

6.3.1.3.1 Test: dhcp.client.ReallocateAddress

When the client rebooted and it remembered its IP address the client tries to reallocate its old configuration by broadcasting a DHCPREQUEST. If it doesn't receive a response the client is allowed to use the lease until it expires.

Requirements:
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 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.
R 227 The client sends a DHCPREQUEST message as specified in 1.2.2.4.3.2 (DHCPREQUEST generated during INIT-REBOOT state).
R 228 The client waits for a DHCPACK message with a 'xid' field matching that the recorded value.

Procedure:
1. Wait for a DHCPDISCOVER message
2. Send a DHCPOFFER message
3. Wait for a DHCPREQUEST message
4. Send a DHCPACK message
5. Verify that the client does not reject the configuration
6. Reboot the DHCP client
7. Wait for a DHCPREQUEST message
8. Send a DHCPACK message

9. Verify that the client sends an ARP request for the suggested address to ensure that the address is not already in use.
10. Verify that the client announces its new IP address by broadcasting an ARP reply.
11. Check if the client accepts the configuration

6.3.1.3.2 Test: dhcp.client.ReallocateAddressNak

Test description:
Test if the client jumps to the INIT state when it receives a DHCPNAK message while trying to reallocate an address in the INIT-REBOOT state.

Requirements:
R 227 The client sends a DHCPREQUEST message as specified in 1.2.2.4.3.2 (DHCPREQUEST generated during INIT-REBOOT state).
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 1.2.3.2 (procedure starting in the INIT state).

Procedure:
1. Wait for a DHCPDISCOVER message
2. Send a DHCPOFFER message
3. Wait for a DHCPREQUEST message
4. Send a DHCPACK message
5. Verify that the client does not reject the configuration
6. Reboot the DHCP client
7. Wait for a DHCPREQUEST message
8. Send a DHCPNAK message
9. Wait for a DHCPDISCOVER message

6.3.1.4 Multiple clients or servers

6.3.1.4.1 Test: dhcp.client.InvalidXidOffer

Test description:
Test if the client ignores DHCPOFFER messages with a ‘xid’ that does not match the one in the most recent DHCPDISCOVER message.

Requirements:
R 210 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.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message with a different value in the ‘xid’ field.
4. Verify that the client doesn’t respond to the DHCPOFFER message and sends another DHCPDISCOVER message.

6.3.1.4.2 Test: dhcp.client.MultipleServers

Test description:
Test if the client can acquire a new address when multiple DHCP servers are attached to the network.

Requirements:
R 209 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 The client extracts the server address from the 'server identifier' option in the selected DHCPOFFER message.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send two DHCPOFFER messages from two different DHCP servers
4. Wait for the first DHCPREQUEST to one of the two servers
5. Send a corresponding DHCPACK message
6. Verify that no second DHCPREQUEST is send to the other DHCP server
7. Verify that the client accepts the configuration

6.3.1.5 Retransmission algorithm

6.3.1.5.1 Test: dhcp.client.TimeoutOffer

Test description:
Test if the client keeps retransmitting DHCPDISCOVER messages when no responses arrive.

Requirements:
R 208 A client stays in the INIT state and retransmits DHCPDISCOVER messages as long as needed to acquire a lease. A semi-exponential back off algorithm may be incorporated that saturates at a certain retransmission delay (e.g. 64 seconds).

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER messages and don't send any response
3. Verify that the client keeps trying to acquire an address

Problem: how long do we have to wait until we can conclude that the test succeeded?

6.3.1.5.2 Test: dhcp.client.TimeoutRequestSelecting

Test description:
Test if the client retransmits the DHCPREQUEST message according to the randomized exponential back off algorithm. If no response was received within 60 seconds the client must jump to the init state and start sending DHCPDISCOVER messages again.

Requirements:
R 202 The client MUST adopt a retransmission strategy that incorporates a randomized exponential back off algorithm to determine the delay between retransmissions.
R 216 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 1.2.3.2. 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.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message
4. Don't send any reply to DHCPREQUEST messages received, verify that client retransmits according to an exponential back off algorithm
5. After a while the client should send another DHCPDISCOVER message

6.3.1.5.3 Test: dhcp.client.TimeoutReallocateAddress

Test description:
Test if the client retransmits requests when it neither received a DHCPACK nor a DHCPNAK reply. The client may decide after employing the retransmission algorithm to use its lease until it expires. Otherwise it must jump to the INIT state and start sending DHCPDISCOVER messages.

Requirements:
R 202 The client MUST adopt a retransmission strategy that incorporates a randomized exponential back off algorithm to determine the delay between retransmissions.
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 1.2.3.2. 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.

Procedure:
1. Let the client allocate an address as described in dhcp.client.AllocateAddress
2. Reboot the DHCP client
3. Wait for a DHCPREQUEST messages, don't send any response and verify the retransmission algorithm.
4. Verify that the client doesn't use its IP address longer than permitted by its lease
5. Check if the client moves to the INIT state and starts sending DHCPDISCOVER messages

6.3.1.6 Changing the IP address of the client

6.3.1.6.1 Test: dhcp.client.RenewChangeAddress

Test description:
Test if the client accepts a new IP address by sending a DHCPACK message in the renewing state with a different (new !) IP address.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the renewal timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPACK message with a new IP address
5. Verify that the client does not reject the new configuration

Note: this test is experimental and not described in the standards, this test should fail.

6.3.1.6.2 Test: dhcp.client.RenewNakChangeAddress

Test description:
Test if the client accepts a new IP address by sending a DHCPNAK in the renewing state and then waiting for a DHCPDISCOVER message.

Requirements:
This test does not verify any new requirements. It just checks if the device is able to change its IP address.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the renewal timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPNAK message
5. Wait for a DHCPDISCOVER message
6. Send a DHCPOFFER message with a new IP address
7. Wait for a DHCPREQUEST message
8. Send a DHCPACK message
9. Verify that the client does not reject the new configuration

6.3.1.7 Test: dhcp.client.RebindingNakChangeAddress

Test description:
Test if the client accepts a new IP address by sending a DHCPNAK in the rebinding state and then waiting for a DHCPDISCOVER message.

Requirements:
This test does not verify any new requirements. It just checks if the device is able to change its IP address.

Procedure:
1. Let the client allocate an IP address as described in dhcp.client.AllocateAddress
2. Wait for the rebinding timer to expire
3. Wait for a DHCPREQUEST message
4. Send a DHCPNAK message
5. Wait for a DHCPDISCOVER message
6. Send a DHCPOFFER message with a new IP address
7. Wait for a DHCPREQUEST message
8. Send a DHCPACK message
9. Verify that the client does not reject the new configuration

6.3.1.8 Invalid DHCP messages

6.3.1.8.1 Test: dhcp.client.CorruptedOffer

Test description:
Test if the client silently ignores corrupted DHCPOFFER messages.

Requirements:
R 2 Corrupted DHCP messages (e.g. invalid IP checksum or invalidUDP checksum) MUST be ignored.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a corrupted DHCPOFFER message (invalid UDP checksum)
4. The client must not respond with a DHCPREQUEST message, but ignores the previous DHCPOFFER message. Instead it must continue as if no one answered by retransmitting the DHCPDISCOVER message.

6.3.1.8.2 Test: dhcp.client.CorruptedAck

Test description:
Test if the client silently ignores corrupted DHCPACK messages.

Requirements:
R 2 Corrupted DHCP messages (e.g. invalid IP checksum or invalidUDP checksum) MUST be ignored.

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message
4. Wait for a DHCPREQUEST message
5. Send a corrupted DHCPACK message
6. Wait for a retransmission of the DHCPREQUEST message
7. Send a valid DHCPACK message

6.3.1.9 Option tests

6.3.1.9.1 Test: dhcp.client.OptionsOptionOverload

Test description:
Test if the client implemented the ‘Option Overload’ option.

Requirements:
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 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. Option concatenation MUST also be done in this order.
R 310

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message with an ‘Option Overload’ option in the ‘options’ field of the DHCP header and the ‘DHCP message type’, ‘IP address lease time’, ‘Server I dentifier’ options and all other options in the ‘file’ field of the DHCP header.
4. Wait for a DHCPREQUEST message
5. Send a DHCPACK message with an ‘Option Overload’ option in the ‘options’ field of the DHCP header and the all other options in the ‘file’ field of the DHCP header.
6. Verify that the client accepts the configuration

6.3.1.9.2 Test: dhcp.client.Options

Test description:
This test will include the following options: Subnet Mask, Router, Domain Name Server, Interface MTU, Host Name, Domain Name, Broadcast Address, Classless Static Route. It is up to the operator of the test suite to verify that the client uses these configuration options.

Requirements:
R 324, R 325, R 326, R 327, R 329, R 332, R 333, R 334

Procedure:
1. Reset the DHCP client
2. Wait for a DHCPDISCOVER message
3. Send a DHCPOFFER message with values for all the options listed in objective.
4. Wait for a DHCPREQUEST
5. Send a DHCPACK message with the same values for all the options in the DHCPOFFER message
6. Verify that the client doesn’t reject the lease
7. Verify that the device is correctly configured

Note: The correct configuration of the device with the values specified in the options can be checked by a script (e.g. expect script) that logs in with telnet or ssh.

6.3.1.9.3 Test: dhcp.client.OptionConcatenation

Test description:
Test if client concatenates DHCP options of the same type and treats them as one DHCP option. We do this by sending a DHCPOFFER with a split Server Identifier option.

Requirements:
R 16 When more than one option with a given type code appears in the DHCP packet, all such options should be concatenated in sequential order. It MUST treat the contents of that option as a single option. Although this feature is primarily used to send options that are longer than 255 bytes, splitting options that are shorter than 255 MAY also may done if deemed necessary. [RFC 3396]

Procedure:
1. Reset the DHCP client.
2. Wait for a DHCPDISCOVER message.
3. Send a DHCPOFFER message with a split Server Identifier and the source IP address not equal to the server's IP.
4. Wait for a DHCPREQUEST and verify that it was unicasted to the server.
5. Send a DHCPACK message.
6. Verify that the client doesn't reject the lease.

6.3.1.9.4 Test: dhcp.client.OptionPad

Test description:
Test if client skips pad options.

Requirements:
R 306

Procedure:
Let the client allocate an IP address as described in dhcp.client.RelayAgent but insert padding options before the Server Identifier.

DHCP Server

6.3.1.10 Allocating a new network address

6.3.1.10.1 Test: dhcp.server.AllocateAddress

Test description:
1. Test if a client is able to allocate a new address from the server.
2. Verify that the server sends an ICMP echo request.

Requirements:
R 264 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 265 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 274 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).
R 286 Servers with knowledge of the client's configuration parameters respond with a DHCPACK message to the client.

Procedure:
1. Send a DHCPDISCOVER message
2. Verify that the client has tried to ping the offered address (this must be done before the DHCPOFFER message)
3. Wait for a DHCPOFFER message
4. Send a DHCPREQUEST message

5. Wait for a DHCPACK message

6.3.1.10.2 Test: dhcp.server.AllocateAddressBroadcastFlag

Test description:
Test if the server broadcasts DHCP replies when the client enabled the broadcast flag.

Requirements:
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 39 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 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.

Procedure:
1. Send a DHCPDISCOVER message with the broadcast flag set
2. Wait for a DHCPOFFER message and check if it was broadcasted
3. Send a DHCPREQUEST message with the broadcast flag set
4. Wait for a DHCPACK message and check if it was broadcasted

6.3.1.10.3 Test: dhcp.server.RequestAddress

Test description:
Test if client is able to allocate a requested address.

Requirements:
R 273 The address requested in the 'Requested IP Address' option, if that address is valid and not already allocated.

Procedure:
1. Send a DHCPDISCOVER message with the IP address to be requested included in the 'Requested IP address' option.
2. Wait for a DHCPOFFER message and verify that the offered IP address matches the requested IP address.
3. Send a DHCPREQUEST message.
4. Wait for a DHCPACK message.

6.3.1.10.4 Test: dhcp.server.AllocateSameAddress

Test description:
Test if the server attempts to allocate the same network address each time the client requests an address even if its previous lease has expired.

Requirements:
R 263 If the client does not provide a 'client identifier' option, the server MUST use the contents of the 'chaddr' field to identify the client.
R 272 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.

Procedure:
1. Allocate a new IP address as described in dhcp.server.AllocateAddress.
2. Wait for the lease timer to expire.
3. Allocate again an IP address as described in dhcp.server.AllocateAddress.
4. Verify that the both distributed IP addresses are equal.

6.3.1.11 Renewing or rebinding current lease

6.3.1.11.1 Test: dhcp.server.RenewAddress

Test description:
Test if a client is able to renew its address.

Requirements:
R 271 The client's current address as recorded in the client's current binding.
R 297 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.

Procedure:
1. Allocate a new address as described in dhcp.server.AllocateAddress
2. Wait until the renewal timer expires
3. Send a DHCPREQUEST message
4. Wait for a DHCPACK message

6.3.1.11.2 Test: dhcp.server.RebindAddress

Test description:
Test if a client is able to rebind its address.

Requirements:
R 299 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.

Procedure:
1. Allocate a new address as described in dhcp.server.AllocateAddress
2. Wait until the rebinding timer expires
3. Send a DHCPREQUEST message
4. Wait for a DHCPACK message

6.3.1.12 Reallocating a network address

6.3.1.12.1 Test: dhcp.server.ReallocateAddress

Test description:
Test if a client can reallocate its address when it has rebooted.

Requirements:
R 263 If the client does not provide a 'client identifier' option, the server MUST use the contents of the 'chaddr' field to identify the client.
R 272 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 296 If the server knows the client, the network is correct and the client's notion of its IP address is correct the server should respond with a DCHPACK message to the client.

Procedure:
1. Allocate an IP address as described in dhcp.server.AllocateAddress
2. Send a DHCPREQUEST message for the InitReboot state
3. Wait for a DHCPACK message

6.3.1.12.2 Test: dhcp.server.ReallocateWrongAddress

Test description:
Test if the server sends a DHCPNAK message if a client tries to reallocate an address but includes a wrong 'requested IP address' option.

Requirements:
R 295 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.

Procedure:
1. Allocate an IP address as described in dhcp.server.AllocateAddress
2. Send a DHCPREQUEST message for the InitReboot state but with a wrong IP address
3. Wait for a DHCPNAK message

6.3.1.12.3 Test: dhcp.server.ReallocateAddressUnknown

Test description:
Test if the server remains silent when an unknown client wants to reallocate its address. This is necessary for coexistence of multiple DHCP servers.

Requirements:
R 293 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.

Procedure:
1. Reset the DHCP server
2. Send a DHCPREQUEST message as if the client is in the InitReboot state
3. Verify that the server doesn't send any DHCP message

6.3.1.12.4 Test: dhcp.server.ReallocateWithDiscover

Test description:
Test if the server reallocates the client's previous address when the client starts from the INIT state instead of the INITREBOOT state.

Requirements:
R 271 The client's current address as recorded in the client's current binding.

Procedure:
1. Allocate an IP address as described in dhcp.server.AllocateAddress
2. Send a DHCPDISCOVER message
3. Wait for a DHCPOFFER message
4. Verify that the server offers the same IP address as it offered in step 1.

6.3.1.13 Reusing network addresses

6.3.1.13.1 Test: dhcp.server.DontReuseAddress

Test description:
Verify that the server does not reuse network addresses when their lease has not expired yet.

Requirements:requirements
R 275 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.

Procedure:
1. Allocate all available network addresses
2. Send another DHCPDISCOVER message (from another DHCP client)
3. Verify that the client does not send another DHCPOFFER message

6.3.1.13.2 Test: dhcp.server.ReuseExpiredAddress

Test description:
Test if the server allocates addresses whose lease have expired when all available addresses have been expired.

Requirements:
R 276 When the available addresses have been exhausted the allocation mechanism will reuse those addresses whose lease has expired.

Procedure:
1. Allocate a network address as described in dhcp.server.AllocateAddress
2. Wait until lease expires
3. Allocate all available network addresses
4. Check if the previous address was distributed again.

6.3.1.13.3 Test: dhcp.server.ReuseReleasedAddressX (X=1,2)

Test description:
Test if the server allocates addresses which have been explicitly released with an DHCPRELEASE message. This can be done by explicitly asking for the released IP address in the DHCPDISCOVER message or allocating all other addresses until the server offers the released IP address.

Requirements:
R 301 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.

Procedure 1:
1. Allocate a network address as described in dhcp.server.AllocateAddress
2. Release the allocated address
3. Allocate all available network addresses
4. Check if the address allocated in step 1 was distributed again

Procedure 2:
1. Allocate a network address as described in dhcp.server.AllocateAddress
2. Release the allocated address
3. Let a second DHCP client request the released address
4. Verify that the server offered that address

6.3.1.14 Allocating an already used IP address

6.3.1.14.1 Test: dhcp.server.AllocateAddressPingReply

Test description:
Test if the server doesn't allocate an address that is already being used, without the server knowing it. The server sends an ICMP echo request to verify this, if an ICMP echo reply is received the server should abandon this address and offer different one.

Requirements:
R 265 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).

Procedure:
1. Send a DHCPDISCOVER message
2. Wait for an ICMP echo request
3. Send an ICMP echo reply
4. Wait for a DHCPOFFER message, retransmit DHCPDISCOVER when needed
5. Send a DHCPREQUEST message
6. Wait for a DHCPACK message
7. Verify that the server didn't give the IP that we have sent an ICMP reply for

6.3.1.14.2 Test: dhcp.server.DeclineAddress

Test description:
Test if the server marks a declined address as not available and returns another address to the client.

Requirements:
R 300 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.

Procedure:
1. Send a DHCPDISCOVER message
2. Wait for a DHCPOFFER message
3. Send a DHCPREQUEST message (is this step really needed, is it not possible that the client already detected that the address is in use ?)
4. Wait for a DHCPACK message
5. Send a DHCPDECLINE message
6. Send a new DHCPDISCOVER message
7. Wait for a new DHCPOFFER message and verify that a new address is being offered
8. Send a DHCPREQUEST message
9. Wait for a DHCPACK message

6.3.1.15 Multiple clients or servers

6.3.1.15.1 Test: dhcp.server.OptimizedOffer

Test description:
Test if the server tries to avoid reusing offered network addresses to another client when multiple clients request a new network address.

Requirements:
R 266 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.

Procedure:
1. Send a number of DHCPDISCOVER messages from different clients
2. Wait for the DHCPOFFER message sent in response to the DHCPDISCOVER messages and verify that they doesn't reuse available network addresses before all have been offered.
3. Measure how long it takes before the server starts reoffering available network addresses.

6.3.1.15.2 Test: dhcp.server.MultipleServers

Test description:
Verify that the server only sends DHCPOFFERS when it has been selected by the client in the DHCPREQUEST message.

Requirements:
R 211 The client extracts the server address from the 'server identifier' option in the selected DHCPOFFER message.
R 289 Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer.

Procedure:
1. Send a DHCPDISCOVER message
2. Wait for a DHCPOFFER message

3. Send a DHCPREQUEST message with a ‘Server identifier’ option different from the received DHCPOFFER message and an ‘requested IP address’ option with a different IP address then the one offered in the DHCPOFFER message
4. Verify that the server does not send a DHCPACK message
5. Send a DHCPDISCOVER message requesting the IP address offered in the previous received DHCPOFFER message
6. Wait for a DHCPOFFER message
7. Send a DHCPREQUEST message
8. Wait for a DHCPACK message and verify that server id still matches the one from the first DHCPOFFER message and that the IP address matches the one requested

6.3.1.16 Other tests

6.3.1.16.1 Test: dhcp.server.RelayAgent

Test description:
Test if the DHCP server is able to work together with a DHCP Relay Agent.

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 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 DHCPACK messages to the address in ‘ciaddr’.

Procedure:
1. Send a DHCPDISCOVER message with ‘giaddr’, ‘hops’, source hardware address and source IP set accordingly to a relayed DHCP message
2. Wait for a valid unicasted DHCPOFFER message to the DHCP Relay Agent
3. Send a DHCPREQUEST message as if it was relayed through a DHCP Relay Agent
4. Wait for a valid unicasted DHCPACK message to the DHCP Relay Agent
5. Wait until the renewal timer expires
6. Send a DHCPREQUEST message directly to the DHCP server (not relayed !)
7. Wait for a DHCPACK message unicasted to the DHCP client (not relayed !)

6.3.1.16.2 Test: dhcp.server.Inform

Test description:
Test if the DHCP server responds to DHCPINFORM messages.

Requirements:
R 302 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 303 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.

Procedure:
1. Send DHCPINFORM message with a 'Parameter Request List' option.
2. Wait for a DHCPACK message and check if the requested options are included.

6.3.1.17 Invalid DHCP messages

6.3.1.17.1 Test: dhcp.server.CorruptedDiscover

Test description:
Test if the DHCP server silently ignores corrupted DHCPDISCOVER messages.

Requirements:
R 2 Corrupted DHCP messages (e.g. invalid IP checksum or invalidUDP checksum) MUST be ignored.

Procedure:
1. Send a corrupted DHCPDISCOVER message
2. Verify that the server doesn't send a DHCPOFFER message

6.3.1.17.2 Test: dhcp.server.CorruptedRequest

Test description:
Test if the DHCP server silently ignored corrupted DHCPREQUEST messages.

Requirements:
R 2 Corrupted DHCP messages (e.g. invalid IP checksum or invalidUDP checksum) MUST be ignored.

Procedure:
1. Send a DHCPDISCOVER message
2. Wait for a DHCPOFFER message
3. Send a corrupted DHCPREQUEST message
4. Verify that the server doesn't respond with a DHCPACK message
5. Retransmit the DHCPREQUEST message (not corrupted)
6. Verify that the server sends a DHCPACK message

6.3.1.18 Option tests

6.3.1.18.1 Test: dhcp.server.OptionClientIdentifier

Test description:
Test if the server uses the Client Identifier option to identify a client when present, and not the hardware address.

Requirements:
R 262 If present the server MUST use the 'client identifier' to identify the client.
R 272 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.

Procedure:
1. Allocate a network address as described in dhcp.server.AllocateAddress with hardware address 1 and a Client Identifier option included
2. Wait for the lease to expire
3. Allocate another network address as described with hardware address 2 but with the same Client Identifier
4. Check if the IP address is the same as the one offered in step 1

6.3.1.18.2 Test: dhcp.server.OptionRelayAgentInformation

Test description:
Test if the server echoes the content of the Relay Agent Information option in every reply.

Requirements:
R 345 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.

Note: What happens when a Relay Agent Information was included in the DHCPDISCOVER message and not in the DHCPREQUEST message? The server shouldn't echo the Relay Agent Information option from the DHCPDISCOVER message.

Procedure:
1. Send a DHCPDISCOVER message with as last option the Relay Agent Information option.
2. Wait it for a DHCPOFFER message and verify that the server echoed the Relay Agent Information option.
3. Send a DHCPREQUEST message including the same Relay Agent Information option.
4. Wait for a DHCPACK message and verify that the server echoed the Relay Agent Information option.

6.3.1.18.3 Test: dhcp.server.OptionRenewalRebindingLeaseTime

Test description:
Test if the server implemented the renewal time, rebinding time and IP address lease time options. Check alse that the renewal time is shorter then the rebinding time and that the rebinding time is shorter than lease time.

Requirements:
R 309, R 315, R 316
R 236 T1 MUST be earlier than T2, which, in turn, MUST be earlier than the time at which the client's lease will expire.

Procedure:
1. Send a DHCPDISCOVER message requesting a renewal time option, a rebinding time option and an IP Address Lease Time option.
2. Wait for a DHCPOFFER message.
3. Verify that three requested options are included and the renewal time is shorter than the rebinding time which on its turn must be shorter than the lease time.

6.3.1.18.4 Test: dhcp.server.OptionConcatenation

Test description:
Test if server concatenates DHCP options of the same type and treats it as a single DHCP option. We split the 'Requested IP Address' option and check if the server offers the correct IP address.

Requirements:
R 16 When more than one option with a given type code appears in the DHCP packet, all such options should be concatenated in sequential order. It MUST treat the contents of that option as a single option. Although this feature is primarily used to send options that are longer than 255 bytes, splitting options that are shorter than 255 MAY also may done if deemed necessary. [RFC 3396]

Procedure:
1. Send a DHCPDISCOVER message with and 'Requested IP address' option split into multiple parts.
2. Wait for a DHCPOFFER message and verify that the offered IP address matches the requested IP address.
3. Send a DHCPREQUEST message.
4. Wait for a DHCPACK message.

6.3.1.18.5 Test: dhcp.server.OptionPad

Test description:
Test if the server skips padding options.

Requirements:
R 306

Procedure:
1. Send a DHCPDISCOVER message with padding options before the 'Requested IP address' option.
2. Wait for a DHCPOFFER message and verify that the offered IP address matches the requested IP address.
3. Send a DHCPREQUEST message.
4. Wait for a DHCPACK message.

6.4 VLAN test methods

6.4.1 Test: upstreamvlan

Purpose:
Traffic to be forwarded in the upstream direction is classified depending on the destination subnet. The modem will set a VLAN tag or forward frames untagged according to the class it is part of. In total three classes are considered: subnet A is forwarded on VLAN1, subnet B is forwarded on VLAN2 and subnet C is forwarded untagged.

Test Setup:
Modem configuration with an Ethernet upstream (ETHoDSL or ETHoATM) interface and configured to behave as described above. The DSLAM forwards tagged traffic unchanged to the test suite and encapsulates untagged traffic in a third VLAN.

Procedure:
For every subnet a TCP connection is generated in the upstream direction, its destination address is chosen to be in the range of the subnet. Verify that the TCP connection is forwarded on the correct VLAN at the upstream interface of the DSLAM.

6.4.2 Test: vlantransparant

Purpose:
Test if the modem is able to forward vlan tagged traffic to the upstream interface, regardless of the vlan id set on the downstream interface.

Test Setup:
The DSLAM is configured in a VLAN-stacking mode. The DSLAM bundles the VLANs on the DSL line in a Service-VLAN and forwards it to the test suite. The test suite can verify the VLAN ID of the frames on the DSL line by looking at the C-VLAN ID.

Procedure:
Generate UDP packets tagged with in random VLAN IDs and send them in the upstream direction on one of the downstream interfaces of the modem. Verify that they are forwarded, and that the C-VLAN is set according to the VLAN-ID.

7 MANAGEMENT TESTING

7.1 Introduction

Chapter 7 is written as continuity of MUSE-II – Deliverable M TF4.4 – Management Testing Objectives document: it identifies Test Steps for all the Test Objectives previously reported on the referred document, as illustrated in Figure 7-1.

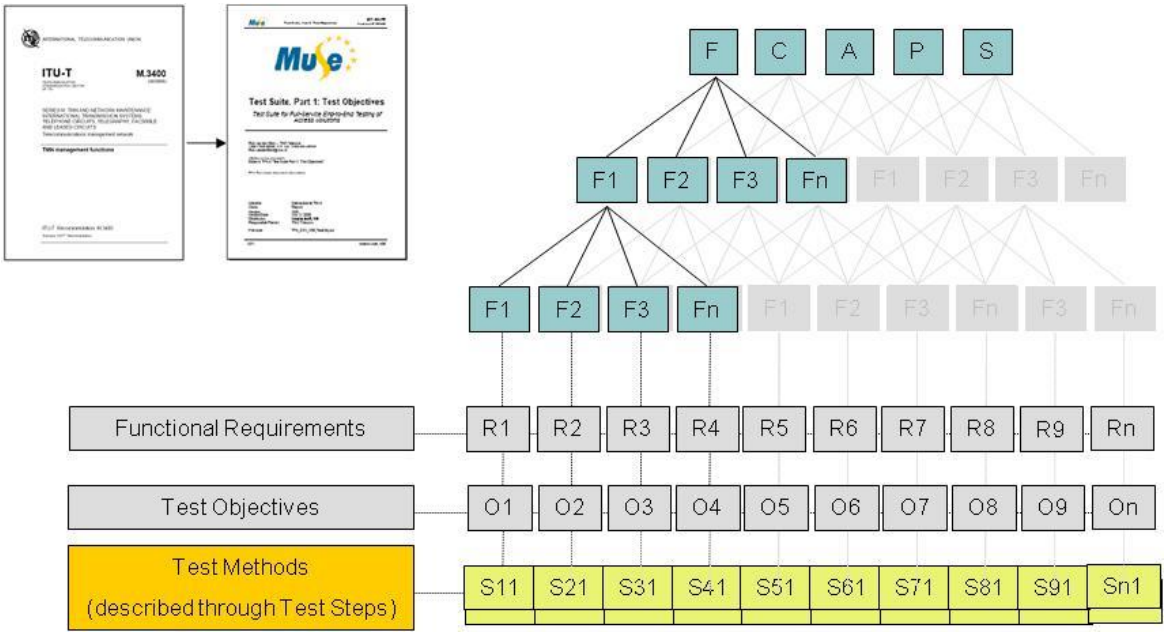


Figure 7-1: Management Testing Framework

Deliverable M TF4.4 started from the TMN management functions described in ITU-T M.3400, obtaining an exhaustive list of all TMN management requirements (functional requirements). It also defined the test objectives that were implicit on each requirement evaluation. Now, it is time to describe the management testing methods, taking into account the following goals:

1. Assure Management Tests validation according to TMN M.3400 model;
2. Provide a generic framework, applicable to all MUSE Sub-Projects;
3. Allow a rapid management tests setup implementation for all practical cases.

As a framework, it was not possible do drill down into specific details without running the risk of losing its aimed generic objectivity, however, an effort was made in order to make easier the future approaches of these test steps to practical cases, where these management testing methods may be used as guidelines.

7.2 Test methodes for Muse Management tests

7.2.1 Test Methods for Fault Management

FM.01.01: Requirement Name: Network RAS goal setting function set
Requirement Description: ITU-T M.3400 – Section 6.1.1

Test Steps:
1. Identify all the possible network outage events;
2. Test and certify that support of access to quantitative goals that are set for the frequency and duration of network outages over a specified period of time, is assured.

FM.01.02: Requirement Name: Service availability goal setting function set
Requirement Description: ITU-T M.3400 – Section 6.1.2

Test Steps:
1. Identify all the possible service outage events;
2. Test and certify that support of access to quantitative goals that are set for the frequency and duration of network outages over a specified period of time, is assured.

FM.01.03: Requirement Name: RAS assessment function set
Requirement Description: ITU-T M.3400 – Section 6.1.3

Test Steps:
1. Test and certify that agent reports network outage to manager;
2. Test and certify that agent reports service outage to manager;
3. Test and certify that manager requests agent to send network outage summary reports, and the agent responds with the requested information;
4. Test and certify that manager requests agent to send service outage summary reports, and the 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 Steps:
1. Test and certify that support of access to a database of outage reports concerning an outage of services to multiple customers is assured; (the report may include the type of services affected, the number of customers affected, and the start and end times of the outage);
2. Test and certify that 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 Steps:
1. Test and certify that support of access to a database of outage reports concerning an outage of a network, or a major part of a network, is assured;
2. Test and certify that 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 Steps:

1. Test and certify that 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 is assured. (this type of report is created after outage has occurred and may be updated during and after the outage has been corrected);
2. Test and certify that the final report includes 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: Alarm Surveillance includes Alarm policy function set
Requirement Description: ITU-T M.3400 – Section 6.2.1

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that 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, is supported.

FM.02.01: Requirement: Alarm Surveillance includes Network fault event analysis, including correlation and filtering function set
Requirement Description: ITU-T M.3400 – Section 6.2.2

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that 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, is supported.

FM.02.03: Requirement Name: Alarm Surveillance includes Alarm status modification function set
Requirement Description: ITU-T M.3400 – Section 6.2.3

Test Steps:

1. Test and certify that 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 is assured. (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 Steps:

1. Test and certify that agent notifies manager of alarm information upon the occurrence of an alarm;

2. Test and certify that manager specifies to the agent the destination address(es) for a specified set of alarm reports;
3. Test and certify that 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. Test Condition Alarm function set.

FM.02.05: Requirement Name: Alarm Surveillance includes Alarm summary function set
Requirement Description: ITU-T M.3400 – Section 6.2.5

Test Steps:

1. Test and certify that agent provides manager (based on a predefined schedule) with a current alarm summary;
2. Test and certify that manager specifies to the agent the destination address(es) for a specified set of current alarm summaries;
3. Test and certify that 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. Test and certify that 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. Test and certify that manager requests agent to send the current schedule information for Current Alarm Summary reporting; agent responds with the schedule information;
6. Test and certify that manager instructs the agent to allow/inhibit reporting of the scheduled current alarm summaries;
7. Test and certify that 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 Steps:

1. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that manager instructs the agent to allow/inhibit logging of log records;
2. Test and certify that manager instructs the agent to assign log attributes as specified by the manager;
3. Test and certify that 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 Steps:

1. Test and certify that agent provides manager with event's unique identity;
2. Test and certify that manager requests agent to select specific event(s) from a general stream of events;
3. Test and certify that 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. Test and certify that manager requests agent to suppress redundant events, but count those events;
5. Test and certify that manager request agent to suppress all events which are implied by root cause event, but enhance information in root cause event;
6. Test and certify that manager requests agent to evaluate significance of event based on one or more other events which are generated and delivered independently;
7. Test and certify that 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. Test and certify that manager requests agent to correlate events based on environmental conditions such as business rules, time of day, configuration values, affecting event significance;
9. Test and certify that manager requests agent to correlate events based on information stored externally;
10. Test and certify that manager requests agent to initiate an action to be taken based on event information;
11. Test and certify that 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. Test and certify that manager receives alarm and other events from agent;
13. Test and certify that manager receives root cause notification from agent;
14. Test and certify that 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 Steps:

1. Test and certify that 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, is assured.

FM.03.01: Requirement Name: Fault localization policy function set
Requirement Description: ITU-T M.3400 – Section 6.3.1

Test Steps:

1. Test and certify that 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 is assured;
2. Test and certify that access availability to parameters of the procedures for escalation if a trouble is not resolved in an allowed time period, is assured.

FM.03.02: Requirement Name: Verification of parameters and connectivity function set
Requirement Description: ITU-T M.3400 – Section 6.3.2

Test Steps:

1. Test and certify that 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, is assured.

FM.03.03: Requirement Name: Network fault localization function set
Requirement Description: ITU-T M.3400 – Section 6.3.3

Test Steps:

1. Test and certify that support of requests for notifications that a root cause of a fault has been found, is assured. (a trouble ticket may be created in databases of other functions);
2. Test and certify that agent sends the alarm to manager;
3. Test and certify that agent sends the message to manager;
4. Test and certify that agent reports the real-time status to manager;
5. Test and certify that agent sends the vendors status to manager;
6. Test and certify that manager directs agent to report the result of automatic or manual testing routines;
7. Test and certify that manager directs agent to open/close trouble ticket;
8. Test and certify that manager directs agent to consolidate with tickets related;
9. Test and certify that manager directs agent to cancel/clear trouble ticket;
10. Test and certify that manager directs agent to update trouble status;
11. Test and certify that manager directs agent to create historical record;
12. Test and certify that manager directs agent to send trouble ticket to proper vendors;
13. Test and certify that manager directs agent to choose the proper procedure for determination process;
14. Test and certify that manager directs agent to select procedure alternative;
15. Test and certify that manager directs agent to perform back-up procedure;
16. Test and certify that manager directs to agent to breakdown diagnostic process;
17. Test and certify that manager directs agent to select problem for diagnostic process based on priorities;

18. Test and certify that manager directs agent to suspend diagnostic due to priorities;
19. Test and certify that manager directs agent to suspend diagnostic due to priorities;
20. Test and certify that manager directs agent to stop diagnostic since the problem has disappeared, and no further diagnosis is required;
21. Test and certify that manager directs agent to set up timer for monitoring whether a diagnostic process completes in an assigned time;
22. Test and certify that manager directs agent to review trouble database;
23. Test and certify that manager directs agent to develop hypothesis in a special condition;
24. Test and certify that manager directs agent to provide detailed information for further analysis;
25. Test and certify that manager directs agent to perform a loop test;
26. Test and certify that manager directs agent to send message to customer about outage;
27. Test and certify that 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 Steps:

1. Test and certify that manager requests agent to send the results of a diagnostic sequence;
2. Test and certify that manager directs the agent to stop a particular diagnostic procedure in progress;
3. Test and certify that 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. Test and certify that manager directs agent to establish a routine schedule for the initiation of a diagnosis;
5. Test and certify that manager requests agent to report the current schedule of diagnosis.;
6. Test and certify that agent sends the current schedule of diagnosis;
7. Test and certify that manager requests agent to send the results of a particular exercise;
8. Test and certify that agent sends the results of an exercise to manager;
9. Test and certify that manager directs agent to stop a particular exercise in progress;
10. Test and certify that manager directs agent to establish a routine schedule for the initiation of an exercise;
11. Test and certify that manager directs agent to send the current schedule of an exercise. Agent responds with the schedule;
12. Test and certify that manager directs agent to establish or release a specific loopback. It may be activated either remotely by manager or by local action;
13. Test and certify that manager directs agent to connect a termination on agent to another termination by a specified path within agent, then test the path;
14. Test and certify that manager directs agent to hold a particular network path;
15. Test and certify that manager directs agent to start or stop a specific program trap;
16. Test and certify that agent automatically reports to manager the occurrence of a program trap;
17. Test and certify that manager directs agent to start or stop a specific trace;
18. Test and certify that agent automatically reports to manager the results of a trace;
19. Test and certify that manager directs agent to start or stop an audit;
20. Test and certify that agent automatically reports to manager the results of an audit;

21. Test and certify that manager directs agent to establish a specified schedule for a given audit;
22. Test and certify that manager requests agent to send the current audit schedule. Agent responds with the test schedule;
23. Test and certify that manager directs agent to schedule a loop insulation test;
24. Test and certify that manager directs agent to start or stop a loop insulation test;
25. Test and certify that manager requests agent to send a current loop insulation test schedule. Agent responds with the schedule;
26. Test schedule routine tests management function;
27. Test start/stop routine tests management function;
28. Test report routine test schedule management function.

FM.03.05: Requirement Name: Running of diagnostic function set
Requirement Description: ITU-T M.3400 – Section 6.3.5

Test Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that manager directs agent to establish or change the administrative domain of a work centre or system;
2. Test and certify that manager directs agent to send an administrative domain. Agent responds with the requested information;
3. Test and certify that manager directs agent to establish or change the training requirements for classes of repair activities;
4. Test and certify that manager directs agent to send training requirements for classes of repair activities. Agent responds with the requested information;
5. Test and certify that manager requests agent to send report of work force information for current or previous interval. Agent responds with the requested information;
6. Test and certify that manager requests agent to send report of work flow for current or previous interval. Agent responds with the requested information;
7. Test and certify that manager requests agent to send report of scheduling statistics for current or previous interval. Agent responds with the requested information;
8. Test and certify that 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 Steps:

1. Test and certify that processes to support customer contact, in order to schedule dispatch to customer premises, are assured.

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 Steps:

1. Test and certify that processes to support the creation of a work order, which may support repair, network growth or service activation, are assured.

FM.04.04: Requirement Name: NE(s) fault correction function set
Requirement Description: ITU-T M.3400 – Section 6.4.4

Test Steps:

1. Test and certify that 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. Test and certify that 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. Test and certify that manager requests agent to reconstruct a service or a single system (main or standby) from a specified dump record;
4. Test and certify that 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 Steps:

1. Test and certify that 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, is assured.
2. Test and certify that inhibition and override of automatic restoration functionality, is assured.

FM.05.01: Requirement Name: Test point policy function set
Requirement Description: ITU-T M.3400 – Section 6.5.1

Test Steps:

1. Test and certify that support of administers tables that define the conditions for providing test access at various points along a circuit, is assured.

FM.05.02: Requirement Name: Service test function set
Requirement Description: ITU-T M.3400 – Section 6.5.2

Test Steps:

1. Test and certify that manager requests agent to test a service to ensure that it is available for operation;
2. Test and certify that 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 Steps:

1. Test and certify that support of requests for tests of an end-to-end circuit and supports the return of test results, is assured.

FM.05.04: Requirement Name: Selection of test suite function set
Requirement Description: ITU-T M.3400 – Section 6.5.4

Test Steps:

1. Test and certify that support of requests for a specific part of a circuit to be tested and also supports the return of results, is assured.

FM.05.05: Requirement Name: Test access network control and recovery function set
Requirement Description: ITU-T M.3400 – Section 6.5.5

Test Steps:

1. Test and certify that agent reports initialization of test system to manager;
2. Test and certify that agent reports initialization of test access system to manager;
3. Test and certify that 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 Steps:

1. Test and certify that when in 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. Test and certify that 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. Test and certify that when in 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 Steps:

1. Test and certify that 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. Test and certify that manager directs agent to execute reversal of tip and ring leads of metallic transmission pair(s) on the circuit under test;
3. Test and certify that manager directs agent to change T&L status of the circuit under test and report the resulting T&L state to the manager;
4. Test and certify that manager directs agent to report the T&L status of the circuit under test;
5. Test and certify that manager directs agent to perform various control functions such as block, select, unselect, and release, on the Multipoint Junction Unit in the circuit;

6. Test and certify that 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 Steps:

1. Test and certify that manager directs agent to connect a test signal generator, and to change or remove a test signal on the circuit under test;
2. Test and certify that manager directs agent to measure analogue transmission characteristics including: tone, noise, impulse noise, intermodular distortion, phase jitter, transients, and peak-to-average ratios;
3. Test and certify that manager directs agent to measure multimeter characteristics including: alternating and direct current voltage, resistance, alternating and direct current, and capacitance;
4. Test and certify that manager directs the agent to perform and report supervision in both directions for alternating and direct current signalling;
5. Test and certify that 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. Test and certify that manager listens selectively to the circuit under test and monitors any transmission pair in either direction;
7. Test and certify that manager directs agent to change the level of the monitor connection;
8. Test and certify that manager directs agent to remove or insert the single frequency notch filter placed in the monitor connection;
9. Test and certify that manager establishes digital data monitor test access and determines the presence of network control codes or customer data;
10. Test and certify that manager directs agent to provide a loopback on the circuit under test and perform a digital loopback test;
11. Test and certify that 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. Test and certify that 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. Test and certify that 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. Test and certify that manager requests agent to simulate a specified failure and mark ensuing actions as dummies;
15. Test and certify that manager requests agent to change the test signal to the DS1, E1 or T1 under tests;
16. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that manager requests agent to report intermediate or final results from a measurement;
2. Test and certify that agent sends the results of a test to the manager;
3. Test and certify that manager directs agent to send the state of the facility carrying the circuit under test;
4. Test and certify that 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 Steps:

1. Test and certify that 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. Test and certify that the integrity of the metallic TAP provided by the "Establish" function is tested and calibrated from the test system;
3. Test and certify that manager directs agent to remove a TAP(s) from service;
4. Test and certify that manager directs agent to restore a TAP(s) into service;
5. Test and certify that 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 Steps:

1. Test and certify that requests for test access to a path or circuit supported by an NE is supported; (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 Steps:

1. Test and certify that access availability to rules for verification and testing and for assigning a trouble to a dispatch administration agent is assured. (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 Steps:

1. Test entering a trouble report: a customer may request that a customer trouble report be created with the appropriate information;
2. Test adding 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. Test cancelling 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. Test modifying trouble information: a service customer may request that information in an existing trouble report be modified;
5. Test enrolling trouble report format definition: a notification of a new trouble report format is sent to a service customer;
6. Test deenrolling trouble report format definition: a notification of the deletion of a trouble report format is sent to a service customer;
7. Test modifying 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 Steps:

1. Test the 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 Steps:

1. Test requesting trouble status: a customer may request status information on an open or closed customer trouble report;
2. Test reviewing trouble history: a customer may request information about past troubles reported for a particular service or circuit;
3. Test requesting 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 Steps:

1. Test and certify that 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, is notified.
2. Test and certify that 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, is notified.

FM.06.06: Requirement Name: Trouble ticket administration function set
Requirement Description: ITU-T M.3400 – Section 6.6.6

Test Steps:

1. Test and certify that 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), is assured;
2. Test and certify that tracking reports are provided for 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 Steps:

1. Test and certify that agent (the S-OSF that supports this function set) provides access to manager to read records of outgoing trouble reports;
2. Test and certify that agent (the S-OSF that supports this function set) provides access to manager to update outgoing trouble records.

7.2.2 Test Methods for Configuration Management

CM.01.01: Requirement Name: Product line budget function set
Requirement Description: ITU-T M.3400 – Section 7.1.1

Test Steps:

1. Test and certify that 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, is assured.

CM.01.02: Requirement Name: Supplier and technology policy function set
Requirement Description: ITU-T M.3400 – Section 7.1.2

Test Steps:

1. Test and certify that 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., is assured. (generally, the guidelines consist of rules for definition of specifications and restrictions such as maximum capacity of a unit);
2. Test and certify that access to data concerning guidelines for qualified suppliers based on product offering, price, features, capability limits of products, operations support, availability, etc., is provided.

CM.01.03: Requirement Name: Area boundary definition function set
Requirement Description: ITU-T M.3400 – Section 7.1.3

Test Steps:

1. Test and certify that manager requests agent to send area boundary definition. Agent responds with requested information;
2. Test and certify that 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 Steps:

1. Test and certify that 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., is assured.

CM.01.05: Requirement Name: Management of planning and engineering process function set
Requirement Description: ITU-T M.3400 – Section 7.1.5

Test Steps:

1. Test and certify that access availability to information about planning tools, and development of planning and engineering methods and procedures, is assured.
2. Test and certify that access to information about the status, costs and schedules of planning and engineering jobs in progress, is provided.

CM.01.06: Requirement Name: Demand forecasting function set
Requirement Description: ITU-T M.3400 – Section 7.1.6

Test Steps:

1. Test and certify that manager requests agent to send a demand forecast for specified services. Agent responds with requested information;
2. Test and certify that manager requests agent to report statistical demand information on services of service customers. Agent responds with the requested information;
3. Test and certify that manager requests agent to report demand information concerning a specific (large) service customer. Agent responds with requested information;
4. Test and certify that 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 Steps:

1. Test and certify that 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, is assured.
2. Test and certify that actions to carry out the design, are supported.

CM.01.08: Requirement Name: Access infrastructure design function set
Requirement Description: ITU-T M.3400 – Section 7.1.8

Test Steps:

1. Test and certify that support of requests to design access circuits, based on customer location, and the requested service features and route, is assured;
2. Test and certify that actions to carry out the design, are supported.

CM.01.09: Requirement Name: Facility infrastructure design function set
Requirement Description: ITU-T M.3400 – Section 7.1.9

Test Steps:

1. Test and certify that support of requests to design facilities based on the location of nodes, product line budget, requested service features, route, and demand forecasts, is assured.
2. Test and certify that actions to carry out the design, are supported.

CM.01.10: Requirement Name: Routing design function set
Requirement Description: ITU-T M.3400 – Section 7.1.10

Test Steps:

1. Test and certify that 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, is assured.
2. Test and certify that responses that contain the proposed route, are supported.

CM.01.11: Requirement Name: NE(s) design function set
Requirement Description: ITU-T M.3400 – Section 7.1.11

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that access to guidelines for technology policy, supplier policy and product line budget, are provided;
3. Test and certify that actions to carry out the design, are supported;
4. Test and certify that access to information about the NE design, is provided;
5. Test and certify that requests to design a group of NE(s), including their transmission media interconnections, are supported.

CM.02.01: Requirement Name: Procurement function set
Requirement Description: ITU-T M.3400 – Section 7.2.1

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that guidelines from Supplier policy, technology policy, etc., are used.

CM.02.02: Requirement Name: Management of installation function set
Requirement Description: ITU-T M.3400 – Section 7.2.2

Test Steps:

1. Test and certify that support of access to information that can be used to monitor the installation process and the deliver of materials and coordinate contractors, is assured.

CM.02.03: Requirement Name: Contracting function set
Requirement Description: ITU-T M.3400 – Section 7.2.3

Test Steps:

1. Test and certify that support of requests for and provides access to status and other information concerning contracting services for installation, is assured;

2. Test and certify that management of the bidding process, contractor(s) selection, negotiation of job schedule and any special circumstances such as environmental concerns, job access restrictions, etc., is supported.

CM.02.04: Requirement Name: Real estate management function set
Requirement Description: ITU-T M.3400 – Section 7.2.4

Test Steps:

1. Test and certify that support of access to information about status, changes, additions or removal of property, buildings, other structures, parking facilities, etc., is assured;
2. Test and certify that access to information concerning the usage of space in buildings, is provided;
3. Test and certify that access to information about maintenance associated with the real estate, is provided.

CM.02.05: Requirement Name: Arrangement of installation with customer function set
Requirement Description: ITU-T M.3400 – Section 7.2.5

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that access responses with the agreed schedule, is supported.

CM.02.06: Requirement Name: Network installation administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.6

Test Steps:

1. Test and certify that support of access to information about the coordination of hardware and software for new installations, upgrades, and maintenance changes across the network, is assured.

CM.02.07: Requirement Name: Material management function set
Requirement Description: ITU-T M.3400 – Section 7.2.7

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that electronic ordering, shipping and receipt of software, is supported.

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 Steps:

1. Test and certify that 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, is assured;
2. Test and certify that actions to dispatch the installation force are supported;

3. Test and certify that access to the schedule and status of the work is provided;
4. Test and certify that jeopardy reports are supported.

CM.02.09: Requirement Name: Installation completion reporting function set
Requirement Description: ITU-T M.3400 – Section 7.2.9

Test Steps:

1. Test and certify that support of access to information about job status and supports notification of completion after acceptance testing as required, is assured;
2. Test and certify that notification of failure to meet successful completion criteria, with the reason for unsuccessful completion, is supported;
3. Test and certify that summary and exception reports for the management of installation jobs are supported.

CM.02.10: Requirement Name: Software administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.10

Test Steps:

1. Test and certify that support for the acceptance of generic programs from suppliers (generic programs include applications, operating systems or middleware) is assured;
2. Test and certify that administration of the versions of generic programs is supported.

CM.02.11: Requirement Name: NE installation administration function set
Requirement Description: ITU-T M.3400 – Section 7.2.11

Test Steps:

1. Test and certify that 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, is assured.

CM.02.12: Requirement Name: Loading software into NEs function set
Requirement Description: ITU-T M.3400 – Section 7.2.12

Test Steps:

1. Test and certify that support for download of software to be stored in an NE is assured. (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 Steps:

1. Test and certify that support of access to a plan for service offerings on a generic basis for a wide range of customers, is assured;
2. Test and certify that ongoing administration of those service offerings is allowed.

CM.03.02: Requirement Name: Service feature definition function set
Requirement Description: ITU-T M.3400 – Section 7.3.2

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that ongoing administration of those service offerings is allowed.

CM.03.03: Requirement Name: Marketing function set
Requirement Description: ITU-T M.3400 – Section 7.3.3

Test Steps:

1. Test and certify that support of access to information about marketing methods, procedures and trained personnel to contact customers about service offerings to meet their business needs, is assured;
2. Test and certify that requests to gather and summarize information indicating existent, latent or potential needs of new or enhanced telecommunication services, is supported;
3. Test and certify that reports on such topics are supported.

CM.03.04: Requirement Name: Management of sales process function set
Requirement Description: ITU-T M.3400 – Section 7.3.4

Test Steps:

1. Test and certify that support of access to information about sales skills, methods, procedures, trained personnel and automated tools to facilitate the selling of services to customers, is assured;
2. Test and certify that 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, is provided.

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 Steps:

1. Test and certify that support of information about the status of negotiations and other interactions with stock holders, general public, regulators and other government agencies, is assured;
2. Test and certify that 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, is supported.

CM.03.06: Requirement Name: Customer identification function set
Requirement Description: ITU-T M.3400 – Section 7.3.6

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that updates of the customer database as appropriate are supported.

CM.03.07: Requirement Name: Customer need identification function set
Requirement Description: ITU-T M.3400 – Section 7.3.7

Test Steps:

1. Test and certify that 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, is assured.

CM.03.08: Requirement Name: Customer service planning function set
Requirement Description: ITU-T M.3400 – Section 7.3.8

Test Steps:

1. Test and certify that 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; is assured;
2. Test and certify that ongoing administration of those service offerings is allowed.

CM.03.09: Requirement Name: Customer service feature definition function set
Requirement Description: ITU-T M.3400 – Section 7.3.9

Test Steps:

1. Test event reporting control management function, where customer's OSF selects and controls the flow of notifications from the provider's OSF;
2. Test customize configuration management function, where customer's OSF requests the provider's OSF to customize the configuration of service resources provided to customer;
3. Test Log control management function, where 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 Steps:

1. Test and certify that 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, is assured;
2. Test and certify that service feature conflicts are identified and resolved during the development of the solution proposal;
3. Test and certify that interactions with the customer to present the proposal are supported.

CM.04.01: Requirement Name: Provisioning policy function set
Requirement Description: ITU-T M.3400 – Section 7.4.1

Test Steps:

1. Test and certify that manager requests agent to send route determination guidelines (determination of economic route, route redundancy, etc.). Agent responds with requested information;
2. Test and certify that 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 Steps:

1. Test and certify that support of access to guidelines for the selection and use of materials is assured.

CM.04.03: Requirement Name: Access route determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.3

Test Steps:

1. Test and certify that support of requests for an access route for a specific service type is assured.
2. Test and certify that responses that state an economic route from the customer point of presence to an appropriate transport network or switch, are supported.

CM.04.04: Requirement Name: Directory address determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.4

Test Steps:

1. Test and certify that support of requests for a directory address is assured.
2. Test and certify that responses that state a telephone number or other network address are supported.

CM.04.05: Requirement Name: Leased circuit route determination function set
Requirement Description: ITU-T M.3400 – Section 7.4.5

Test Steps:

1. Test and certify that 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 Steps:

1. Test and certify that manager requests the creation of a telecommunications service by an agent;
2. Test and certify that manager requests the deletion of a telecommunications service by an agent;
3. Test and certify that manager requests the modification of a telecommunications service by an agent;
4. Test and certify that 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 Steps:

1. Test and certify that when a service resource is created, an indication of creation is sent to the manager by the agent;
2. Test and certify that when a service resource is deleted, an indication of deletion is sent to the manager by the agent;

3. Test and certify that when the configuration of a service resource is changed, an indication of configuration change is sent to the manager by the agent;
4. Test and certify that 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. Test and certify that manager requests agent to transmit information about a service resource to the manager;
6. Test and certify that manager requests agent to change the administrative state of a service resource;
7. Test and certify that agent reports progress of a telecommunications service request to a manager;
8. Test and certify that 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 Steps:

1. Test and certify that support of requests for network resources and responds with selected resources and the associated service features is assured;
2. Test and certify that access to a network resource database is provided;
3. Test and certify that requests for selection and assignment of resources and service features that meet any designated selection criteria are supported.

CM.04.09: Requirement Name: Interexchange circuit design function set
Requirement Description: ITU-T M.3400 – Section 7.4.9

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that responses stating the selected resources are supported.

CM.04.10: Requirement Name: Access circuit design function set
Requirement Description: ITU-T M.3400 – Section 7.4.10

Test Steps:

1. Test and certify that support of requests for access circuit design is assured.
2. Test and certify that responses that state the access points from the customer to the network are supported.

CM.04.11: Requirement Name: Leased circuit design function set
Requirement Description: ITU-T M.3400 – Section 7.4.11

Test Steps:

1. Test and certify that manager requests agent to configure dynamic links;
2. Test and certify that manager requests agent to reconfigure dynamic links;
3. Test and certify that manager requests agent to configure dynamic link endpoints;
4. Test and certify that manager requests agent to configure connections;
5. Test and certify that manager requests agent to reconfigure connections;
6. Test and certify that 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 Steps:

1. Test and certify that support of requests for facility design, along a specified route, is assured.
2. Test and certify that responses that state the selected resources are supported.

CM.04.13: Requirement Name: Manage pending network changes function set
Requirement Description: ITU-T M.3400 – Section 7.4.13

Test Steps:

1. Test and certify that 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, is assured.
2. Test and certify that actions to carry out the change are supported.
3. Test and certify that confirmation and jeopardy reports are supported;
4. Test and certify that confirmation of requests when all requested actions have been confirmed, are supported;
5. Test and certify that jeopardy reports, as appropriate, are supported.

CM.04.14: Requirement Name: Network connection management function set
Requirement Description: ITU-T M.3400 – Section 7.4.14

Test Steps:

1. Test and certify that support of requests for a particular set of cross-connections required for implementation of a circuit design, is assured;
2. Test and certify that actions to request the cross-connections to be established in NEs or groups of NEs are supported.

CM.04.15: Requirement Name: Circuit inventory notification function set
Requirement Description: ITU-T M.3400 – Section 7.4.15

Test Steps:

1. Test and certify that when a circuit resource is created, an indication of creation is sent to manager from agent;
2. Test and certify that when a circuit resource is deleted, an indication of deletion is sent to manager from agent;
3. Test and certify that when the configuration of a circuit resource is changed, an indication of configuration change is sent to manager from agent;
4. Test and certify that 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 Steps:

1. Test and certify that 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 Steps:

1. Test and certify that manager requests that the agent report the current configuration of each entity;
2. Test and certify that 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. Test and certify that manager notifies agent of the presence of a newly installed entity;
4. Test and certify that manager notifies agent of the disconnection of an entity;
5. Test and certify that manager notifies agent to begin monitoring the newly installed entity;
6. Test and certify that manager notifies agent that a previously unequipped entity is now equipped;
7. Test and certify that manager notifies agent that a previously equipped entity is no longer equipped;
8. Test and certify that 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. Test and certify that 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. Test and certify that agent reports the identity of each assigned channel for each equipped entity or for a specified entity;
11. Test and certify that manager directs agent to set parameters associated with a specified entity;
12. Test and certify that manager directs agent to set performance thresholds for the specified channel;
13. Test and certify that manager directs agent to insert or remove a channel from the complement of through-channels;
14. Test and certify that manager directs agent to interconnect two specified channels operating at the same rate;
15. Test and certify that manager directs agent to remove the interconnection between two specified channels;
16. Test and certify that manager directs agent to begin a transmission test on a given circuit;
17. Test and certify that manager directs agent to perform a balance test/adjustment;
18. Test and certify that manager directs agent to look for a transponder signal on the given circuit;
19. Test and certify that the manager directs agent to set or change report periods.
20. Test and certify that the manager requests agent to send the current periods to the manager;
21. Test and certify that manager requests agent to restart an equipment, service or the system. The restart may be soft or hard;
22. Test and certify that 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 Steps:

1. Test and certify that manager directs agent to set agent system clock to current calendar, date and time;

2. Test and certify that manager directs agent to make a backup copy of the designated agent database file for purposes of archiving for future restoration.
3. Test and certify that manager directs the agent to terminate a process between a manager and a agent;
4. Test and certify that manager directs agent to route automatic messages generated by agent to one or multiple communications channels;
5. Test and certify that 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 Steps:

1. Test and certify that 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. Test and certify that manager reconfigures the database within a agent while it is in service;
3. Test and certify that 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. Test and certify that manager reads agent for all or part of its database contents;
5. Test and certify that 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 Steps:

1. Test and certify that support of access to information concerning NE resources that are assigned to services or that are currently available for assignment is assured;
2. Test and certify that utilization levels of resources and sends notifications when utilization exceeds thresholds is monitored;
3. Test and certify that requests for utilization information are responded.

CM.04.21: Requirement Name: NE(s) resource selection and assignment function set
Requirement Description: ITU-T M.3400 – Section 7.4.21

Test Steps:

1. Test and certify that 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, is assured. (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 Steps:
1. Test and certify that 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, is assured;
2. Test and certify that resources to form the required connection are selected and bound.

CM.04.23: Requirement Name: Loading program for service feature(s) function set
Requirement Description: ITU-T M.3400 – Section 7.4.23

Test Steps:
1. Test and certify that 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, is assured;
2. Test and certify that loading includes 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 Steps:
1. Test and certify that support of notifications from an NE about changes in the features that the NE supports is assured.

CM.04.25: Requirement Name: NE(s) inventory query function set
Requirement Description: ITU-T M.3400 – Section 7.4.25

Test Steps:
1. Test and certify that 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, is assured.

CM.04.26: Requirement Name: Manage pending changes in NE(s) function set
Requirement Description: ITU-T M.3400 – Section 7.4.26

Test Steps:
1. Test and certify that 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, is assured;
2. Test and certify that notification of changes that result from differences between assigned and installed NE configurations, is supported.

CM.04.27: Requirement Name: Storage of parameters and cross-connects function set
Requirement Description: ITU-T M.3400 – Section 7.4.27

Test Steps:
1. Test and certify that support of access to NE information about its parameters and cross-connects is assured.

CM.04.28: Requirement Name: Storage and execution of service features
Requirement Description: ITU-T M.3400 – Section 7.4.28

Test Steps:

1. Test and certify that support of access to NE information about its service feature settings and the capabilities defined by those settings is assured.

CM.04.29: Requirement Name: Self-inventory function set
Requirement Description: ITU-T M.3400 – Section 7.4.29

Test Steps:

1. Test and certify that support of requests of information from an NE about its equipment configuration is assured.

CM.05.01: Requirement Name: Priority service policy function set
Requirement Description: ITU-T M.3400 – Section 7.5.1

Test Steps:

1. Test and certify that support of guidelines for determining which services have priority for restoration in the event of a catastrophic failure, is assured. (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 Steps:

1. Test and certify that support of notifications of an out-of-service status of services that are designated to have priority service features, is assured.
2. Test and certify that actions for restoration of such services, where such actions may usurp resources from lower priority services, based on designated priority service features, are supported. (for example, an emergency service would be designated as a priority service);
3. Test and certify that access to data concerning priority levels is supported.

CM.05.03: Requirement Name: Message handling systems network status function set
Requirement Description: ITU-T M.3400 – Section 7.5.3

Test Steps:

1. Test and certify that manager requests agent to transmit the message storage status data of store-and-forward communication to manager;
2. Test and certify that 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 Steps:

1. Test and certify that manager requests agent to transmit the status of dynamic provisioning to manager;
2. Test and certify that 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 Steps:

1. Test and certify that manager requests agent to transmit the switching activities and current status of automatic transmission restoration;
2. Test and certify that 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 Steps:

1. Test and certify that manager requests agent to send current status information;
2. Test and certify that agent reports to manager the value of a monitored parameter. It may be sent on demand by manager or on a scheduled basis;
3. Test and certify that manager directs agent to establish a schedule for the reporting of status information;
4. Test and certify that manager directs agent to send the current schedule of status reporting agent responds with the schedule;
5. Test and certify that manager sends agent timetable of when a specified service is to be available for use;
6. Test and certify that manager directs agent to allow or inhibit automatic restoration in an M+N or duplex system;
7. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that support of access to the current state of a resource is assured;
2. Test and certify that this information is available to queries and is also 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 Steps:

1. Test and certify that 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 is assured. (automatic notification of change of state may be initiated by the NE).

7.2.3 Test Methods for 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 Steps:

1. Test and certify that support of processes and systems to improve accurate and efficient usage measurement for products and services, is assured;
2. Test and certify that access to information concerning the metrics of the usage data stream is provided.

AM.01.02: Requirement Name: Management of the usage measurement process function set
Requirement Description: ITU-T M.3400 – Section 8.1.2

Test Steps:

1. Test and certify that support for the management of processes and systems to ensure accurate and efficient usage measurement for products and services, is assured;
2. Test and certify that management reports that may include total number of records, time criteria, lost records, multiple records, mutilate records, etc., is provided;
3. Test and certify that notifications as the reports are requested or defined, are supported.

AM.01.03: Requirement Name: Usage aggregation function set
Requirement Description: ITU-T M.3400 – Section 8.1.3

Test Steps:

1. Test and certify that support of access to summaries of service-level usage events by customer by service/product as described by specific carrier-defined criteria, is assured;

AM.01.04: Requirement Name: Service usage correlation function set
Requirement Description: ITU-T M.3400 – Section 8.1.4

Test Steps:

1. Test and certify that support to associate usage data based on provider-defined criteria related to a single product/service instance but possibly across multiple networks, is assured. (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 Steps:

1. Test and certify that 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, is assured;

AM.01.06: Requirement Name: Usage distribution function set
Requirement Description: ITU-T M.3400 – Section 8.1.6

Test Steps:

1. Test and certify that support to distribute (sends notification of) the billable and informational formatted usage data to one or more processes, as requested or defined, is assured. (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);

2. Test and certify that usage deletion functionality for usage information that will not continue in the data stream, is included.

AM.01.07: Requirement Name: Usage surveillance function set
Requirement Description: ITU-T M.3400 – Section 8.1.7

Test Steps:

1. Test and certify that support to monitor all usage data to detect deviation from established norms, is assured.
2. Test and certify that access to a database containing records of translation errors, general software errors, usage information recording errors, network routing errors, and potential fraud, is provided.

AM.01.08: Requirement Name: Usage error correction function set
Requirement Description: ITU-T M.3400 – Section 8.1.8

Test Steps:

1. Test and certify that support of access to usage data records after investigation and correction of usage data records found to be suspect or in error, is assured. (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 Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that definition of the set of usage measurement criteria to be applied to a usage event, is assured;
2. Test and certify that 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, is supported;
3. Test and certify that access to identification of customer account/configuration and identification of product/service, is provided.

AM.01.11: Requirement Name: Network usage correlation function set
Requirement Description: ITU-T M.3400 – Section 8.1.11

Test Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that support of access to usage data, records, errors, and reports for subsequent access by other functions or applications is assured. (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 Steps:

1. Test and certify that support of access to raw usage data, records, errors (e.g. translation, software, recording, network routing, etc.), and reports, is assured. (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 Steps:

1. Test and certify that support for collection of usage data is assured.

AM.01.15: Requirement Name: Usage validation function set
Requirement Description: ITU-T M.3400 – Section 8.1.15

Test Steps:

1. Test and certify that 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, is assured. (for example, checking each usage element to verify that a valid value has been recorded);
2. Test and certify that verification that usage data is collected from scheduled NE(s) in timely fashion, is supported; (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 Steps:

1. Test and certify that disposition determination of logged usage data, which should provide access to the data, and schedules reporting of bulk usage data, is assured.

AM.01.17: Requirement Name: Usage generation function set
Requirement Description: ITU-T M.3400 – Section 8.1.17

Test Steps:

1. Test and certify that manager directs agent to set parameters to a charging data collection process;
2. Test and certify that manager directs the agent to remove a charging data collection process;

3. Test and certify that manager directs the agent to start up a defined charging data collection process;
4. Test and certify that manager directs the agent to stop a defined charging data collection process;
5. Test and certify that manager requests the agent to report data of the defined and/or activated data collections;
6. Test and certify that manager directs the agent to change parameters in a charging data collection definition;
7. Test and certify that 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. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that support for management of data tables reflecting corporate strategies for the pricing of product lines, is assured.

AM.02.02: Requirement Name: Tariff and price administration function set
Requirement Description: ITU-T M.3400 – Section 8.2.2

Test Steps:

1. Test and certify that manager directs agent to create a tariff class corresponding to a certain service, origination and destination;
2. Test and certify that manager directs agent to delete a tariff class;
3. Test and certify that manager directs agent to change a tariff class;
4. Test and certify that manager requests the agent to report the defined tariff class data; agent replies with the data;
5. Test and certify that manager directs agent to create a tariff;
6. Test and certify that manager directs the agent to delete a tariff;
7. Test and certify that manager directs the agent to change a tariff;
8. Test and certify that manager requests agent to report tariff data, agent replies with the data;
9. Test and certify that manager directs the agent to create a new tariff period of the day;
10. Test and certify that manager directs the agent to delete an existing tariff period of the day;
11. Test and certify that manager directs the agent to change a tariff period of the day;
12. Test and certify that manager requests agent to report tariff period of the day, agent replies with the data;
13. Test and certify that manager directs the agent to create a day class into the calendar table;
14. Test and certify that manager directs the agent to delete a day class from the calendar table;
15. Test and certify that manager directs the agent to change a day class in the calendar table;

16. Test and certify that 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 Steps:

1. Test and certify that 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 is assured. (it may support reading of usage information from the Usage Me,asurements: 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 Steps:

1. Test and certify that support of access to guidelines for the apportionment of usage charges, is assured.
2. Test and certify that guidelines reflects 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 Steps:

1. Test and certify that support for the application of corporate strategies to the pricing of individual products/services, is assured;
2. Test and certify that usage Measurement functions with the pricing information necessary to generate billing data, is supplied;
3. Test and certify that the Collections and Finance functions with the requisite information to answer customer pricing questions, are supplied.

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 Steps:

1. Test and certify that support for a means by which the TMN and the public may determine rates and charges, is assured.

AM.02.07: Requirement Name: Rating usage function set
Requirement Description: ITU-T M.3400 – Section 8.2.7

Test Steps:

1. Test and certify that support for the financial components of the billable records is assured. (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), is assured;
2. Test and certify that rating information is applied to the usage data obtained from the Usage Measurement functionality;

3. Test and certify that this function set supports 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 Steps:

1. Test and certify that support for reading bill line items, grouped by customer, and provides access to the total charge, after application of any appropriate discounts or surcharges, is assured.

AM.03.01: Requirement Name: Planning of the billing process function set
Requirement Description: ITU-T M.3400 – Section 8.3.1

Test Steps:

1. Test and certify that support for plans processes and systems to improve accurate and efficient billing and collections for products and services, is assured.

AM.03.02: Requirement Name: Management of the billing process function set
Requirement Description: ITU-T M.3400 – Section 8.3.2

Test Steps:

1. Test and certify that support for the management of processes and systems to ensure accurate and efficient billing and collections for products and services, is assured.

AM.03.03: Requirement Name: General accounting operations function set
Requirement Description: ITU-T M.3400 – Section 8.3.3

Test Steps:

1. Test and certify that support to manage the base chart of accounts for categorization, tracking and reporting of financial expenditures, is assured;
2. Test and certify that monitoring of financial operations to ensure compliance to proper accounting practices, is supported;
3. Test and certify that periodic reconciliation of account balances for the purpose of generating financial results, is supported.

AM.03.04: Requirement Name: General ledger function set
Requirement Description: ITU-T M.3400 – Section 8.3.4

Test Steps:

1. Test and certify that support for the tracking of equity, income from operations, costs and expenses, nonoperating income and expense, and taxes is assured;
2. Test and certify that it is providing 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 Steps:

1. Test and certify that support the tracking of receipts due (including the amount, the date and identification of the account) for products and services rendered and payments received, is assured;

2. Test and certify that posting of transactions into the ledger is supported;
3. Test and certify that reading of invoice and payment data and provides access to summaries of such information, is supported.

AM.03.06: Requirement Name: Accounts payable function set
Requirement Description: ITU-T M.3400 – Section 8.3.6

Test Steps:

1. Test and certify that support for payment to contractors, suppliers, other service providers, insurance, principal and interest, rents and leases, taxes, utilities, is assured. (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 Steps:

1. Test and certify that the support for the administration and payment of employee salary, etc., is assured.

AM.03.08: Requirement Name: Benefits administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.8

Test Steps:

1. Test and certify that support for the administration of employee benefits is assured.

AM.03.09: Requirement Name: Pension administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.9

Test Steps:

1. Test and certify that support for the administration of employee pensions is assured.

AM.03.10: Requirement Name: Taxation function set
Requirement Description: ITU-T M.3400 – Section 8.3.10

Test Steps:

1. Test and certify that 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, is assured.

AM.03.11: Requirement Name: Human resources function set
Requirement Description: ITU-T M.3400 – Section 8.3.11

Test Steps:

1. Test and certify that 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, is assured.

AM.03.12: Requirement Name: Invoice assembly function set
Requirement Description: ITU-T M.3400 – Section 8.3.12

Test Steps:

1. Test and certify that 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, is assured.

AM.03.13: Requirement Name: Sending invoice function set
Requirement Description: ITU-T M.3400 – Section 8.3.13

Test Steps:

1. Test and certify that support for reading the assembled invoices and the preparation and distribution of the formatted invoices to customers, is assured.

AM.03.14: Requirement Name: Customer tax administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.14

Test Steps:

1. Test and certify that support of access to tax tables for the computation of taxes for customer invoice components, is assured.

AM.03.15: Requirement Name: In-call service request function set
Requirement Description: ITU-T M.3400 – Section 8.3.15

Test Steps:

1. Test and certify that support for on-demand, real-time request for usage information while a call is in progress or at its completion, is assured. (it may initiate the processing of the usage information while the call proceeds. Processing of the usage information may be destructive or non-destructive);
2. Test and certify that access to the complete usage information after the conclusion of the call is supported;
3. Test and certify that a time and charges quotation at the request of the party being charged for the call is supported.

AM.03.16: Requirement Name: Storage of invoice function set
Requirement Description: ITU-T M.3400 – Section 8.3.16

Test Steps:

1. Test and certify that support of access to the long and short term storage of billing data is assured.

AM.03.17: Requirement Name: Receipt of payment function set
Requirement Description: ITU-T M.3400 – Section 8.3.17

Test Steps:

1. Test and certify that support for the customer interface through which customers may make valid forms of remuneration for services provided, is assured;
2. Test and certify that crediting the customer's account is supported;
3. Test and certify that notifications of the received payment is supported.

AM.03.18: Requirement Name: Inquiry response function set
Requirement Description: ITU-T M.3400 – Section 8.3.18

Test Steps:
1. Test and certify that support for the interface through which customers may have access to account balance, rating, and subscription information, is assured.

AM.03.19: Requirement Name: Collections function set
Requirement Description: ITU-T M.3400 – Section 8.3.19

Test Steps:
1. Test and certify that support of access to delinquent accounts is assured. (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 Steps:
1. Test and certify that support of access to the customer account, including account balance, one-time and recurring charges, and history, is assured;
2. Test and certify that adjustment of customer balances according to credit, debit, and consumption information, is supported;
3. Test and certify that reading of a customer service profile is supported.

AM.03.21: Requirement Name: Customer profile administration function set
Requirement Description: ITU-T M.3400 – Section 8.3.21

Test Steps:
1. Test and certify that support for inputs from Service Negotiation & Planning and provides access to a database for the list of services of each individual customer, is assured.

AM.04.01: Requirement Name: Budgeting function set
Requirement Description: ITU-T M.3400 – Section 8.4.1

Test Steps:
1. Test and certify that 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, is assured;
2. Test and certify that access to the annual (or other periodic) budget is provided;
3. Test and certify that modification of the budget when variations between performance and objectives arise, is supported.

AM.04.02: Requirement Name: Auditing function set
Requirement Description: ITU-T M.3400 – Section 8.4.2

Test Steps:
1. Test and certify that support for the regular examination, checking, and adjusting of financial records is assured.

AM.04.03: Requirement Name: Cash management function set
Requirement Description: ITU-T M.3400 – Section 8.4.3

Test Steps:
1. Test and certify that support for cash flow analysis is assured;

2. Test and certify that reconciliation between payments and receipts and the identification of the potential need for borrowing to bring them in line with the budget, is supported;
3. Test and certify that short-term cash management (acquisition of cash needed to run the business) by borrowing against lines of credit, is supported.

AM.04.04: Requirement Name: Raising equity function set
Requirement Description: ITU-T M.3400 – Section 8.4.4

Test Steps:

1. Test and certify that support of access to data and reports for long-term cash management through investments and the liquidation of assets, is assured;
2. Test and certify that determination for and management of stock offerings, including SEC filings and generation of prospectuses, is supported.

AM.04.05: Requirement Name: Cost reduction function set
Requirement Description: ITU-T M.3400 – Section 8.4.5

Test Steps:

1. Test and certify that support of access to corporate policies for reducing costs and the coordination of implementation plans is assured.

AM.04.06: Requirement Name: Profitability analysis function set
Requirement Description: ITU-T M.3400 – Section 8.4.6

Test Steps:

1. Test and certify that support of access to data and reports concerning the assessment of the revenues and expenses of products to determine the profit or loss, is assured;

AM.04.07: Requirement Name: Financial reporting function set
Requirement Description: ITU-T M.3400 – Section 8.4.7

Test Steps:

1. Test and certify that support of access to financial information to be provided to employees, stockholders, government agencies, and the public, is assured;

AM.04.08: Requirement Name: Insurance analysis function set
Requirement Description: ITU-T M.3400 – Section 8.4.8

Test Steps:

1. Test and certify that support of access to data and plans for risk assessment and the determination of insurance needs, is assured.

AM.04.09: Requirement Name: Investments function set
Requirement Description: ITU-T M.3400 – Section 8.4.9

Test Steps:

1. Test and certify that support for the management of corporate investments is assured.

AM.04.10: Requirement Name: Assets management function set
Requirement Description: ITU-T M.3400 – Section 8.4.10

Test Steps:

1. Test and certify that support for the tracking of current and long-term assets, including inventory and depreciation is assured. (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 Steps:

1. Test and certify that support for the tracking of current and long-term liabilities is assured.

7.2.4 Test Methods for Performance Management

PM.01.01: Requirement Name: QoS performance goal setting function set
Requirement Description: ITU-T M.3400 – Section 5.1.1

Test Steps:

1. Test and certify that support for the management of guidelines for the assessment of all Quality of Service (QoS) performance measures, by area and component(s), is assured.

PM.01.02: Requirement Name: Network performance goal setting function set
Requirement Description: ITU-T M.3400 – Section 5.1.1

Test Steps:

1. Test and certify that support for the management of guidelines for the assessment of network performance quality and availability in order to support service assurance and service offerings, is assured.

PM.01.03: Requirement Name: Subscriber service quality criteria function set
Requirement Description: ITU-T M.3400 – Section 5.1.3

Test Steps:

1. Test and certify that 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, is assured.

PM.01.04: Requirement Name: QoS performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.4

Test Steps:

1. Test and certify that 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, is assured.

PM.01.05: Requirement Name: Network performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.5

Test Steps:

1. Test and certify that support of access to the assessment summary of network performance quality and availability, is assured.

PM.01.16: Requirement Name: NE(s) performance assessment function set
Requirement Description: ITU-T M.3400 – Section 5.1.6

Test Steps:

1. Test and certify that support of access to analyses of NE quality and availability performance parameters in order to support service assurance and/or service offerings, is assured;
2. Test and certify that information to the Network performance characterization function is provided.

PM.01.17: Requirement Name: Data integrity check function set
Requirement Description: ITU-T M.3400 – Section 5.1.17

Test Steps:

1. Test and certify that 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, is assured.

PM.02.01: Requirement Name: Performance monitoring policy function set
Requirement Description: ITU-T M.3400 – Section 5.2.1

Test Steps:

1. Test and certify that 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. Test and certify that 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. Test and certify that manager directs the agent to assign designated values to the quality parameters associated with each grade of service;
4. Test and certify that manager directs the agent to send current values of grade of service profiles. Agent responds with the requested information;
5. Test and certify that 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. Test and certify that manager directs the agent to send current values of PM impairment criteria. Agent responds with the requested information;
7. Test and certify that 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. Test and certify that manager directs the agent to send current values of PM trend analysis pattern. Agent responds with the requested information;

9. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that 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, is assured;
2. Test and certify that access to information concerning identified root causes is provided;
3. Test and certify that non-redundant notifications of trails that are found to generate persistent threshold crossing alerts, are generated.

PM.02.03: Requirement Name: Data aggregation and trending function set
Requirement Description: ITU-T M.3400 – Section 5.2.3

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that access to trending information, that supports the extrapolation of historical data to predict future performance and to identify persistent or worsening impairments, is provided.

PM.02.04: Requirement Name: Circuit-specific data collection function set
Requirement Description: ITU-T M.3400 – Section 5.2.4

Test Steps:

1. Test and certify that support for collecting all applicable data for a given circuit across multiple NEs is assured. (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 Steps:

1. Test and certify that 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. Test and certify that 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. Test and certify that agent automatically reports to manager the current busy/idle status of circuit groups for display on a terminal or other device;

4. Test and certify that agent automatically reports to manager the current congestion status of exchanges for display on a terminal or other device;
5. Test and certify that 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. Test and certify that upon request by an operator, manager commands agent to assign or remove HTR status to destinations, and to override automatic HTR designations;
7. Test and certify that upon request of an operator, agent reports to manager the HTR status of destinations;
8. Test and certify that agent automatically reports to manager the current congestion status of the common channel signalling network for display on a terminal or other device.
9. Test and certify that 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 Steps:

1. Test and certify that agent reports to manager circuit group traffic data and calculated network management parameters automatically according to a schedule;
2. Test and certify that agent reports to manager circuit group traffic data and calculated network monitoring parameters in response to an operator request;
3. Test and certify that agent reports to manager measurements of the traffic load on the exchange and its major components according to a schedule;
4. Test and certify that agent reports to manager measurements of traffic load on the exchange and its major components in response to an operator request;
5. Test and certify that agent reports to manager measurements of exchange switching congestion according to a schedule;
6. Test and certify that agent reports to manager measurements of exchange switching congestion in response to an operator request;
7. Test and certify that agent reports to manager measurements of CCSS traffic according to a schedule;
8. Test and certify that agent reports to manager CCSS traffic measurements in response to an operator request;
9. Test and certify that agent reports to manager CCSS network congestion measurements according to a schedule;
10. Test and certify that agent reports to manager CCSS congestion measurements in response to an operator request;
11. Test and certify that agent reports to manager data on traffic affected by network management controls according to a schedule;
12. Test and certify that 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 Steps:

1. Test and certify that 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, is assured;
2. Test and certify that 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, is provided.

PM.02.08: Requirement Name: NE(s) trend analysis function set
Requirement Description: ITU-T M.3400 – Section 5.2.8

Test Steps:

1. Test and certify that support for reporting of trends that are detected by processing the historical data of an NE or group of NEs, is assured.

PM.02.09: Requirement Name: Performance monitoring data accumulation function set
Requirement Description: ITU-T M.3400 – Section 5.2.9

Test Steps:

1. Test and certify that manager request the agent to send current PM data;
2. Test and certify that 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. Test and certify that manager directs the agent to start/stop the collection of PM data;
4. Test and certify that 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 Steps:

1. Test and certify that 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, is assured;
2. Test and certify that Storage implies that performance registers within an NE are readable on demand without resetting the count;
3. Test and certify that Reporting implies 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 Steps:

1. Test and certify that 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), is assured.

PM.03.02: Requirement Name: Traffic control function set
Requirement Description: ITU-T M.3400 – Section 5.3.2

Test Steps:

1. Test and certify that upon request from an operator, manager directs agent to modify manual network management traffic controls;
2. Test and certify that upon request from an operator, manager directs agent to modify automatic network management traffic controls;
3. Test and certify that manager directs agent to activate or deactivate an automatic control that has been previously established;
4. Test and certify that 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 Steps:

1. Test and certify that 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. Test and certify that 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. Test and certify that 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. Test and certify that 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. Test and certify that 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 Steps:

1. Test and certify that manager directs agent to establish a schedule for the reporting of PM data;
2. Test and certify that manager directs agent to send the current PM data reporting schedule. Agent responds with the schedule;
3. Test and certify that manager directs agent to assign designated values to PM attributes;
4. Test and certify that manager requests agent to send current PM attributes;
5. Test and certify that agent sends the currently assigned PM attributes to manager;
6. Test and certify that manager directs agent to set or change the PM parameter threshold;
7. Test and certify that manager instructs agent to suspend/resume the PM data collection activity for a given monitored entity or set of monitored entities;
8. Test and certify that manager instructs the agent to originate historical data based on some screening criteria (e.g. suppress "all-zero" data);

9. Test and certify that manager instructs the agent about the duration of the PM data collection interval for a given entity or set of entities;
10. Test and certify that manager directs agent to send the current PM threshold;
11. Test and certify that 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 Steps:

1. Test and certify that support for commands to change traffic controls and provides access to data concerning status and execution of the controls, is assured.

PM.03.06: Requirement Name: Audit report function set
Requirement Description: ITU-T M.3400 – Section 5.3.6

Test Steps:

1. Test and certify that support for reports on control information available at the NE, is assured.

PM.04.01: Requirement Name: Recommendations for performance improvement function set
Requirement Description: ITU-T M.3400 – Section 5.4.1

Test Steps:

1. Test and certify that 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, is assured.

PM.04.02: Requirement Name: Exception threshold policy function set
Requirement Description: ITU-T M.3400 – Section 5.4.2

Test Steps:

1. Test and certify that 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, is assured.

PM.04.03: Requirement Name: Traffic forecasting function set
Requirement Description: ITU-T M.3400 – Section 5.4.3

Test Steps:

1. Test and certify that support for reports on predicted changes in demand, from a combination of extrapolation of history and an evaluation of business factors, is assured. (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 Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that 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, is assured.

PM.04.06: Requirement Name: Traffic exception analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.6

Test Steps:

1. Test and certify that 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, is assured. (traffic exception analysis is analysis of traffic patterns to detect blocking conditions that exceed thresholds);
2. Test and certify that reports of traffic blocking conditions that exceed thresholds are generated;
3. Test and certify that 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.), are provided.

PM.04.07: Requirement Name: Traffic capacity analysis function set
Requirement Description: ITU-T M.3400 – Section 5.4.7

Test Steps:

1. Test and certify that 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 is assured.

PM.04.08: Requirement Name: Network performance characterization function set
Requirement Description: ITU-T M.3400 – Section 5.4.8

Test Steps:

1. Test and certify that 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, is assured.

PM.04.09: Requirement Name: NE(s) performance characterization function set
Requirement Description: ITU-T M.3400 – Section 5.4.9

Test Steps:
1. Test and certify that agent reports PM data to manager;
2. Test and certify that 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 Steps:
1. Test and certify that support for collecting and analysing traffic data from an NE or group of NEs, is assured;
2. Test and certify that reports are 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 Steps:
1. Test and certify that 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, is assured.

7.2.5 Test Methods for Security Management

SM.01.01: Requirement Name: Legal review function set
Requirement Description: ITU-T M.3400 – Section 9.1.1

Test Steps:
1. Test and certify that support of access to data concerning legal review of corporate documents, service offerings and policies to protect the enterprise against claims and litigation, is assured.

SM.01.02: Requirement Name: Physical access security function set
Requirement Description: ITU-T M.3400 – Section 9.1.2

Test Steps:
1. Test and certify that 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.), is assured.

SM.01.03: Requirement Name: Guarding function set
Requirement Description: ITU-T M.3400 – Section 9.1.3

Test Steps:
1. Test and certify that support for human monitoring of access such as checking identification badges or checking bags and packages for people entering and leaving a building, is assured.

SM.01.04: Requirement Name: Personnel risk analysis function set
Requirement Description: ITU-T M.3400 – Section 9.1.4

Test Steps:

1. Test and certify that support for requests for checking the trustworthiness of current and prospective employees is assured. (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 Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that support for analysis of significant shifts in revenue that might indicate fraud or theft of service, is assured.

SM.02.02: Requirement Name: Support element protection function set
Requirement Description: ITU-T M.3400 – Section 9.2.2

Test Steps:

1. Test and certify that support for the determination of need, monitoring and analysis of alarm systems that support structures that house network equipment, is assured. (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 Steps:

1. Test and certify that support of access by customers to security alarm information that indicates security attacks on their portion of the network, is assured.

SM.02.04: Requirement Name: Customer (external user) profiling function set
Requirement Description: ITU-T M.3400 – Section 9.2.4

Test Steps:

1. Test and certify that 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 Steps:

1. Test and certify that support for reading of usage data and customer profiles from other functions, is assured. (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 Steps:

1. Test and certify that support for investigation of customer and internal users whose usage patterns indicate possible fraud or theft of service, is assured. (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 Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that manager requests the agent to send specified alarm information history; agent responds with the specified information;
2. Test and certify that agent notifies manager of security alarm information (including identification of the NE) upon the occurrence of a security alarm;
3. Test and certify that 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 Steps:

1. Test and certify that support of checks for signs of software intrusion (e.g. the presence of a known virus) in the TMN, is assured; (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 Steps:

1. Test and certify that support of access to report information about security alarms so that containment and recovery activities may be initiated, is assured. (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 Steps:

1. Test and certify that support for the access and mechanisms, such as maintaining back copies of data and monitoring for data corruption, to secure business data, is assured.

SM.03.02: Requirement Name: Exception report action function set
Requirement Description: ITU-T M.3400 – Section 9.3.2

Test Steps:

1. Test and certify that support for exception reports such as security alarm is assured. (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 Steps:

1. Test and certify that support for receiving input on usage anomalies to initiate action to limit the security breach (e.g. remove user's access privileges, etc.), is assured;
2. Test and certify that requests to restore any corrupted data or equipment is supported. (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 Steps:

1. Test and certify that support for litigation against a perpetrator of an illegal action, is assured; (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 Steps:

1. Test and certify that support for actions to catch an intruder is assured; (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 Steps:

1. Test and certify that support for requests to access backup files in order to restore service after detection of a security violation, is assured.

SM.03.07: Requirement Name: Administration of customer revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.7

Test Steps:

1. Test and certify that 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), is assured.

SM.03.08: Requirement Name: Protected storage of customer data function set
Requirement Description: ITU-T M.3400 – Section 9.3.8

Test Steps:

1. Test and certify that support for the backup and restoration of stored customer data that can be used in support of intrusion recovery, is assured.

SM.03.09: Requirement Name: Severing external connections function set
Requirement Description: ITU-T M.3400 – Section 9.3.9

Test Steps:

1. Test and certify that 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, is assured. (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 Steps:

1. Test and certify that support of requests for restoration of the network configuration after detection of a security violation, is assured.

SM.03.11: Requirement Name: Administration of network revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.11

Test Steps:

1. Test and certify that 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), is assured.

SM.03.12: Requirement Name: Protected storage of network configuration data function set
Requirement Description: ITU-T M.3400 – Section 9.3.12

Test Steps:

1. Test and certify that support for the storage of network configuration data that can be used in support of intrusion recovery, is assured;
2. Test and certify that backup of such data, and for restoration of such backed up data upon request, is allowed.

SM.03.13: Requirement Name: Severing internal connections function set
Requirement Description: ITU-T M.3400 – Section 9.3.13

Test Steps:

1. Test and certify that 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, is assured.

SM.03.14: Requirement Name: NE(s) intrusion recovery function set
Requirement Description: ITU-T M.3400 – Section 9.3.14

Test Steps:

1. Test and certify that support for the access to backup files in order to restore NE or element management information after detection of a security violation, is assured.

SM.03.15: Requirement Name: Administration of NE(s) revocation list function set
Requirement Description: ITU-T M.3400 – Section 9.3.15

Test Steps:

1. Test and certify that 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), is assured.

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 Steps:

1. Test and certify that support for data storage and provides access to that data for backup in support of intrusion recovery, is assured.

SM.04.01: Requirement Name: Security policy function set
Requirement Description: ITU-T M.3400 – Section 9.4.1

Test Steps:

1. Test and certify that support for the access to company guidelines for establishing and maintaining a secure environment for personnel, hardware, and software, is assured.

SM.04.02: Requirement Name: Disaster recovery planning function set
Requirement Description: ITU-T M.3400 – Section 9.4.2

Test Steps:

1. Test and certify that 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, is assured.

SM.04.03: Requirement Name: Manage guards function set
Requirement Description: ITU-T M.3400 – Section 9.4.3

Test Steps:

1. Test and certify that support of access to information about the management of physical and mechanized devices used to provide security, is assured.

SM.04.04: Requirement Name: Audit trial analysis function set
Requirement Description: ITU-T M.3400 – Section 9.4.4

Test Steps:

1. Test and certify that 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, is assured.

SM.04.05: Requirement Name: Security alarm analysis function set
Requirement Description: ITU-T M.3400 – Section 9.4.5

Test Steps:

1. Test and certify that support of access to guidelines for the monitoring, evaluating, and correlating security alarms, is assured.

Test Objectives: Assure the support of access to information to determine the need

SM.04.06: Requirement Name: Assessment of corporate data integrity function set
Requirement Description: ITU-T M.3400 – Section 9.4.6

Test Steps:

1. Test and certify that 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, is assured.

SM.04.07: Requirement Name: Administration of external authentication function set
Requirement Description: ITU-T M.3400 – Section 9.4.7

Test Steps:

1. Test and certify that 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 is assured;
2. Test and certify that authentication path involving external authenticators is supported;
3. Test and certify that if a customer has been authenticated by an authentication agent outside the TMN, this function does 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 Steps:

1. Test and certify that 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, is assured.

SM.04.09: Requirement Name: Administration of external certification function set
Requirement Description: ITU-T M.3400 – Section 9.4.9

Test Steps:

1. Test and certify that 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, is assured.

SM.04.10: Requirement Name: Administration of external encryption and keys function set
Requirement Description: ITU-T M.3400 – Section 9.4.10

Test Steps:

1. Test and certify that 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), is assured.

SM.04.11: Requirement Name: Administration of external security protocols function set
Requirement Description: ITU-T M.3400 – Section 9.4.11

Test Steps:

1. Test and certify that support for the management of joint implementation agreements with other jurisdictions to assure interoperability of security protocols is assured. (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);
2. Test and certify that management for the administration of external security protocols is supported.

SM.04.12: Requirement Name: Customer audit trial function set
Requirement Description: ITU-T M.3400 – Section 9.4.12

Test Steps:

1. Test and certify that support for a customer to establish and configure audit trails to obtain information about service usage, is assured;
2. Test and certify that customer access to usage and security event information related to their portion of the network, is allowed;

SM.04.13: Requirement Name: Customer security alarm management function set
Requirement Description: ITU-T M.3400 – Section 9.4.13

Test Steps:

1. Test and certify that support for the customer access to security alarm information that indicates security attacks on their portion of the network, is assured.

SM.04.14: Requirement Name: Testing of audit trail mechanism function set
Requirement Description: ITU-T M.3400 – Section 9.4.14

Test Steps:

1. Test and certify that support for testing to ascertain that designated events are recorded in a security log, is assured.

SM.04.15: Requirement Name: Administration of internal authentication function set
Requirement Description: ITU-T M.3400 – Section 9.4.15

Test Steps:

1. Test and certify that support for receiving requests for and distributes codes for verification that internal users are who they present themselves to be, is assured;

SM.04.16: Requirement Name: Administration of internal access control function set
Requirement Description: ITU-T M.3400 – Section 9.4.16

Test Steps:

1. Test and certify that 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 Steps:

1. Test and certify that support of requests for and distributes Access Control Certificates that permit internal users access to previously agreed upon sets of capabilities, is assured;

SM.04.18: Requirement Name: Administration of internal encryption and keys function set
Requirement Description: ITU-T M.3400 – Section 9.4.18

Test Steps:

1. Test and certify that 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), is assured;
2. Test and certify that information on which encryption algorithms are to be used and in which mode, is provided.

SM.04.19: Requirement Name: Network audit trail management function set
Requirement Description: ITU-T M.3400 – Section 9.4.19

Test Steps:

1. Test and certify that support for internal users, generally security personnel, to establish and configure audit trails to obtain information about network usage, is assured;
2. Test and certify that internal user access to network usage and security event information is collected and allowed.

SM.04.20: Requirement Name: Network security alarm management function set
Requirement Description: ITU-T M.3400 – Section 9.4.20

Test Steps:

1. Test and certify that support for the collection of security alarm information that indicates network security violations, is assured;

2. Test and certify that internal user access to such data is allowed.

SM.04.21: Requirement Name: NE(s) audit trail management function set
Requirement Description: ITU-T M.3400 – Section 9.4.21

Test Steps:

1. Test and certify that manager requests agent to report security audit;
2. Test and certify that manager instructs the agent to allow or inhibit logging of log records security alarms;
3. Test and certify that manager instructs the agent to assign log attributes as specified by the manager what information to log;
4. Test and certify that manager directs the agent to allow/inhibit audit trail;
5. Test and certify that manager directs agent to establish a schedule to initiate, suspend or resume audit trails;
6. Test and certify that manager directs agent to send the current audit trail schedule. Agent responds with the schedule;
7. Test and certify that 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 Steps:

1. Test and certify that support for the collection of security alarms detected by lower level functions, is assured;
2. Test and certify that access to such information, possibly including information resulting from the correlation of such alarms, is provided.

SM.04.23: Requirement Name: Administration of keys for NEs function set
Requirement Description: ITU-T M.3400 – Section 9.4.23

Test Steps:

1. Test and certify that 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, is assured;
2. Test and certify that distribution of these keys to NEs and communicating entities is supported; (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 Steps:

1. Test and certify that 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, is assured;

Test and certify that distribution of these keys to communicating entities is supported. (such keys may be used for authentication, integrity and confidentiality).

7.3 References

[1] MUSE-II: Deliverable M TF4.4, December 2006

[2] ITU-T M.3400: TMN management functions

[3] TestSuite Part1, Muse 2005

[4] TestSuite Part2, Muse 2005

8 XDSL SPECIFIC TESTING

8.1 Introduction

This chapter 8 specifies the methodologies for testing the (xDSL) objectives as defined in chapter 9 of "Test Suite, Part 1: Test Objectives". These defined test objectives address a 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.

A distinction is made between functional and conformance tests. 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.
Both types of tests have their pros and cons, and each of these tests serve its own range of test applications. Functional tests seem to be 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.

Test Cases are defined, as much as possible, in a way that the test procedure can be easily applied to any xDSL flavor. However, for some test cases it is necessary to make a distinction between the xDSL flavors because of one of the following reasons:

- The requirement is different for each xDSL flavor.
- The requirement is exclusive for only one xDSL flavor
- The test objective is different for each xDSL flavor.
- The test objective is exclusive for only one xDSL flavor
- The test method is different for each xDSL flavor.
- The test method is exclusive for only one xDSL flavor

In case a test objective can not be tested in an xDSL general way, the test methodology is split in the relevant flavors and made exclusive per flavor.

8.2 Test configurations

Each test case refers to a preferable or required test set-up and xDSL configuration profiles. In this section all the referred test set-ups and configuration profiles are described.

8.2.1 Set-ups

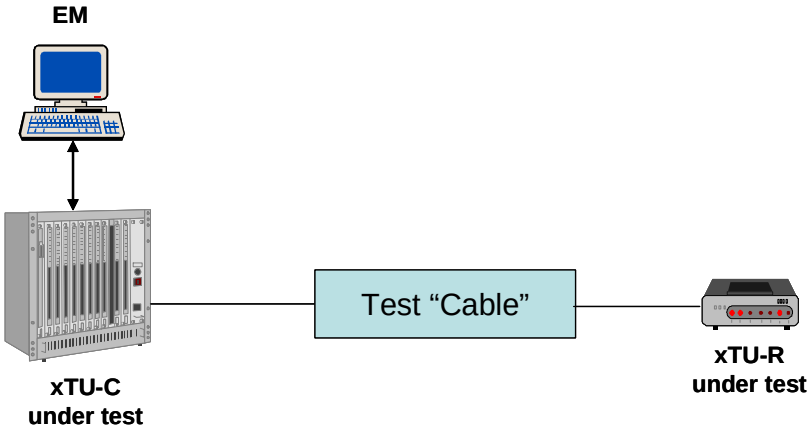


Figure 8-1 Basic test set-up for configuration management tests.

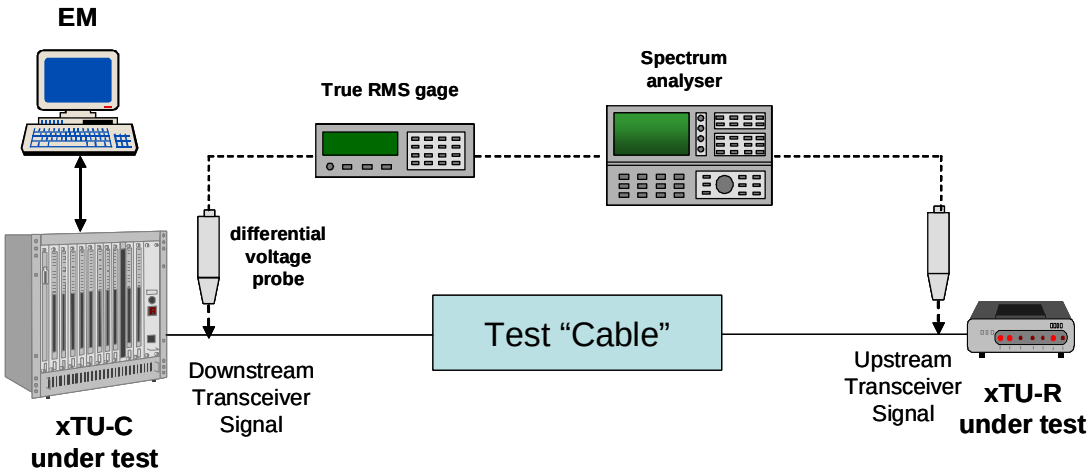


Figure 8-2 Basic test set-up for testing transmitter characteristics.

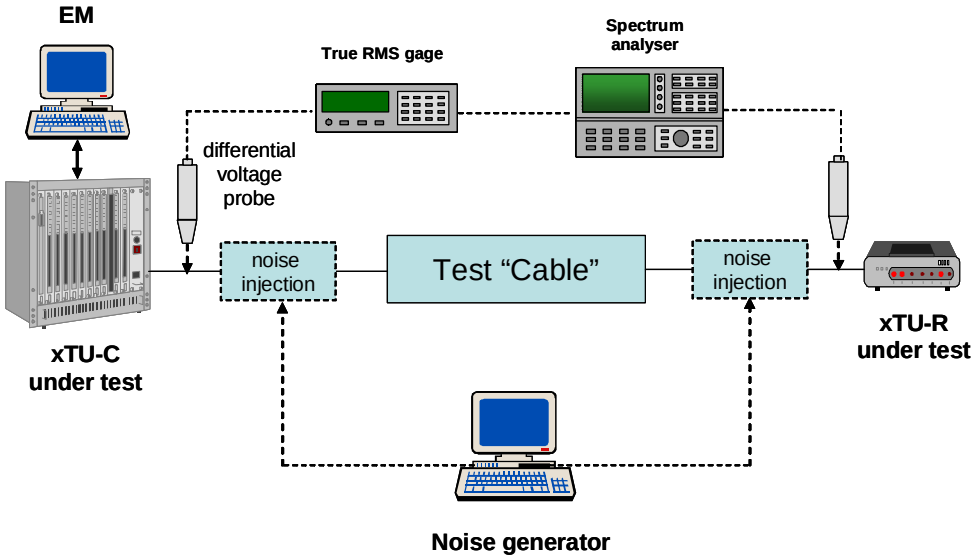


Figure 8-3: Basic test set-up for testing performance under noisy stress conditions.

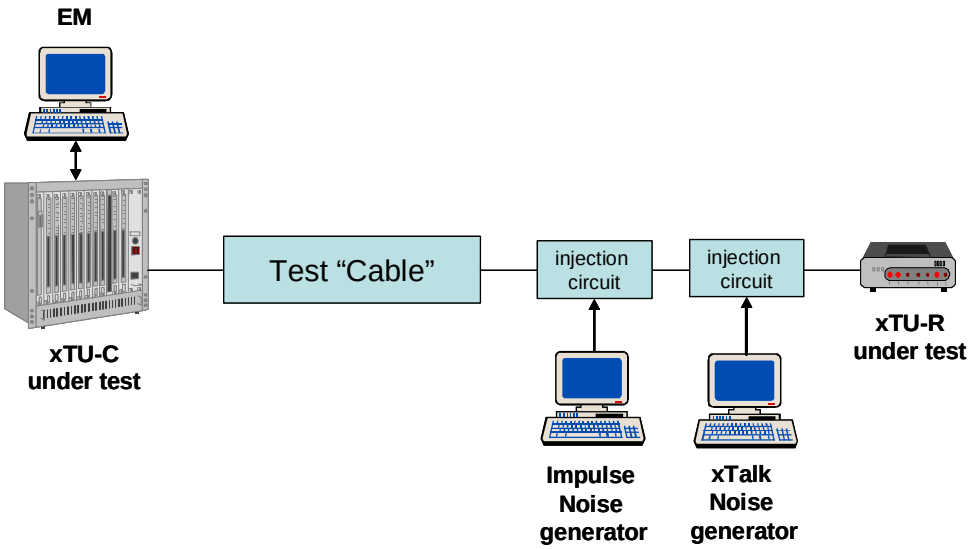


Figure 8-4: Basic test set-up for testing performance under differential mode injected impulsive and stationary noise.

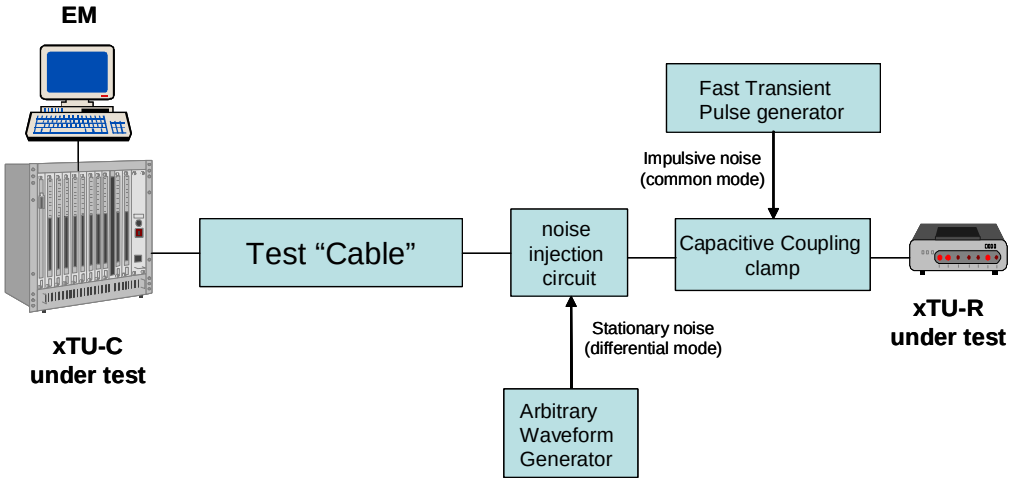


Figure 8-5: Basic test set-up for testing performance under common mode injected impulsive and stationary noise.

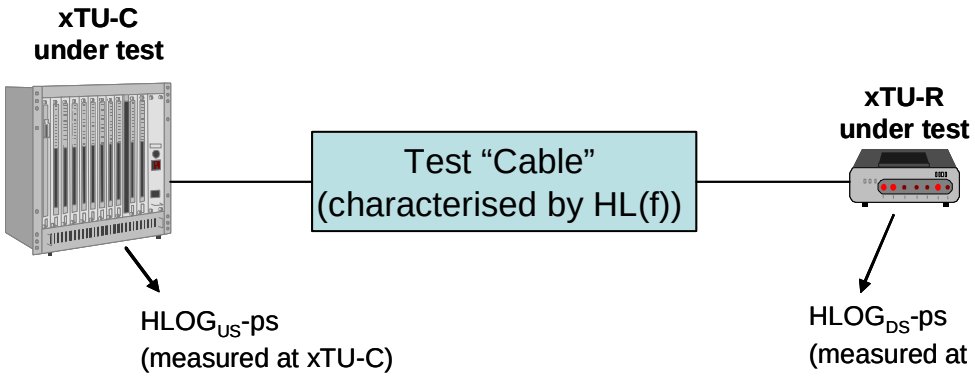


Figure 8-6: Test configuration for HLOG collection, see the sections “Report of loop diagnostic parameters” and “SELT tests”.

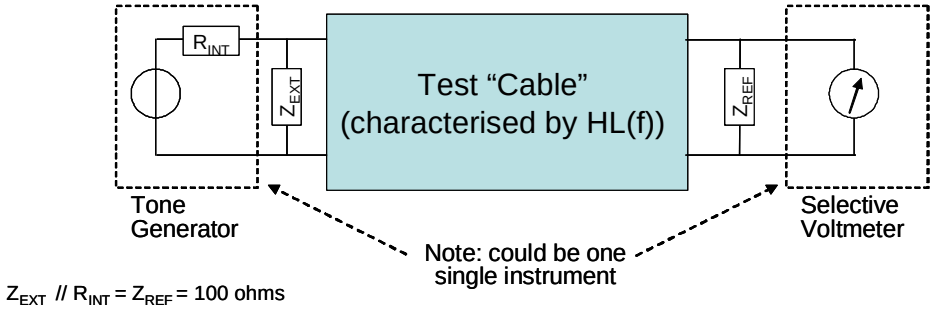


Figure 8-7: Reference measurement of HL(f).

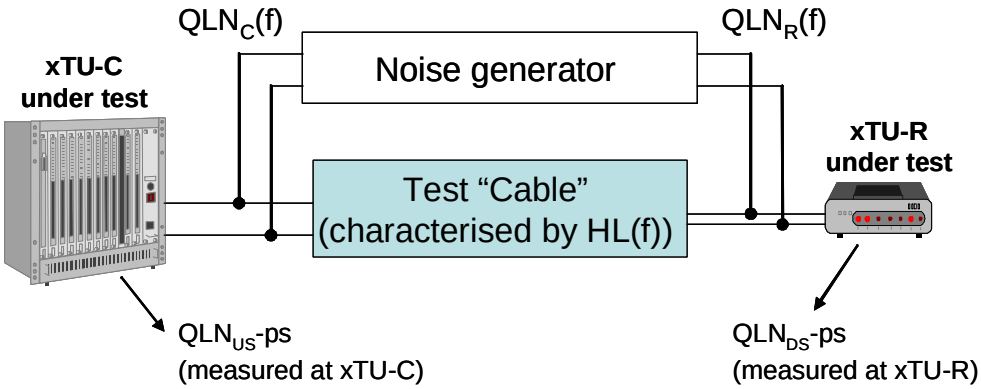


Figure 8-8: Test configuration for QLN collection.

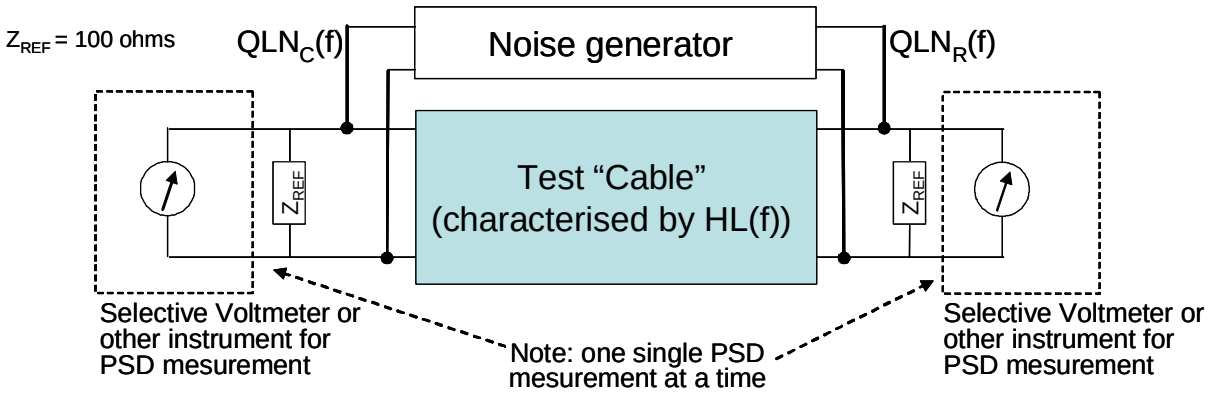


Figure 8-9: Reference measurement of QLNR(f) and QLNC(f).

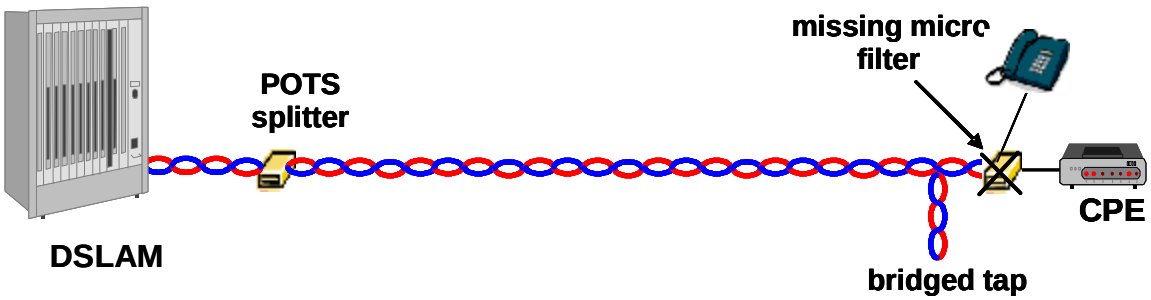


Figure 8-10: Reference set-up for SELT tests: complete copper loop with impairments.

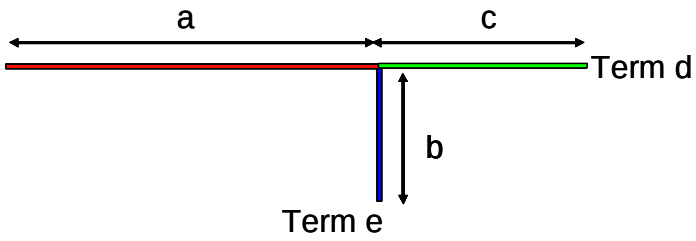


Figure 8-11: Reference set-up for SELT tests: copper loop with Bridge Tap.

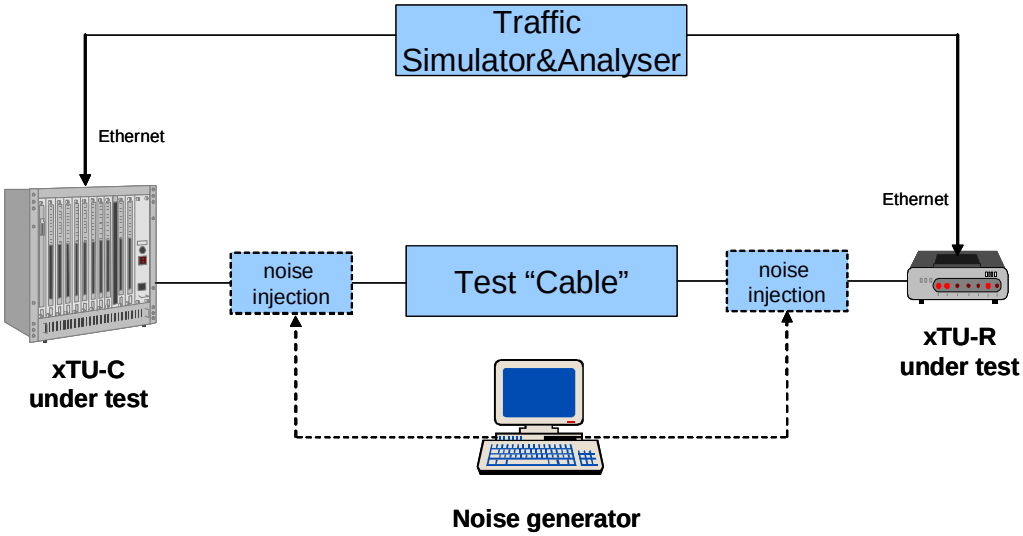


Figure 8-12: Set-up for layer 2 throughput and BER testing in case of a DSLAM with Ethernet network interface.

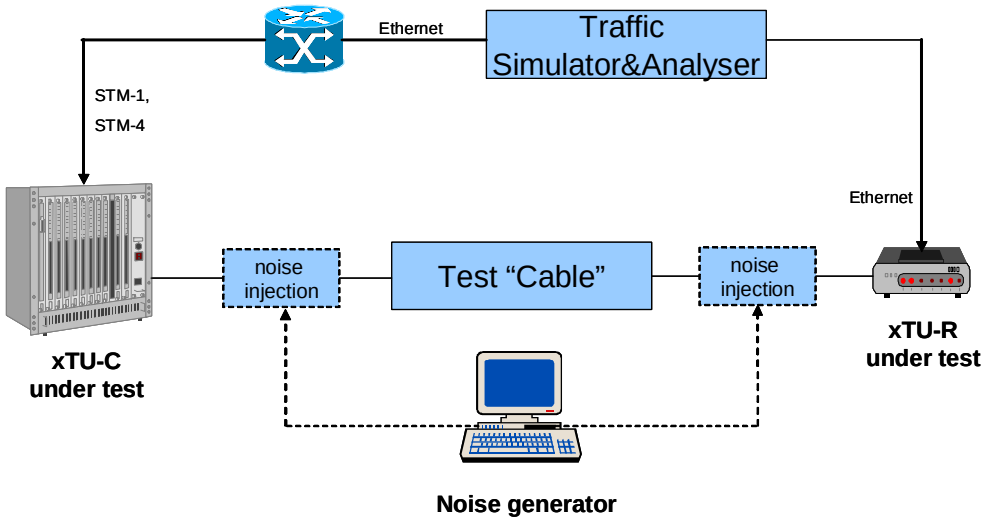


Figure 8-13: Set-up for layer 2 throughput and BER testing in case of a DSLAM with ATM network interface.

8.2.2 Test loops

The two counter parts of the xDSL system under test are connected through a test loop or loop simulator as depicted in the section with test set-ups. The loop is to cause amplitude distortion due to insertion loss, echo due to impedance mismatch, and phase distortion due to delay variations. A loop set is to stress the transmission and the various loops should therefore cover:

1. A variety of impedances, to stress the echo-canceller of the modem. It should represent a variety of impedances observed in the field.
2. A range of insertion loss shapes, as function of the frequency, to stress one aspect of the equalizer. This is simple for "straight-forward" loops, but not for loops with bridge taps. When the insertion loss at a mid-band frequency is the same of two very different cables (with different length) then the shape of their (normalized) insertion losses are almost the same.
3. A range of group/phase delay variations to stress another aspect of the equalizer. Especially bridge taps[5] cause significant delay variations and are severe stressors for modems. However, bridge taps do not occur in many European counties.

For the purpose of ***functional testing***, it is sufficient to choose one type of test loop, physical or via the simulator. Depending on the test purpose one can select a country-specific loop that is considered as representative for that country or a "standard" test loop as defined by ETSI. ETSI has 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. to emulate most loops in Europe, the set of test loops for testing xDSL varies from four up to eight loops.
Beyond loops predefined by ETSI, for testing purposes other loops can be obtained by combining segments of standard loop models, typically in a straight or bridge-tapped fashion. This is the case for DSL Forum Test Plans that, as related to the requirements from European Operators defined several straight loops of PE04 and PE05 loop model ranging up to 5 km for ADSL1, ADSL2 and ADSL2+.
For VDSL2, along with straight loops of PE04 and TP100, topologies with impedance mismatch or very short bridge tap at the end of the loop are under consideration to assess equipment robustness in the presence of relevant echo from the hybrid circuit of the modem.

Note that it depends on the test campaign which test loop is selected. In case there is chosen for a country-specific test loop it is important that all the characteristics are known and well documented for the reason of reproducibility. Another disadvantage of using non standard country-specific test loops is the difficulty to inter-compare test results from different laboratories. The use of a standard test conditions allows operators and other players to directly compare test results. At the end of this chapter a section can be found with examples of test loops being used in practice.

[5] Bridged taps are un-terminated twisted-pair cable connected in parallel across the cable in consideration. The taps may be remainders of anterior services on the same wire pair or may have been included willingly in order to maintain more flexibility. Bridged taps act as an open-ended second line in parallel causing signals travels up and down the bridged tap resulting in more severe ISI problems and discontinuities.

8.2.3 Noise sources

For the purpose of performance testing under noisy stress conditions the transmitted signal of the xDSL system under test is impaired by noise injected close to the receiver input. This noise represents crosstalk noise, RFI ingress noise, impulse noise, etc. The noise can be sub-divided into two main groups, namely

1. Stationary noise.
2. Non-stationary noise (Impulse Noise).

8.2.3.1 Stationary crosstalk noise

For the purpose of ***conformance testing*** there is referred to ETSI and DSLF where the noise scenarios are defined and described in detail.
For the purpose of ***functional testing***, it is sufficient to choose one type of noise scenario. Depending on the test purpose one can select a country-specific noise scenario that is considered as representative for that country or a "standard" noise scenario as defined by ETSI. ETSI has 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).
Note that it depends on the test campaign which noise model is selected. In case there is chosen for a country-specific noise model it is important that all the characteristics are known and well documented for the reason of reproduction. Another disadvantage of using non standard country-specific noise models is the difficulty to inter-compare test results from different laboratories. The use of a standard test conditions allows operators and other players to directly compare test results.
At the end of this chapter a section can be found with examples of crosstalk noise profiles being used in practice.

8.2.3.2 Non-stationary noise

The above mentioned 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. These topics are left for further study in these standards, and include:

- 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;
- noise that is bursty and impulsive in nature.

8.2.3.3 Impulse noise

The last couple of years, awareness has been raised about the problem of impulse noise. In particular British Telecom has been active in investigating the problems of repetitive electrical impulse noise (REIN), and in specifying tests to measure the robustness of modem links against this type of noise.

It is now commonly accepted that impulse noise has a significant impact on the Quality of Experience of triple play services delivered by xDSL. Impulse noise consists of short bursts of noise that originate from outside the cable. Such impulse noise may not lead to a reduction of the achievable bandwidth, but can lead to the occurrence of short bursts of bit errors.

Currently, increasing the robustness of xDSL transmission (in particular VDSL2) against impulse noise is an important issue in various standardisation bodies. Mechanisms such as Impulse Noise Protection (INP) are already part of the ADSL2+ and VDSL2 standards. Methods such as Impulse Noise Monitoring (INM) are under study: these methods should aid the operator in selecting the appropriate INP settings for a particular xDSL line. As a novel approach in xDSL, retransmission schemes are considered to be added to the VDSL standards, as an alternative method to combat impulse noise.

All different sort of impulse events could be observed on the line: short/long pulses, single/composite pulses, pulse trains, etc, etc.

In standardisation much attention has been given to REIN: repetitive noise consisting of short bursts (shorter than 1 ms) of noise. In addition, SHINE has been defined as individual impulse noise events with lengths larger than 10 ms. Although robustness against REIN and SHINE is indeed important, it should not be the exclusive focus of attempts to counteract impulse noise.

The measurements in the Dutch access network suggest that the majority of impulse noise events on problematic ADSL2+ lines in the Netherlands is non-repetitive in nature. In fact, individual impulse noise events with length between 1 ms and 10 ms are suspected to cause the most impulse noise related problems for the Dutch access network. For this type of impulse noise the acronym ‘PEIN’: Prolonged Electrical Impulse Noise is introduced. PEIN is defined to consist of all non-repetitive impulse noise events that have duration between 1 ms and 10 ms. Table 8-1 shows that PEIN is complementary to REIN and SHINE. To counteract PEIN, it is expected that large INP values INP > 4) or other impulse noise protection mechanisms will be required. The impulse noise protection test methods should not focus exclusively on relatively short pulses (shorter than 1 ms), or on REIN and SHINE, but also on PEIN.

Impulse Noise	Typical Burst length	Repetitive?	Desired modem behaviour
REIN	< 1 ms	Yes	No bit errors
PEIN	1 – 10 ms	No	No bit errors
SHINE	> 10 ms	No	No sync loss[6]

Table 8-1: Differences between various forms of impulse noise. PEIN fills the gap between the already defined REIN and SHINE impulse noise.

[6] Because of the length of a SHINE burst, it is unrealistic to expect the modem to be able to survive such a noise event without bit errors. Therefore, the main question for SHINE events is whether the modem loses synchronisation or not.

In test document DSLF TR-100 are tests methods described for testing the ADSL2(+) system on the robustness against REIN. SHINE and PEIN are still under study. In case of PEIN there is a proposal to mimic the real-world impulse noise situation as close as possible by playing back in the lab the samples that were recorded on operational lines in the field. The impulse noise injection will be done directly on the differential mode of the link under test, in order to have maximum control over the disturbing impulse. This method will give a typical country specific PEIN test.

8.2.3.4 Noise injection

Figure 8-15 illustrates the set-up for injecting noise into the xDSL link under test. The noise is injected through an adding element (differential mode noise injection network) close to the receiver under test. The noise injection method is similar to the crosstalk injection method specified in ITU-T [x13] clause 5.1.2.1 and ETSI [x1] clause 5.1.2.-5.1.4.

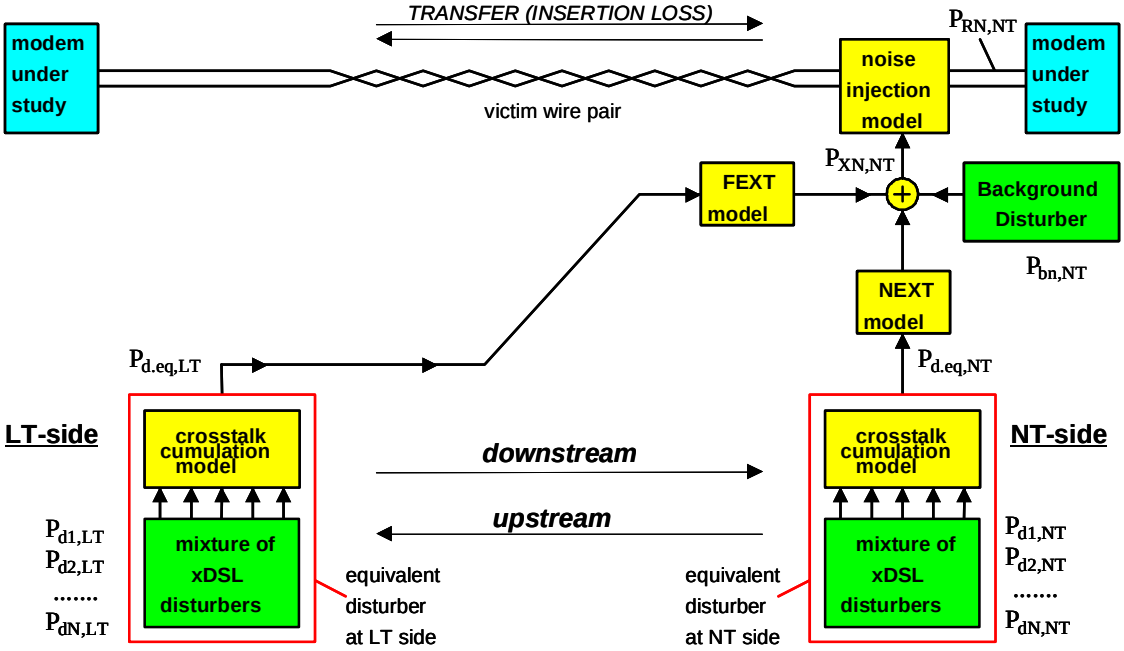


Figure 8-15: Flow diagram for evaluating stationary crosstalk noise, to be injected at a single end of a test loop.

A distinction can be made between “single-end” noise injection and “double-end” noise injection.
Single-end injection saves a noise generator, but increases the time for measurements, and may fool systems that configure themselves on the bases of observed SNR in both directions (e.g. advanced power-back-off mechanisms). Furthermore this choice for noise injection may result in “tricky implementations” that boost the performance on the side under stress trading off on the performance of the unimpaired side.
Double-end injection requires two noise generators and can speed-up the time for measurements. This choice for noise injection compels implementations to show their best performances on both sides contemporarily.

Mark that double-end injection is not the same as two times a single-end injection because a receiver receives both the near-end injected noise plus the attenuated far-end injected noise hence measured performances are lower than with single-end injection especially for short loops (i.e. low attenuation on the far-end noise). So double-end injection requires some reduction of the (single-end) noise levels before it can be injected. This prevents measurement errors, especially at short loops (VDSL and enhanced-SDSL).

The injection of noise as a differential mode signal across the wire pairs is widely adopted for testing. This is because the noise models are mainly defined as differential voltages induced at the xTU-C/R transceiver.
Certain noise models, such as impulse noise specified by CISPR, are described as a common mode voltage to be contemporarily applied to tip and ring wires. This requires specific injection circuits and methods, such as a capacitive clamp coupled along a short segment of the line (e.g. 1 m) and inducing the disturbing common mode voltage by capacitive coupling. These kind of test setups are more critical than differential mode ones in terms of repeatability and calibration of the coupling of the disturbing signal onto the copper pair. Furthermore the effects of the common mode noise depend on the LCL of the simulated line and of the SUT's transceiver.
The figures 8-16 and 8-17 show detailed schemes of noise injection circuits.

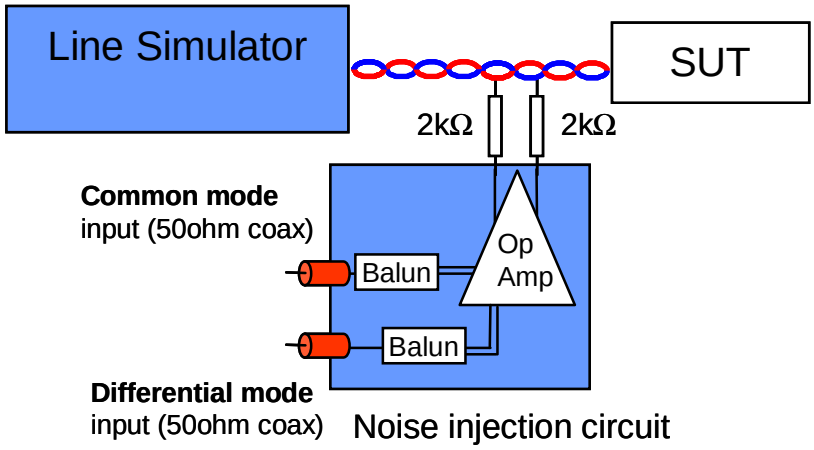


Figure 8-16: Noise injection scheme with both differential and common mode inputs.

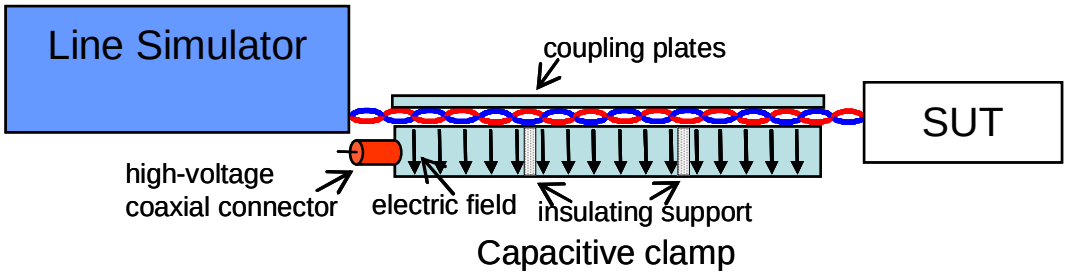


Figure 8-17: Capacitive clamp for common mode noise injection.

8.2.4 System configuration profiles

Before one can start with a test campaign the xDSL system under test need to be configured. The xDSL physical layer is configured by the so-called xDSL line and channel profile. In general this profile contains the following physical layer parameters:

Line Profile parameter	Channel Profile parameter
Line Standard (Transmission Mode)	Data Path Mode (ATM, PTM)
Rate Adaptation Mode	Ds/Us Minimum Impulse Noise Protection
Ds/Us SNR margin (max-trgt-min)	Ds/Us Maximum Interleaving Delay
DPBO configuration parameters	Ds/Us transmit rate (max-min)
UPBO configuration parameters	
Profile (VDSL2)	
PSD mask (VDSL2)	
Ds/Us Maximum nominal aggregate transmit power	

Table 8-2: Generic xDSL configuration profiles.

At the end of this chapter a section can be found with examples of system configuration profiles for various variants of xDSL.

8.3 Testing management capabilities

This section specifies xDSL management tests completing the test methods specified in management chapter (chapter 8) and better detailing as related to xDSL specific features.
To manage the xDSL part of an end-to-end chain, it is needed to access the related network resources for configuration and monitoring. As a matter of fact what is mainly configurable and monitor-able in the xDSL system is the DSLAM, or a GPON ONU hosting an xDSL line card, and the xDSL link whose configuration is mainly dictated xTU-C itself. The counterpart CPE is not generally part of the Network Operator management domain (and responsibility) and relevant xDSL information generated on the CPE is usually collected by the DSLAM/ONU via the xDSL EOC.

Beyond the xDSL system (xTU-C, xTU-R, copper pair), a mean to manage it is needed. Such management resource is usually an Element Manager (EM), hence while doing the test it is verified the correct integration between DSLAM/ONU functionalities and their integration into the EM MIB. Generally speaking, access to the xDSL system can be done via also a Local Craft Terminal. Ad-hoc management GUIs could be used as well, also on the Remote side of the system. Such control applications are not for network operation but they are typically developed for debugging/testing purposes.
Although the following is not possible on the field, in a lab environment, the verification of correct parameters configuration can be double-checked also on the CPE's monitoring application.

For the rest of this chapter only the EM will be mentioned as the system and related application for managing the DSLAM/ONU equipment.

Given the above (and as stated also in part 1, chapter 9), this section focuses on the methods for testing:

- capabilities for configuration management
- capabilities for monitoring and diagnostics

The first group deals with settings only, and in principle the related test method aims to verify if the specific feature is supported or not. Hence if the feature is supported, it shall be verified that after configuring a specific setting, this has actually taken place by:

- verifying on the EM that the setting is correctly reported; this is a high level verification;

- verifying that the setting has the expected effect on the real xDSL chain; this is the appropriate verification which falls outside “management testing” onto “functional testing”.
- The second group deals with the collection of information, alarms and performance parameters, originating in the physical layer and reported to the EM. Verification of such management features goes from the monitoring of status of a line in normal operational conditions to the collection of performances and alarms as related to degrade/defect conditions that have to be generated on the line.

The second group deals with the collection of information, alarms and performance parameters, originating in the physical layer and reported to the EM. Verification of such management features goes from the monitoring of status of a line in normal operational conditions to the collection of performances and alarms as related to degrade/defect conditions that have to be generated on the line.

8.3.1 Configuration management tests

Configuration management should be capable of configuring all kinds of *line parameters* as well as *channel parameters*. In this section the tests are focused on the verification of the configurability of relevant parameters and a “light” procedure to verify that configuration has actually taken place.

Many of the tests below have a test counterpart in section “Testing Transceiver signal Characteristics” or “Testing Performance Under Noisey Stress Conditions”. The tests in these sections are focused on the verification or measurement of actual line conditions and on the values of the related parameters. The associated test procedures are more complex and time consuming than those of “Configuration management tests” but implicitly verify also the configurability of the feature under test.
In this chapter both “Configuration management tests” and “Functional tests” are specified so that the test operator is given basic building blocks to plan the test campaign, by adopting one of the following options:

- Perform “Functional tests” directly for a longer but deeper validation of the implementation(s) under test.
- Perform only “Configuration management tests” for a shorter validation in case there is a good degree of confidence on the implementation(s) under test or it is a regression test campaign on already verified implementation(s).

Table 8-3 gives a generic list of the configuration parameters that should be supported by the xDSL system under test. Note that some configuration parameters have only relevance for one particular xDSL system or line code. Table 8-3 contains checkboxes that assign a parameter to an xDSL flavour. The test consists of the verification if one configuration parameter is supported or not. When supported, the test engineer should mark the corresponding checkbox.
Table 8-4 gives a generic list of parameters monitored by the management systems. Note that some of these parameters are not applicable for all the xDSL types, e.g., have only relevance for one xDSL type or line code. As table 8-4 contains checkboxes that assign a parameter to an xDSL flavour. The test consists of the verification if one configuration parameter is supported or not. When supported, the test engineer should mark the corresponding checkbox.

Testing configuration management capabilities					
Configuration Parameter	***xDSL types***				***Supported***
System Parameters	*ADSL*	*SDSL*	*ADSL2(+)*	*VDSL(2)*	
Applicable Standard			*x*	*x*	
Deployment Scenario				*x*	
Transmit Parameters					
Band Plan				*x*	
Band Number				*x*	
Power management state forced			*x*	*x*	
DS maximum nominal PSD	*x*	*x*	*x*	*x*	
US maximum nominal PSD	*x*	*x*	*x*	*x*	
DS maximum nominal Aggregate Transmit Power	*x*	*x*	*x*	*x*	
US maximum nominal Aggregate Transmit Power	*x*	*x*	*x*	*x*	
DS MIB PSD mask				*x*	
US MIB PSD mask				*x*	
UPBO		*x*		*x*	
DPBO	*x*	*x*	*x*	*x*	
DS Sub-carrier Masking	*x*		*x*	*x*	
US Sub-carrier Masking	*x*		*x*	*x*	
DS RFI bands			*x*	*x*	
US RFI bands			*x*	*x*	
DS PSD shaping			*x*	*x*	
US PSD shaping			*x*	*x*	
L0-Time			*x*	*x*	
L2-Time			*x*	*x*	
L2-ATPR			*x*	*x*	
Line Parameters					
Target DS NM	*x*		*x*	*x*	
Target US NM	*x*		*x*	*x*	
Maximum DS NM	*x*		*x*	*x*	
Maximum US NM	*x*		*x*	*x*	
Minimum DS NM	*x*		*x*	*x*	
Minimum US NM	*x*		*x*	*x*	
SNRM_MODE				*x*	
DS Rate adaptation mode	*x*		*x*	*x*	
US Rate adaptation mode	*x*		*x*	*x*	
DS Up-shift Noise Margin			*x*	*x*	
US Up-shift Noise Margin			*x*	*x*	
DS Down-shift Noise Margin			*x*	*x*	
US Down-shift Noise Margin			*x*	*x*	
DS Minimum Data Rate	*x*		*x*	*x*	
US Minimum Data Rate	*x*		*x*	*x*	
DS Target Data Rate	*x*	*x*	*x*	*x*	
US Target Data Rate	*x*	*x*	*x*	*x*	
DS Maximum Data Rate	*x*		*x*	*x*	
US Maximum Data Rate	*x*		*x*	*x*	
DS Rate Adaptation Ratio			*x*	*x*	
US Rate Adaptation Ratio			*x*	*x*	
Minimum Data Rate in low power state DS			*x*	*x*	
Latency Mode	*x*		*x*	*x*	
DS Maximum Interleave Delay	*x*		*x*	*x*	
US Maximum Interleave Delay	*x*		*x*	*x*	
DS Minimum Impulse Noise Protection			*x*	*x*	
US Minimum Impulse Noise Protection			*x*	*x*	

FORCEINP mode				*x*	

Table 8-3: Generic configuration parameter list to be verified.

Testing monitoring management capabilities					
Reported Parameter	***xDSL types***				***Supported***
	ADSL	*SDSL*	*ADSL2(+)*	*VDSL(2)*	
Downstream Signal-to-Noise Ratio Margin	*x*	*x*	*x*	*x*	
Upstream Signal-to-Noise Ratio Margin	*x*	*x*	*x*	*x*	
Downstream Attainable bit Rate	*x*		*x*	*x*	
Upstream Attainable bit Rate	*x*		*x*	*x*	
Downstream Actual Aggregate Transmit Power	*x*	*x*	*x*	*x*	
Upstream Actual Aggregate Transmit Power	*x*	*x*	*x*	*x*	
Downstream Actual data Rate	*x*	*x*	*x*	*x*	
Upstream Actual data Rate	*x*	*x*	*x*	*x*	
Downstream Interleave Delay	*x*	*x*	*x*	*x*	
Upstream Interleave Delay	*x*	*x*	*x*	*x*	
Downstream Impulse Noise Protection			*x*	*x*	
Upstream Impulse Noise Protection			*x*	*x*	
Downstream Line Attenuation			*x*	*x*	
Upstream Line Attenuation			*x*	*x*	
Downstream Signal Attenuation			*x*	*x*	
Upstream Signal Attenuation			*x*	*x*	

Table 8-4: Generic monitoring parameter list to be verified.

8.3.1.1 Line profile configuration test

Test Objective	To verify the ability to configure an xDSL profile.
Test Configura-tion	See Figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a line profile according to the generic profile given in Table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end of this chapter. § Let the modems train. § Check the EM on all the line profile configuration parameters.
Expected Result	The EM shall report line parameters coherent with the configured line profile. Correct line configuration may be double checked also from the CPE monitoring application running on a PC connected to it (not shown in Figure 8-1).

Note: punctual verification of achieved training rates and margins belongs to the set of "xDSL performance" tests (see section "Testing Performance Under Noisey Stress Conditions").

8.3.1.2 Rate adaptation test

Test Objective	To verify the ability to adapt training rates to channel conditions when a “rate adaptive at init” xDSL profile is applied.
Test Configura-tion	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section “Test Loops” with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a “rate adaptive at init” line profile according to the generic profile given in table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end of this chapter. § Let the modems train. § Check on the EM all the line parameters. § Then drop down the line, increase the loop length, let the modems retrain. § Check again on the EM all the line parameters.
Expected Result	The comparison of the two sets of line parameters shall show that the system adapts the line rates to loop conditions while guaranteeing the Target Noise Margin.

8.3.1.3 Seamless Rate Adaptation (SRA) test

The SRA functionality allows changing the current bitrate during Showtime in order to adapt it to changes in the noise margin due to variations of the noise level on the line, especially cross-talk due to adjacent xDSL systems.
This is particularly useful for ADSL2+ and VDSL2 deployments which are typically done with rate adaptive profiles with a wide bitrate range. Infect with these profiles, the line typically operates at a NM equal to the target NM (instead of a potentially higher NM in case of a fixed rate profile).

Test Objective	To verify the ability to adapt training rates to channel conditions when a “dynamic rate adaptive” xDSL profile is applied.
Test Configuration	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section “Test Loops” with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	1. Set a “dynamic rate adaptive” line profile according to the generic profile given in table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found in at the end of this chapter. 2. Set the downstream Upshift NM and downstream Upshift Minimum Time Interval. 3. Set the downstream Downshift NM and DS Downshift Time Interval. 4. Apply AWGN on the CPE side of the loop tuning the PSD in a way that the modems train with a downstream NM almost half way between the downstream Upshift and Downshift NM. Record the downstream rate. 5. Decrease the AWGN PSD by an amount that brings the downstream NM above the Upshift NM and wait for twice the related time interval. Record the current downstream rate. 6. Bring back the AWGN to the initial level. Record the new initial downstream rate. 7. Increase the AWGN PSD by an amount that brings the downstream NM below the Downshift NM and wait for twice the related time interval. Record the current downstream rate. Note: the same procedure is applicable for the upstream direction: upstream Upshift and Downshift parameters need to be configured and the AWGN need to be injected on the DSLAM/ONU side.
Expected Result	After noise decrease (increase) the system reacts increasing (decreasing) the data rate in a seamless way, i.e. without dropping the line or occurrence of CRC errors.

8.3.1.4 Dual latency test

Test Objective	To verify the ability a dual latency xDSL profile.
Test Configuration	See figure 8-12 or 8-13. The xTU-C and xTU-R are connected through a loop according to the section “Test Loops” with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a line profile according to the generic profile given in table 8-2. The specific completion of the line profile for this test requires that data paths with different latencies are configured: one low latency path (no delay or 1 ms both in downstream and upstream) and one high latency path (e.g. 16ms both in downstream and upstream). § Create one ATM PVC or PTM Ethernet connection associated to each latency path. § Let the modems train. § Send Ethernet traffic on both the DSLAM network interface and the CPE LAN interface. Ethernet frames shall be such that two separate traffic streams are encapsulated over the two Layer 2 connections.
Expected Result	The DS Ethernet streams show one-way delays coherent with the configured latencies. Same applies to the upstream Ethernet streams.

8.3.1.5 Impulse noise related configuration capabilities

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. Other mechanisms which are still under study within the standardization are Frame Blanking, Frame Repetition and retransmission. The level of Impulse Noise Protection can be configured by two parameters; minimum INP and maximum delay. These parameters give the boundaries for the xDSL system to synchronize. The actual INP and delay value depend on line quality and the limitations of the framing parameters, e.g., the interleaving dept D and 1/S (the maximum number of FEC codewords that the modem is capable of transmitting during one DMT symbol).
In the ITU standards a clear difference is made between mandatory and optional framing and configuration values, e.g.:

	Standard	Mandatory	Optional
INP_min	ITU G.992.5	0, ½, 1 and 2	4, 8 and 16
	ITU G.993.2	No explicit values	No explicit values
Interleaving dept D_0	ITU G.992.5	1, 2, 4, 8,16, 32, 64	From 64 up to 511 in steps of 32
	ITU G.993.2	D_max depending on the profile	No explicit values
S_0	ITU G.992.5	$1/3 \leq S_0 < 64$	$1/16 \leq S_0 < 1/3$
	ITU G.993.2	(1/Smax) depending on the profile (See table 8-6)	Extended values depending on the profile (See table 8-6)

Table 8-5: Mandatory and Optional configuration values.

Parameter	8a	8b	8c	8d	12a	12b	17a	30a
(1/Smax) DS	24	24	24	24	24	24	48	28
(1/Smax) US	12	12	12	12	24	24	24	28
Extended (1/Smax) DS	64	64	64	64	64	64	64	32
Extended (1/Smax) US	32	32	32	32	64	64	64	32

Table 8-6: Mandatory and Extended (Optional) 1/S parameters.

8.3.1.5.1 Supported INP_min & delay_max settings

To verify what values of INP_min and delay_max are supported by the xDSL system under test the following configuration test can be performed

Test objective	Determine the downstream and upstream INP_min & delay_max settings supported by the xDSL system under test
Test configuration (Set-up)	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section “Test Loops” with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Procedure	Determine the supported INP_min & delay_max settings: ▪ Initialize the modem link with INP_min varying from 0 up to the maximum supported INP_min value. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end

	of this chapter. ▪ INP_min = 0 symbols ▪ Read out: o Actual INP dn o Actual delay dn o Actual INP up o Actual delay up ▪ Repeat the measurement for: INP_min = ½, 1, 2, 3, … , INP_min(max supported). ▪ Repeat each INP_min setting with delay_max = 4, 5, 6, … , 16ms and 32ms and 64ms. ▪ If the actual INP ≥ INP_min, the INP_min setting is supported ▪ If the actual delay ≤ delay_max, the delay_max setting is supported
Expectation	Overview of all the INP_min & delay_max settings supported by the xDSL system under test
Note: punctual verification of actual interleaving delays and Impulse Noise Protection belongs to the set of "xDSL performance" tests under impulsive noise (see the section "Testing Performance Under Noisy Stress Conditions").	

8.3.1.6 Alarm reporting tests

8.3.1.6.1 Loss of Link (LOL) tests

Test Objective	To verify the correct report of the Loss of Link alarm on the DSLAM.
Test Configuration	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a line profile according to the generic profile given in table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end of this chapter. § Let the modems train. § Disconnect the line cable form either the xTU-R or the xTU-C. § Check on the EM the line status and alarm indications.
Expected Result	The EM shall report the line as down(/disabled/not connected) and a Loss of Link (LOL) alarm along with a Loss of Signal (LOS) indication. Note: in this situation the absence of the signal form the line results in the LOS primitive at the DSLAM. Meanwhile, no power-off message (e.g. Dying Gasp for ADSL, power-status bits for SHDSL) has been received from the xTU-R. The two events (LOS AND no-power-off) are logically integrated into a LOL alarm.

8.3.1.6.2 Loss of Power (LOP) tests

Test Objective	To verify the correct report of the Loss of Power alarm on the DSLAM.
Test Configuration	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a line profile according to the generic profile given in table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end of this chapter. § Let the modems train. § Power off the xTU-R. § Check on the EM the line status and alarm indications.
Expected Result	The EM shall report the line as down(/disabled/not connected) and a Loss of Power (LOL) alarm along with a Loss of Signal (LOS) indication. Note: in this situation the absence of the signal form the line results in the LOS primitive at the DSLAM. Meanwhile, a power-off message (e.g. Dying Gasp for ADSL, power-status bits for SHDSL) has been received from the xTU-R. The two events (LOS AND power-off) are logically integrated into a LOP alarm.

8.3.1.6.3 Loss of Frame (LOF) tests

Test Objective	To verify the correct report of the Loss of Frame indication on the DSLAM.
Test Configuration	See figure 8-1. The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. There is no noise applied.
Method of Procedure	§ Set a line profile according to the generic profile given in table 8-2. The specific completion of the line profile should be based on realistic values and is left to the responsibility of the test engineer, examples can be found at the end of this chapter. § Let the modems train. § Generate on the line a sequence of micro-interruptions. The duration need to be short (some μs) to avoid the line drop; the micro-interruption rate need to be sufficiently high to generate a high BER condition. Check on the EM the line status and alarm indications.
Expected Result	The EM shall report the line as up(/enabled/connected) and a Loss of Frame (LOF) indication.

8.3.1.7 Loop Diagnostic Tests

This section defines tests related to the functionality of Loop Diagnostic on the line. A basic test for report of Loop Diagnostic parameters is specified first. Then tests on the accuracy of the Channel Characteristic function H(f) and of the Quiet Line Noise function QLN(f) are defined. As a matter of fact these functions represent the most important information about the status of the line for the purposes of maintenance, troubleshooting and for assessments of service upgrades.

8.3.1.7.1 Report of Loop Diagnostic parameters

Test Objective	To verify the correct report of Loop Diagnostic parameters on the DSLAM/ONU.
Test Configuration	See figure 8-3. The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. A Loop Diagnostic session is initiated from either the xTU-C or the xTU-R.
Expected Result	The Loop Diagnostic session is correctly established and related parameters are exchanged between the xTU-C and the xTU-R: § Channel Characteristics Function H(f) per sub-carrier; § Quiet Line Noise PSD QLN(f) per sub-carrier; § Signal-to-Noise Ratio SNR(f) per sub-carrier; § Line Attenuation (LATN); § Signal Attenuation (SATN); § Signal-to-Noise Margin (SNRM); § Attainable Net Data Rate (ATTNDR); § Actual Aggregate Transmit Power (ACTATP);

8.3.1.7.2 Accuracy test of Channel Characteristics Function H(f)

Test Objective	To verify the accuracy of the H(f) reported on the DSLAM/ONU.
Test Configura-tion	See figure 8-3. § The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. § No noise applied.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § Before actually performing the Loop Diagnostic session, while the loop is closed on both sides with the characteristic impedance of the xDSL system under test without connecting any equipment, measure the H(f) of the loop. Be this function $H_L(f)$. Be $H_{US}(f)$ the upstream Channel Characteristics Function (considered over the upstream carrier set appropriate for the xDSL system under test) measured by the ATU-C. Be $H_{DS}(f)$ the downstream Channel Characteristics Function (considered over the downstream carrier set appropriate for the xDSL system under test) transmitted by the ATU-R to the ATU-C. A Loop Diagnostic session is initiated from the ATU-C.
Expected Result	§ Both $H_{US}(f)$ and $H_{DS}(f)$ Channel Characteristics Functions per subcarrier are available at the ATU-C. In the defined upstream frequency range(s), the function MODULE(log10[|$H_{US}(f)$|]) (i.e. loop atten.) is equal to MODULE(log10[|$H_L(f)$|])) with a maximum error of TBD per subcarrier. In the downstream defined frequency range(s), the function MODULE(log10[|$H_{DS}(f)$|]) (i.e. loop atten.) is equal to MODULE(log10[|$H_L(f)$|])) with a maximum error of TBD per subcarrier.

8.3.1.7.3 Accuracy test of Quiet Line Noise PSD QLN(f)

Test Objective	To verify the accuracy of the QLN(f) reported on the DSLAM/ONU.
Test Configura-tion	See figure 8-3. § The xTU-C and xTU-R are connected through a loop according to the section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test. § Noise is injected on both sides of the loop. For example this noise could be composed of white noise + self-disturbers of the xDSL system under test.
Method of Procedure	§ Before actually performing the Loop Diagnostic session, while the loop is closed on both sides with the characteristic impedance of the xDSL system under test without connecting any equipment, measure at the xTU-C side the PSD of the noise signal actually injected on the loop. Be this function $QLN_C(f)$. Be $QLN_R(f)$ a similar function measured at the CPE side of the loop. Be $QLN_{US}(f)$ the upstream QLN function (considered over the upstream carrier set appropriate for the xDSL system under test) measured by the xTU-C. Be $QLN_{DS}(f)$ the downstream QLN function (considered over the upstream carrier set appropriate for the xDSL system under test) transmitted by the ATU-R to the ATU-C. A Loop Diagnostic session is initiated from the ATU-C.
Expected Result	§ Both $QLN_{US}(f)$ and $QLN_{DS}(f)$ Quiet Line Noise PSDs per sub carrier are available at the ATU-C. In the defined US frequency range(s), the $QLN_{US}(f)$ is equal to $QLN_C(f)$ with a maximum error of TBD per subcarrier. In the defined DS frequency range(s), the $QLN_{DS}(f)$ is equal to $QLN_R(f)$ with a maximum error of TBD per subcarrier.

8.3.1.7.4 Impulse Noise Monitoring

Impulse noise monitor (INM) shall provide information (independent of the current FEC and Interleaver settings) for the operator to determine the required INP_min and Delay_max settings for the current service/bit rate (active during measurement).
In order to determine the required **INP_min setting** the INM provides a histogram of Impulse Length (IL) counted in integer multiples of "impulse corrupted" DMT symbols. Figure 8-18 shows the INM functional block diagram.

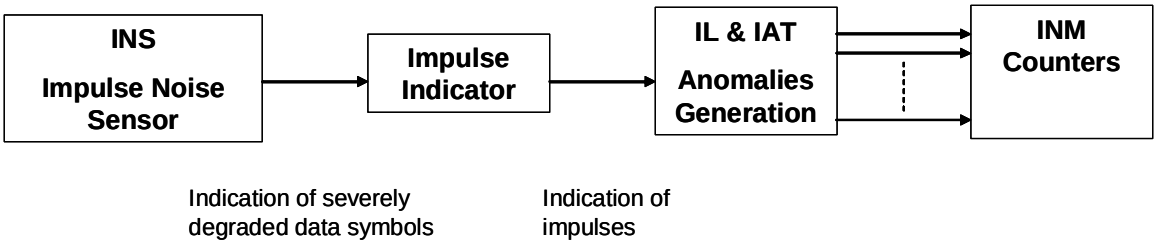


Figure 8-18: Impulse Noise Monitor Functional Block Diagram

The Impulse Noise Sensor (INS) indicates whether a data symbol is severely degraded or not. A data symbol is considered to be severely degraded when it would lead to severe errors on the gamma interface when there would be no Impulse Noise Protection (i.e. RS only used for coding gain). The implementation details for this sensor are vendor discretionary.
The Impulse Indicator indicates groups of consecutive severely degraded data symbols as Impulses. If a Sync symbol occurs between two corrupted data symbols, the Impulse Indicator shall disregard it.

The Impulse Length (IL) is defined as the number of data symbols in an Impulse.

If a sync symbol occurs between two consecutive groups of respectively N1 and N2 severely degraded data symbols, the two groups will form a single Impulse of length N1+N2 data symbols. The counters of these anomalies represent the IL histogram. By using the histogram of IL, the highest IL can be determined for which the probability of occurrence is not low enough to be within boundaries of Quality of Experience, if uncorrected. This IL value could be used as INP_min value.

The INM also includes a “pulse-gap-bridging” mechanism, i.e. to consider an impulse which is following a first impulse within a time interval (from end of impulse 1 to start of impulse 2) smaller than a certain value (“pulse-gap-bridging value”) as one long impulse. So, impulse noises that come as a correlated train of separate smaller impulses can be treated as one long impulse.

In order to determine the required **delay_max** setting, the INM provides a histogram of Inter-arrival Time (IAT) counted in integer multiples of DMT symbols. Inter-arrival time shall be defined as the time between the start of 2 impulses (after pulse-gap-bridging), expressed as an integer number of DMT symbols. In a REIN case, this would indicate directly the REIN period. By using the histogram of IT, the smallest IT is determined, for which the probability of occurrence is not low enough to be within boundaries of Quality of Experience, if uncorrected. This IT value could be used as delay_max value.

INM is still under study within the standardisation, e.g. there is still discussion about the characterisation of the different type of impulse noise events that exists and how INM it should interpret. Additionally, the parameters that have to be reported to determine the INP_min and delay_max correctly are under discussion.

INM is a useful tool that can help the operator to determine the best INP_min and delay_max setting. Test methods to test the INM configuration capabilities and performance will be necessary. However, test methods will be under study until INM is completely standardised.

8.3.1.8 SELT tests

This section defines tests related to the functionality of Single Ended Loop Testing (SELT) on the line. This functionality is not mandatory for a specific xDSL flavour. Nevertheless, as it requires the capability of transmitting a pulse signal with certain characteristics and to receive and analyse its echo as reflected by the line, it can be easily integrated into xDSL chipsets.
As shorter the stimulating pulse as more precise are these reflectometry techniques. Hence xDSL transceivers with a wider spectrum (such as VDLS2 ones) could achieve a better measurement resolution especially for short loops.

By means of the SELT measurements it is possible to assess the line length. Furthermore the SELT measurements allow identifying different types of impairment conditions through the copper loop down to the home wiring environment: presence of open or short circuits, of bridge taps.
Typically a SELT measurement is initiated by the DSLAM/ONU which receives and analyses the echo signal. Post processing of the information is done by the EM which provides results in the form of:

- line length estimation;
- termination type;
- TDR (Time Domain Reflectometry) graph.

These information are again fundamental for the purposes of maintenance, troubleshooting (especially under out-of-service conditions) and for assessments of service upgrades.

8.3.1.8.1 Loop length estimation test

Test Objective	To verify the correct assessment of the loop length by means of a SELT measurement.
Test Configura-tion	See figure 8-10 § The xTU-C is connected through a straight loop according to the section “Test Loops” with a loop length that is representative for the copper network. § The other side of the loop is terminated with an open or a short circuit.
Method of Procedure	A SELT session is initiated from the xTU-C.
Expected Result	The EM shall report SELT measurement results: § line length estimation; § termination type; § TDR (Time Domain Reflectometry) graph. The estimated line length is equal to the actual length with a maximum error of TBD%. (Note: the required accuracy may be change for different length ranges, as for longer loops the reflected signals is more attenuated with more uncertainty in the measurement) The reported termination type is coherent with the actual termination. The TDR graph is coherent with the one of a straight loop with the indication of the echo corresponding to the actual line length.

8.3.1.8.2 Loop length estimation test with bridge tap

Test Objective	To verify the correct assessment of the loop length in the presence of a bridge tap by means of a SELT measurement.
Test Configura-tion	§ See figure 8-10 and figure 8-11. The xTU-C is connected through a loop with a bridge tap according to the section “Test Loops” with a loop length that is representative for the copper network. § The other side of the loop is terminated with an open or a short circuit. § The bridge tap is terminated with an open or a short circuit.
Method of Procedure	A SELT session is initiated from the xTU-C.
Expected Result	The EM shall report SELT measurement results: § line length estimation; § termination type; § TDR (Time Domain Reflectometry) graph. The estimated line length is equal to the actual length with a maximum error of TBD%. (Note: the required accuracy may be change for different length ranges, as for longer loops the reflected signals is more attenuated with more uncertainty in the measurement) The reported termination type is coherent with the actual termination. The TDR graph is coherent with the one of a loop with a bridge tap. The indication of the echoes corresponding to the overall line length and to the distance at which the bridge tap is located.

8.3.1.9 PSD configuration tests

8.3.1.9.1 Band plan, limit PSD mask and US0 type

Test Objective	To verify the ability to configure the downstream and upstream band plan, limit PSD mask and US0 type on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in the section “Test Loops” with no noise applied.
Method of Procedure	§ Configure the xTU-C and xTU-R with the required band plan, limit PSD mask and US0 type § Set an xDSL line profile that demands a maximum bit rate and power spectrum use. The power mode, carrier masking and shaping (if supported) are all off. § Let the modems train. § Record the actual and attainable downstream and upstream bit rates and noise margin.
Expected Result	The EM shall report a band plan, limit PSD mask and US0 type value coherent with the one configured on the xDSL profile.

8.3.1.9.2 Maximum downstream and upstream PSD configuration test

Test Objective	To verify the ability to configure the maximum downstream and upstream PSD on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in the section "Test Loops" with no noise applied.
Method of Procedure	§ Set an xDSL profile that demands a maximum bit rate and power spectrum use. The power mode, carrier masking and shaping (if supported) are all off. § Let the modems train. § Record the actual and attainable downstream and upstream bit rates and noise margin. § Apply the above profile with a maximum downstream and upstream PSD reduced by 20dBm/Hz. § Let the modems train and record the actual and attainable downstream and upstream bit rates and noise margins.
Expected Result	The EM shall report a downstream and upstream PSD (or, as an alternative, aggregate downstream and upstream power) value coherent with the one configured on the profile. Correct downstream and upstream PSD configuration may be double checked also by verifying that after the configuration of a reduced downstream and upstream PSD, the attainable downstream and upstream rate is lower than the one with nominal downstream and upstream PSD. Comparison of the other recorded parameters may be of help in verifying that the downstream PSD configuration has taken place.

Note: punctual verification of the downstream PSD level belongs to the set of "Functional tests" (see section "Testing Transceiver Signal Characteristics").

8.3.1.9.3 RFI egress band configuration test

Test Objective	To verify the ability to configure the downstream RFI egress bands on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in the section "Test Loops" with no noise applied.
Method of Procedure	§ Set an xDSL profile that demands a maximum bit rate and power spectrum use. The power mode, carrier masking and shaping (if supported) are all off. § Let the modems train. § Record the "reference" actual downstream and upstream carrier load, the "reference" attainable downstream and upstream bit rates and noise margin and, if available, the "reference" SNR-pc. § Set an xDSL profile an egress RFI band set as "notched" . The related RFI band shall be as defined in the relevant recommendation (avoiding the pilot tone). § Let the modems train. § Record the actual downstream and upstream carrier load, the attainable downstream and upstream bit rates and noise margin and, if available, the SNR-pc.
Expected Result	The EM shall show a bit allocation table coherent with the notching of the specified RFI egress band (i.e. tones falling over the RFI band carry a very lower number of bits than with an undisturbed channel). The SNR-pc shall show the notching of the RFI egress band as compared with the "reference" SNR-pc. Correct downstream RFI egress band configuration may be double-checked also by verifying that the attainable downstream rate is lower than the one with no RFI egress band configured.

Note: punctual verification of the RFI bands configuration belongs to the set of "Functional tests" (see section "Testing Transceiver Signal Characteristics").

8.3.1.9.4 Downstream and Upstream Power Back-Off (PBO) configuration test

In FTTCab, FTTCurb and FTTB deployments, for coexistance of VDSL2 systems with xDSL ones deployed from the exchange, the DPBO and UPBO functionalities are adopted for PSD shaping.
Genearally speaking the DPBO settings depend on the distance between the Exchange and the Cabinet/Building and the electrical model of the cables between them.
The UPBO settings are little more difficult to define. Tipically they are defined by means of simulations with the aim of optimising the achievable US bitrate given the maximum length representative of the cable bundle deployed from that specific Cabinet/Building and under the hypothesis of the noise mix in that bundle.
For examples of VDSL2 profiles with DPBO and UPBO refer to the section at the end of this chapter.

Test Objective	To verify the ability to configure the downstream and/or upstream PBO on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in section “Test Loops” with no noise applied.
Method of Procedure	§ Set an xDSL that profile without PSD shaping. Other line profile parameters are arbitrary. § Let the modems train. § Record the “reference” actual downstream and upstream carrier load, the “reference” attainable downstream and upstream bit rates and noise margin and, if available, the “reference” SNR-pc. § Set an xDSL profile that defines DPBO and UPBO shaping. § Let the modems train. § Record the actual downstream and upstream carrier load, the attainable downstream and upstream bit rates and noise margin and, if available, the SNR-pc.
Expected Result	The EM shall show a bit allocation table coherent with the configured DPBO and UPBO shaping (i.e. monitored tones with reduced power carry a lower number of bits than with the “reference” PSD configuration). The SNR-pc shall show the expected PSD shaping due to the applied DPBO and UPBO settings, as compared with the “reference” SNR-pc. Correct DPBO and UPBO shaping configuration may be double-checked also by verifying that the attainable downstream and upstream rates are lower than those with no PSD shaping configured.

Note: punctual verification of the downstream and upstream PSD shaping belongs to the set of “Functional tests” (see section “Testing Transceiver Signal Characteristics”).

8.3.1.9.5 Downstream and upstream PSD shaping configuration test

In some deployment scenarios, an operator may choose to force xDSL modems to transmit at levels lower than those specified by the Limit PSD masks in the applicable recommendation. Besides power cut-back and power back-off, the MIB PSD mask is an additional tool that allows operators to shape the Transmit PSD that provide some control of the Transmit PSD. The MIB PSD mask shall lie at or below the Limit PSD mask specified in the selected recommendation. Its definition shall be under the network management control (a CO-MIB-controlled mechanism), as defined in G.997.1.

Test Objective	To verify the ability to configure the downstream and/or upstream PSD shaping on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in section “Test Loops” with no noise applied.
Method of Procedure	§ Set an xDSL that profile without PSD shaping. Other line profile parameters are arbitrary. § Let the modems train. § Record the “reference” carrier load. § Set an xDSL profile that uses PSD shaping, e.g. o A PSD shaped according to the PSD shaping rules defined in the country specific access rules. o A PSD shaped by easily reducing the power density of a number of DMT carriers. § Other line profile parameters are arbitrary. § Let the modems train. § Record the carrier load.
Expected Result	The EM shall show a bit allocation table coherent with the configured PSD shaping (i.e. monitored tones with reduced power carry a lower number of bits than with the “reference” PSD configuration).

Note: punctual verification of the downstream and upstream PSD shaping belongs to the set of “Functional tests” (see section “Testing Transceiver Signal Characteristics”).

8.3.1.9.6 Downstream and upstream Carrier mask configuration test

Test Objective	To verify the ability to configure the downstream and upstream carrier mask on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in “Test Loops” with no noise applied.
Method of Procedure	§ Set an xDSL profile that demands a maximum bit rate and power spectrum use. The power mode, carrier masking and shaping (if supported) are all off. § Let the modems train. § Record the actual downstream and upstream carrier load, the actual attainable downstream and upstream bit rates and noise margin. § Apply the above profile with a downstream and upstream carrier mask that inhibits the use of a set of 20 contiguous highly loadable tones (avoiding the pilot tone). § Let the modems train § Record the actual downstream and upstream carrier load, the actual attainable downstream and upstream bit rates and noise margin.
Expected Result	The EM shall show a bit allocation table coherent with the configured carrier mask (i.e. masked tones carry 0 bits). Correct carrier mask may be double checked also by verifying that, with the inhibition of the above tones, the attainable downstream and upstream rate is lower than the one with nominal carrier mask. Comparison of the other recorded parameters may be of help in verifying that the carrier mask configuration has taken place.

8.3.1.9.7 Maximum downstream and upstream aggregate power configuration test

Test Objective	To verify the ability to configure the maximum aggregate downstream and upstream power (i.e. aggregate output power) on a per-line basis.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop as defined in "Test Loops" with no noise applied.
Method of Procedure	§ Set an xDSL profile that demands a maximum bit rate and power spectrum use. The power mode, carrier masking and shaping (if supported) are all off. § Let the modems train. § Record the downstream and upstream maximum actual aggregate transmit power, the actual and attainable bit rates and noise margin. § Apply the above profile with a maximum downstream and upstream power reduced by 10 dBm. § Let the modems train § Record the downstream and upstream maximum actual aggregate transmit power, the actual and attainable bit rates and noise margin.
Expected Result	The EM shall report an aggregate downstream and upstream power value coherent with the one configured on the profile. Correct aggregate downstream and upstream power may be double checked also by verifying that after the configuration of a reduced aggregate downstream and upstream power, the attainable downstream and upstream rate is lower than the one with nominal aggregate output power. Comparison of the other recorded parameters may be of help in verifying that the aggregate downstream and upstream power configuration has taken place.

Note: punctual verification of the aggregate downstream and upstream power level belongs to the set of "Functional tests" (see section "Testing Transceiver Signal Characteristics").

8.4 Testing Transceiver Signal Characteristics

8.4.1 Introduction

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 band, up to 30 MHz.

In ETSI spectral management standard part 1 [x**5**] the access rules for each xDSL type are described by defining the requirements for the total signal power and PSD mask for different resolution bands. These requirements are defined as follows:

§ **Total signal power (aggregate power)**: the mean signal power into a constant resistive load $\mathbf{R_{ETSI}}$ shall not exceed a level of P_{max}, measured within a prescribed frequency band.
§ **Power Spectral Density (PSD) mask**: the narrow-band signal power (NBSP) into a resistive load impedance $\mathbf{R_{ETSI}}$, shall not exceed the prescribed PSD limits. The PSD masks are defined by so-called breakpoints, which specify the spectral power limit at a certain frequency. The complete PSD is constructed by drawing a straight line between the break points (defined on a logarithmic (Hz) - linear (dB) scale).

The section with test configurations, at the end of this chapter, provides examples of PSD masks and power back-off requirements being used in practice.

Other motives for testing the transceiver signal characteristics are some new features in the next generation xDSL systems, e.g. PSD shaping and power management. The purpose of PSD shaping is that the transmitted PSD within the boundaries of the mask and some pilot tone restrictions can be tailored to almost every PSD shaped wanted. One implementation of PSD shaping is VDSL/Cab PSD shaping, where the PSD of the VDSL/Cab system located in the street cabinet is shaped to protect the attenuated ADSL2+ systems from the local exchange.

8.4.2 Measurement difficulties

There are some difficulties to conquer before a PSD or aggregate power is measured correctly. This section lists these difficulties.

8.4.2.1 Offset and resolution errors in PSD measurements

The PSD, or Power Spectral Density, of a signal voltage is a quantity that is not related to any resolution bandwidth at all. Measuring PSD according to its definition would require an evaluation of the auto-correlation, followed by a Fourier transform.
Such an approach is inconvenient, and has made approximate measurements by means of spectrum analyzer the common approach. This approximation relies on the Wiener–Khinchin theorem (also spelled as *Khintchine*), that states that the narrow-band signal power, divided by the filter bandwidth, is a fair approximation of the PSD value. Such an approximation can easily result in various measurement errors, as will be explained below.

Many spectrum analyzers are constructed as selective voltmeters, using band filters that are not rectangular in shape, using logarithmic amplifiers to facilitate a device with high dynamic range, and using a top detector to identify the spectral “level” of a signal. An additional low-pass “video” filter behind that detector suppresses rapid variations of the detected signal, and is commonly present as well.
Such a device is an excellent instrument for measuring the spectral levels of harmonic signals but runs into trouble when measuring the PSD of signals that fill-up the full resolution band of the filters. The cumulation of the following effect can easily cause a resolution or offset error in PSD measurements:

- The resolution bandwidth (RBW) should be small enough to detect relevant variations in the PSD, but should not be too small.
- The RBW is often representing the 3dB bandwidth of the filter, while the exact filter shape outside this RBW is also influencing on what the detector will indicate.
- When two signals, with the same PSD but with very different time domain characteristics, subsequently arrive at the top detector of a spectrum analyzer, it will indicate two different values. Think of two signals where one has a low crest factor and the other a high crest factor. The top detector will indicate higher values for the second signal.

- The log conversion in the analyzer will also respond differently on the crest factor; high peaks will be more suppressed then low peaks, making the PSD measurement even more dependent on the time-domain characteristics of the signal under test.
- The level presented on the analyzer screen will a slightly change with the settings of the low-pass video filter.

Spectrum-analyzers are often calibrated for harmonic signals only. Without special measures, the above reasons can easily cause an offset error of a few dB when measuring the PSD of stationary signals that are random in nature.

A solution against the above resolution errors does hardly exist. Only the combination of multiple measurements (with different RBW-values) can bring a pragmatic solution: for instance using 1 kHz near steep edges of a PSD, and 10 or 100 kHz near flat parts of the spectrum.
A solution for minimizing above offset errors is an *additional* calibration by means of a source with ***known*** PSD level. This result in a correction factor to adjust the value derived from the "narrow-band signal power" divided by the "resolution bandwidth". A suitable source with known PSD level might be a synthetic noise source that generates a rectangular spectrum (see figure 8-19). If the aggregate power is measured with an accurate ***true*** RMS meter (that really *squares* the signal voltage before its *mean* values is determined) one can reconstruct the in-band PSD value. Figure 8-20 illustrates how the spectrum of such a synthetic signal will appear on the screen of a spectrum analyzer (without any offset correction or transformation from [dBm] into [dBm/Hz]).

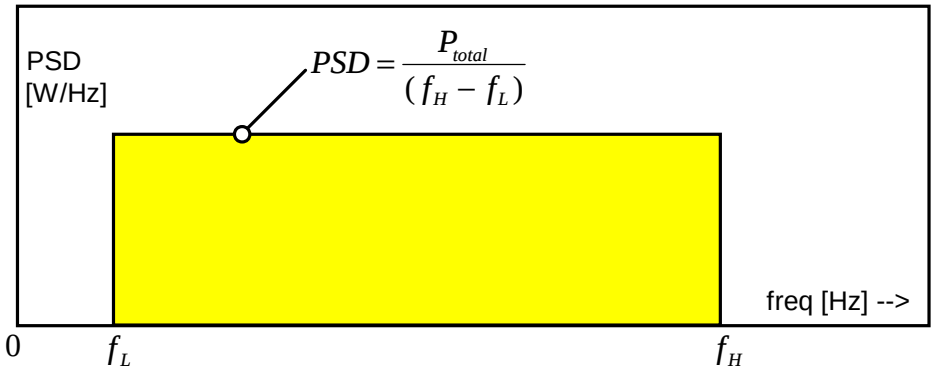


Figure 8-19 Target PSD of a synthetic calibration signal.

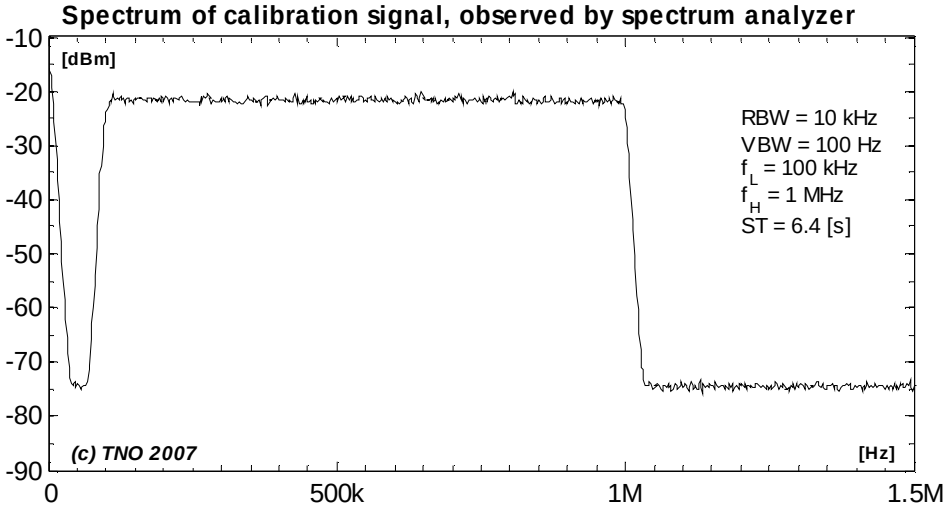


Figure 8-20: Spectrum of the synthetic signal of figure 8-19, as it will appear on the screen of a spectrum analyzer.

This calibration principle works as follows. When the aggregate power P_{total} of the synthetic noise is measured with a ***true*** RMS meter, and when the band (f_H-f_L) is known, the PSD-level of the in-band signal can easily be derived (see expression in figure 8-19) . If (f_H-f_L) is much wider then the resolution bandwidth of the spectrum analyzer, the offset between observed PSD (by the spectrum analyzer), and true PSD value can be found. Note that this calibration is only valid when the analyzer settings do not change afterwards, and when the time-domain characteristics of the signal under test are equivalent with those from the synthetic noise generator.

8.4.2.2 Impedance mismatch and far-end injection

The ideal method for measuring the PSD or the aggregate power of an xTU-C or xTU-R is to have the modem under test sending its transmit signal without a counterpart modem, into a constant resistive reference impedance to which the modem under test is connected. In DSL Forum TR-067 this is referred to as “continuously sending” mode. The ETSI requirements are specified with respect to these nominal conditions as shown in figure 8-21.

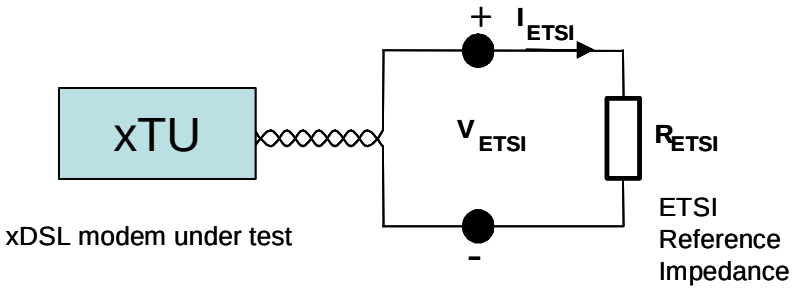


Figure 8-21 Nominal conditions according to ETSI.

Marketplace products (and also evolution prototypes) seldom offer this mode of operation. So, the nominal conditions for which the ETSI requirements hold differ from the practical lab conditions in which the compliance measurements will be taken. The PSD and aggregate power measurements are traditionally performed with xTU-C and xTU-R connected together via a test loop or cable simulator, as depicted in figure 8-22.

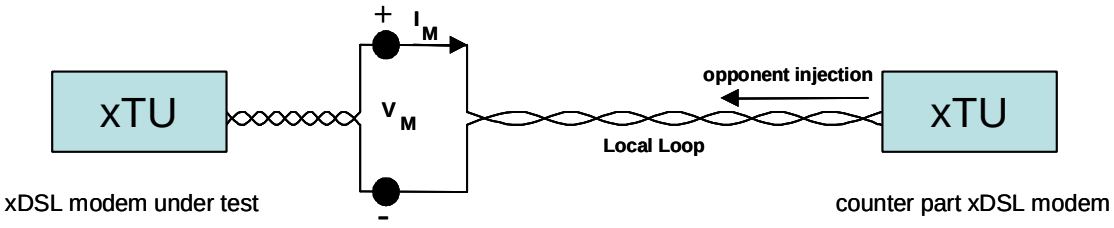


Figure 8-22 General practical lab conditions.

Note that in case of the traditionally performed PSD and aggregate power measurements, under lab conditions, the modem under test is connected to a test loop or loop simulator terminated by the load impedance of its opponent. Both the impedance of the test loop and the load of the counter part modem are complex while under nominal conditions the modem is connected to constant resistive reference impedance. These differences between the nominal and practical lab conditions will complicate the compliance measurements and affect their results. The following complications can be observed:

- Due to the presence of a counter part modem, the outcome of the compliance measurements (spectrum and RMS value of the measured voltage) taken at the xTU-C Port (or the xTU-R port) will be increased by the attenuated PSD transmitted by the opponent (counter part injection). In case of systems using echo cancellation for their bidirectional bit transfer, the influence of the counter part modem can be considerable for short test loops, while for the longer test loops it might be negligible. In case of Frequency Division Duplexed (FDD) systems, the influence of the counter part modem is for short and long loops negligible.
- Due to the impedance of the test loop terminated by the load impedance of the counter part modem, the outcome of the compliance measurements taken at the xTU-C Port (or the xTU-R port) will give a wrong interpretation of spectral behaviour of the modem under test. The prescribed constant resistive reference impedance R_{ETSI} approximates the design impedance for most DSL technologies as good as possible (e.g., HDSL and SDSL is equal to 135Ω, whereas for ADSL R_{ETSI} is 100Ω). While the complex impedance of the test loop terminated by the load impedance of the counter part modem as function of the frequency vary in the range about 100Ω up to 1000Ω. As a result the measured PSD can have a value that is about 10% higher than the real transmitted PSD.

Both complications will result in a measured total power and PSD that is not directly comparable to the prescribed requirements. To enable an appropriate evaluation of the measured PSD and the total power they should be compensated for both complications.

Impedance mismatch compensation

To compensate for the impedance mismatch, the complex input impedance of the test loop terminated by the load impedance of the counter part modem must be determined.
With this complex input impedance, the relation between the voltage measured over the ETSI nominal impedance and the voltage measured over the test loop (or loop simulator) terminated by the counter part modem can be determined from which the measured total power or PSD can be compensated to comparable values.

Far end injection compensation

One method to keep the effects of the injected signal sent from the counterpart xTU as small as possible, is to measure the xDSL signal at Transmitter side in case the counterpart transmit signal is sufficiently attenuated. This can be achieved by connecting the xTU-C and xTU-R via a simulation circuitry with high attenuation. The test setup shall provide sufficient isolation between the two modems, so that:

1. the modem under test sends a "regular" xDSL showtime signal as it is connected to a counterpart modem;
2. the xDSL signal can be measured at Transmitter side, meanwhile the signal sent from the counterpart xTU is sufficiently attenuated to have negligible effects in the band over which the PSD measurement is performed.

Figure 8-23 shows an attenuator that may be used for PSD and aggregate power measurement tests:

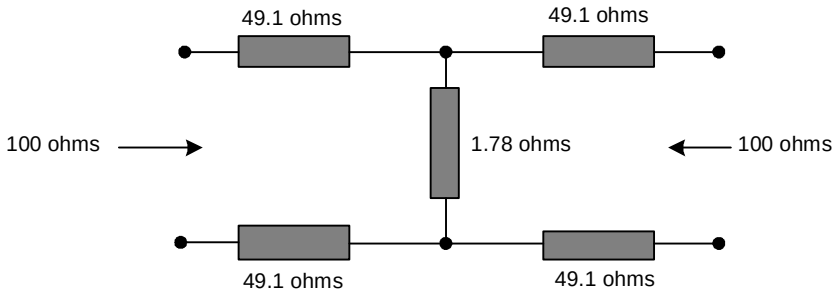


Figure 8-23: 40 dB attenuator.

However, there are test cases that require that the transceiver characteristics are measured when the xTU-C and xTU-R connected via short test loops, e.g., in case of power cut back tests. For these cases, the measured PSD can be compensated for far end injected when the PSD's on both sides of the xDSL link is measured. Namely, the PSD measured at xTU-1 will be the combination of the PSD transmitted by the xTU-1 (e.g., xTU under test) and the (attenuated) PSD transmitted by the remote (Far-End) xTU-2. The same holds for the total signal power measured at xTU-1, it consists of the sum of the power transmitted by xTU-1 and the (attenuated) power transmitted by xTU-2. Formulating this into an equation results in equation (1) with three unknown variables, PSD_{xTU-1}, PSD_{xTU-1} and the attenuation of the test cable $\alpha_{Test\ Cable}$. To solve this equation, we need an additional measurement at the xTU-2 resulting in equation (2).

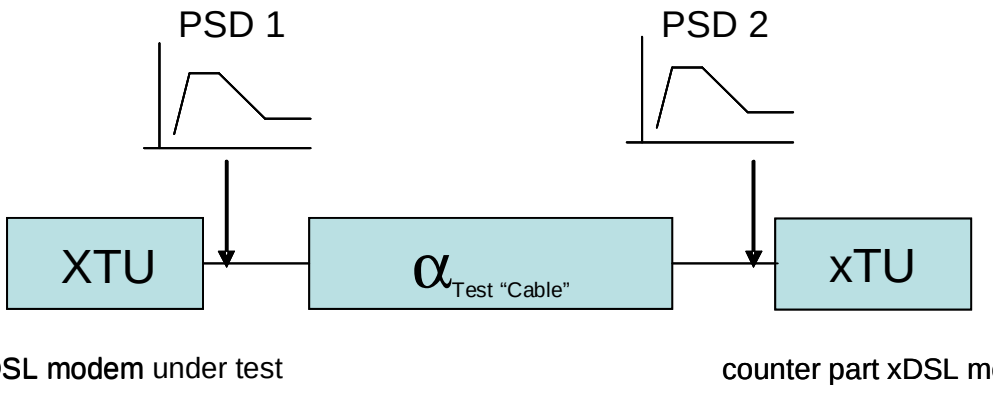


Figure 8-24: PSD Far-End compensation.

Equation 1: $PSD\ 1 = PSD_{xTU\text{-}1} + \alpha^2_{Test\ Loop} \times PSD_{xTU\text{-}2}$

Equation 2: $PSD\ 2 = PSD_{xTU\text{-}2} + \alpha^2_{Test\ Loop} \times PSD_{xTU\text{-}1}$

With these two equations $PSD_{xTU\text{-}1}$ and $PSD_{xTU\text{-}2}$ can be determined.

8.4.2.3 Calibration

When the PSD is measured using a spectrum analyzer, the output must be calibrated to obtain the proper PSD in dBm/Hz. A PSD is measured at the transmitter side under study using a high impedance differential voltage probe connected to a spectrum analyzer. The latter is assumed to measure the voltage over a so-called resolution bandwidth. Internally this voltage spectrum is translated to dBm using the spectrum analyzers reference impedance (normally 50 or 75 Ω). To obtain the PSD in dBm/Hz the right noise bandwidth must be determined. The method to obtain the right noise bandwidth is performed during the calibration of the spectrum analyzer.

8.4.2.3.1 Spurious response errors in out-of-band spectra

Non linear effects at the input of a spectrum analyzer cause a (weak) inter-modulation of all spectral components in a signal. Since the spectra generated by xDSL transmitters are usually spread-out over a wide frequency band, all these inter-modulation products will also be spread-out over a wide frequency interval. This effect is called “spurious response” and will manifest itself as if an extra noise floor is added to the spectrum being measured.
This effect is weak in state-of-the-art spectrum analyzers, but cannot be ignored when spectral differences are exceeding values in the order of 50 dB. Especially when measuring out-of-band spectra, this may become a problem.

A solution against “spurious response” in out-of-band measurements is using a passive analog filter to remove most of the in-band power, before the filtered signal is fed to the spectrum analyzer. If this filter has steep edges, and a known filter response, the measured spectra can be adjusted afterwards to compensate for non-ideal filter curves.

8.4.3 Testing total transmit power

The total transmit power is the power aggregated over a frequency band that is significantly wider than 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.
As mentioned in the previous section, a reliable measurement requires that at least the specific characteristics of the test setup (load impedance, pass-band) are met. When power back-off characteristics are to be analysed, the setup should facilitate different PBO settings by using different loop lenghts.

For all the PSD and power measurements specified in the test cases below the general test procedures defined in the previous section shall be applied.

The PSD and aggregate transmit power of DMT modulated xDSL systems depends on the used set of DMT carriers and the PSD value of these carriers. By masking and shaping the PSD and the aggregate power, if supported by the xDSL system under test, can be changed. Before the measurement, the PSD and transmit power parameters in the line configuration should be checked and set on the required settings, e.g. according to the valid access rules.

8.4.3.1 Downstream and Upstream aggregate transmit power measurement test

Test Objective	To measure the aggregate downstream and upstream power (i.e. aggregate output power) and verify its compliance with the power limits specified in the relevant recommendation or region depended access rules.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a long test loop to attenuate the far-end-injection with no noise applied. In case PBO mechanisms are included to be tested, the xTU-C and xTU-R are connected through several short test loops, so far-end-injection needs to be compensated as prescribed in the previous sections.
Method of Procedure	• Set the xDSL line profile containing those PSD parameters and mechanism to be tested, e.g. PBO and shaping. • Let the modems train • Measure the downstream total power at the XTU-C over the signal band defined in the relevant recommendation. • Measure the upstream total power at the XTU-R over the signal band defined in the relevant recommendation. • Compensate the outcome for impedance mismatch and far-end-injection (see the previous sections).
Expected Result	The aggregate downstream and upstream power shall fulfil the power limits, relevant to the XTU-C implementation under test, as defined in the relevant recommendation or country specific access rules.

8.4.3.2 Downstream and Upstream Power Cut-Back (PCB) test

The implementation details of PCB of ADSL1 and SDSL are well standardised while the details of the PCB implementation for the second generation xDSL systems are left open.

The PCB implementation of ADSL1 is only defined for the downstream transmit PSD; the ADSL1 PCB function reduces the downstream transmit PSD when the received upstream power exceeds some specified level. The PCB implementation of SDSL is applied for both transmit directions and is based on the "estimated power loss". So, the PCB of these first generation xDSL systems is based on the power level of the received signal.

The PCB implementation in next generation xDSL systems is up to the vendor. For ADSL2+ the application of downstream and upstream PCB depends on negotiation between the counterpart transmitter and receiver and it is mainly driven by this latter. Typically ADSL2+ DSLAMs do not require the application of upstream PCB to counterpart CPEs and, like in ADSL1, upstream power lays around 12 dBm. On the other hand some ADSL2+ CPEs require to the DSLAM to apply an ADSL1-like PCB mechanism while other CPEs are able to operate in full power (around 19 dBm) from the DSLAM even with null loop (i.e. no downstream PCB applied).

Test Objective	To verify the the Power Cut-Back mechanism on the aggregate downstream and, if applicable, the upstream power and verify its compliance with the power limits specified in the relevant recommendation or region depended access rules.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop that is varied in length so that the attenuation is increased from 0 to 14 dB (@300 kHz).
Method of Procedure	• Set the xDSL line profile without PSD shaping. • For each loop length: – Let the modems train – Measure the downstream total power at the XTU-C over the signal band(s) defined in the relevant recommendation. – Measure the upstream total power at the XTU-R over the signal band(s) defined in the relevant recommendation. – Compensate the outcome for impedance mismatch and far-end-injection (see the previous sections) • Generate graphs of the aggregate downstream and upstream power as a function of the loop length or attenuation @300kHz.
Expected Result	Where mandatory, the aggregate downstream power shall show the application of the PCB mechanism. Generally speaking the graphs of the aggregate downstream and upstream power as a function of the loop length allow to understand the PCB policies applied by the implementations under test.

8.4.4 Power Spectral Density

Power Spectral Density measurement tests have the objective of verifying that the xTU-C and xTU-R PSDs do not exceed the masks set forth by relevant recommendation or country specific access rules. These measurements should include both the passband and stopband frequencies.

Hence the test setup shall support the PSD mask measurement over the entire downstream and upstream band(s) and provide enough dynamic range to allow the measurements be done over both the passband and stopband frequencies into a given resolution bandwidth (typically 10 kHz).

8.4.4.1 Downstream and upstream PSD measurement test

Test Objective	To measure the downstream and upstream PSD and verify its compliance to the PSD mask specified in the relevant recommendation or country specific access rules.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a long test loop to attenuate the far-end-injection. There is no noise applied. For multi-band systems like VDSL2, the xTU-C and xTU-R may be connected through short test loops, so far-end-injection needs to be compensated as prescribed in the previous sections. Alternative for multi-band systems The measurement may be divided into several sub-measurements with the systems configured to switch on one single downstream band and one single upstream band (of the chosen bandplan) at a time. These bands may be adjacent. Each sub-measurement would reduce itself to a single-band PSD measurement and the configured loop length would be as long as possible while guaranteeing that all the carries are loaded.
Method of Procedure	• Set the xDSL line profile containing those PSD parameters to be tested. • Let the modems train • Measure the PSD at the xTU-C over the signal band(s) defined in the relevant recommendation; use the calibration method and filtering as described in the previous sections. • Measure the PSD at the xTU-R over the signal band(s) defined in the relevant recommendation; use the calibration method and filtering as described in the previous sections. • Compensate the measured PSD for impedance mismatch and far-end-injection (see the previous sections).
Expected Result	The downstream and upstream PSD shall fulfil the mask (if applicable related to a bandplan and profile), relevant to the xTU-C and xTU-R implementation under test, as defined in the relevant recommendation or country specific access rules.

8.4.4.2 RFI egress band measurement test

This test completes "RFI egress band configuration test". Additional to the verification of the correct configurability of the feature, with this test it is measured that the line signal fulfils the configured PSD shaping with RFI band notching.

Test objective	To measure the actual PSD and verify it fulfils the configured shaping with RFI band notching. For certain xDSL systems it is required that several arbitrary frequency bands are notched simultaneously and that the PSD of the transmitted signal is

	reduced below a specific level in those bands.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a chosen loop with a loop length that is xDSL dependent. The resulting signal attenuation must be limited to allow the system under test to use carries over the whole frequency band. There is no noise applied For multi-band systems like VDSL2, the xTU-C and xTU-R may be connected through short test loops, so far-end-injection needs to be compensated as prescribed in the previous sections. Alternative for multi-band systems The measurement may be divided into several sub-measurements with the systems configured to switch on one single downstream band and one single upstream band (of the chosen bandplan) at a time. These bands may be adjacent. Each sub-measurement would reduce itself to a single-band PSD measurement and the configured loop length would be as long as possible while guaranteeing that all the carries are loaded.
Method of Procedure	§ Set an xDSL line profile that sets an egress RFI band as "notched". The related RFI band shall be as defined in the relevant recommendation (avoiding the pilot tone). § Let the modems train and measure the PSD at the xTU-C and the xTU-R over the relevant signal band.
Test Result	With reference to the nominal downstream and upstream PSD measured in test "Downstream and Upstream PSD measurement test", the measured downstream and upstream PSD shall show the notching in the frequency range of the configured RFI egress band(s) and, where required, the PSD level shall be below the one specified by the relevant recommendation.

8.4.4.3 Downstream and upstream carrier mask measurement test

This test completes test "Downstream and Upstream carrier mask configuration test". Additional to the verification of the correct configurability of the feature, with this test it is measured that the line signal fulfils the configured carrier mask.

Test Objective	To measure the actual downstream and upstream PSD and verify it fulfils the configured carrier mask.
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a chosen loop with a loop length that is xDSL depending. The resulting signal attenuation must be limited to allow the system under test to use carries over the whole frequency band. There is no noise applied.
Method of Procedure	• Set an xDSL line profile that sets a carrier mask that inhibits the use of masked tones in the frequency band defined in the relevant recommendation (avoiding the pilot tone). • Let the modems train and measure the PSD at the xTU-C and the xTU-R over the relevant signal band. • Monitor all the tones by checking the carrier load and compare them with the configured carrier mask.
Expected Result	With reference to the nominal downstream and upstream PSD measured in "Downstream and Upstream PSD measurement test", the measured downstream and upstream PSD shall show a negligible power level over the frequency range corresponding to actually masked tones.

8.4.5 Power Back Off

Power Back Off (PBO) is implemented to save power, reduce crosstalk to other xDSL systems in the same loop and to limit the received power level for the counter part connected to short loops to prevent signal distortion. In case of VDSL/Cab upstream PBO the VDSL/Cab links connected to short loops have a reduced power level which protects the links on long loop length with high signal attenuation.
The Power Back-off 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).

UPBO (specified for VDSL2) is pointed out to solve the Near-Far problem on the VDSL2 upstream performance. 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. UPBO tries to reduce the power level of the upstream transmit PSD of the shorter lines.

DPBO (specified for ADSL2(+) and VDSL2) is aimed to solve the spectral compatibility issue between legacy DSL technologies deployed from the CO and DSL 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. DPBO mitigates the spectral incompatibility between ADSL2+ and VDSL2 is also known as *PSD shaping*. The transmit PSD is shaped through the so called “MIB PSD mask” that allows operators to shape the transmitted PSD to almost every PSD shaped wanted within the boundaries of the mask and some pilot tone restrictions. 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.

PSD shaping may be mandatory by the network provider, assimilated into the access rules.

8.4.5.1 Downstream and upstream PSD shaping measurement test

This test completes test “Downstream and Upstream PSD shaping configuration test”. Additional to the verification of the correct configurability of the feature, with this test it is measured that the line signal fulfils the configured PSD shaping.

Test Objective	To measure the actual downstream and upstream PSD and verify it fulfils the configured shaping.

Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a loop which can depend on the PSD shaping. There is no noise applied. For multi-band systems like VDSL2, the xTU-C and xTU-R may be connected through short test loops, so far-end-injection needs to be compensated as prescribed in previous sections. Alternative for multi-band systems The measurement may be divided into several sub-measurements with the systems configured to switch on one single downstream band and one single upstream band (of the chosen bandplan) at a time. These bands may be adjacent. Each sub-measurement would reduce itselt to a single-band PSD measurement and the configured loop length would be as long as possible while guaranteeing that all the carries are loaded.
Method of Procedure	• Set an xDSL line profile using PSD shaping according to country specific access rules or a free chosen test shape. • Let the modems train and measure the PSD at the xTU-C over the signal band defined in the relevant recommendation, use the calibration method. • Compensate the measured PSD for impedance mismatch and far-end-injection.
Expected Result	With reference to the nominal downstream and upstream PSD, the measured shaped PSD's shall show a PSD according to the requested shape.

8.4.5.2 Downstream Power Back Off measurement test

Test Objective	To measure the modified transmit PSD mask based on the DPBO configuration parameters
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a long test loop to attenuate the far-end-injection. There is no noise applied. For multi-band systems like VDSL2, the xTU-C and xTU-R may be connected through short test loops, so far-end-injection needs to be compensated as prescribed in the previous sections. Alterantive for multi-band systems The measurement may be divided into several sub-measurements with the systems configured to switch on one single downstream band and one single upstream band (of the chosen bandplan) at a time. These bands may be adjacent. Each sub-measurement would reduce itselt to a single-band PSD measurement and the configured loop length would be as long as possible while guaranteeing that all the carries are loaded.
Method of Procedure	• Set the xDSL line profile containing relevant DPBO settings (note: test may be repeated for different values of DPBOESEL) • Let the modems train • Query the management system to obtain the upstream and downstream power. • Measure the PSD at the xTU-R and xTU-C over the signal band defined in the relevant recommendation, use the calibration method. • Measure the downstream total power at the XTU-C over the signal band(s) defined in the relevant recommendation. • Measure the upstream total power at the XTU-R over the signal band(s) defined in the relevant recommendation. • Compensate the measured PSD for impedance mismatch and far-end-injection
Expected Result	The downstream PSD shall fulfil the mask resulting from the applied DPBO configuration as specified in G.997.1. The downstream ATP shall not exceed the maximum ATP prescribed for the configured xDSL profile.

8.4.5.3 Upstream Power Back Off measurement test

Test Objective	To measure the modified transmit PSD mask based on the UPBO configuration parameters
Test Configuration	See figure 8-2. The xTU-C and xTU-R are connected through a long test loop to attenuate the far-end-injection. There is no noise applied. For multi-band systems like VDSL2, the xTU-C and xTU-R may be connected through short test loops, so far-end-injection needs to be compensated as prescribed in previous sections. Alternative for multi-band systems The measurement may be divided into several sub-measurements with the systems configured to switch on one single downstream band and one single upstream band (of the chosen bandplan) at a time. These bands may be adjacent. Each sub-measurement would reduce itselt to a single-band PSD measurement and the configured loop length would be as long as possible while guaranteeing that all the carries are loaded.
Method of Procedure	• Set the xDSL line profile containing relevant UPBO settings; more specifically the parameter UPBOKL (kl_0) shall be forced (note: test may be repeated for different values of UPBOKL) • Let the modems train • Query the management system to obtain the upstream and downstream power. • Measure the PSD at the xTU-R and xTU-C over the signal band defined in the relevant recommendation, use the calibration method. • Measure the downstream total power at the XTU-C over the signal band(s) defined in the relevant recommendation. • Measure the upstream total power at the XTU-R over the signal band(s) defined in the relevant recommendation. • Compensate the measured PSD for impedance mismatch and far-end-injection
Expected Result	The downstream PSD shall fulfil the mask resulting from the applied UPBO configuration as specified in G.997.1. The upstream ATP shall not exceed the maximum ATP prescribed for the configured xDSL profile.

8.4.6 Power management

First generation xDSL supports only an “on” and an “off” state. Second generation xDSL supports more advanced power management functionality; it can reduce the overall power consumption while maintaining the always-on functionality. With several millions of deployed DSL modems, a significant amount of energy can be saved if the modems engage in this “standby/sleep” state. Furthermore from a spectral management point of view, the cross talk reduces when unused modems are sleeping.
A second generation xDSL line has three possible power management states, namely:

- *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.*

8.4.6.1 Power management tests

A prerequisite for the following tests is that the aggregate transmit power at both the xTU-C and xTU-R in L0 state is measured beforehand with the reference conditions applied throughout these tests:

§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s.
Power states transitions are enabled.

§ The xTU-C and xTU-R are connected through a chosen loop with a loop length that is xDSL dependent. The resulting signal attenuation shall be sufficient to avoid application of any PBO, still not to high to allow the system under test to synchronise at fairly high rates.
§ AWGN @ -140dBm/Hz shall be applied to both ends of the loop.

Be X_{DS} dBm the DS aggregate transmit power measured at the xTU-C in the above reference conditions.
Relevant link parameters (actual and attainable bit rates, noise margins, transmitted power and loop attenuation) shall be noted down from the DSLAM/ONU management system.

8.4.6.2 Entry into L2 state from L0 state test

Test Objective	To verify the correct transition from L0 to L2 state as initiated from xTU-C (management command or Layer 2/3 traffic cease). To verify the correct application of downstream PCB associated to the L2 Request.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Expected Result	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The minimimum data rate in L2 mode is set to 128 kbit/s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L0 state. Procedure 1 L0 to L2 state transition request initiated from xTU-C, associated with a minimum and maximum downstream Power Cut Back (PCBds) equal to 10 dB. Procedure 2 L0 to L2 state transition request triggered by a sudden ceasing of Layer 2/3 traffic (i.e.: end of a ping command or FTP download).

Expected Result	Procedure 1 § The transition is GRANTed (i.e: not rejected) by the xTU-R. § The measured downstream aggregate transmit power equals (X_{DS} -10)±1 dBm. § Other relevant link parameters are changed coherently: the downstream rate is reduced and this is reflected by the downstream bin allocation. The transition takes place without dropping the line or occurrence of CRC errors. Procedure 2 § The transition is GRANTed (i.e: not rejected) by the xTU-R. § The downstream rate is lowered down to the minimum data rate in L2 mode (128 kbit/s) and this is reflected by the downstream bin allocation. § Other relevant link parameters are back to their initial values. The transition takes place without dropping the line or occurrence of CRC errors.

8.4.6.3 Exit from L2 state to L0 state test

Test Objective	To verify the correct transition from L2 to L0 state as initiated from either xTU-C or xTU-R (management command or Layer 2/3 traffic initiation). To verify that line parameters are brought back to the initial values in L0 state.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section ”Test Loops” with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The minimum data rate in L2 mode is set to 128 kbit/s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. The xTU-C and xTU-R are in L2 state. Procedure 1 L2 to L0 state transition request initiated from either xTU-C or xTU-R. Procedure 2 L0 to L2 state transition request triggered by initiation of Layer 2/3 traffic flow (i.e: ping command or FTP download) .
Expected Result	For both Procedure 1 and 2 § The transition is GRANTed (i.e: not rejected) by the xTU-R or xTU-C. § The measured downstream aggregate transmit power is back to the initial value of X_{DS} dBm in the original L0 state. § Other relevant link parameters are back to their initial values. The transition takes place without dropping the line or occurrence of CRC errors.

8.4.6.4 L2 Trim test

Test Objective	To verify the correct application of DS PCB associated to an L2 Trim Request.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The minimum data rate in L2 mode is set to 128 kbit/s. § The L2-ATPR is set to 11 dB § The xTU-C and xTU-R are in L0 state. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. The xTU-C and xTU-R are in L2 state. Procedure 1 1. L0 to L2 state transition request initiated from xTU-C, associated with a minimum and maximum downstream Power Cut Back (PCBds) equal to 6 dB. 2. L2 Trim Request initiated from xTU-C, associated with a proposed new downstream Power Cut Back (PCBds) equal to 10 dB. Note: given the initial high downstream rate condition, the overall PCB of 16 dB should still allow a valid operating condition, hence acceptance of the trim by the xTU-R.
Expected Result	1. The L0 to L2 transition is GRANTed by the xTU-R (as in “Entry into L2 state from L0 state test”). § The L2 Trim Request is GRANTed (i.e: not rejected) by the xTU-R. § The measured downstream aggregate transmit power equals X_{DS} dBm. § Other relevant link parameters are changed coherently: the downstream rate is reduced but still above the minimum data rate in L2 mode (128 kbit/s); this is reflected by the downstream bin allocation. The transition takes place without dropping the line or occurrence of CRC errors.

8.4.6.5 L2 Trim with L2-ATPR violation test

Test Objective	To verify the respect of the L2-ATPR parameter as the maximum PCB value allowed for an L2 Trim Request.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The L2-ATPR is set to 11 dB. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L0 state. 1. L0 to L2 state transition request initiated from xTU-C, associated with a minimum and maximum downstream Power Cut Back (PCBds) equal to 6 dB. 2. L2 Trim Request initiated from xTU-C, associated with a proposed new downstream Power Cut Back (PCBds) equal to 12 dB.
Expected Result	§ The L0 to L2 transition is REJECTed by the xTU-R. § No downstream PCB is applied nor downstream rate change is observed.

8.4.6.6 L0-time test

Test Objective	To verify the respect of the L0-time parameter as the minimum duration within link state L0 (before transition to a different link state).
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The L0-time is set to 60 s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L2 state. 1. L2 to L0 state transition request initiated from xTU-C. 2. L0 to L2 state transition request initiated from xTU-C within 30 s.
Expected Result	§ The L2 to L0 transition is GRANTed by the xTU-R (as in "Entry into L2 state from L0 state test"). § The L0 to L2 transition is REJECTed by the xTU-R.

8.4.6.7 L2-time test

Test Objective	To verify the respect of the L2-time parameter as the minimum duration within link state L2 before using the power trim procedure.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The L2-time is set to 75 s. § The xTU-C and xTU-R are connected through a chosen loop with a loop length that is xDSL dependent. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L0 state. 1. L0 to L2 state transition request initiated from xTU-C. 2. L2 Trim request initiated from xTU-C within 60 s.
Expected Result	§ The L2 to L0 transition is GRANTed by the xTU-R (as in "Entry into L2 state from L0 state test"). § The L2 trim request is REJECTed by the xTU-R.

8.4.6.8 Entry into L3 state from L0 state test

The test for "entry into L3 state" is specified only for L0 to L3 transition triggered by an xTU-C or xTU-R command.
Other entries to L3 may be from L0 or L2 as related to a Loss of Power issued by the xTU-R. Such cases are covered by the Loss of Power test.

Test Objective	To verify the correct transition from L0 to L3 state as initiated from either xTU-C or xTU-R.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section "Test Loops" with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L0 state. L0 to L3 state transition request initiated from either xTU-C or xTU-R.
Expected Result	§ The transition is GRANTed (i.e: not rejected) by the xTU-R (or xTU-C). § Both xTUs stop transmission.

8.4.6.9 Exit from L3 state to L0 state test

The test for “exit from L3 state” is specified in the case of xTU-R still powered on, though in idle state.

Test Objective	To verify the correct transition from L3 to L0 state as initiated from xTU-C.
Test Configuration	See figure 8-1. § The xTU-C and xTU-R are connected through a loop according to section “Test Loops” with a loop length that is representative for the deployment of the xDSL system under test.
Method of Procedure	§ xDSL profile shall be configured in Rate Adaptive mode with minimum data rates set to 32 kbit/s. § The minimum data rate in L2 mode is set to 128 kbit/s. § AWGN @ -140dBm/Hz shall be applied to both ends of the loop. § The xTU-C and xTU-R are in L3 state. The xTU-R power switch is in the ON position. L3 to L0 state transition request initiated from xTU-C.
Expected Result	§ The transition is GRANTed (i.e: not rejected) by the xTU-R. § A short initialisation procedure starts and it is completed within 3 s. Achieved DS aggregate transmit power and relevant link parameters shall be similar to those in the original L0 state. Note: the short initialisation procedure is anyway a brand new initialisation which is not supposed to bring back exactly the same link condition.

8.5 Testing performance under noisy stress conditions

8.5.1 Introduction

The purpose of transmission performance tests under noisy stress conditions is to obtain a value judgment of xDSL transceivers performance under circumstances that is representative to the deployment in operational access networks.

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. Crosstalk noise is typically stationair in nature. Only the occurrence of stationary noise will give an oversimplification of the reality, the existence of non-stationary noise should be taken into account as well.
Impulse noise is an example of non-stationary noise which consists of short bursts of noise that originate from outside the cable. Such impulse noise need not lead to a reduction of the achievable bandwidth, but can lead to the occurrence of short bursts of bit errors. Existing transmission systems are designed to cope (to some extent) with these types 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 parameters that are commonly used to evaluate the performance of an xDSL system under specified stress conditions, e.g. cable length and noise are:

1. the achieved bit rate at given noise margin, or
2. the actual noise margin at given bit rate.

Therefore, the performance of an xDSL transceiver is generally expressed and visualised by one of the following two curves:

1. Bit rate reach curve; this curve is the most common way to express the xDSL transceiver performance.
2. Noise margin[7] reach length curve; this curve is suitable in case the bit rate is fixed and one is interested in the transceiver performance as function of the loop length.

The noise margin is a valuable performance parameter for testing xDSL systems that do not support the rate adaption transmit mode where the DSL systems determines the best bit rate under the constraints of an achieved noise margin of 6 dB. XDSL systems that typically do not support the rate adaption mode are those systems that have a fixed correlation between the modulation scheme and the bitrate, e.g. CAP and PAM modulated systems.

Besides the bitrate-reach and noise margin-reach performance is the bit error rate (BER) an important parameter to evaluate the performance of a xDSL system. The BER is related to the CRC (or code violation) count which is reported by the xDSL management.

The transmission performance tests can be performed according to the philosophy of functional or conformance testing
Table **8**-7 gives the steps of these transmission performance tests.

	Functional test		**Conformance Test**
1		Verification test of the used reported parameters	Verification test of the used reported parameters
2	If no rate adaption mode supported	Measure at one test loop length the noise margin at two bit rates in a way that they are closely around the 6 dB. Obtain the bitrate at 6dB by interpolation.	Measure the noise Margin at all the bitrate and length combinations for all the noise and cable models as prescribed in ETSI or DSLF.
	If rate adaption mode is supported.	Use a line profile with a noise margin target is 6 dB. Measure the bitrate vs. length curve.	
3			Check if all the measured noise margins are above the 6 dB

Table 8-7: Performance test steps overview.

The following paragraphs will describe functional performance testing in more detail. For more details on conformance testing there is referred to e.g., ETSI [x1] chapter 5 and DSLF [x7] Annex B.

[7] The actual noise margin at given bit rate 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.

8.5.2 Reported line parameter verification tests

The performance tests will fully rely on the performance parameters reported by the element manager. Therefore it is necessary to test the reliability of these reported parameters. The used reported performance parameters are:

- Noise margin
- (Attainable) bit rate
- CRC or code violations

8.5.2.1 Reported noise margin verification test

Before the reported noise margin can be used for performance testing it should be validated.

Purpose	The margin performance tests rely on the noise margin reported by the element manager. Therefore it is necessary to test the reliability of this reported parameter.
Test Configuration	The test setup is depicted in figure 8-3. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI (see table 8-10 and table 8-11).
Test Procedure	1. Set an xDSL profile using the ***fixed rate*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the performance tests. 2. Connect CPE and DSLAM to the test loop, with the noise injected at the specified reference power level on the receiver side under test only. 3. Force a new initialization and wait for modems to sync. 4. Wait for 3 minutes after initialization for bit swaps to settle. 5. Check reported margin and document as **initial_reported_margin** 6. Increase the noise power level by 1 dB on the at the receiver side under test only, e.g. xTU-C or xTU-R. 7. Wait for 1 minute. 8. Repeat steps 6 and 7 until the noise power is increased by (**initial_reported_margin** – 1) dB. 9. At this point the power level of the noise is at the (**initial_reported_margin** – 1) dB level. 10. Increase the noise power level by 1 dB on the at the receiver side under test only, e.g. xTU-C or xTU-R. 11. Wait for 1 minute. 12. At this point the power level of the noise is at the (**initial_reported_margin**) dB level. 13. 14. Increase the noise power level by 1 dB on the at the receiver side under test only, e.g. xTU-C or xTU-R. 15. Wait for 1 minute. 16. At this point the power level of the noise is at the (**initial_reported_margin + 1**) dB level. 17. Repeat steps 15 and 16 until the xDSL link losses synchronization. Document the noise power level. 18. Repeat steps 2 to 18 for every test loop (Optional).
Expected Result	The xDSL modem passes the margin verification test if The difference between the injected noise power level at 0dB noise margin and at sync loss should be in the order of 2 dB

8.5.2.2 Reported (Attainable) bit rate verification test

Purpose	The purpose of this test is to verify the configured and reported bitrate by performing an Ethernet Packet Throughput test.
Test Configuration	The test setup is depicted in figure 8-12 or figure 8-13. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI (see table 8-10 and table 8-11).
Test procedure	1. Set an xDSL profile using the ***rate adaption*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the bitrate vs. reach performance tests. 2. Configure an Ethernet connection between the CPE and DSLAM. 3. Inject the reference noise and let the xDSL link train. 4. Read the reported (EM) up and downstream bit rates and noise margins. Check to which protocol layer the reported bit rate is related. 5. Start the downstream throughput test by sending large (1500 Bytes) frames in the downstream direction with a selected frame length and frame rate that corresponds with the bit rate reported by the EM. The test shall be run for 60 seconds. 6. Record analyzer throughput rate results as frames per second. 7. If the count of received frames is equal to the count of offered frames, increase the rate of the offered stream and repeat steps 5 and 6. If the count of received frames is less than the count of offered frames, decrease the rate of the offered stream and repeat steps 5 and 6. 8. Calculate the actual bit rate at layer 2 from the measured Ethernet frame rate and frame size. Translate the resulting bit rate to the actual bit rate at the reported protocol layer taking into account the complete encapsulation overhead schemes. 9. Repeat step 5 to 8 for the upstream direction.
Expected Result	The measured bit rates should correspond with the reported bit rates.

8.5.2.3 Testing reported code violation

Test Purpose	Checking the reported code violation parameters
Set-up	VDSL2: profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Cable length L=750m, Noise ETSI or Country specific. ADSL2(+): rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Cable length L=2000m, Noise ETSI or Country specific. INP_min = 1 symbols, delay_max = 8ms for the upstream and downstream channel.
Test Procedure	▪ Initialize the modem link ▪ Read out: o Actual INP dn o Actual delay dn o Actual INP up o Actual delay up

	Generate a single impulse event at the downstream receiver: ▪ PSD = -90 dBm/Hz, τ = 10µs ▪ Read out: o Count of coding violations (CO) ▪ Repeat the measurement for: o PSD = -90 dBm/Hz, τ = 125µs o PSD = -90 dBm/Hz, τ = 250µs Generate a single pulse train event at the downstream receiver: ▪ PSD = -90 dBm/Hz, τ = 10µs, T = 4ms ▪ Read out: o Count of coding violations ▪ Repeat the single pulse train measurements for:. o PSD = -90 dBm/Hz, τ = 10µs, T = 7ms o PSD = -90 dBm/Hz, τ = 10µs, T = 7.9ms o PSD = -90 dBm/Hz, τ = 10µs, T = 8ms o PSD = -90 dBm/Hz, τ = 10µs, T = 8.1ms o PSD = -90 dBm/Hz, τ = 10µs, T = 9ms
Expected result	The definition of the code violation parameter can be determined

8.5.3 Testing margin

The noise margin reach curve can be obtained by reading out the reported noise margin from the management system or by measuring the noise margin. In case the noise margin is read out, the reliability of the reported noise margin should be verified. This is done by a so-called "margin verification test". In case the noise margin is measured, there can be chosen to measure the noise margin up to BER=10^{-7} or up to loss of synchronization.

§ The measurement of the noise margin up to BER=10^{-7} is very laborious because it contains a complete BER test. Note that this noise margin is well defined in the DSL standards.

§ The measurement of the noise margin up to loss of synchronization is time efficient compared to the noise margin up to BER=10^{-7}. Note that the noise margin up to loss of synchronization is not defined in the DSL standards. Comparison of the noise margin up to loss of synchronization and the noise margin up to BER=10^{-7} requires the measurement of both noise margins.

This document describes noise margin tests where the noise margin reach curve is obtained by measuring the "sync loss" margin and by reading out the noise margin reported by the element manager.

8.5.3.1 Obtaining Noise Margin – Reach curve by measuring Sync Loss Margin

Purpose	The performance of the xDSL system under test should be obtained and expressed in a noise margin reach curve. The noise margin is obtained by measuring the sync loss margin.
Test Configuration	The test setup is depicted in figure 8-3. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI (see table 8-10 and table 8-11).
Test Procedure	1. Set an xDSL profile using the ***fixed rate*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the performance tests. 2. Connect CPE and DSLAM to the test loop with the length of interest and with the noise injected at the specified reference power level at the receiver side under test only. Check the reference power injected noise level and document as **initial_injected_noise_power_level** 3. Force a new initialization and wait for modems to sync. 4. Wait for 3 minutes after initialization for bit swaps to settle. 5. Increase the noise power level by 1 dB on the at the receiver side under test only, e.g. xTU-C or xTU-R. 6. Wait for 1 minute. 7. Repeat steps 6 and 7 until the xDSL link losses synchronization. Document the **injected_noise_power_level as injected_noise_power_level_at_sync_loss.** 8. The “sync loss” margin is difference between **initial_injected_noise_power_level** and **injected_noise_power_level_at_sync_loss.** 9. The noise margin at BER = 10^{-7} can be calculated out of the sync loss margin (see Note). 10. Document the noise margin at BER = 10^{-7} and sync loss margin as function of the configured loop length. 11. Repeat step 2 up to 10 to obtain the margins for all the loop lengths of interest. 12. Optional: repeat steps 2 to 9 for every test loop.
Expected Result	Two noise margin reach curves, one with noise margin at BER = 10^{-7} and one at sync loss.
Note	The noise margin at BER = 10^{-7} should be in the order of 2 dB less than at sync loss. From the reported margin verification test, the relation between noise margin at BER = 10^{-7} and at sync loss is known.

8.5.3.2 Obtaining Noise Margin – Reach curve by reading out the reported Noise Margin

Purpose	The performance of the xDSL system under test should be obtained and expressed in a noise margin reach curve. The noise margin is obtained by reading out the reported noise margin
Test Configura-tion	The test setup is depicted in figure 8-3. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI (see table 8-10 and table 8-11).
Test Procedure	1. Set an xDSL profile using the ***fixed rate*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the performance tests. 2. Connect CPE and DSLAM to the test loop with length # of interest and with the noise injected at the specified reference power level on the receiver side under test only. 3. Force a new initialization and wait for modems to sync. 4. Wait for 3 minutes after initialization for bit swaps to settle. 5. Check reported margin and document as **reported_margin@loop_length_#** 6. Repeat steps 2 and 5 until the margins at all loop lengths of interest are measured and the noise margin reach curve is completed. 7. Optional; repeat steps 2 to 10 for every test loop
Expected Result	(Reported) noise margin reach curve

8.5.4 Testing bit rate

The bit rate reach curve can be obtained by reading out the reported bit rate from the management system or by measuring the noise margin. In case the noise margin is read out, the reliability of the reported noise margin should be verified. This is done by a so-called “layer 2 throughput test”.

The condition on which this test can be performed is that the xDSL system under test must support the rate adaption mode where the DSL systems determines the best bit rate under the constraints of an achieved noise margin of 6 dB.

Typically the expected result for these tests is defined as being the measured rate-reach curve above a reference performance objective curve defined either with simulations or by means of defining the objectives by engineering the results obtained from benchmarking marketplace equipment.

8.5.4.1 Rate-reach performance test without PSD shaping

Purpose	The performance of the xDSL system under test without PSD shaping should be obtained and expressed in a bit rate reach curve.
Test Configura-tion	The test setup is depicted in figure 8-3. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI or DSL Forum.
Test Procedure	1. Set an xDSL profile without PSD shaping using the ***rate adaption*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the performance tests. 2. Connect CPE and DSLAMDSLAM/ONU to the test loop with length # of interest and with the noise injected at the specified reference power level on the receiver side under test only. 3. Force a new initialization and wait for modems to sync. 4. Wait for 3 minutes after initialization for bit swaps to settle. 5. Check reported bit rate and document as **reported_bit_rate@loop_length_#** 6. Collect the reported noise margin 7. Repeat steps 2 and 6 until the bit rates at all loop lengths of interest are measured and the bit rate reach curve is completed. 8. Optional; repeat steps 2 to 10 for every test loop
Expected Result	(Reported) bit rate reach curve vs loop length shall be above a reference performance objective curve, unless for a given percentage of test points. The reported noise margin shall be above the target margin, unless for a given percentage of test points.

8.5.4.2 Rate-reach performance test with DPBO and UPBO shaping

Purpose	The performance of the xDSL system under test with DPBO and UPBO PSD shaping should be obtained and expressed in a bit rate reach curve.
Test Configuration	The test setup is depicted in figure 8-3. The loop and noise conditions are chosen according to the sections “Test Loops” and “Noise Sources”, they can be country specific or chosen from ETSI or DSL Forum. Note: with respect to performance tests without PSD shaping it is advisable that the applied noise models contain self-disturbers defined with the same DPBO and UPBO shaping as configured on the system under test.
Test Procedure	1. Set an xDSL profile with DPBO and UPBO shaping using the ***rate adaption*** mode. The other parameters are arbitrary however it is preferable to use the same profile as planned for the performance tests. 2. Connect CPE and DSLAMDSLAM/ONU to the test loop with length # of interest and with the noise injected at the specified reference power level on the receiver side under test only. 3. Force a new initialization and wait for modems to sync. 4. Wait for 3 minutes after initialization for bit swaps to settle. 5. Check reported bit rate and document as **reported_bit_rate@loop_length_#** 6. Collect the reported noise margin 7. Repeat steps 2 and 6 until the bit rates at all loop lengths of interest are measured and the bit rate reach curve is completed. 8. Optional; repeat steps 2 to 10 for every test loop
Expected Result	(Reported) bit rate reach curve vs loop length shall be above a reference performance objective curve, unless for a given percentage of test points. The reported noise margin shall be above the target margin, unless for a given percentage of test points. Beyond the comparison with the reference performances under the applied shaping settings, it is useful to compare with the actual (and reference) performances of the system without PSD shaping. This gives a criterion to verify that the performance loss due to shaping is within certain limits.

8.5.5 Testing resistance against slowly transmission impairments

To protect the xDSL system against transmission impairments that slowly varies with time (temperature induced line changes, small changes in crosstalk noise spectrum and the increase of RFI (Radio frequency Interferers) at night) xDSL uses a mechanism called On-line reconfiguration (OLR). On-line reconfiguration allows changes to the Physical Media Dependent (PMD) function, which organizes the bit allocation, without interruption of service and without errors.

Types of OLR include bit swapping, dynamic rate repartitioning (DRR) and seamless rate adaptation (SRA). DRR and SRA are still under study within the standardization. However, bit-swapping is a proved OLR concept already used in legacy generation DMT receivers like ADSL1. Bit-swapping reallocates bits and power (i.e., margin) among the allowed sub-carriers without modification of the higher layer features of the physical layer.

When, e.g., the amplitude of RFI is changed a receiver detects that the SNR on a specific tone or a group of tones has degraded beyond a certain threshold. The bit-swapping mechanism attempts to find other tones that can accommodate one or more additional bits from the tones affected by the RFI signal. A bit-swap request command is sent from receiver to the transmitter through a protected reverse channel. Depending on the implementation the receiver waits for hand-shaking acknowledgements after which the bit-swapping mechanism reconfigures the bit and gain (*bi, gi*) parameters without changing the total data rate.

8.5.5.1 On-line Reconfiguration (OLR) – Bit swapping (BSwap) test

VDSL2 uses a broad frequency spectrum up to 30MHz and is therefore vulnerable for RFI which may occur on several frequencies simultaneously with amplitudes that vary very rapidly. Important parameters for the bit-swapping procedure to test are therefore:
1. The number of tones that can be changed in one bit-swap request.
2. The time needed for one bit-swap to be completed.

8.5.5.1.1 Basic bit-swap functionality test

Aim	The purpose of this sub-test is to verify basic functionality of bit swapping.
Set-up	The test setup is depicted in figure 8-3. Profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific, INP_min = 0, delay_max = 0ms, average cable length for the xDSL system under test.
Procedure	Initialize the modem link. 1. Record the values from the bits&gains allocation table. 2. Randomly select one sub-carrier with allocated bits in the upstream or downstream band. 3. Apply one interfering tone of power -110 dBm at the frequency corresponding to the selected sub-carrier at the xTU-R (downstream carrier) or the xTU-C (upstream carrier). 4. Take notice of any bit-swap operation by checking bits and gain setting on the selected carrier. Verify on CRC errors and if the modems do not retrain. 5. Increase the power level of interfering tone by 1 dB *and wait at least 10 seconds*. Take notice of any bit-swap operation and CRC errors. Verify the modems do not retrain. 6. Record the values from the downstream bits allocation and gains allocation table. 7. *Ensure that the modem runs error-free for at least one minute after the bit swap.* 8. Repeat steps 2-7 untill the modems will retrain. 9. Repeat steps 2-7 for other sub-carriers or a set of sub-carriers.
Expectations	The VTU-O and VTU-R pair which is subject to this test is expected to be able to reconfigure the bit and gain (b_i,g_i) parameters among the allowed sub-carriers without interruption in data transfer and without errors.

8.5.5.1.2 Testing the maximum number of swapped tones

Aim	The purpose of this sub-test is to verify the maximum number of tones that can be swapped in one request.
Set-up	The test setup is depicted in figure 8-3.

	Profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific, INP_min = 0, delay_max = 0ms, average cable length for the xDSL system under test.
Procedure	Initialize the modem link. 1. Record the values from the bits&gains allocation table. 2. Randomly select N sub-carriers with allocated bits in the upstream and/or downstream band. 3. Apply N interfering tones of power -110 dBm at the frequencies corresponding to the selected sub-carriers at the xTU-R (downstream carrier) or the xTU-C (upstream carrier). 4. Obtain the bits and gains settings on the selected carriers. 5. Increase the power level of the interfering tones by the value of the lowest reported noise margin in dB's and wait at least 10 seconds. Take notice of any bit-swap operation and CRC errors. Verify the modems do not retrain. 6. Record the values from the downstream bits allocation and gains allocation table. 7. Ensure that the modem runs error-free for at least one minute after the bit swap. 8. Increase N and repeat steps 2-7 until the modems will retrain.
Expectations	N is the maximum number of tones that can be reconfigured (bit and gain (b_i,g_i) parameters) by the bit-swap algorithm without interruption in data transfer and without errors.

8.5.5.1.3 Testing the bit-swap speed

Aim	The purpose of this sub-test is to verify the speed of the bit swapping.
Set-up	The test setup is depicted in figure 8-3. Profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific, INP_min = 0, delay_max = 0ms, average cable length for the xDSL system under test.
Procedure	1. Define two noise profiles that will interfere with N sub-carriers. Note that N < max number of swapped tones. 2. Inject noise profile 1 at a realistic power level. 3. Initialize the modem link. 4. Record the values from the bits&gains allocation table. 5. Decrease the noise power level gradual to zero and start (at the same time) injecting the second noise profile by increasing the power level gradually to a realistic power level, e.g., to a power level that corresponds to a noise margin of about 0dB on the selected sub-carriers. Note that the degree of the gradual increase of the noise power level defines the bit-swap speed. The time period T of the gradual increase and decrease is given in table 8-8. 6. Record the values from the bits&gains allocation table. 7. Ensure that the modem runs error-free for at least one minute after the bit swap. 8. Decrease the noise power level of profile 2 and start injecting the first

	noise profile by gradually increasing the power level at a speed given in table 8-8. 9. Repeat step 4-7 until the CRC errors or retrains are observed.
Expectations	The time period at which CRC errors or retains start occurring defines the maximum bit-swap speed.

Test	Time Period T
1	120 s.
2	60 s.
3	30 s.
4	15 s.
5	10 s.
6	5 s.
7	1 s.
8	0.5 s.
9	0.1 s.
10	0.05 s.

Table 8-8: The time period T of the gradual increase and decrease.

8.5.6 Testing bit rate using INP_min and Delay_max configuration

As mentioned earlier the Impulse Noise Protection mechanism deployed in the current VDSL2 systems comprises of Reed-Solomon (RS) coding and interleaving. The number of redundant bytes in a RS codeword, interleaver depth, interleaver block length and the number of bits per DMT symbol determine a system's capability to mitigate the effects of an impulse noise event. When configuring a VDSL2 connection the user indirectly sets these parameters by defining the following two configuration parameters:

- INP_min – minimum impulse noise protection. The disruption of at least this number of DMT symbols can be overcome by the system in case transmitted data is hit by a strong impulse.
- Delay_max – maximum interleaving delay. A maximal time interval over which data symbols may be spread.

Note that the system itself chooses the actual values of these two parameters so that they optimally meet other requirements such as minimum noise margin and data rate. According to the ITU-T VDSL2 standard:

INP denotes the number of DMT symbols or fractions thereof 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 rule is:

INP = 2 x delay x FEC overhead (Equation 1)

Equation 1 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.

Bitrate performance	
Aim	Determine the bitrate performance as function of the INP_min and delay_max setting
Set-up	The test setup is depicted in figure 8-1. VDSL2: profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. ADSL2(+): rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific.
Procedure	Initialize the modem link with INP_min = 0 and delay_max = 0ms. Cable length = 250m. ▪ Read out: o Actual BitRate dn o Actual INP dn o Actual delay dn ▪ Repeat the measurement for: o INP_min = ½, 1, 2, 4, 8, 16 • Repeat the measurement for each INP_min setting: • delay_max = 2ms, 4ms, 8ms, 16ms, 32ms, 63ms ▪ Repeat the measurement for the following cable lengths o VDSL2: 500m up to 1500m in steps of 250m. o ADSL2(+); 500m up to 4000m in steps of 500m.
Expectations	Bitrate decreases when the INP increases or the delay decreases.

8.5.7 Testing resistance against impulsive noise

In the former section the bitrate performance in case of a required configuration with an INP_min and Delay_max is determined. However, these test results do not show the achieved resistance against impulse noise. In this section the DSL system is tested if the it can mitigate the impact of impulse noise according to the INP setting expectations.

The resistance again impulse noise is tested is two steps:
1. Testing the INP mechanism using synthetic impulse noise.
2. Testing under the country specific situation using impulse noise under a realistic scenario, e.g., REIN, SHINE or PEIN.

8.5.7.1 Single pulse event

In this section the impact of a single pulse on the probability of occurrence of a CRC event is studied. Impulse events are characterized by τ, which is the duration (or the width) of the pulse. The specified time interval τ is filled with random nearly white Gaussian noise, *i.e.*, white noise with Power Spectral Density PSD = -90dBm/Hz in the range [0-30] MHz as in figure 8-25. The test in this section is whether the system really can cope with impulse events that destroy less than INP_actual DMT symbols in an interval shorter than Delay_actual. Here index “actual” indicates the value of the parameter chosen by the system, as opposed to the minimum requirement INP_min specified by the user.

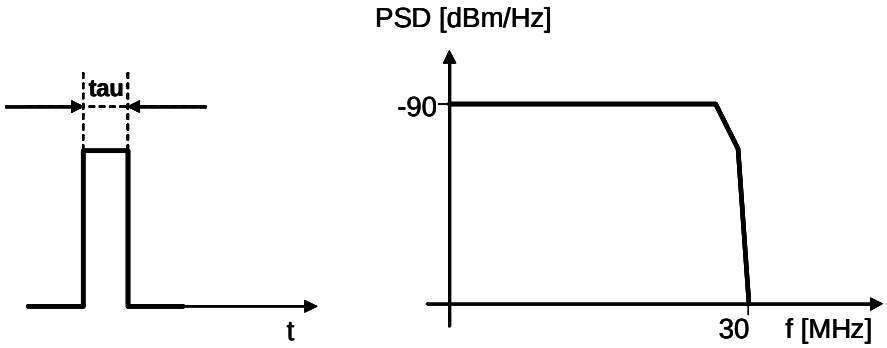


Figure 8-25: Impulse structure in time and frequency domain.

After an impulse is injected the Code Violation (CV) counter of the downstream and upstream channel are read out. An increase in the number of Code Violations indicates that the decoder could not correct the errors in the received data stream. Impulse noise events that result in an increase of the code violation counter are registered and studied whether they are in agreement with the expectations.

Figure **8**-26 shows an example of a single impulse event. In the figure is shown how the pulse width is expected to be related to the number of destroyed DMT symbols. In the worst case, a pulse slightly wider than 550µs may hit four DMT symbols. However, the probability of such an event is quite low, as the starting point of this pulse must be close to the end of a DMT symbol.

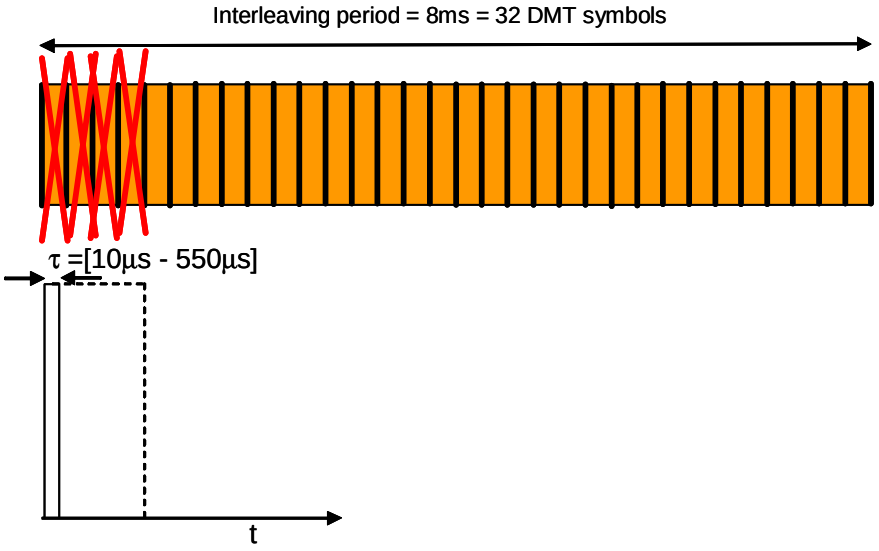


Figure 8-26: Example of a single impulse event.

Aim	Determine the robustness against a single impulse event
Set-up	The test setup is depicted in figure 8-4. VDSL2: profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. Cable length = 750m. ADSL2(+): rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific.

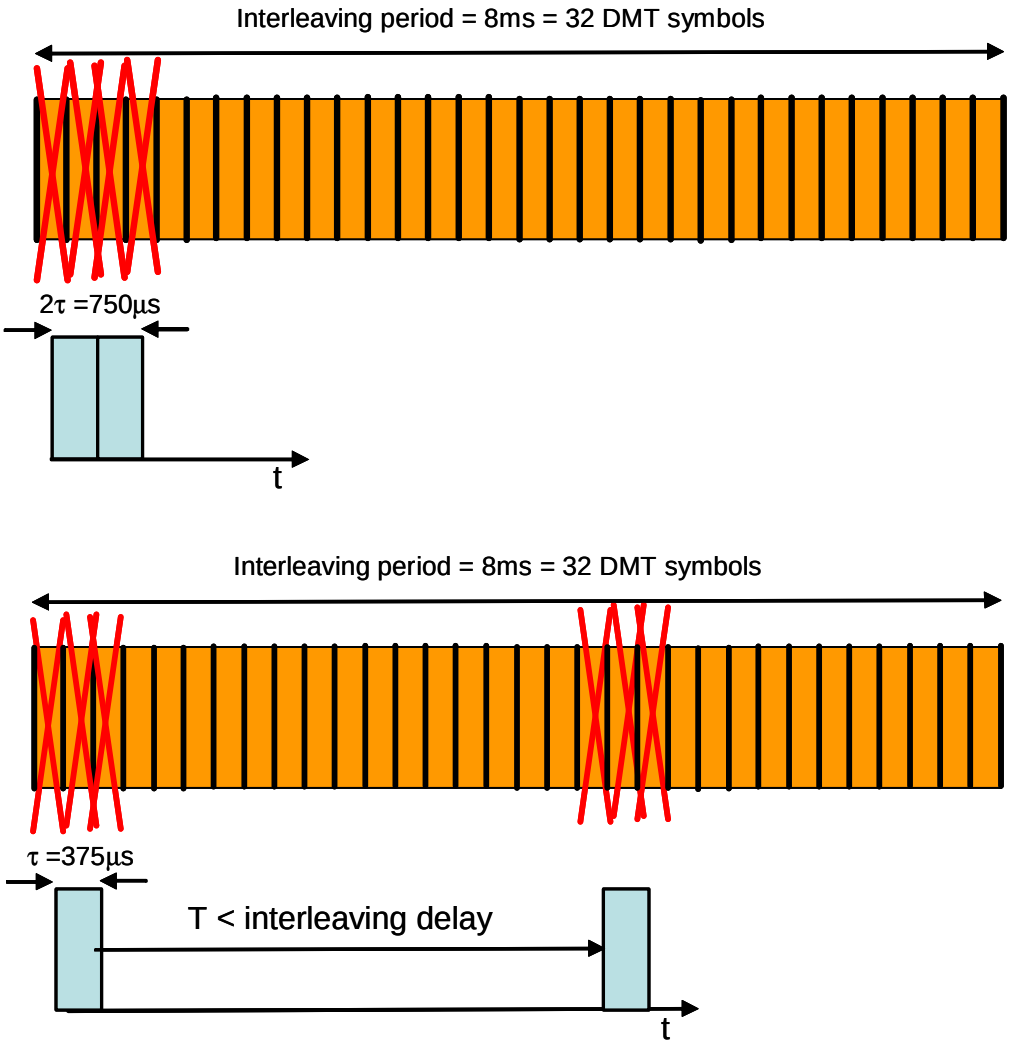
	Cable length = 2000m.
Procedure	Initialize the modem link with INP_min = 1 and delay_max = 8ms. ▪ Read out: o Actual INP dn o Actual delay dn o Count of coding violations (CO) Generate a single impulse event: ▪ PSD = -90 dBm/Hz, τ = 10µs ▪ Read out: o Count of coding violations (CO) ▪ Repeat the measurement for: o PSD = -90 dBm/Hz, τ = 20µs o PSD = -90 dBm/Hz, τ = 50µs o PSD = -90 dBm/Hz, τ = 125µs o PSD = -90 dBm/Hz, τ = 250µs o PSD = -90 dBm/Hz, τ = 275µs Initialize the modem link with INP_min = 2 and delay_max = 8ms. ▪ Read out: o Actual INP dn o Actual delay dn o Count of coding violations (CO) ▪ Generate 10 times a single impulse event: o PSD = -90 dBm/Hz, τ = 10µs ▪ Read out for each impulse event: o Count of coding violations (CO) ▪ Repeat the measurement for: o PSD = -90 dBm/Hz, τ = 125µs o PSD = -90 dBm/Hz, τ = 250µs o PSD = -90 dBm/Hz, τ = 275µs o PSD = -90 dBm/Hz, τ = 500µs o PSD = -90 dBm/Hz, τ = 550µs o PSD = -90 dBm/Hz, τ = 750µs Repeat the measurement for INP_min = 4 and delay_max = 8ms and the following single impulse events: o PSD = -90 dBm/Hz, τ = 250µs o PSD = -90 dBm/Hz, τ = 500µs o PSD = -90 dBm/Hz, τ = 550µs o PSD = -90 dBm/Hz, τ = 750µs o PSD = -90 dBm/Hz, τ = 800µs o PSD = -90 dBm/Hz, τ = 1ms o PSD = -90 dBm/Hz, τ = 1,1ms o PSD = -90 dBm/Hz, τ = 1.25ms Repeat the measurement for INP_min = 8 and delay_max = 8ms and the following single impulse events: o PSD = -90 dBm/Hz, τ = 1ms o PSD = -90 dBm/Hz, τ = 1.25ms o PSD = -90 dBm/Hz, τ = 1.5ms o PSD = -90 dBm/Hz, τ = 1.75ms

	o PSD = -90 dBm/Hz, τ = 2ms o PSD = -90 dBm/Hz, τ = 2.25ms o PSD = -90 dBm/Hz, τ = 2.5ms Repeat the measurements for the upstream channel Repeat in case of VDSL2 the measurement for other PSD shapes.
Expectations	The robustness increases linear with the INP value

8.5.7.2 Pulse train events

Using a pulse train event we check the validity of the INP definition related to the time period in which INP_actual DMT symbols can always be received without any errors (see definition of INP).

In this section the impact of a pulse doublet (two pulses of the same width τ separated by time interval T) on the occurrence of a code violation is studied. In a single set of measurements the pulse width (τ) is taken as a parameter and spacing between the pulses (T) is varied. Figure 8-27 shows schematically this method.



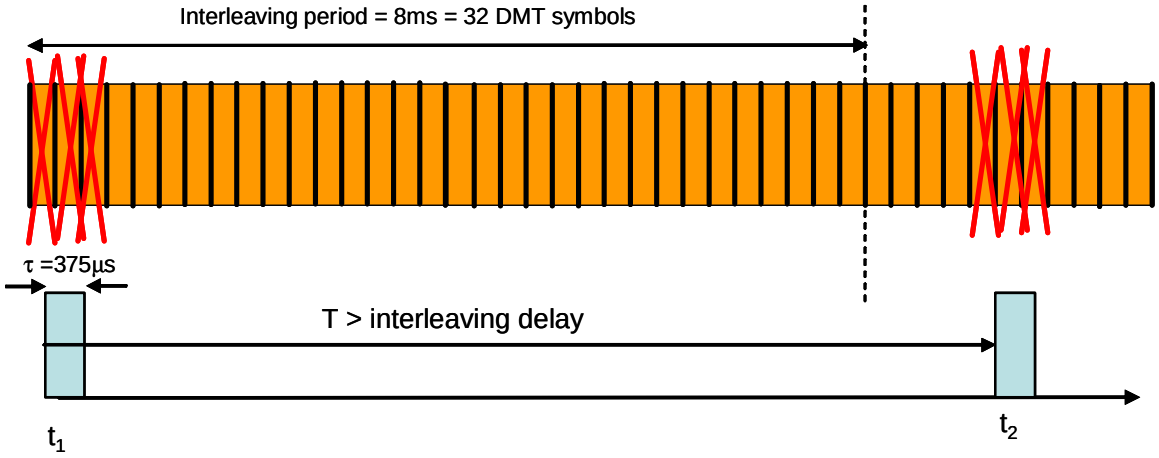


Figure 8-27: Pulse trains tests by varying the spacing between the pulses (T).

Aim	Determine the impact of the interleaving delay on robustness against a pulse train impulse event.
Set-up	The test setup is depicted in figure 8-4. VDSL2: profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. Cable length = 750m. ADSL2(+): rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. Cable length = 2000m.
Procedure	Initialize the modem link with INP_min = 4 and delay_max = 8ms. ▪ Read out: o Actual INP dn o Actual delay dn o Count of coding violations (CO) Generate a single pulse train: ▪ PSD = -90 dBm/Hz, τ = 375µs, T=0ms ▪ Read out: o Count of coding violations (CO) ▪ Repeat the measurement for: o PSD = -90 dBm/Hz, τ = 375µs, T=1ms o PSD = -90 dBm/Hz, τ = 375µs, T=2ms o PSD = -90 dBm/Hz, τ = 375µs, T=7ms o PSD = -90 dBm/Hz, τ = 375µs, T=(8-τ)ms o PSD = -90 dBm/Hz, τ = 375µs, T=8ms o PSD = -90 dBm/Hz, τ = 375µs, T=(8+τ)ms o PSD = -90 dBm/Hz, τ = 375µs, T=10ms
Expectations	According to the INP definition should the system mitigate the pulse trains with T > interleaving delay. **INP_actual DMT symbols can be completely corrected within the interleaver delay (Delay_actual).**

8.5.7.3 Testing resistance against a realistic set of impulsive noise events

To be sure that the deployed xDSL lines will be resistant against the impulsive noise that occurs in the access network, the xDSL line under test will be tested against a set of realistic country specific impulse noise. This set of impulsive noise can be a combination of REIN, SHINE and PEIN.

Aim	Determine the robustness of the xDSL line under test against a set of realistic impulse events.
Set-up	The test setup is depicted in figure 8-4. VDSL2: profile free, no PSD shaping, rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. Cable length = 750m. ADSL2(+): rate adaptive mode with no bitrate limitation, Loop; ETSI or Country specific, Noise: ETSI or Country specific. Cable length = 2000m.
Procedure	Initialize the modem link with the required* INP_min and delay_max setting. ▪ Read out for the upstream and downstream channel: o Actual INP o Actual delay o Count of coding violations Generate the set of impulse events. ▪ Read out for the upstream and downstream channel: o Count of coding violations.
Expectations	If the INP/delay setting is properly chosen, the xDSL system under test is able to mitigate all the impulse noise. No code violations are measured. If the set of impulsive events violates the INP/delay setting, code violations are measured.
Note	* This setting should be pre-determined based on knowledge about the impulse noise characteristics of the impulse noise as it occurs in the operational access network.

This test can be used to optimize the DSL line under test for a better robustness against the set of impulsive events. If code violations are measured, the system can be reconfigured to a higher impulse noise protection level. By repeating the test until no code violations are measured or the number of code violation stay within the boundary of acceptance, the xDSL line is optimized for the set of impulsive noise.

8.5.8 Inter comparing test results

8.5.8.1 Introduction

The main objective to perform a performance test is to be able to give a value judgment of the xDSL system under test on basis of the test results.
However, the use of (country) specific test loops and noise profiles make a value judgement of the test results difficult. Additionally, comparison with test results from other laboratories or judgement by a third party will be difficult. Note that this problem does not arise when functional performance tests are performed under standardised test loops and noise profiles or when a conformance test is performed.

There are two approaches in performing a functional performance test, namely:

1. The functional performance test can be performed under (country) specific conditions using a country specific test loop and noise profile. To make a value judgement, the results can be compared with:
    a. the test results of a functional performance test performed on a reference modem under the same (country) specific conditions.
    b. the simulation results of a performance simulation based on a hypothetical system performing at Shannon limit minus 7 dB.
    c. the simulation results of a standardised performance model.
2. The functional performance test can be performed under standardised test loops and noise profiles. To make a value judgement, the results can be compared with:
    a. the performance requirements prescribed in the standard.
    b. the test results of another test lab.

Stress conditions	Output use
(country) specific	Comparable with the test results of a functional performance test performed on a reference modem under the same (country) specific conditions
	Comparable with the simulation results of a performance simulation based on a hypothetical system performing at Shannon limit minus 7 dB.
	Comparable with the simulation results of a standardised performance model
standardised	Comparable with the performance requirements prescribed in the standard
	Comparable with the test results of another test lab

8.5.8.2 Results tested under (country) specific testing

The advantage of performing a functional performance test under (country) specific conditions is that the results are directly applicable to give an absolute value judgment of the system under test for that particular (country) specific situation. The disadvantage of a performance test under (country) specific conditions is that the outcome is specific and therefore not easily comparable. For a qualification how the systems performs relatively to other comparable systems or standardised performance requirements is not directly possible.

To compare the performance of the system under test with the performance of a comparable system, this comparable system should be tested under the same conditions. These test results are directly comparable.

Another method is obtain a relative performance qualification is to compare the test results with the simulation results of a performance simulation based on a hypothetical system performing at Shannon limit minus 7 dB under the same conditions or a standardised performance model, e.g. ETSI, under the same conditions. Figure 8-28 depicts an example of a diagram that shows how close the system under test approaches a hypothetical curve (e.g. Shannon limit minus 7 dB) or standardised calculation model (e.g. ETSI).

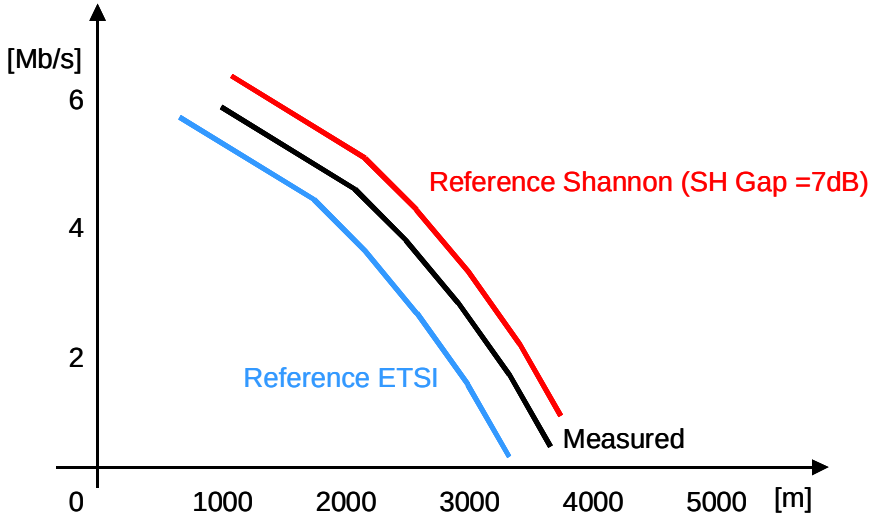


Figure 8-28: Example of performance comparison with other labs/countries.

Table 8-9 gives the procedure to simulate the performance of the xDSL system under test which can be used for comparison.

Purpose	Value judgment of the achieved performance of the xDSL system under test based on a performance comparison with simulated performance.
Test Configuration	ETSI TS 101 830-2 describes in detail how the performance of an xDSL system can be simulated.
Test Procedure	1. Defining the simulation setup: a. test loop model that describes the test loop used in the performance test (see chapter 7 of ETSI TS 101 830-2). b. noise model that corresponds to the injected noise profile used in the performance test. c. cross talk model that corresponds with the cross talk coupling and cross talk injection used in the performance test (see chapter 8 of ETSI TS 101 830-2). d. transmitter signal model that describes the transmitted signal power density of the xDSL system under test (see chapter 4 of ETSI TS 101 830-2). e. generic receiver model that describes the generic receiver capabilities of the xDSL system under test (see chapter 5 of ETSI TS 101 830-2). f. specific receiver model that describes the specific receiver capabilities of the xDSL system under test (see chapter 6 of ETSI TS 101 830-2). 2. Simulate the simulation set up as defined in step 1 for the same reach as the performance test. 3. Plot the simulated performance and the measured performance together into one diagram.
Expected Result	The diagram with both bit rate reach curve provides the insight to give a performance qualification of the xDSL system under test.

Table 8-9: Procedure to simulate reference performance of the xDSL system under test.

8.5.8.3 Results tested under standardised conditions

The advantage of performing a functional performance test under standardised conditions is that the results are comparable with all system tests under the same conditions. Furthermore, the test results can be compared with the performance requirements prescribed in that same standard.

8.6 Example test configurations

8.6.1 Example test loops

Many loops have been identified in various standards. Some loop sets are recently developed and are excellent in nature (ETSI-VDSL use only 4 loops to cover most stress conditions from practice) others are just a bunch of loops collected in the past but the rationale behind them are weak (ETSI-HDSL use 8 loops, and they have been reapplied to SDSL)

Table 8-10 gives some examples of ETSI test loops.

Name	Impedance	Cable type	reference
ETSI ADSL Loop #2	115Ω	PE05	ETSI TS 101 388
ETSI SDSL Loop #2	120Ω	PE04	ETSI TS 101 524
ETSI VDSL Loop #2	150Ω	-	ETSI TS 101 270

Table 8-10: Some examples of ETSI test loops.

8.6.2 Example noise profiles for stationary crosstalk noise

Suggestions/examples for noise models to use are given in table 8-11.

xDSL type	Name	Comments	Reference
ADSL1	X.LT.FB	Combined Alien & Self crosstalk model intended to represent a medium penetration scenario, type “FA” for injection at the LT side (testing the upstream receiver)	ETSI TS 101 388
	X.NT.FB	Combined Alien & Self crosstalk model intended to represent a medium penetration scenario, type “FA” for injection at the NT side (testing the downstream receiver)	
SDSL	XS.LT.B	Self crosstalk model intended to represent a medium penetration scenario, type “A” for injection at the LT side (testing the upstream receiver)	ETSI TS 101 524
	XS.NT.B	Self crosstalk model intended to represent a medium penetration scenario, type “A” for injection at the LT side (testing the downstream receiver)	
	XA.LT.B	Alien crosstalk model intended to represent a medium penetration scenario, type “A” for injection at the LT side (testing the upstream receiver)	

	XA.NT.B	Alien crosstalk model intended to represent a medium penetration scenario, type “A” for injection at the NT side (testing the downstream receiver)	
VDSL Cabinet	XS.LT.A	Self crosstalk model intended to represent a mixed scenario including full ADSL, type “A” for injection at the LT side located in a street cabinet (testing the upstream receiver)	ETSI TS 101 270-1
	XS.NT.A	Self crosstalk model intended to represent a mixed scenario including full ADSL, type “A” for injection at the NT side (testing the downstream receiver)	
	XA.LT.A	Alien crosstalk model intended to represent a mixed scenario including full ADSL, type “A” for injection at the LT side located in a street cabinet (testing the upstream receiver)	
	XA.NT.A	Alien crosstalk model intended to represent a mixed scenario including full ADSL, type “A” for injection at the NT side (testing the downstream receiver)	
VDSL Exchange	XS.LT.D	Self crosstalk model intended to represent a high penetration scenario, type “A” for injection at the LT side located in the exchange (testing the upstream receiver)	ETSI TS 101 270-1
	XS.NT.D	Self crosstalk model intended to represent a high penetration scenario, type “A” for injection at the LT side (testing the downstream receiver)	
	XA.LT.D	Alien crosstalk model intended to represent a high penetration scenario, type “A” for injection at the LT side located in the exchange (testing the upstream receiver)	
	XA.NT.D	Alien crosstalk model intended to represent a high penetration scenario, type “A” for injection at the NT side (testing the downstream receiver)	

Table 8-11: Suggestions/examples for ETSI noise models.

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

Note that the noise profiles mentioned in table only apply for the equivalent disturbers G1 and G2, representing a real scenario containing many xDSL disturbers. Other type of disturbers, e.g. broadcast RF noise, amateur RF noise, impulse noise and line sharing noise are left for further study.
Detailed specifications for the components of the noise models together with a brief explanation can be found in e.g. ETSI [x1] clause 5.5.
Another example of VDSL2 noises for testing G.993.2 Annex B system is the approach used by the DSL Forum.
As explained in "Part 1", the DSL Forum has adopted the ETSI VDSL2 noise framework but the following assumptions where made to derive a useful and effective model for VDSL2 Performance Test Plans:

- adopt as a basis the VDSL2 noise models and mixes the Medium Density (MD) noise scenario by ETSI;
- three topologies are specified:
  - from Exchange (MD_EX);
  - from Cabinet with 27 dB @ 1 MHz of attenuation from the Exchange (MD_Cab27);
  - from Cabinet with 72 dB @ 1 MHz of attenuation from the Exchange (MD_Cab72);
- for all the three scenarios above, ETSI has specified:
  - the mix of self-disturbers;
  - the mix of alien-disturbers;
  - the PSDs of alien-disturbers;
- consider 8x band-profiles under the category of VDSL2/EX;
- consider 12x and 17x band-profiles under the category of VDSL2/Cab27;
- consider 30x band-profiles under the category of VDSL2/Cab72;
- for VDSL2 self-disturbers, adopt the ETSI MD mix considering disturbers with the same VDSL2 band-profile applied to the SUT and the related PSD mask; this means that VDSL2 self-disturbers are considered as homologous to and co-located with the VDSL2 system under test;
- for alien-disturbers, adopt the ETSI MD mix and the PSDs associated to the VDSL2/x category related to the VDSL2 band-profile applied to the SUT;

Given the above, a noise model is defined as associated with a specific VDSL2 band-profile.

Basic noise PSDs associated with each main band-profile are defined as follows:

Noise model	Associated VDSL2 band-profile	Self noise disturbers	Alien noise disturbers
n_BA8b	BA8b	ETSI MD_EX Mix	ETSI MD_EX mix and PSDs
n_BB8b	BB8b		
n_BA12a	BA12a	ETSI MD_Cab27 mix	ETSI MD_Cab27 mix and PSDs
n_BB12a	BB12a		
n_BA17a	BA17a		
n_BB17a	BB17a		
n_BA30a	BA30a	ETSI MD_Cab72 mix	ETSI MD_Cab72 mix and PSDs
n_BB30a	BB30a		
n_BA17a _D&UPBO	BA17a _D&UPBO	ETSI MD_Cab27 mix	ETSI MD_Cab27 mix and PSDs
n_BA30a _D&UPBO	BA30a _D&UPBO	ETSI MD_Cab72 mix	ETSI MD_Cab72 mix and PSDs

Note: for each noise model, self noise disturbers have a basic VDSL2 PSD defined by the associated VDSL2 band-profile.

The settings for noise generators G1 and G2 shall be as follows.

The crosstalk coupling functions NEXT and FEXT shall be calculated using the transfer function equations from ETSI TS 101 270-1 [x3], section 9.3.2.

For the generic n_XYZ noise applies the following:

- the alien noise disturber frequency domain profiles are associated with the ETSI noise scenario (MD_EX, MD_CAB27 or MD_CAB72) in a unique way; these are given in dBm/Hz
- the self noise disturber frequency domain profile depends on the number (N) of self disturbers and is associated with the VDSL2 Band-profile XYZ which implicitly defines the single self-disturber PSD template for the LT side (US bands) and the NT side (DS bands), coherently with ITU-T G.993.2 [x24].

The number N of self disturbers for MD_EX, MD_CAB27 and MD_CAB72 scenario shall be as defined below.

	MD_EX	**MD_CAB27**	**MD_CAB72**
Number of self disturbers	13	15	15

Be $P_{Alien\text{-}XYZ,SS}$ the alien PSD for the generic n_XYZ noise at the SS side (SS=LT, NT) in W/Hz. Be $P_{SingleSelf\text{-}XYZ,SS}$ the single self-disturber PSD template for the generic n_XYZ noise at the SS side (SS=LT, NT) in W/Hz.

The PSD of the noise generators G1 and G2 for the generic n_XYZ noise is a weighted sum of the self-crosstalk and alien-crosstalk components.

- G1 = (XA.LT.n_XYZ ∗ XS.LT.n_XYZ), with NEXT coupling function
- G2 = (XA.NT.n_XYZ ∗ XS.NT.n_XYZ), with FEXT coupling function

At CPE side:

- G1 = (XA.NT.n_XYZ ∗ XS.NT.n_XYZ), with NEXT coupling function
- G2 = (XA.LT.n_XYZ ∗ XS.LT.n_XYZ), with FEXT coupling function

Symbol "∗" refers to the FSAN crosstalk sum $P_{XYZ,SS}$ of two PSDs in W/Hz, the alien $P_{Alien\text{-}XYZ,SS}$ and self-crosstalk $P_{Self\text{-}XYZ,SS}$ PSD:

$$P_{XYZ,SS} = [P_{Alien\text{-}XYZ,SS}^{1/0.6} + P_{Self\text{-}XYZ,SS}^{1/0.6}]^{0.6}$$

XA.LT.n_XYZ and XA.NT.n_XYZ refer to the alien crosstalk profiles. Self-crosstalk profiles XS.LT.n_XYZ and XS.NT.n_XYZ are specified in the table below and describe the self-crosstalk portion of an equivalent disturber co-located at the LT and NT end of the loop.

	MD_EX	**MD_CAB27**	**MD_CAB72**
XS.LT.n_XYZ	$P_{SingleSelf\text{-}XYZ,LT}$ + 6.7dB	$P_{SingleSelf\text{-}XYZ,LT}$ + 7.1dB	$P_{SingleSelf\text{-}XYZ,LT}$ + 7.1dB
XS.NT.n_XYZ	$P_{SingleSelf\text{-}XYZ,NT}$ + 6.7dB	$P_{SingleSelf\text{-}XYZ,NT}$ + 7.1dB	$P_{SingleSelf\text{-}XYZ,NT}$ + 7.1dB

The values 6.7 dB and 7.1 dB simulate the power generated by the sum of 13 and 15 disturbers, which is added to the single self-disturber PSD $P_{SingleSelf\text{-}XYZ,SS}$ for the generic n_XYZ noise at the SS side (SS=LT, NT).

For the calculation of $P_{SingleSelf\text{-}XYZ,SS}$ the following steps shall be applied:

- identify the **basic PSD template**: this corresponds to the associated VDSL2 Band-profile XYZ as per ITU-T G.993.2/Amd.1, sections B.2.4 and B.2.5 and is defined in accordance with the ITU-T G.993.2/Amd.1, section B.4

- where required, apply to the above basic PSD template the DPBO and UPBO shaping of the associated VDSL2 Band-profile XYZ to calculate a **shaped PSD template**
  (Note: for upstream shaped PSD templates the kl_0 value varies with the Test Point)

- apply a flattening operation that consists in lowering (in 0.1 dBm/Hz steps) all the highest levels of the above shaped PSD template down such that the power under the resulting template (all-bands) is equal to the MAXNOMATP of the associated VDSL2 Band-profile XYZ (as per Table 6-1/G.993.2). The calculated **flattened PSD template** corresponds to the single self-disturber PSD $P_{SingleSelf\text{-}XYZ,SS}$

All measurements with noise models n_XYZ shall be done with the noise model calculated for the loop length corresponding to the specific test point.

8.6.3 Example system configuration profiles

The configured value for each parameter depends on the test case and the overall aim of the test. The tables below give per xDSL type an example:

8.6.3.1 ADSL1 profiles

The following generic ADSL1 profiles are defined for G.992.1 implementations regardless of being associated to Annex A or B. Because of the different frequency range for Annex A and B, especially in the Upstream, the rate profiles differ for Annex A and B. No G992.2 (ADSL1-lite) profiles are not taken in consideration because these are not relevant for existing access networks.

ADSL1 profiles for Annex A

Profile name	**AnA1_RA_F_8000k**	**AnA1_Fix_F_4832k**
Operation mode	G.992.1 An. A only	G.992.1 An. A only
Adaptation mode	Rate Adaptive	Fixed
Interleaving	Fast	Fast
Interleaving delay	0 ms (or Low)	0 ms (or Low)
DS rate [kbit/s] (max-trgt-min)	8128-8128-32	4832
US rate [kbit/s] (max-trgt-min)	832-832-32	640
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnA1_RA_I_8000k**	**AnA1_Fix_I_4832k**
ADSL mode	G.992.1 An. A only	G.992.1 An. A only
Adaptation mode	Rate Adaptive	Fixed
Interleaving	Interleaved	Interleaved
Interleaving delay	16 ms (or High)	16 ms (or High)
DS rate [kbit/s] (max-trgt-min)	8128-8128-32	4832
US rate [kbit/s] (max-trgt-min)	832-832-32	640
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnA1_Fix_F_1504k**	**AnA1_Fix_F_832k**
Operation mode	G.992.1 An. A only	G.992.1 An. A only
Adaptation mode	Fixed	Fixed
Interleaving	Fast	Fast
Interleaving delay	0 ms (or Low)	0 ms (or Low)
DS rate [kbit/s] (max-trgt-min)	1504	832
US rate [kbit/s] (max-trgt-min)	320	320
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnA1_Fix_I_1504k**	**AnA1_RA_I_832k**
ADSL mode	G.992.1 An. A only	G.992.1 An. A only
Adaptation mode	Fixed	Fixed
Interleaving	Interleaved	Interleaved
Interleaving delay	16 ms (or High)	16 ms (or High)
DS rate [kbit/s] (max-trgt-min)	1504	832
US rate [kbit/s] (max-trgt-min)	320	320
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0

ADSL1 profiles for Annex B

Profile name	**AnB1_RA_F_8000k**	**AnB1_Fix_F_6140k**
Operation mode	G.992.1 An. B only	G.992.1 An. B only
Adaptation mode	Rate Adaptive	Fixed
Interleaving	Fast	Fast
Interleaving delay	0 ms (or Low)	0 ms (or Low)
DS rate [kbit/s] (max-trgt-min)	8128-8128-32	6140
US rate [kbit/s] (max-trgt-min)	832-832-32	640
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnB1_RA_I_8000k**	**AnB1_Fix_I_6140k**
ADSL mode	G.992.1 An. B only	G.992.1 An. B only
Adaptation mode	Rate Adaptive	Fixed
Interleaving	Interleaved	Interleaved
Interleaving delay	16 ms (or High)	16 ms (or High)
DS rate [kbit/s] (max-trgt-min)	8128-8128-32	6140
US rate [kbit/s] (max-trgt-min)	832-832-32	640
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnB1_Fix_F_4096k**	**AnB1_Fix_F_864k**
Operation mode	G.992.1 An. B only	G.992.1 An. B only
Adaptation mode	Fixed	Fixed
Interleaving	Fast	Fast
Interleaving delay	0 ms (or Low)	0 ms (or Low)
DS rate [kbit/s] (max-trgt-min)	4096	864
US rate [kbit/s] (max-trgt-min)	384	160
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0
Profile name	**AnB1_Fix_I_4096k**	**AnB1_RA_I_864k**
ADSL mode	G.992.1 An. B only	G.992.1 An. B only
Adaptation mode	Fixed	Fixed
Interleaving	Interleaved	Interleaved
Interleaving delay	16 ms (or High)	16 ms (or High)
DS rate [kbit/s] (max-trgt-min)	4096	864
US rate [kbit/s] (max-trgt-min)	384	160
DS/US NM [dB] (max-trgt-min)	31-6-0	31-6-0

8.6.3.2 ADSL2 and ADSL2plus profiles

The following generic ADSL2 and ADSL2plus profiles are defined for G.992.3 and G.992.5 implementations regardless of being associated to Annex A or B. This latter shall be defined depending on the system under test. In G.992.3 and G.992.5, the line profile contains several parameters (e.g: nominal PSD and power, carrier mask, …) that are considered as set to the default value specified in G.992.3 or G.992.5.
These have to be considered as Common Line Settings.
General Profiles below identify "latency+INP" combinations relevant for Fast and Interleaved Mode tests. These profiles are the Low delay profile (F-1/0) and the High delay profiles (I-16/2 and I-16/0.5).

General Profiles

Profile name	Parameter	Setting	Description
Low delay profile (F-1/0)	Maximum delay	1	[G.997.1] 7.3.2.2 : The value 1 indicates the Fast Latency Path shall be used in the G.992.1 operating mode and S and D shall be selected such that S<=1 and D=1 in G.992.2, G.992.3 and G.992.4 operating modes.(ed. Note: and G.992.5)
	Minimum INP	0 symbols	
High delay profile A (I-16/2)	Maximum delay	16 ms	One way interleaving delay ⌈S*D⌉/4
	Minimum INP	2 symbols	
High delay profile B (I-16/0.5)	Maximum delay	16 ms	One way interleaving delay ⌈S*D⌉/4
	Minimum INP	0.5 symbols	

Finally specific test profiles are specified which define reference settings for DS/US rates and for the Rate Adaptation mode.
Because of the different frequency range for Annex A and B, especially in the Upstream, the rate profiles differ for Annex A and B. Each of the line profiles below specifies only the ATSE, the RA-MODE and the required DS/US rates. For the applicable combination of Maximum delay and Minimum INP, one specific *General Profile* is referred to. For all the other parameters, the *Common Line Settings* shall apply.
Deviations from these common profiles are indicated in the test description of each test. Specific profiles for further annexes (e.g.: I, J, L, M) of G.992.3 and G.992.5 are not specified here but, where needed, in the relevant sections.
No G992.4 (ADSL2-lite) profiles are not taken in consideration because not relevant for existing access networks.

ADSL2 profiles for Annex A

Profile name	**AnA2_RA_F_16000k**	**AnA2_Fix_F_7290k**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.3 An. A only	G.992.3 An. A only
RA-MODE	AT_INIT	MANUAL
DS rate [kbit/s] (max-min)	16000-32	7290-7290
US rate [kbit/s] (max-min)	2016-32	800-800
Profile name	**AnA2_RA_I_16000k**	**AnA2_Fix_I_7290k**
General Profile	I-16/0.5	I-16/2
Operation mode (ATSE)	G.992.3 An. A only	G.992.3 An. A only
RA-MODE	AT_INIT	MANUAL
DS rate [kbit/s] (max-min)	16000-32	7290-7290
US rate [kbit/s] (max-min)	2016-32	800-800
Profile name	**AnA2_Fix_F_5952k**	**AnA2_Fix_F_2400k**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.3 An. A only	G.992.3 An. A only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	5952-5952	2400-2400
US rate [kbit/s] (max-min)	640-640	352-352
Profile name	**AnA2_Fix_I_5952k**	**AnA2_Fix_I_2400k**
General Profile	I-16/2	I-16/2
Operation mode (ATSE)	G.992.3 An. A only	G.992.3 An. A only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	5952-5952	2400-2400
US rate [kbit/s] (max-min)	640-640	352-352

ADSL2 profiles for Annex B

Profile name	**AnB2_RA_F_16000k**	**AnB2_Fix_F_7290k**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.3 An. B only	G.992.3 An. B only
RA-MODE	AT_INIT	MANUAL
DS rate [kbit/s] (max-min)	16000-32	7290-7290
US rate [kbit/s] (max-min)	2016-32	800-800
Profile name	**AnB2_RA_I_16000k**	**AnB2_Fix_I_7290k**
General Profile	I-16/2	I-16/2
Operation mode (ATSE)	G.992.3 An. B only	G.992.3 An. B only
RA-MODE	AT_INIT	MANUAL
DS rate [kbit/s] (max-min)	16000-32	7290-7290
US rate [kbit/s] (max-min)	2016-32	800-800

Profile name	**AnB2_Fix_F_3456**	**AnB2_Fix_F_864k**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.3 An. B only	G.992.3 An. B only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	3456-3456	864-864
US rate [kbit/s] (max-min)	448-448	160-160
Profile name	**AnB2_Fix_I_3456**	**AnB2_Fix_I_864k**
General Profile	I-16/2	I-16/2
Operation mode (ATSE)	G.992.3 An. B only	G.992.3 An. B only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	3456-3456	864-864
US rate [kbit/s] (max-min)	448-448	160-160

ADSL2plus profiles for Annex A

Profile name	**AnA2plus_RA_F_30000k**	**AnA2plus_Fix_F_10000k**	**AnA2plus_Fix_F_7290k**
General Profile	F-1/0	F-1/0	F-1/0
Operation mode (ATSE)	G.992.5 An. A only	G.992.5 An. A only	G.992.5 An. A only
RA-MODE	AT_INIT	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	30000-32	10000-10000	7290-7290
US rate [kbit/s] (max-min)	2016-32	832-832	800-800
Profile name	**AnA2plus_RA_I_30000k**		**AnA2plus_Fix_I_7290k**
General Profile	I-16/0.5		I-16/2
Operation mode (ATSE)	G.992.5 An. A only		G.992.5 An. A only
RA-MODE	AT_INIT		MANUAL
DS rate [kbit/s] (max-min)	30000-32		7290-7290
US rate [kbit/s] (max-min)	2016-32		800-800

Profile name	**AnA2plus_Fix_F_5952k**	**AnA2plus_Fix_F_2400k**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.5 An. A only	G.992.5 An. A only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	5952-5952	2400-2400
US rate [kbit/s] (max-min)	640-640	352-352
Profile name	**AnA2plus_Fix_I_5952k**	**AnA2plus_Fix_I_2400k**
General Profile	I-16/2	I-16/2
Operation mode (ATSE)	G.992.5 An. A only	G.992.5 An. A only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	5952-5952	2400-2400
US rate [kbit/s] (max-min)	640-640	352-352

ADSL2plus profiles for Annex B

Profile name	**AnB2plus_RA_F_30000k**	**AnB2plus_Fix_F_10000k**	**AnB2plus_Fix_F_7290k**
General Profile	F-1/0	F-1/0	F-1/0
Operation mode (ATSE)	G.992.5 An. B only	G.992.5 An. B only	G.992.5 An. B only
RA-MODE	AT_INIT	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	30000-32	10000-10000	7290-7290
US rate [kbit/s] (max-min)	2016-32	832-832	800-800
Profile name	**AnB2plus_RA_I_30000k**		**AnB2plus_Fix_I_7290k**
	I-16/2		I-16/2
Operation mode (ATSE)	G.992.5 An. B only		G.992.5 An. B only
RA-MODE	AT_INIT		MANUAL
DS rate [kbit/s] (max-min)	30000-32		7290-7290
US rate [kbit/s] (max-min)	2016-32		800-800

Profile name	**AnB2plus_Fix_F_3456**	**AnB2plus_Fix_F_864**
General Profile	F-1/0	F-1/0
Operation mode (ATSE)	G.992.5 An. B only	G.992.5 An. B only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	3456-3456	864-864
US rate [kbit/s] (max-min)	448-48	160-160
Profile name	**AnB2plus_Fix_I_3456k**	**AnB2plus_Fix_I_864**
	I-16/2	I-16/2
Operation mode (ATSE)	G.992.5 An. B only	G.992.5 An. B only
RA-MODE	MANUAL	MANUAL
DS rate [kbit/s] (max-min)	3456-3456	864-864
US rate [kbit/s] (max-min)	448-448	160-160

The table below defines generic ADSL2 and ADSL2plus profiles regardless of being associated to Annex A or B. This latter shall be defined depending on the system under test. In G.992.3 and G.992.5, the line profile contains several parameters (e.g: nominal PSD and power, carrier mask, …) that are considered as set to the default value specified in G.992.3 or G.992.5. These have to be considered as Common Line Settings. The table below identifies "latency+INP" combinations (*General Profile*s) relevant for Fast and Interleaved Mode tests. These profiles are the Low delay profile (F-1/0) and the High delay profiles (I-16/2 and I-16/0.5).

Profile name	Parameter	Setting	Description
Low delay profile (F-1/0)	Maximum delay	1	[G.997.1] clause 7.3.2.2 : The value 1 indicates the Fast Latency Path shall be used in the G.992.1 operating mode and S and D shall be selected such that S<=1 and D=1 in G.992.2, G.992.3 and G.992.4 operating modes.(ed. Note: and G.992.5)
	Minimum INP	0 symbols	
High delay profile A (I-16/2)	Maximum delay	16 ms	One way interleaving delay ⌈S*D⌉/4
	Minimum INP	2 symbols	
High delay profile B (I-16/0.5)	Maximum delay	16 ms	One way interleaving delay ⌈S*D⌉/4
	Minimum INP	0.5 symbols	

Finally specific test profiles are specified which define reference settings for DS/US rates and for the Rate Adaptation mode.
Because of the different frequency range for Annex A and B, especially in the Upstream, the rate profiles differ for Annex A and B. Each of the line profiles below specifies only the ATSE, the RA-MODE and the required DS/US rates. For the applicable combination of Maximum delay and Minimum INP, one specific *General Profile* is referred to. For all the other parameters, the *Common Line Settings* shall apply.
Deviations from these common profiles are indicated in the test description of each test. Specific profiles for further annexes (e.g.: I, J, L, M) of G.992.3 and G.992.5 are not specified here but, where needed, in the relevant sections.
No G992.4 (ADSL2-lite) profiles are not taken in consideration because these are not relevant for existing access networks.

8.6.3.3 SHDSL profiles

Profile name	**S_2w_2304k**	**S_4w_4608k**
Regional Setting	Annex B	Annex B
Wire Mode	2 Wire	4 Wire
PSD	Symmetric	Symmetric
Bit rate [kbit/s] (max-min)	2304-192	4608-192
DS/US NM [dB] (trgt-worst)	TBD-TBD	TBD-TBD

8.6.3.4 VDSL1 profiles

These profiles can be defines similarly to those specified in section “VSL2 profiles”.

8.6.3.5 VDSL2 profiles

For VDSL2 systems, the first settings to be defined are related to the VDSL2 Band-profile. This defines the used frequency spectrum and the allocation of DS and US bands, the associated PSD mask and maximum aggregate transmit power (ATP), finally the type of US0 mask is defined which identifies if the system is compatible with POTS or ISDN legacy services.

VDSL2 Band-profile	BA8b	BA12a	BA17a	BA30a	BA17a_D&UPBO	BA30a_D&UPBO
Profile	8b	12a	17a	30a	17a	30a
Annex	B	B	B	B	B	B
Limit PSD Mask (short name)	998-M2x-A (B8-4)	998-M2x-A (B8-4)	998E17-M2x-NUS0 (B8-8)	998E30-M2x-NUS0 (B8-12)	998E17-M2x-NUS0 (B8-8)	998E30-M2x-NUS0 (B8-12)
US0 type	A	A	NA	NA	NA	NA
MAXNOMATPds	+20.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm
VDSL2 Band-profile	**BB8b**	**BB12a**	**BB17a**	**BB30a**	**BB17a_D&UPBO**	**BB30a_D&UPBO**
Profile	8b	12a	17a	30a	17a	30a
Annex	B	B	B	B	B	B
Limit PSD Mask (short name)	998-M2x-B (B8-6)	998-M2x-B (B8-6)	998ADE17-M2x-B (B8-11)	998ADE30-M2x-NUS0-B (B8-14)	998ADE17-M2x-B (B8-11)	998ADE30-M2x-NUS0-B (B8-14)
US0 type	B	B	B	NA	B	NA
MAXNOMATPds	+20.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm	+ 14.5 dBm

The following generic VDSL2 profiles are defined for G.993.2 Annex B implementations regardless of being associated to VDSL2overPOTS or VDSL2overISDN deployments. This shall be defined depending on the system under test.

The line settings encompass several parameters (e.g: nominal PSD and power, carrier mask, xPBO, …) that are considered as set to the default value specified in G.993.2. These have to be considered as Common Line Settings. With these defaults the system operates with full PSD, i.e. no DPBO, no UPBO, no RFI notches nor any other type of PSD shaping is applied.

Common Line Settings with full-PSD for band profiles BA8b, BB8b, BA12a, BB12a, BA17a, BB17a, BA30a, BB30a

Parameter	Setting	Description
All parameters but those specified below	Default value	
Power management state forced (PMSF)	0	
Power management state enabling (PMMode)	0	
Loop diagnostic mode forced (LDMF)	0	
Automode cold start forced	0	
DPBO	off	
UPBO	off	
RFI notches	off	
MAXSNRMds	$FFFF_{16}$	
MAXSNRMus	$FFFF_{16}$	
TARSNRMds	6 dB	
TARSNRMus	6 dB	
MINSNRMds	0 dB	
MINSNRMus	0 dB	
MSGMINds	16 kbps	
MSGMINus	16 kpbs	
Preemption option flag, ds	00_{16}	
Preemption option flag, us	00_{16}	
Short packet option flag, ds	00_{16}	
Short packet option flag, us	00_{16}	
FORCEINP	1	

As for VDSL2, it is relevant to test with shaping, the following specific Common Line Settings are defined for operation with DPBO and UPBO which are adopted in real networks:

Common Line Settings with D&UPBO for band profiles BA17a_D&UPBO, BB17a_D&UPBO, BA30a_D&UPBO, BB30a_D&UPBO

Parameter	BA17a_ D&UPBO	BB17a_ D&UPBO	BA30a_ D&UPBO	BB30a_ D&UPBO	Description
All parameters but those specified below	Value as specified in the previous **Common Line Settings** table				
DPBOEPSD	ADSL2plus Annex A	ADSL2plus Annex B	ADSL2plus Annex A	ADSL2plus Annex B	PSD mask at the exchange
DPBOESEL	27dB@1MHz	27dB@1MHz	72dB@1MHz	72dB@1MHz	E-side electrical length
DPBOESCMA	0.1924	0.1924	0.1924	0.1924	Model of loss of E-side cable (NOTE)
DPBOESCMB	0.5960	0.5960	0.5960	0.5960	
DPBOESCMC	0.2086	0.2086	0.2086	0.2086	
DPBOMUS	-95 dBm/Hz	-95 dBm/Hz	-95 dBm/Hz	-95 dBm/Hz	Minimum usable receive PSD
DPBOFMIN	138 kHz	254 kHz	138 kHz	254 kHz	Minimum frequency from which on the DPBO shall be applied
DPBOFMAX	2208 kHz	2208 kHz	2208 kHz	2208 kHz	Maximum frequency up to which the DPBO shall be applied
UPBOKLF	0	0	0	0	Force electrical loop length $\Rightarrow kl_0$ is estimated during training
UPBOKL	estimated during training	estimated during training	estimated during training	estimated during training	US electrical loop length (kl_0)
UPBOA US0	40.00	40.00	40.00	40.00	A value US band 1
UPBOB US0	0	0	0	0	B value US band 1
UPBOA US1	47.30	47.30	47.30	47.30	A value US band 1
UPBOB US1	21.14	21.14	21.14	21.14	B value US band 1
UPBOA US2	54.00	54.00	54.00	54.00	A value US band 2
UPBOB US2	16.29	16.29	16.29	16.29	B value US band 2
UPBOA US3	54.00	N/A	54.00	40.00	A value US band 3
UPBOB US3	16.29	N/A	16.29	0	B value US band 3
UPBOA US4	N/A	N/A	40.00	N/A	A value US band 4
UPBOB US4	N/A	N/A	0	N/A	B value US band 4

NOTE: the values of DPBOESCMA, B and C are referred to a PE 0.4mm loop.

General Profiles below identify “latency+INP” combinations relevant for Fast and Interleaved Mode tests. These profiles are the Low delay profile (F-1/0) and the High delay profiles (I-8/2).

General Profiles

General line-setting	Parameter	Setting	Description
Low delay profile (F-1/0)	delay_maxn ds	1	
	delay_maxn us	1	
	INP_minn ds	0 symbols	
	INP_minn us	0 symbols	
High delay profile (I-8/2)	delay_maxn ds	8 ms	One way interleaving delay ⌈S*D⌉/4
	delay_maxn us	8 ms	One way interleaving delay ⌈S*D⌉/4
	INP_minn ds	2 symbols	
	INP_minn us	2 symbols	

Specific line-setting are specified which define reference settings for DS/US rates and for the Rate Adaptation mode. For the applicable combination of Maximum delay and Minimum INP, one specific *General line-setting* is referred to.

Specific line-setting	General line-setting	RA-Mode	DS net datarate (kbit/s) (max- min)	US net datarate (kbit/s) (max-min)
RA_F_150_150	F-1/0	AT_INIT	150000-128	150000-64
RA_I_150_150	I-8/2	AT_INIT	150000-128	150000-64

Finally, the complete settings for the System Under Test (SUT) are defined by the association between a VDSL2 band-profile with its *Common Line Settings* (with full-PSD or with D&UPBO) and a Specific line-setting. These are called Profile-line combinations

VDSL2 Profile-line combinations for Annex B (both for VDSL2oPOTS and VDSL2oISDN)

Profile-line combination	Band-profile	Specific line-setting
BA8b_RA_F_150_150	BA8b	RA_F_150_150
BA8b_RA_I_150_150	BA8b	RA_I_150_150
BB8b_RA_F_150_150	BB8b	RA_F_150_150
BB8b_RA_I_150_150	BB8b	RA_I_150_150
BA12a_RA_F_150_150	BA12a	RA_F_150_150
BA12a_RA_I_150_150	BA12a	RA_I_150_150
BB12a_RA_F_150_150	BB12a	RA_F_150_150
BB12a_RA_I_150_150	BB12a	RA_I_150_150
BA17a_RA_F_150_150	BA17a	RA_F_150_150
BA17a_RA_I_150_150	BA17a	RA_I_150_150
BA17a_D&UPBO_RA_F_150_150	BA17a_D&UPBO	RA_F_150_150
BA17a_D&UPBO_RA_I_150_150	BA17a_D&UPBO	RA_I_150_150
BB17a_RA_F_150_150	BB17a	RA_F_150_150
BB17a_RA_I_150_150	BB17a	RA_I_150_150
BA17a_D&UPBO_RA_F_150_150	BB17a_D&UPBO	RA_F_150_150
BB17a_D&UPBO_RA_I_150_150	BB17a_D&UPBO	RA_I_150_150
BA30a_RA_F_150_150	BA30a	RA_F_150_150
BA30a_RA_I_150_150	BA30a	RA_I_150_150
BA30a_D&UPBO_RA_F_150_150	BA30a_D&UPBO	RA_F_150_150
BA30a_D&UPBO_RA_I_150_150	BA30a_D&UPBO	RA_I_150_150
BB30a_RA_F_150_150	BB30a	RA_F_150_150
BB30a_RA_I_150_150	BB30a	RA_I_150_150
BB30a_D&UPBO_RA_F_150_150	BB30a_D&UPBO	RA_F_150_150
BB30a_D&UPBO_RA_I_150_150	BB30a_D&UPBO	RA_I_150_150

8.6.4 Example PSD specifications

Examples of PSD mask specifications can be found in e.g., ETSI SpM-standard (part1) and the ITU-T recommendations.
Table 8-29 gives per xDSL type an example for the PSD mask specifications.

xDSL type	Access rule reference
ADSL over POTS (EC)	ETSI TR 101 830-1 clause 11.1
ADSL FDD over POTS	ETSI TR 101 830-1 clause 11.2
ADSL over ISDN (EC)	ETSI TR 101 830-1 clause 11.3
ADSL FDD over ISDN	ETSI TR 101 830-1 clause 11.4
ADSL2+ over POTS (EC)	ITU G.992.5 clause Annex A.1.2 and A.2.2
ADSL2+ FDD over POTS	ITU G.992.5 clause Annex A.1.3 and A.2.2
ADSL2+ over ISDN (EC)	ITU G.992.5 clause Annex B.1.2 and B.2.2
ADSL2+ FDD over ISDN	ITU G.992.5 clause Annex B.1.3 and B.2.2
SDSL (TC-PAM)	ETSI TR 101 830-1 clause 10.5
SDSL (2B1Q)	ETSI TR 101 830-1 clause 10.11
VDSL	ETSI TR 101 830-1 clause 12.1

Table 8-29: suggestions/examples for PSD mask specifications per xDSL type.

8.7 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).

9 FIBRE SPECIFIC TESTING

9.1 Introduction

Chapter 9 specifies methodologies for testing fibre specific issues.
There is a wide variety of optical access systems. Systems are based on P2P and P2MP architectures, using one or several wavelengths for signal transmission purposes and they can work analogue or digital. Moreover, they can be divided on pure fibre optic systems and hybrid ones using fibre and copper paths (e.g. P2P optical Ethernet + VDSL). Many test methods descibed in this chapter refer to specific requirements on fibre optic based systems (e.g. sensitivity to reflections, differential fibre distance in P2MP systems). Nevertheless, there are also some common test methodologies (e.g. chromatic dispersion test), independent on the type of fibre optic system.

9.2 Test configurations

This paragraph presents selected test configurations to be used in test methodologies for fibre optic based systems. Each test configuration refers to specific tests, which are described in following paragraphs.

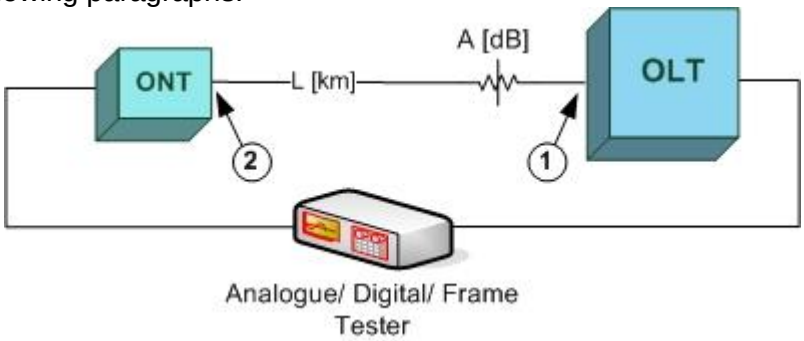


Figure 9-1: Test configuration for optical reach measurement

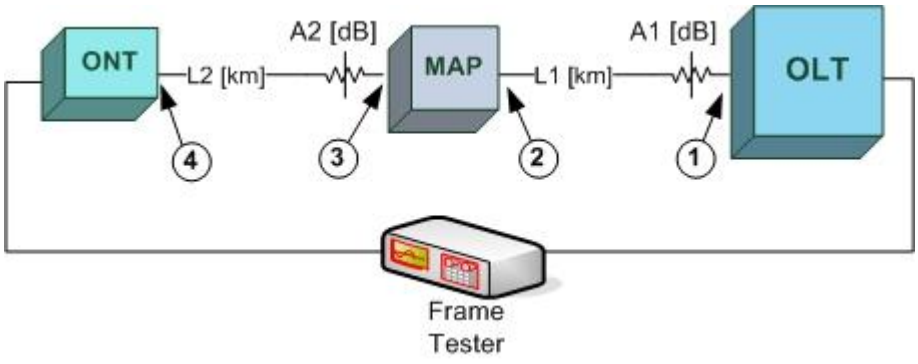


Figure 9-2: Test configuration for optical reach measurements - XL PON

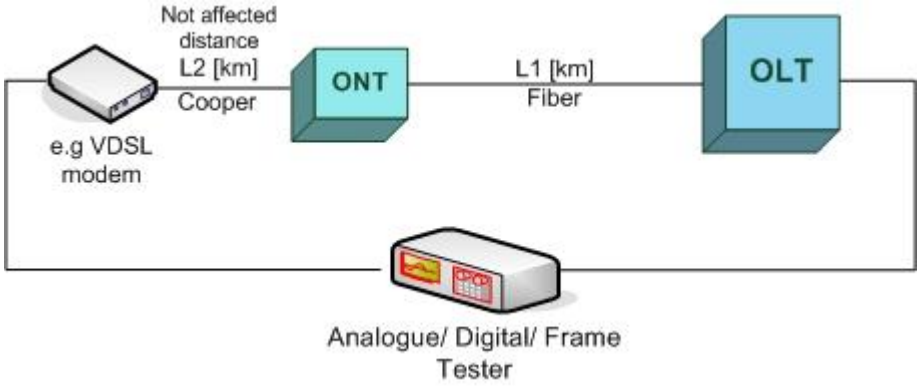


Figure 9-3: Test configuration for optical reach measurements - hybrid P2P system (e.g. fibre + copper)

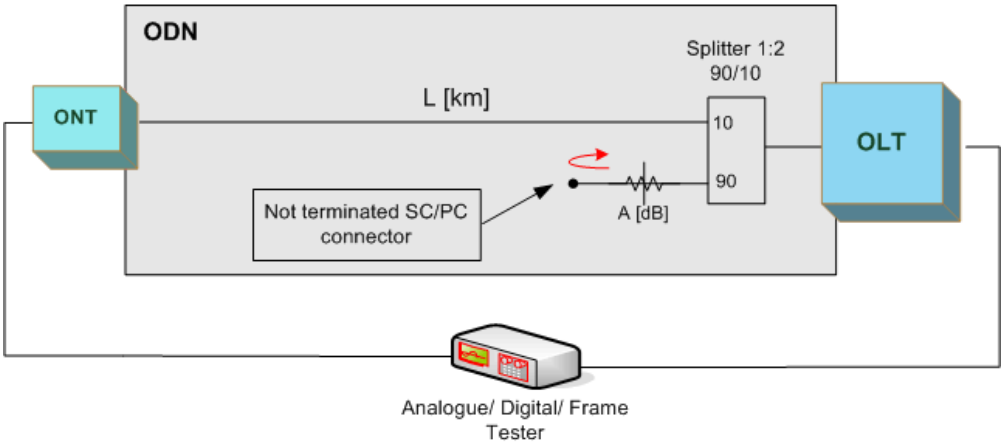


Figure 9-4: Test configuration for ORL sensitivity measurements - P2MP system

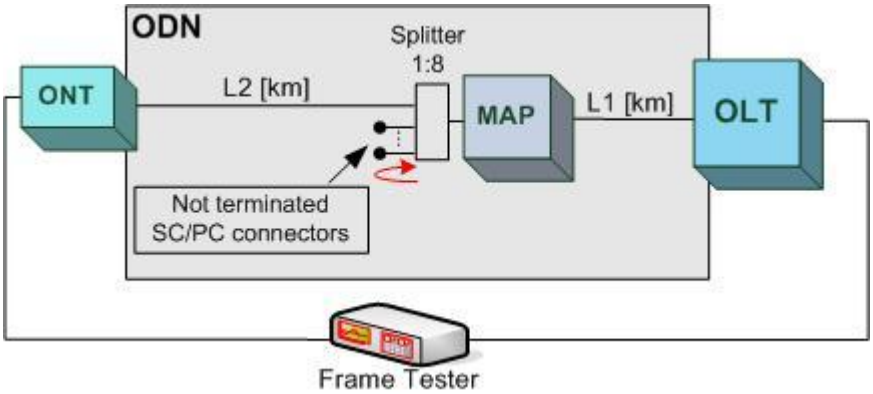


Figure 9-5: Test configuration for ORL sensitivity measurements - XL-PON

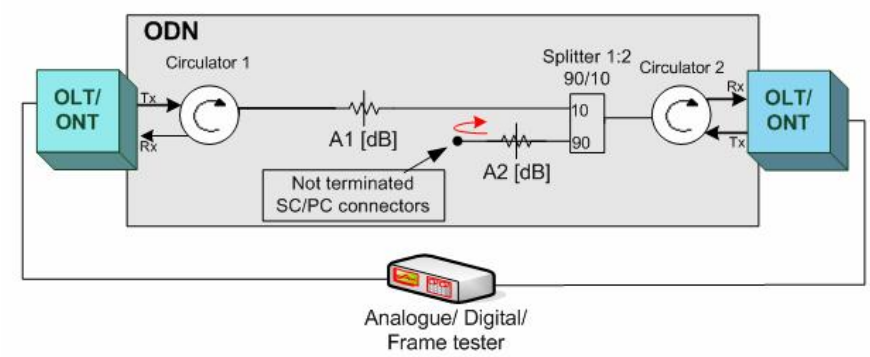


Figure 9-6: Test configuration for ORL sensitivity measurements - P2P system with optical circulators

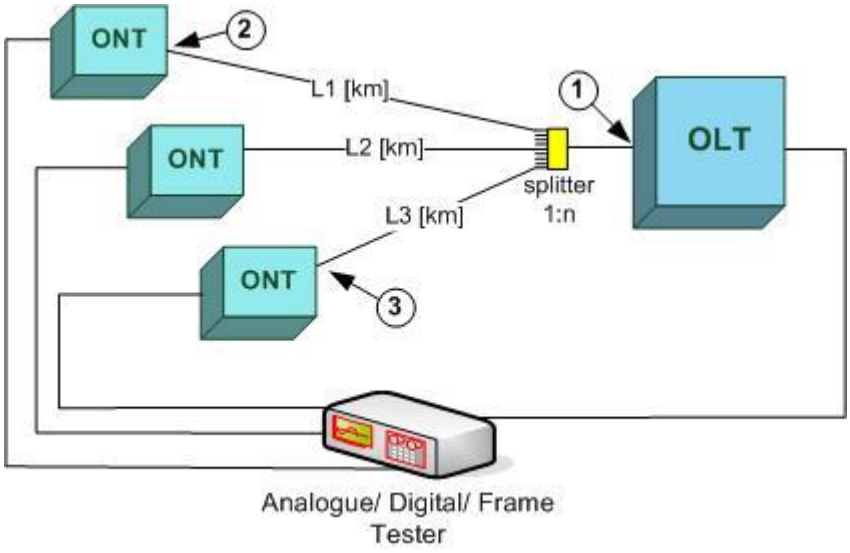


Figure 9-7: Test configuration for differential fibre distance measurement - pure fibre optic system

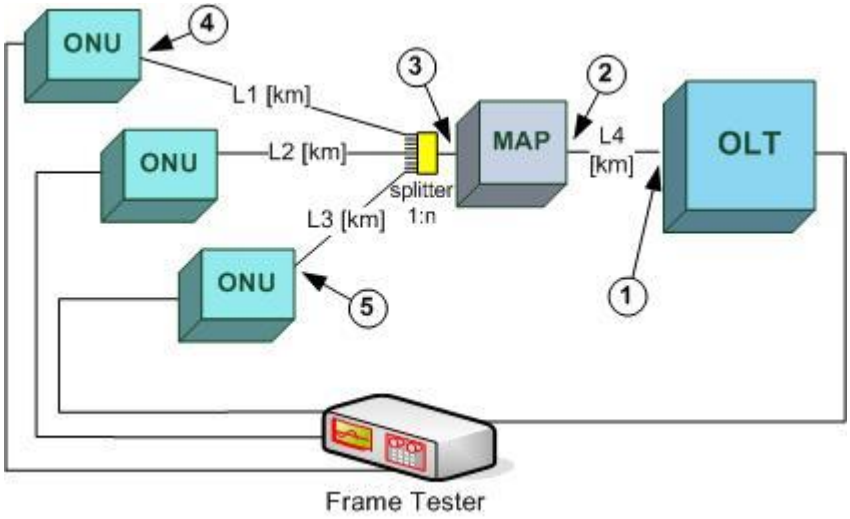


Figure 9-8: Test configuration for differential fibre distance measurement - XL PON

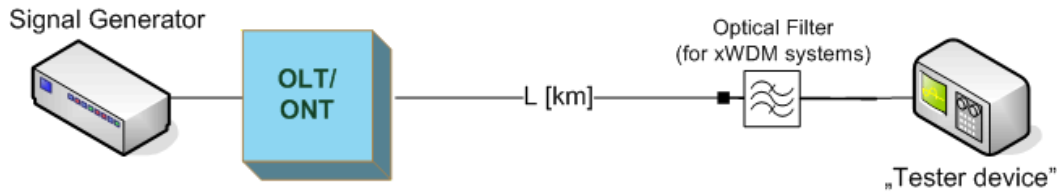


Figure 9-9: Test configuration for optical signal measurements - P2P system (upstream and downstream) and P2MP system (downstream)

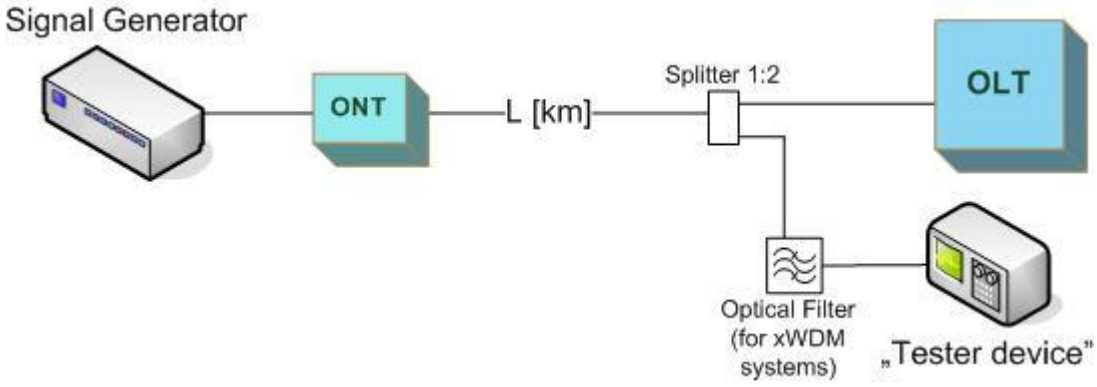


Figure 9-10: Test configuration for optical signal measurements - P2MP system (upstream)

9.3 Transceiver characteristic

The increasing demand for high-speed communication in access networks has stimulated the development of optical transceiver modules mainly consisting of transmitter, receiver and electronic devices. There are several quasi standards or MSA (created by industry consortia of vendors) that specify compact transceiver modules for access network applications e.g. SFP, XFP. In order to achieve interoperability between vendors, different standard organisations have defined test methods to determine the transceiver performance. However, there are several different standards to refer to. ANSI and TIA/EIA have published recommendations for implementing the SONET standards. Standards created by the ITU-T and by the IEC also describe appropriate test procedures for synchronous networking systems and optical networks in general. However, over the last decades Ethernet evolved as a low-cost, high-performance technology for access network applications with documents published by ANSI/IEEE. Hence, in this section state-of-the-art test equipment and measurement methods targeting standard access networks applications are described in the form of a synopsis with references for relevant standards if they apply as well. To accomplish transmitter signal compliance tests, original standard documents, test procedures as well as application notes provided by companies selling corresponding measurement instruments have to be considered.

Considerations within this chapter will focus on the testing of optical transceivers typically used to implement access network configurations described in section 9.2. Sketched measurement methods are restricted to digital transmission techniques although niche applications such as analogue signal transmission (e.g. TV distribution services) are recommended design options in some PON standards. However, measurement methods to specify analogue formatted signals may differ completely from their digital counterparts e.g with respect to associated testing requirements and measuring apparatus.

Depending on the worst case attenuation/dispersion requirements of currently projected access networks supporting a maximum reach of 20 km (standards oriented) different transmitter types will be needed. Due to their broad lasing spectrum (up to 4 nm) FP lasers are being applied mainly to implement short range systems operating at 1300 nm. In contrast, directly modulated standard DFB lasers may support data rates up to 4.25 Gb/s over 20 km despite considerable transmission impairments due to chromatic dispersion (assumption 1 dB penalty) over the full wavelength spectrum between 1270 nm to 1610 nm. However, lengthening the transmission span and/or raising the data rates up to 10 Gb/s will require additional measures to meet the signal transport requirements of such high-performance access networks. Promising approaches to mitigate accompanying transmission impairments include EDC (refers to electronic mitigation techniques), FEC (refers to error correction strategies) e.g. according to ITU-T G.707 and external modulators to create high-performance light sources that allow for bridging transmission distances up to 70 km at 1610 nm and 100 km around 1300 nm. The following sections will discuss basic measurement methods to evaluate the performance of transmitters and receivers needed to design future-proofed fibre optical links.

9.3.1 Optical transmitter

Table 9-1 shows basic parameters to characterise transmitters for access network applications.

Spectral characteristics
central frequency
frequency deviation
line width
SMSR
chirp
Mean launch power
Extinction ratio
Eye pattern (mask)

Table 9-1: Important parameters for access network transmitters

Spectral content is a fundamental characteristic of an optical signal. Corresponding parameters to characterise access systems are the central frequency (nominal operating wavelength), maximum and minimum frequency deviation, line width and side mode suppression ratio (SMSR) that indicates the laser type used. Also of importance are the maximum chirp (refers to the laser wavelength shift caused by direct laser modulation, see section 9.3.3), mean launch power (MLP) and extinction ratio (ER) that can be derived from an eye pattern. Eye pattern mask tests are performed usually to specify the transmitter pulse shape characteristics. ER and MLP are essential elements in the assessment of transmitters typically used by telecommunication standards to evaluate the performance of a link. In contrast, 10 GbE emphasizes novel measurement methods.

9.3.1.1 Output power measurement methodology

Applicable to following systems:

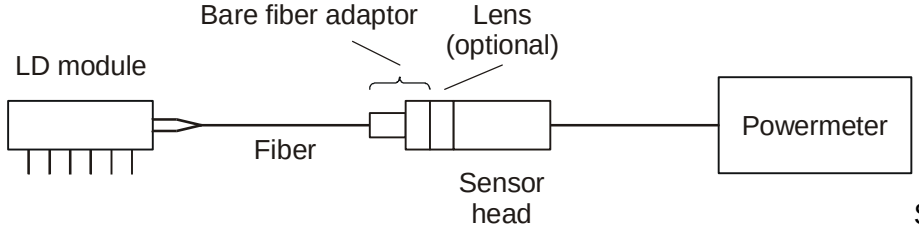
External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

The determination of the absolute average optical power (normally expressed in dBm) is a basic measurement task to specify transmitters and receivers (sensitivity) as well as to obtain path power levels e.g. for eye safety considerations, [IEC EN 60825-2]. Measurements may be performed using power meters or optical spectrum analysers (OSA). As far as power meters are concerned, a number of attractive equipment solutions is available for power measurements applications showing an overall accuracy in the order of +/- 0.02 dB. Commercial standard products usually contain photodetectors to detect the incoming light. Here, large area In GaAs detector types provide an excellent linearity and a low wavelength dependence in the long wavelength range combined with excellent sensitivity characteristics. Optical power meters may be equipped with or without external optical heads showing potentially interface modules with large core multimode fibres to launch the incoming light. OSAs represent an alternative to powermeters but suffer from a limited accuracy in the range of +/- 0.2 dB. Table 9-2 shows the most important parameters to characterise power meters. The accuracy of power meters inherently depends on calibrations needed to measure the optical power over an adequate dynamic range and a given wavelength range. Spectral responsivity and linearity are usually stored in the optical head. For most test applications calibration verifications are optional, only the wavelength range is to be selected. However, the polarisation state of the incoming light mostly is completely unpredictable. Hence, the polarisation-dependent responsivity (polarisation-dependent loss) of the power meter should be as low as possible. OSAs represent an alternative to power meters but suffer from a limited accuracy in the range of +/- 0.2 dB. A wide power dynamic range is the most important OSA specification allowing accurate mesurements of high power values and low noise floors. Current applications need to control OSNR levels from 20 dB up to 35 dB. Considerably larger OSNR values have to be measured in future access networks with link data rates up to 10 Gb/s. However, even field-portable OSAs meet these requirements.

Calibration
Spectral responsivity
Linearity
PDL
Reflectivity of the optical head
Reflection

Table 9-2: Important parameters for optical power measurements

Power measurement methods are specified in [TIA/EIA-455-95]. More information may be found in [Derickson], [Hewlett-Packard]. Figure 9-11 shows a principal configuration to measure the laser output power using a power meter. Please note: Power meters are not an adequate equipment to perform measurements in the upstream direction of P2MP systems, see paragraph 9.5.3.



Source: Derickson

Figure 9-11: Power measurement of a pigtailed laser diode

9.3.1.2 Optical spectrum measurement methodology

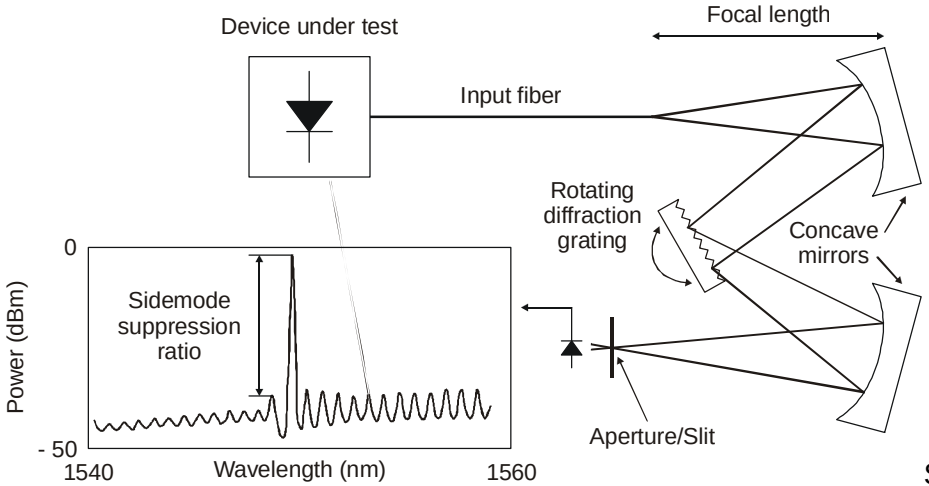
Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

The most important parameters for optical sources in access networks are wavelength, line width (spectral width), SMSR and isolation. Moreover, optical sources in high-speed access networks are typically single-longitudinal mode lasers with narrow spectral line width. Modulation of the laser injection current (directly modulated laser - DML) results in an unwanted laser frequency modulation, or chirp, that broadens the spectral line width of the laser.

- *Wavelength*

Optical spectrum analyser (OSA) and wavemeter are most important commercially available equipment options to measure the absolute wavelength comimg from an optical source. Moreover, an OSA can divide a lightwave signal into its constituent wavelengths. Hence, it provides a view of the spectral content of e.g. WDM signals by taking a scan at the wavelength range of interest, Figure 9-12. Here, the most important specification is a large optical rejection ratio (ORR) allowing for high channel counts and small channel spacings (< 50 GHz), [EXFO I]. Moreover, the line width of an unmodulated DFB laser is in the order of 10 MHz (see also paragraph 'linewidth'). However, the minimum width that can be displayed by an OSA is limited by the implemented filter (typical resolution bandwidth e.g. +/-5 pm/1550 nm - ~1 GHz). Direct modulation of DFB lasers broadens the line width. Depending on their sophistication the performance of currently available OSAs may be sufficient to display accurately the spectral line width of lasers for data rates up to 10 Gb/s.



Source: Derickson

Figure 9-12: OSA and a scan for a DFB laser

The most common OSAs for fibre optic applications are diffraction grating based instruments. Figure 9-12 shows a sketch of an OSA using this technique as well as information on a measured DFB laser including single lasing wavelength property, optical power, wavelength and side mode suppression ratio (SMSR). The absolute wavelength is an important parameter for the design and operation of WDM based access networks.

Alternatively, the wavelength of an optical signal can be measured more precisely using a wavemeter showing a resolution in the picometer range (typically +/- 3 pm). However, no line width information is provided. More information on wavelength measurements may be found in [IEC 61280-1-3], [TIA 526-3].

- *Linewidth*

The line width of a laser is measured during continuous wave operation. Since the line width of DFB lasers typically is in the order of 10 MHz, OSA does not provide sufficient wavelength resolution to evaluate details of the actual mode shape. To evaluate the width of such fine laser lines, considerable resolution improvements are required usually provided by using complex heterodyne and homodyne analysis tools with a typical resolution of 1 MHz. For single-longitudinal mode lasers, the spectral line width is defined as the full width of the largest spectral peak, measured 20 dB down from the maximum amplitude of the peak.

- *SMSR*

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 (see Figure 9-12). The SMSR specification is intended to minimize the occurrence of BER degradations due to mode partition noise. Hence the SMSR specification is relevant only to SLM laser sources. In practice, SMSR is usually measured using OSA. State-of-the-art equipment provides analysing optical spectra in the 600 nm to 1700 nm wavelength range.

- *Isolation*

Optical isolators are required usually in high-speed communication systems to prevent transmitters from having undesired effects due to backscattered optical signals. The underlying technique of the isolation is based on a Faraday Rotator using single crystals. Depending on the material used standard optical isolators may provide superior performance between 500 nm to 2000 nm (low insertion loss, isolation >40 dB within their specified wavelength range). Isolation is also an important property of optical components e.g. in WDM transport systems. Couplers demand isolation of one wavelength region from another and channel filters are used to isolate specific wavelength channels in a channel grid making it possible to multiplex different data signals. The transmission performance of an 18 channel CWDM DeMultiplexer is examplarily shown in Figure 9-27. Isolation here is the difference between the maximum reflectance of a given channel in the passband of an adjacent channel and the minimum reflectance in the reflect band. Measurement configurations are mainly based on tunable optical sources or broadband sources as stimulus and an OSA to perform the sweeping. Common available CWDM DeMultiplexers based on TFF techniques may be manufactured to provide sufficient isolation for both unidirectional and bidirectional operation. Here, isolation is crucial, because bidirectional DeMultiplexers have both input and output channels at the same side of the device and input light for one direction can appear on the output port for the other direction.

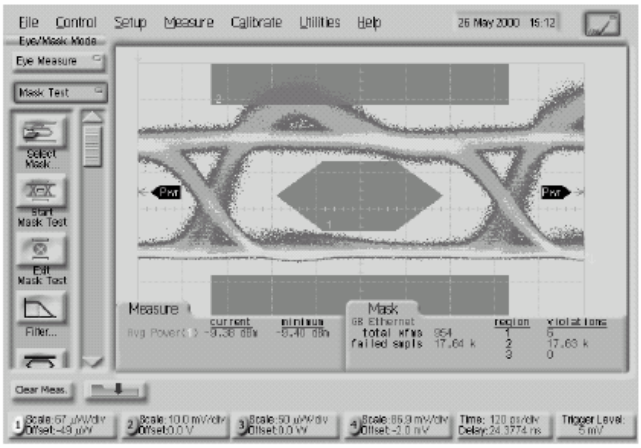
9.3.1.3 Eye diagram measurement methodology

Applicable to following systems:

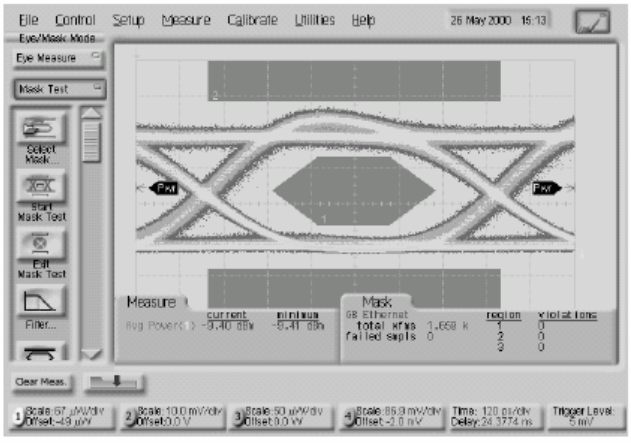
External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
X	x	x	x	x		x	x	x

Eye diagram testing is a key element in the quality assessment and manufacturing of optical transmitters and provides an easy view of digital performance. Various communication standards recommend eye diagram testing procedures and define an allowable shape of the transmitter output waveform through an eye mask. An eye mask typically consists of three polygons placed above, below and within the eye diagram, enclosing keep-out regions that must not be violated, [Agilent II]. Mask shapes are typically defined by the specific communications standards.
Directly modulated high-speed lasers often exhibit significant overshoot and ringing that are not compliant with an eye diagram test, Figure 9-13 (a). Hence, all corresponding standards require that eye mask tests be performed with an optical receiver that has a filtered response. With filtering the same laser can be shown to be mask test compliant, Figure 9-13 (b). The reduced bandwidth (filtered) receiver will behave similarly to the system level receivers typically used in actual transmission systems. Further information on optical eye pattern measurements may be found in [TIA/EIA-526-4A], [ITU-T G.957], [IEEE Std 802.3-2005], [TIA 526-3], [Tektronix I], [Agilent I], [Agilent III].

(a)



(b)



Source: Agilent

Figure 9-13: Eye mask violated by an unfiltered waveform (a) and mask test with filter (b)

Eye diagrams can be an powerful indicator of performance of both transmitters and digital transmission systems. Measurements are typically performed using digital communication analyzers. The primary components of an optical detection system (box with dashed lines in Figure 9-14) are a photodetector, a low-pass filter, a digitising oscilloscope, and an optical power meter. Figure 9-14 also shows the standard-prescribed way of measuring the eye pattern pictured in [IEC 61280-2-2]. Instead of an overall quality assessment by mask tests a series of separate eye parameters can also be specified to characterise the transmitter performance. Common measurements include:

- Extinction ratio
- Rise/fall time
- Jitter

An important issue that applies primarily to high-speed signal analysis is the minimum quality of the equipment to be used. The two key parameters that affect a digital storage oscilloscope's measurement accuracy are bandwidth and sample rate. More information may be found in [Agilent IV].

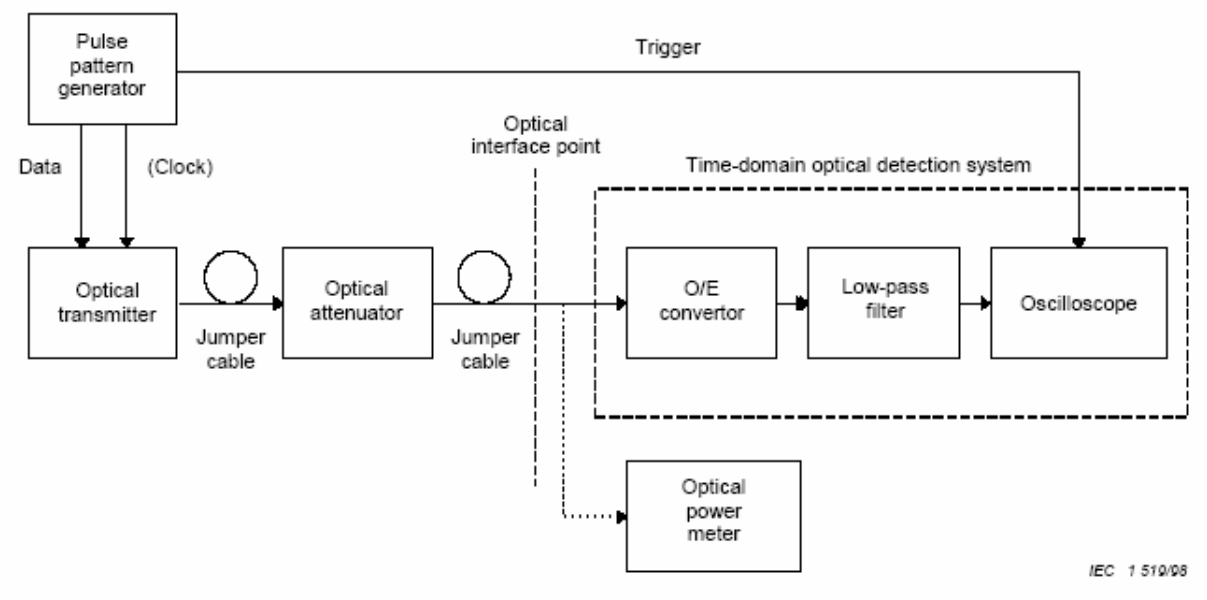
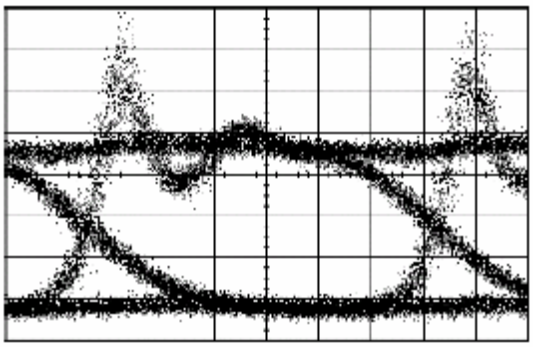


Figure 9-14: Optical eye pattern, waveform, and extinction ratio measurement configuration

As mentioned above transmitters usually are qualified by using a digital communication analyser to perform and measure eye parameters and mask tests. Optionally, waveforms can be viewed using sampling oscilloscopes in order to identify and troubleshoot bit pattern impairments. However, only a few bits can be shown simultaneously compared to the overall presentation of information provided by eye diagrams. In contrast, the performance assessment alternative BER (ratio of the numbers of erroneous bits bits received to the total number of bits received) testing is typically used to qualify/quantify a receiver or a complete communication system.

- *Interpretation of eye diagram shape*

Eye diagrams are a simple and useful tool for evaluating transmitters and transmission systems. The basic information contained in an eye diagram include eye opening, distortions of the signal's amplitude due to noise effects and timing errors (due to variations of the rising/falling edges). Moreover, in order to assess comprehensively the transmitter signal, it is important to consider not only the eye opening, but also the overshoot and undershoot characteristics. As can be seen in Figure 9-15, the rising signal edge of a fairly directly modulated laser (DML) ends in an undesirable, energy wasting high frequency ring and ringing. The shape of the ring is a function of several parameters of the laser used, but typically grows in both amplitude and frequency at a higher ER (this is one of the reasons why the 10 GbE standard prescribes a low ER in the order of 3 - 4 dB). High frequency overshoot can be viewed by taking unfiltered measurements (see paragraph 9.3.1.3 above). This also is the recommended procedure for rise and fall time determinations.



Source: Agilent

Figure 9-15: Eye diagram measured in an unfiltered mode

- *Extinction ratio*

Extinction ratio (ER) is the ratio of the average power used to transmit the logic 'one' level to the power used to transmit logic 'zero' level of a digital signal typically expressed in dB. It represents a measure of how efficiently laser power is used. The most prevalent measurement approach is a digitising oscilloscope using a calibrated O/E converter. ER measurements are typically made in a filtered bandwidth as the filter performs an integrating effect to simulate the signal that will be seen by the decision circuit. Different standards define minimum requirements for extinction ratio values and describe a methodology for making corresponding measurements. For example, ER minimums between 8 dB to 10 dB are specified for SDH transmitters depending upon the application and standards for GbE define ER greater than 9 dB. Further information on ER measurements may be found in [IEC 61280-2-2].

- *Rise/fall time*

In order to get the most accurate assessment, the recommended procedure is to measure rise and fall times with the fully unfiltered bandwidth. Gigabit Ethernet allows an exception to this procedure. For some signals rise time characteristics are based on 10 % to 90 % thresholds. Alternatively, signals may be measured with rise time characteristics based on 20 % to 80 % thresholds which vary common in many of today's device specifications. Sampling oscilliscopes are the most important equipment used today to perform so called signal integrity measurements. However, rise/fall times may also be measured most accurately using analogue oscilloscopes. Here, the bandwidth of the instrument must be sufficient to accurate display the waveforms. Information on the required bandwidth for digital and analogue applications may be found in [Agilent V]. Misalignment of the rising/falling edges may narrow the size of eye opening and increase the potential for data errors. Jitter is an important source to impair high-speed digital signals.

- *Total jitter*

To run high-level communication systems a clock recovery system (e.g. clock data recovery) is needed that demand controlled jitter specifications to avoid timing inconsistencies. Jitter measurements refer to the measurement of the time variances of the rising and falling edges of an eye diagram as these edges affect the crossing points of the eye. Due to the sampling techniques used, a communications analyser cannot guarantee whether or not a device actually passes the jitter standard. Hence, in order to fully characterize a device as standards compliant, corresponding standards require additional equipment for jitter testing.

9.3.2 Optical receiver

Optical receivers represent the interface between the fibre optic path and the electronic processing equipment of a transmission system. A photo diode converts the incoming light to an electrical signal that is fed to the decision circuit. There are two detector types that can be be distinguished. PIN (positive intrinsic negative) diodes are widely used to design optical telecommunications systems. This type of photo diode owes much of its success to its simple, low cost yet rugged structure. Avalanche photo diodes (APD) are more complex but offer a combination of high speed and high sensitivity unmatched by PIN detectors. Critical receiver performance parameters for access network applications are shown in Table 9-3:

Sensitivity
Overload
Reflectance
Burst mode capability

Table 9-3: Important receiver parameters for access network applications

The most important specification of receivers is sensitivity at a given data rate. Typical PIN based receiver sensitivities for a BER of 10^{-10} are −26 dBm at a bit rate of 2.5 Gb/s, or −18 dBm at 10 Gb/s. Receiver overload is the maximum acceptable value of the received average power at the interface to the optical head, [IEC 61280-2-1]. A peculiarity of PON is the burst-mode operation, which needs accurate and fast handling of the optical power levels. The bursts received by the OLT have different amplitudes, because they are generated by various Optical Network Units. These operating conditions require specific control techniques, because the signal thresholds and levels must be changed very rapidly. Moreover, a peculiarity of the burst modus is the determination of the average optical power without using idle patterns (see section 9.5.3).

9.3.2.1 Sensitivity measurement methodology

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

The amount of power required by the receiver to ensure adequate system performance is given by the receiver sensitivity. Several standards define the receiver sensitivity as the minimum acceptable value of mean received power to achieve a given BER e.g. 10^{-12}. It takes into account power penalties caused by use of a transmitter under standard operating conditions with worst-case values of transmitter eye mask, extinction ratio, optical return loss, receiver connector degradations and measurement tolerances, [IEEE Std 802.3-2005]. If this is not done, a correction for the receiver sensitivity due to a measurement under too benign conditions can be estimated from the ER and relative eye opening of the test transmitter. This estimation may be preferred to testing with a strict worst-case signal, which may be difficult to generate. The level of the achievable performance depends on the actual data pattern used.
Test signals should have negligible impairments such as intersymbol interference, jitter and RIN. BER measurements determine the requested optical power limits. Figure 9-16 shows a receiver sensitivity measurement configuration recommended in [IEC 61280-2-1]. More information may be found in [TIA/EIA-526-5], [EIA/TIA-455-127], [TIA 526-3], [ITU-T G.695].
In contrast, the 10 GbE standard emphasizes measurement methods such as stressed eye sensitivity and optical modulation amplitude (OMA) in order to evaluate the system performance, instead of the ER and MLP combination widely used by other standards, [Tektronix I]. This novel test method will be already supported commercially by the availability of corresponding reference transmitters, reference receivers and software that allows the user e.g. to inject compliant and variable OMA to stress the receiver under test.

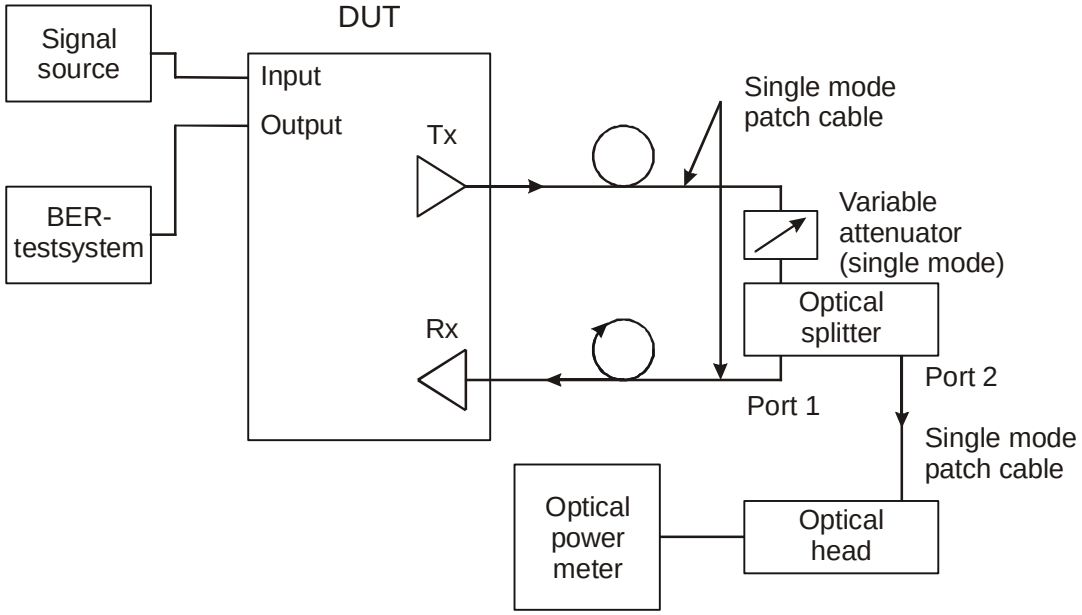


Figure 9-16: Receiver sensitivity measurement configuration

It should be noted, that the receiver sensitivity does not include power penalties associated with the path, such as dispersion, jitter, or reflections. These effects are specified separately by the allocation of a maximum optical path penalty (section 9.3.3). Further information may be found in [TIA/EIA-526-3].

9.3.2.1.1 Saturation measurement methodology

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Too high optical power levels can overload an optical receiver causing it to saturate and introduce distortions in the response signal levels and thereby induce an increase in the bit error rate (BER) for digital data signals. Normally, the measurement of received average optical power level should be done over at least the full dynamic range (between the sensitivity and saturation levels) of the optical receiver.
The measurement of the received optical power level is required to find out where the average received optical power is very low, near-to, or below the sensitivity level of the optical receiver. In addition, the measurement of the received optical power level is also useful because it can prevent the user to conditions where the average optical power is very high, near-to, or above the so-called saturation (overload) level of the optical receiver. Both ends of the power range, the high end and the low end, are important because average optical power levels below the sensitivity level or above the overload level (saturation region) can lead to incorrect data performance or errors.

9.3.3 Optical power budget calculation

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Power budget calculations are an essential tool to judge and design fibre optic links in order to ensure error-free data transmission even under worst-case conditions including aging effects, temperature conditions, system upgrades etc. over the life time of components (e.g. > 20 years for the passive optical plant). Optical power budget refers to the available optical transmitter power (launched into a fibre) and the minimum power at a receiver input needed to transmit a given data rate at a given BER over the interconnecting optical path. Table 9-4 highlights an exemplary calculation for a P2P access network application**.** Assuming a receiver sensitivity of –18 dBm (BER 10^{-12} @ 10 Gb/s) and a laser output power of 0 dBm a power budget of 18 dB is available, that corresponds well with the performance of state-of-the-art devices. From available power budget we must subtract out all of the penalties and losses e.g. for fibres, connectors and splices. Moreover, to ensure proper system operation the receiver overload level (not shown) must be considered, [IEC 61280-2-1]. The term penalties is an indication for extra optical power required at the receiver to account for signal degradations e.g. due to path penalty. Optical path penalty (see paragraph 9.5.4) is the reduction of receiver sensitivity due to distortion of the transmitter signal waveform (e.g. dispersion, jitter, reflections) during its transmission over the fibre path, [IEEE Std 802.3-2005]. Recommended path penalties for short-haul systems are limited to a maximum of 1 dB [ITU-T G.984.2] or even higher e.g. 1.5 dB [ITU-T 695]. The definition of optical path penalty is especially for upcoming systems, based on pre-distortion of the signal at the transmitter side. For access systems, this type of penalty consists of TDP and PMD.

Transmitter output power	0 dBm
Receiver sensitivity	-18 dBm
Power budget	**18 dB**

Power budget	18 dB
Insertion Loss ODN**	
Fibre loss (20 km, 0.4 dB/km*)	8 dB
4 Connectors	2 dB
10 Splices	1 dB
Path penalties	1 dB
Power margin	**6 dB**

* ITU-T G.652 D ** see section 9.6.1

Table 9-4: Power budget calculation for a P2P transmission system (10 Gb/s, 20 km). For access network applications the term path penalties include both TDP und PMD (PMD contribution only beyond 10 Gb/s and 20 km).

From available power budget we must subtract out all of the penalties and losses e.g. for fibres, connectors and splices. Moreover, to ensure proper system operation the receiver overload level (not shown) must be considered, [IEC 61280-2-1].

The term penalties is an indication for extra optical power required at the receiver to account for signal degradations e.g. due to path penalty. Path penalty (see paragraph 9.5.4) is the reduction of receiver sensitivity due to distortion of the transmitter signal waveform (e.g. dispersion, jitter, reflections) during its transmission over the fibre path, [IEEE Std 802.3-2005]. For access systems, this type of penalty consists of TDP and PMD (see paragraph 9.6.4). Integral part of the path penalty is the TDP that tests for transmitter impairments with chromatic dispersion effects for a transmitter to be used with SSMF. In addition, a common way to characterise this phenomenon is dispersion power penalty described e.g. in [TIA-526-10], [TIA/EIA-526-5]. Another fibre path property is polarisation mode dispersion (PMD) discussed in more detail in paragraph 9.6.4. For standard access network applications (10 Gb/s over 20 km) the amount of total PMD can be typically neglected corresponding to a low contribution to the path penalty calculation. Note that a SNR reduction that corresponds to an additional sensitivity reduction, e.g. due to optical amplification, is not considered a path penalty.

9.4 Testing performance under stress conditions

9.4.1 Determination of optical reach

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Purpose	The purpose of this test is to determine the optical reach of the SUT		
Type of external interfaces	**Analogue**	**Digital**	**Framed digital**
Evaluation parameters	CNR, CSO, CTB, Group Delay	BER, Delay	Frame Loss Ratio, Frame Delay (Bidirectional RFC 2544 test)
Evaluation parameters requirements	Find out the evaluation parameter requirements, which are adequate for the most demanded services planned for the system.		
Test configuration	Pure fibre optic systems: See Figure 9-1 XL-PON: See Figure 9-2 Hybrid systems: See Figure 9-3		
Test methods / Pure fibre optic system	1. Set up the system according to Figure 9-1. 2. Measure the reach according to “General procedure”.		

	XL-PON	1. Set up the system according to Figure 9-2. Set the <u>average</u> fibre length L2 [km] (theoretical average for the MAP-ONT link e.g. L2= ($L2_{MIN_theoret}$ + $L2_{MAX_theoret}$)/2). If needed, use attenuator A2 (see note 3). 2. Measure the <u>OLT-MAP reach</u> according to "General procedure", <u>step:a-d</u>, where A **ó** A1 and L **ó** L1. 3. Set the <u>average</u> fibre length L1 [km] (theoretical average for the OLT-MAP link e.g. L1= ($L1_{MIN_theoret}$ + $L1_{MAX_theoret}$)/2). If needed, use attenuator A1 (see note 3). 4. Measure the <u>MAP-ONT reach</u> according to "General procedure", <u>step:a-g</u>, where A **ó** A2 and L **ó** L2. 5. In order to detect the total XL-PON reach ($L_{XL\text{-}PON}$), set L1=(measured OLT-MAP reach) and L2=(measured MAP-ONT reach). A1 and A2 should be set according to step 3 and 5, respectively. 6. Check whether the XL-PON system meets the evaluation parameter requirements for $L_{XL\text{-}PON}$= (OLT-MAP reach) + (MAP-ONT reach).
	Hybrid system	1. Set up the system according to Figure 9-3. 2. The copper distance (L2) should not have any impact on the measurements (the optimum copper length should be set in order to assure the most efficient performance). 3. Measure the reach according to "General procedure", where A **ó** A1 and L **ó** L1.
	General procedure	<u>P2P and P2MP systems</u> (see note 1 and 2) a) Use a fibre length equal to the theoretical maximum reach **L**=$_{MAX_theoret}$ [km] that should be supported by the SUT. If needed, use an attenuator (see note 3). b) Configure and start transmission for the considered direction (in case of frames transmission run RFC 2544 test). c) By increasing/decreasing the fibre length L, find out the optimum reach (see note 4) the system meets the evaluation parameter requirements. For digital systems, the time needed to test the evaluation parameter performance depends on the bitrate and required BER/ Frame Loss Ratio. d) Save the results of reach $\mathbf{L_{MAX1}}$ and the performance of evaluation parameters. <u>Next steps are devoted to P2MP systems</u> e) Determine the theoretical maximum splitting ratio (1:n) that should be supported by the SUT. Assuming the "worst case" with 1:2 splitters that introduce IL=3.5 dB, set the attenuation **A**=3.5Log_2(n) [dB]. f) By increasing/decreasing the fibre length, find out the optimum setup (reach) the system meets the evaluation parameter requirements. g) Save the results for reach $\mathbf{L_{MAX2}}$ and evaluation parameters ($\mathbf{L_{MAX2}}$ takes into account the splitter insertion loss).
Expected results		In case of standardized systems, the optical reach has to meet the standard requirements (e.g GPON: 20 km according to ITU-T G.984.2). Otherwise the system should meet the given reach specifications.
Note		[1] When upstream and downstream signals are transmitted via separate fibres, each transmission direction has to be considered separately. [2] When upstream or downstream signals are transmitted using xWDM, each wavelength should be considered separately. [3] The minimum optical power budget must be sufficient (for upstream and downstream signals). If required (min. optical power budget [dB] > L[km] * fibre attenuation [dB/km]), use an attenuator to meet the minimum optical power budget requirements (min. optical power budget [dB] < L[km] * fibre attenuation [dB/km] + A[dB]).

	[4)] Accuracy of 1 km is desired

9.4.2 Sensitivity to reflection (P2MP, no optical circulators)

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x		x	x	x	x	x

The distance/attenuation effect

The total amount of Optical Return Loss (ORL) depends not only on the type of the reflective event, but also on the location of this event, e.g. the fibre length to the first reflective event. Generally, when the length of the fibre increases the amount of total backscattered light by the fibre itself increases, and the impact of discrete reflection events decreases. This means, for a short fibre link without intermediate reflective events, the reflection is the preponderant contribution of the total ORL, since the amount of reflected light is not highly attenuated by the fibre. Reflections beyond longer fibre length are attenuated by absorption and scattering effects and the backscattered light becomes the major contribution to the total ORL.

The effect of not terminated splitter

Figure 9-17 sketches P2MP network configurations for the purpose of ORL analysis. In approach B) a splitter 1:n is placed close to the OLT (e.g distance 1 m). One of the splitter outputs is connected to the ONU, whilst others are not terminated in order to force high backreflection (glass-to-air backreflection). The results of ORL calculations for these configurations show that the smaller the splitting ratio the lower the ORL see Table 9-5. For this reason, the “worst-case” configuration (splitter 1:2 with splitting ratio 90/10) will be considered to test the ORL system sensitivity, approach A).

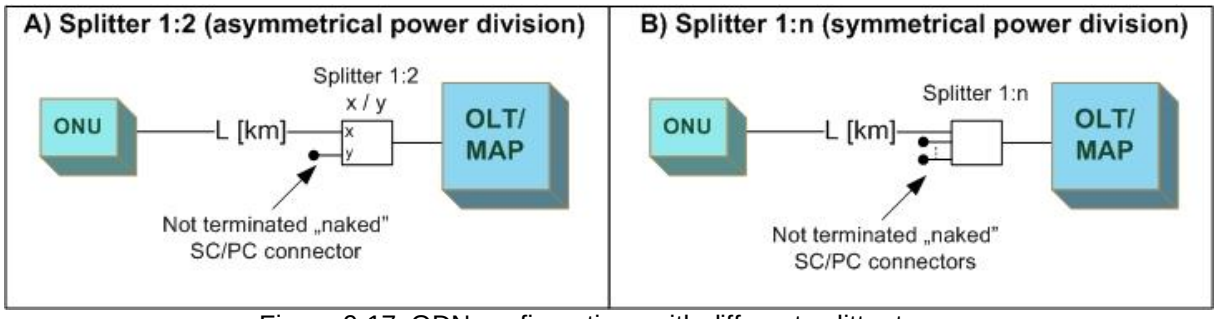


Figure 9-17: ODN configurations with different splitter types

Configuration number (Figure 9-17)	Splitter type			Theoretical ORL[1] [dB] (to the OLT Tx)	Comments
	Splitting ratio	Power division x [%] / y [%]			
1	**1:2**	Asymmetrical	**10/90**	**15.4**	x- output to ONT; y- output to not terminated end (ref.= -14.5 dB);
2			20/80	16.4	
3			30/70	17.6	
4			40/60	18.9	
5	1:2	Symmetrical		20.5	One output to ONT, whilst other(s) to not terminated end(s) (ref.= -14.5 dB);
6	1:4			21.8	
7	1:8			24.1	
8	1:16			26.8	
9	1:32			29.7	

Table 9-5: Impact of different ODN configurations on ORL characteristics

NOTE[1]: For ORL calculation purposes it was assumed that glass-to-air backreflections equal to -14.5 dB (~ 3.5 %). It should be also noted that the calculation takes into account only one stage splitter power division and the dominant glass-to-air backreflections (other reflection events are not considered since they are negligible). Adding additional splitter stages (e.g. 2 x splitter 1:2 90/10 with not terminated ends) would decrease the total ORL. However, the impact of the second stage splitter on total ORL is relatively low and can be omitted for the purpose of this analysis.

<table>
<tr><td colspan="2">Purpose</td><td colspan="3">The purpose of this test is to determine the ORL sensitivity in P2MP systems.</td></tr>
<tr><td colspan="2">Type of external interfaces</td><td>Analogue</td><td>Digital</td><td>Framed digital</td></tr>
<tr><td colspan="2">Evaluation parameters</td><td>CNR, CSO, CTB, Group Delay</td><td>BER, Delay</td><td>Frame Loss Ratio, Frame Delay
(Bidirectional RFC 2544 test)</td></tr>
<tr><td colspan="2">Evaluation parameters requirements</td><td colspan="3">Find out the evaluation parameter requirements, which are adequate for the most demanded services planned for the system.</td></tr>
<tr><td colspan="2">Test configuration</td><td colspan="3"><u>Pure fibre optic system and hybrid system</u>
See Figure 9-4. The splitter 1:2 (90/10) is placed close to the OLT (e.g 1 m). Then, one of the splitter outputs is connected to the ONT (10% of power), whilst the other (90% of power) is not terminated in order to force high backreflection (glass-to-air backreflection). Additionally, between splitter and unterminated end a variable attenuator is used.
<u>XL-PON</u>
In case of XL-PON system, where MAP has build-in splitter 1:8, the configuration 7 from Table 9-5 is used (only build-in splitter). One of the splitter outputs is connected to the ONT, whilst others are not terminated in order to force high backreflection (glass-to-air backreflection).</td></tr>
<tr><td rowspan="2">Test method</td><td>Pure fibre optic system</td><td colspan="3">1. Setup the system according to Figure 9-4, incorporating a fibre length that equals to the theoretical maximum reach $\mathbf{L}_{MAX_theoret}$ [km] that should be supported by the SUT and A = 20 dB (minimum reflection, maximum ORL).
2. Configure and start the transmission on the tester (it is assumed that for A = 20 dB and $\mathbf{L}_{MAX_theoret}$ the system meets the evaluation parameter requirements). In the case of frame transmission run the RFC 2544 test.
3. Decrease the attenuation A by e.g. 2 dB.
4. Check whether the system meets the evaluation parameter requirements. In that case repeat step 3 and 4 until A = 0 dB and proceed with step 5. Otherwise (if the system does not meet the evaluation parameter requirements) save that attenuation A_{MIN} the system meets the evaluation parameter requirements and proceed with step 5.
5. Detect the ORL of the ODN according to the section 9.6.2 (Optical Return Loss) and save the result as minimum ORL (ORL_{MIN}).
RESULT: For ORL≥ORL_{MIN} system meets the evaluation parameter requirements.</td></tr>
</table>

	XL-PON	1. Setup the system according to Figure 9-5, incorporating a fibre length L1 [km] that equals to the theoretical average for the OLT-MAP link e.g L1= ($L1_{MIN_theoret}$ + $L1_{MAX_theoret}$)/2). 2. Configure and start the transmission on the tester (in case of frame transmission run the RFC 2544 test). 3. Check whether the system meets evaluation parameter requirements. In that case save the ODN configuration and proceed to step 4. Otherwise terminate (using optical terminators) one of the unterminated ends and repeat step 2 and 3. 4. Test the ORL of the saved ODN configuration according to the section 9.6.2 (Optical Return Loss) and save the result as a minimum ORL (ORL_{MIN}). RESULT: For ORL≥ORL_{MIN} system meets the evaluation parameter requirements.
	Hybrid system	For hybrid P2MP systems (fibre + copper or ether), the copper/ether distance between ONU and end device should not have any impact on the measurement result (the optimum copper length should be set in order to assure the most efficient performance). Besides, this test method is identical to that described in the paragraph pure fibre optic system or XL-PON system.
Expected results		In case of standardized systems, the minimum accepted ORL has to meet the standard requirements (e.g. BPON: 32/20 dB according to ITU-T G.983.1). Otherwise, the system should meet given ORL assumptions.
Note		

9.4.3 Sensitivity to reflection (P2MP, with optical circulators)

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x		x	x	x	

Purpose	The purpose of this test is to determine the ORL sensitivity in P2P systems with optical circulators.		
Type of external interfaces	**Analogue**	**Digital**	**Framed digital**
Evaluation parameters	CNR, CSO, CTB, Group Delay	BER, Delay	Frame Loss Ratio, Frame Delay (Bidirectional RFC 2544 test)
Evaluation parameters requirements	Find out the evaluation parameter requirements, which are adequate for the most demanded services planned for the system.		
Test configuration	See Figure 9-6. The splitter 1:2 (90/10) is placed close to the optical circulator (e.g. distance 1 m). Then, one of the splitter outputs is connected to the ONT (10% of power) via the variable attenuator A1, whilst the other (90% of power) is unterminated in order to force high backreflection (glass-to-air backreflection). Additionally, between splitter and unterminated end, variable attenuator A2 is used.		

Test method	1. Set up the system according to Figure 9-4, with **A2** = 20 dB. 2. Determine the OLT/ONT receiver sensitivity according to the section 9.3.2.1 and save the results. 3. Determine the ORL of the ODN according to the section 9.6.2 (Optical Return Loss) and save the result. 4. Decrease the attenuation **A2** by e.g 2 dB and repeat steps 2 and 3 until **A2** = 0 dB.
Expected results	ORL vs. receiver sensitivity dependency. In case of standardized systems, the minimum accepted ORL has to meet the standard requirements. Otherwise the system should meet given ORL assumptions.
Note	

9.4.4 Differential fibre distance

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x		x		x	x	x

Purpose		The purpose of this test is to determine differential fibre distance for P2MP systems.	
Type of external interfaces		**Digital**	**Framed digital**
Evaluation parameters		BER, Delay	Frame Loss Ratio, Frame Delay (Bidirectional RFC 2544 test)
Evaluation parameters requirements		Find out the evaluation parameter requirements, which are adequate for the most demanded services planned for the system.	
Test configuration		Pure fibre optic systems: see Figure 9-7 XL-PON: see Figure 9-8	
Test methods	Pure fibre optic system	1. Set up the system according to Figure 9-7, with L0 - theoretical differential distance, L1= L_{MAX} described in paragraph 9.4.1 (Determination of optical reach), L3= L_{MIN} = L1-L0, L 2= L_{AVG} = (L1+L3)/2 (see note 1 and 2). 2. Test the differential distance according to the paragraph 'General procedure'.	
	XL-PON	1. Set up the system according to Figure 9-8, with L0 - theoretical differential distance, L1 = L_{MAX} (described in the paragraph 9.4.1 (Determination of optical reach), L3= L_{MIN}= L1-L0, L2 = L_{AVG} = (L1+L3)/2, L4 = L_{MAX} (determined in the paragraph 9.4.1 (Determination of optical reach) see note 1 and 2. 2. Test the differential distance according to the paragraph 'General procedure'.	
	Hybrid system	For hybrid P2MP systems (fibre + copper or ether), the copper/ether distance between ONU and end device should not have any impact on the measurement value (optimum copper length should be set in order to assure the most efficient performance). Besides, this test method is identical to that described in the paragraph 'Pure fibre optic system' or 'XL-PON system'.	

	General procedure	1. Configure and start bidirectional transmission on the tester. 2. Stop transmission after the time needed to assess the evaluation parameter performance (for digital systems depending on the bitrate and required BER/ Frame Loss Ratio). 3. Save the settings of the configuration setup and the performance results of the evaluation parameters. 4. If the system meets the evaluation parameter requirements and L3>0, decrease the fibre length **L3** (e.g. by 1 km), otherwise increase it. 5. Repeat steps a-d until accuracy of 1 km is achieved.
Expected results		In case of standardized systems, the optical reach has to meet standard requirements (e.g. GPON: 20 km according to ITU-T G.984.2). Otherwise, the system should meet given differential distance assumptions.
Note		[1)] If the upstream or downstream transmission is based on xWDM, each wavelength should be considered separately. [2)] The minimum optical power budget must be sufficient (for upstream and downstream signals). If required (min. optical power budget [dB] > L[km] * fibre attenuation [dB/km]), use an attenuator to meet the minimum optical power budget requirements (min. optical power budget [dB] < L[km] * fibre attenuation [dB/km] + A[dB]).

9.4.5 Sensitivity to crosstalk

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x		x

Purpose	The purpose of this test is to check the xWDM system performance in the case of adjacent wavelength transmission.		
Type of external interfaces	**Analogue**	**Digital**	**Framed digital**
Evaluation parameters	CNR, CSO, CTB, Group Delay	BER, Delay	Frame Loss Ratio, Frame Delay (Bidirectional RFC 2544 test)
Evaluation parameters requirements	Find out the evaluation parameter requirements, which are adequate for the most demanded services planned for the system.		

Test methods	1. Configure the xWDM system in order to avoid signal transmissions via adjacent wavelengths. If possible, turn on a laser (λ_i) and turn off the other lasers transmitting light in the same direction. 2. Configure and start the transmission on the tester. 3. Save the performance results of the evaluation parameters (case I- only λ_i). 4. Repeat steps 1-3 for different λ_i with i=1…N and N – number of possible wavelengths 5. Configure the system in order to ensure simultaneous signal transmission via all adjacent wavelengths. 6. Configure and start the transmission on the tester. 7. Save the performance results of the evaluation parameters (case II- all wavelengths). 8. Compare the results from both cases and assess the impact of the transmission via adjacent wavelengths on the system performance.
Expected results	The mutual interference of signals transmitted at adjacent wavelengths can be neglected.
Note	

9.5 Testing optical signal quality on different parts of optical path

9.5.1.1 OSNR

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Principles of OSNR measurements

The measurement of the OSNR (Optical Signal to Noise Ratio) may be performed with an OSA (Optical Spectrum Analyzer). OSNR usually expressed using a resolution bandwidth of 0.1 nm is determined by equation (Eq.1) [ITU-T G.Sup39]:

$$OSNR = 10\log\frac{P_i}{N_i} + 10\log\frac{B_m}{B_r} \qquad \text{(Eq.1)}$$

with:

P_i Optical signal power expressed in watts at the *i*-th channel.

N_i Interpolated value of the noise power expressed in watts, measured with the noise equivalent bandwidth of the OSA, B_m, at the *i*-th channel:

$$N_i = \left(\frac{N(n_i - \Delta n) + N(n_i + \Delta n)}{2} \right)$$

Δn Interpolation offset equal to one-half of the channel spacing (channel spacing 200 GHz, Δn = 100 GHz).

B_r Reference optical bandwidth. (B_m and B_r must be expressed using identical units - [GHz] or [nm]). Typically, the optical reference bandwidth amounts to 0.1 nm [ITU-T G.Sup39].

The commonly agreed procedure to determine OSNR using a measurement data base is shown in Figure 9-18. In order to achieve accurate results, the resolution bandwidth must be matched to the bit rate of the signal, e.g. at 40 Gb/s the minimum resolution bandwidth 1 nm is recommended [ITU-T G.Sup39].

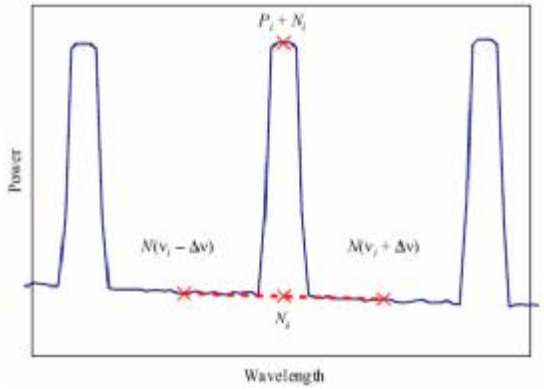


Figure 9-18: Examplary measurement of OSNR using an OSA

Purpose	The purpose of this test is to determine the OSNR at different reference points of P2P and P2MP systems.
Test configuration	<u>P2P systems (downstream and upstream):</u> See Figure 9-9 (for non-WDM systems no filters are needed). In downstream direction a signal generator (or live signal) is connected to the OLTs external interface and the ONT is replaced by an Optical Spectrum Analyzer. In upstream direction the OLT is replaced by an OSA and the ONT is connected to the signal source. *Breakpoints e.g.:* Reference points 1 and 2 in Figure 9-1 or Figure 9-2. <u>P2MP systems:</u> **Downstream**: see Figure 9-9 (for non-WDM systems no filters are needed). Signal generator (or live signal) is connected to the OLTs external interface. An OSA is connected instead of one of the ONTs. *Breakpoints e.g.:* Reference points 2 and 3 in Figure 9-5 or reference point 4 in Figure 9-2 **Upstream**: see Figure 9-10 (for non-WDM systems no filters are needed). An OSA is connected via optical splitter (1:2) in parallel to the OLT. However, OLTs can not be simply replaced by an OSA due to network protocol requirements to establish data communications. A Signal generator (or live signal) is connected to the external interface of one of the ONTs. *Breakpoints e.g.:* Reference point 1 in Figure 9-5 or reference point 3 in Figure 9-2
Test method	1. Connect all elements of the test configuration with $L=L_{MAX_theoret}$ (maximum theoretical optical reach). 2. Turn on the signal source, OLT/ONU and OSA. 3. Set the appropriate measurement resolution bandwidth, start the measurement procedure and await the results presented by the OSA. 4. Using OSA markers, save the power level at the signals main wavelength, v_i, and on both sides of the central signal, $v_i \pm \Delta v$, with Δv equal to one-half of the channel spacings (xWDM regime) or equal to arbitrarily chosen values according to the noise power requirements of the signals side skirt (non-WDM regime). 5. Save the optical spectrumand calculate the OSNR using equation (Eq.1). 6. If the calculated OSNR is larger than the minimum accepted OSNR, increase the fibre length L. Otherwise decrease it. 7. Repeat step 3-6 until the minimum accepted OSNR is achieved.

Expected results	OSNR vs. fibre length dependency.
Note	OSNR requirements depend on the system type and the modulation format (digital, analogue). For this reason, each case should be treated individually.

9.5.2 Q-factor/BER estimation

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
	x	x	x	x		x	x	x

Principles of Q-factor measurements

Q-factor measurements are performed using Digital Signal Analyser (DSA), providing different Q-factor estimation methods. Among them the dual decision circuit method is considered as the most accurate and convenient approach. Here, optical/electrical converted input signal are splitted and fed into two decision circuits that are triggered by the recovered clock. Decision circuit 1 is adjusted to its optimum position within the eye-diagram and serves as a reference. Decision circuit 2 can be adjusted to arbitrary values regarding the sampling phase and threshold levels. Signal differences of the decision circuit outputs are detected by an EXOR circuitry and counted as bit errors, as shown in Figure 9-19. This method works well with live traffic signals and is used to perform in-service measurements on optical systems.

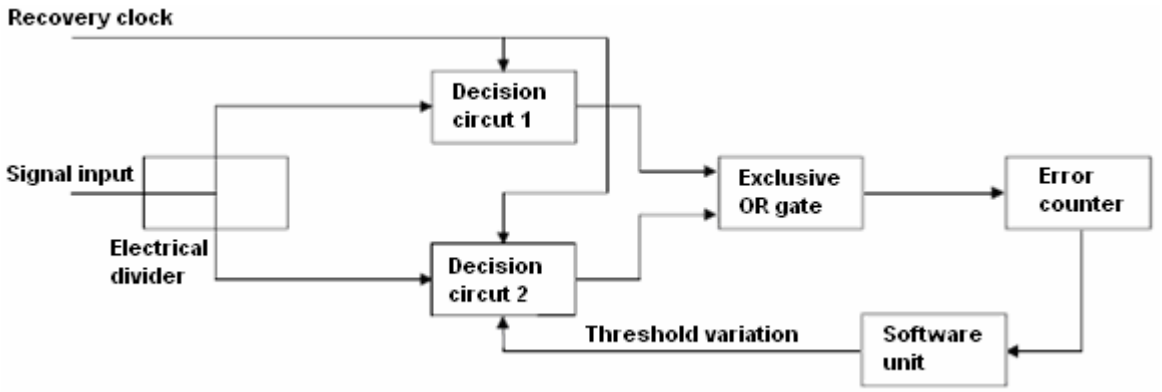


Figure 9-19: Block diagram of a dual decision circuit scheme representing a submultiple of the Q-factor measurement configuration

After measuring the Q-factor, BER can be obtained by the use of an approximation for the erfc function:

$$BER(Q) = \frac{1}{2} \times \left[2 \times e^{-\left(\frac{Q}{\sqrt{2}}\right)^2} \times \frac{a0 + a1 \times \frac{Q}{\sqrt{2}} + a2 \times \left(\frac{Q}{\sqrt{2}}\right)^2}{\left[b0 + b1 \times \frac{Q}{\sqrt{2}} + b2 \times \left(\frac{Q}{\sqrt{2}}\right)^2 + b3 \times \left(\frac{Q}{\sqrt{2}}\right)^3 \right] \times \sqrt{p}} \right] \quad \text{(Eq.2)}$$

With:

a0 = 1.69071595 b0 = 1.90764542
a1 = 1.45117156 b1 = 3.79485940
a2 = 0.50003230 b2 = 2.90845448
b3 = 1.00000000

The maximum accuracy of this approximation is better than 2×10^{-6} for $Q > 1.5$, which is more than sufficient for the Q-factor application [ITU-T O.201]. Figure 9-20 plots BER vs Q-factor according to equation (Eq.2).

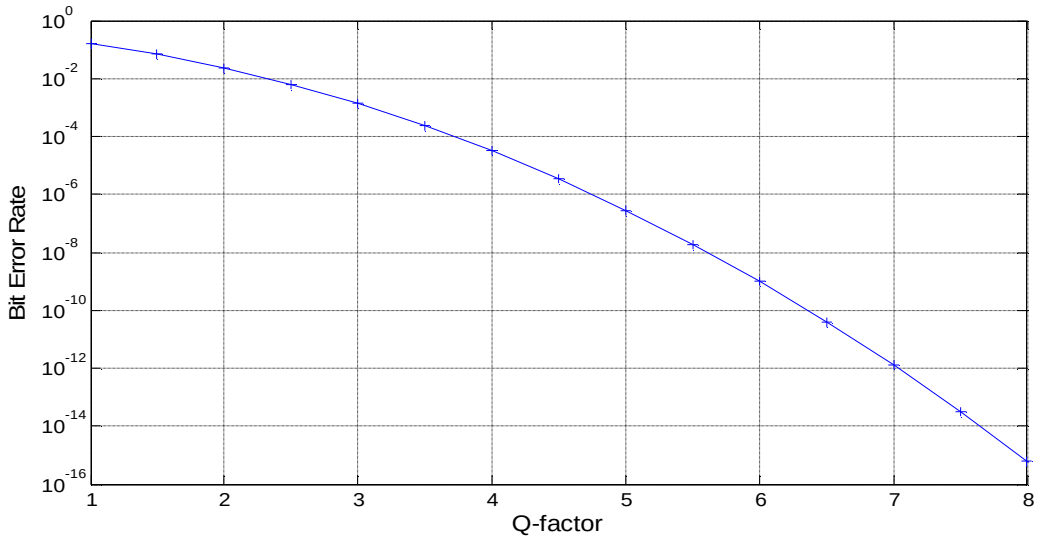


Figure 9-20: BER vs Q-factor according to equation 2 (Eq.2)

Purpose	This test describes the Q-factor determination including BER estimation for P2P and P2MP systems.
Test configuration	P2P systems: See Figure 9-9. For downstream testing a signal generator (or live signal) is connected to any OLTs external interface and the ONT is replaced by a Digital Signal Analyser. For upstream testing the OLT is replaced with a DSA and the ONT is connected to the signal source. For xWDM systems filters are required in order to measure the Q-factor at selected wavelengths. P2MP systems: Downstream: See Figure 9-9. The signal generator (or live signal) is connected to the OLT external interface and the OSA is connected instead of any of the ONTs. Upstream: See Figure 9-10. An OSA is connected via optical splitter (1:2) in parallel to the OLT. However, OLTs can not be simply replaced by an OSA due to network protocol requirements to establish data communications. A signal generator (or live signal) is connected to the external interface of one of the ONTs. . For xWDM systems filters are required, in order to measure the Q-factor at selected wavelengths.

Test method	1. Determine the maximum accepted BER (e.g BER=1xE-10) 2. Connect all elements of the test configuration, where $L=L_{MAX_theoret}$ (maximum theoretical optical reach) 3. Configure the signal generator and the OLT/ONU. 4. Start Q-factor/BER measurements with DSA. 5. Read and save the Q-factor/BER results from the DSA. (After finishing the measurement, a BER estimation should be presented by the DSA. If the DSA shows only the Q-factor, use equation 2 (Eq.2) for BER calculations). 6. If the calculated BER (from DSA) is grater than the maximum accepted BER, decrease the fibre length L. Otherwise increase it. 7. Repeat step 4-6 until the maximum accepted BER is achieved.
Expected results	Q-factor/BER vs. fibre length dependancy.
Note	

9.5.3 Received optical power level

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x		x	x	x

Principles of received optical power level measurements

Measurements of received optical power level for P2P and for P2MP systems (downstream direction only) may be performed using power meters. Here, data signals are transmitted continuously and the received power level presented by a power meter relates to the mean value between P0 (power level of logical 0) and P1 (power level of logical 1), as shown in Figure 9-21.



Figure 9-21: Continuous data pulse and corresponding power levels

Power meters however are not an adequate equipment to perform measurements in the upstream direction of a P2MP system (TDMA format). Here, the ONT usually transmits data in bursts during a time slot assigned by the OLT. Outside this time slot the specific ONT laser is turned off and the transmitted power level should be zero. Power meters inherently present the overall mean received power and take into account the breaks between these bursts, which leads to a smaller value of the measured received optical power level. This is illustrated in Figure 9-22.

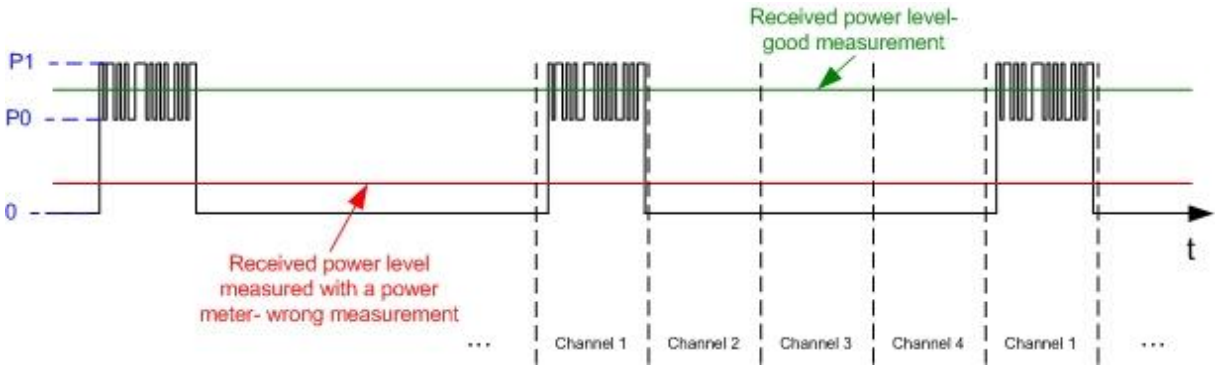


Figure 9-22: Burst mode data pulse and corresponding power levels

Digital oscilloscopes represent a solution to this shortcoming. Received power levels can be determined by measuring the mean power levels of different data bursts and by averaging the obtained results (green line in Figure 9-22).

Purpose	The purpose of this test is to determine the received optical power level for P2P and P2MP systems.
Test configuration	P2P systems: See Figure9-9. For downstream testing a signal generator (or live signal) is connected to any OLTs external interface and the ONT is replaced by a power meter. For upstream testing the OLT is replaced with a power meter and the ONT is connected to the signal source. For xWDM systems filters are required in order to measure the received optical power at selected wavelengths. P2MP systems: Downstream: See Figure 9-9. The signal generator (or live signal) is connected to the OLT external interface and a power meter is connected instead of any of the ONTs. Upstream: See Figure 9-10. A digital oscilloscope is connected via optical splitter (1:2) in parallel to the OLT. However, the OLT can not be simply replaced by an oscilloscope due to network protocol requirements to establish data communications. A signal generator (or live signal) is connected to the external interface of one of the ONTs. Ordinary digital oscilloscopes do not feature built-in optical/electrical converters. As a result, a corresponding converter should be connected in front of an oscilloscope. For xWDM systems filters are required in order to measure the received optical power level at selected wavelengths.

Test method	<u>P2P (upstream and downstream) & P2MP (downstream):</u> 1. Connect all elements of the test configuration. 2. Configure the signal generator and the OLT/ONU. 3. Turn on the power meter and await the wavelength setting procedure. 4. Start the measurement of the received optical power level using a power meter 5. Read and save the results from the power meter. 6. Calculate the accuracy according to the power meter specifications. <u>P2MP Upstream:</u> 1. Connect all elements of the test configuration. 2. Configure the signal generator and the OLT/ONU. 3. Determine the insertion loss of the optical splitter used in the procedure and connect the digital oscilloscope. Save the result as $IL_{SPLITTER}$ [dB]. 4. Turn on the digital oscilloscope and await readiness for operation. 5. Stretch the signal shown by the oscilloscope so that a single burst is displayed. 6. Measure the mean power level P_M and the standard deviation σ of a single burst. Save the results. 7. Add IL introduced by the splitter to the result ($P_{M_ONT} = P_M + IL_{SPLITTER}$).
Expected results	The received power level meets the specifications.
Note	

9.5.4 Optical path penalty

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Purpose	The purpose of this test is to determine the optical path penalty for P2P and P2MP systems.
Test configuration	For both P2P and P2MP systems specifications with resect to optical reach and optical receiver sensitivity are required. See sections 9.5.3 and 9.3.2.1.
Test method	1. Determine the optical receiver sensitivity for a short (L→0) fibre distance between transmitter and receiver executing the procedure described in section 9.3.2.1. Save the result as P_0 [dBm]. 2. Determine the optical reach of the SUT executing the procedure described in 9.5.3. Save the result as L_{MAX} [km]. 3. Determine the optical receiver sensitivity for L_{MAX} [km] of fibre between transmitter and receiver executing the procedure described in 9.3.2.1. Save the result as P_1 [dBm]. 4. Calculate the optical path penalty: OPP [dB] = $P_0 – P_1$.

Expected results	In case of standardized systems, the optical path penalty has to meet the standard requirements (e.g GPON: optical path penalty max 1 dB according to ITU-T G.984.2). Otherwise the optical path penalty should not exceed given values.
Note	

9.6 ODN characteristic

The term optical distribution network (ODN) refers to the transport network portion between the central office and the subscriber premises. ODNs are typically based on P2P or P2MP topologies in which only unpowered components (fibres, multiplexers, connectors etc.) are used to form a passive optical network. Power splitting PONs (PS-PON) are becoming an increasingly popular architecture for FTTP configurations that may reduce the amount of fibre and central office equipment compared to P2P architectures, however, at the expense of a more complex transmission regime. For access network applications several standards recommend a maximum span length of up to 20 km using low/zero water peak SSMF, [ITU-T G.652], that support full spectrum operation between 1270 nm and 1610 nm.

However, in order to consolidate the amount of centralised equipment there is an effort to upgrade the performance of PS-PONs with respect to the expansion of reach (100 km), higher splitting ratios in the order of 1000 and projected data rates up to 10 Gb/s. Conceptually, optical amplifiers are needed that boost the signal strength to meet the minimum receiver sensitivity (see section 9.3.2.1). In contrast, previous ODN considerations were restricted to system implementations without costly amplification and optical dispersion compensation throughout the fibre plant.

To ensure the compliance of a prescribed access network performance it is essential to determine comprehensively loss and dispersion characteristics of the thorough ODN. Path attenuation specifications should be worst-case values including losses of all passive optical devices, and any additional margin to cover allowances for future modifications to the network configuration, performance variations due to environmental factors and degradation effects. This paragraph describes the most important access network parameters insertion loss, optical return loss, chromatic dispersion, polarisations mode dispersion and spectral response are described to provide a basis for measurements on the entire fibre optical plant. Useful ODN measuring equipment include: OSA (field portable instruments are available to offer practical testing solutions), power meters, OTDR, PDLA and reflectometer. More information may be found in [FIA 2005],.[EN 50346].

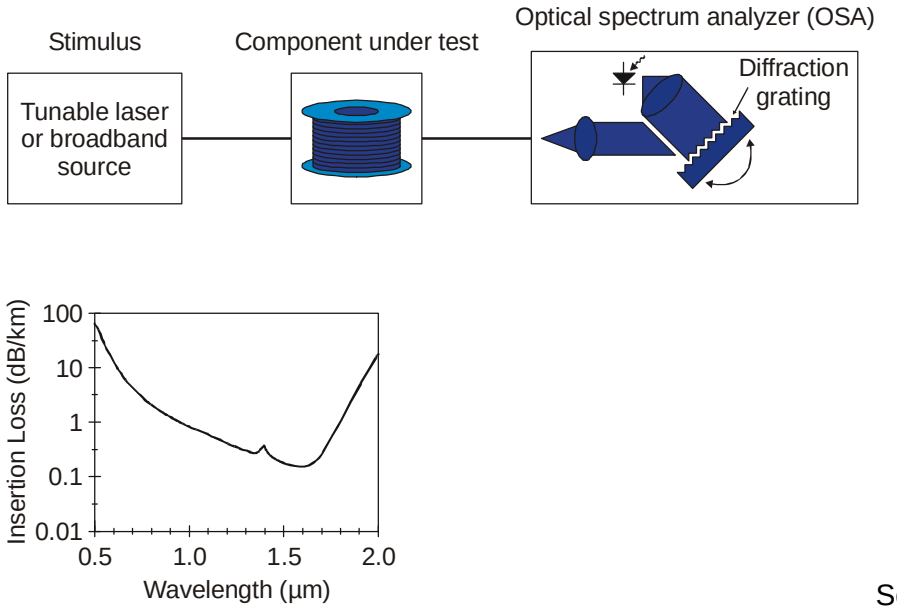
9.6.1 Insertion Loss

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Insertion loss (IL) or attenuation (mostly expressed in dB) is the most fundamental of all the measurements required to assess fibre optic components as well as fibre optical paths. It relates the launched input power to the output power available at the inspected network portion/DUT and can vary as a function of wavelength and polarisation. A typical set-up to measure the insertion loss is illustrated in Figure 9-23. The chart in this figure highlights an exemplary measurement of the spectral attenuation profile of a SSMF. Tunable laser and broadband light sources that can be used as optical stimulus as well as OSA and power meter at the receiving side may be combined in several ways. In general, the simplest approach requires an optical source and a power meter, however, measurement results imply no wavelength information. In contrast, OSAs provide information on both wavelength and optical power. In some cases a polarisation scrambler may be useful to depolarise the incoming light. IL can also be measured with commercially available equipment such as Photonic Dispersion and Loss Analyser (PDLA). PDLA are multi-purpose gadgets to characterise optical components in one step of a procedure including chromatic dispersion, loss and polarisation mode dispersion.

Optical time domain reflectometers (OTDR) are an alternative instrument to measure the insertion loss of optical fibre spans. More information on IL measurements with power meters and OTDR may be found in [TIA-526-7], [TIA/EIA-455-61A], [IEC 61300-3-7], [IEC 61280-4-2], [TIA/EIA 455-180-A], [Telcordia GR-196].



Source: Derickson

Figure 9-23: Configuration to determine IL and exemplary measurement of a SSMF (related to the fibre length in km) with broadband light source.

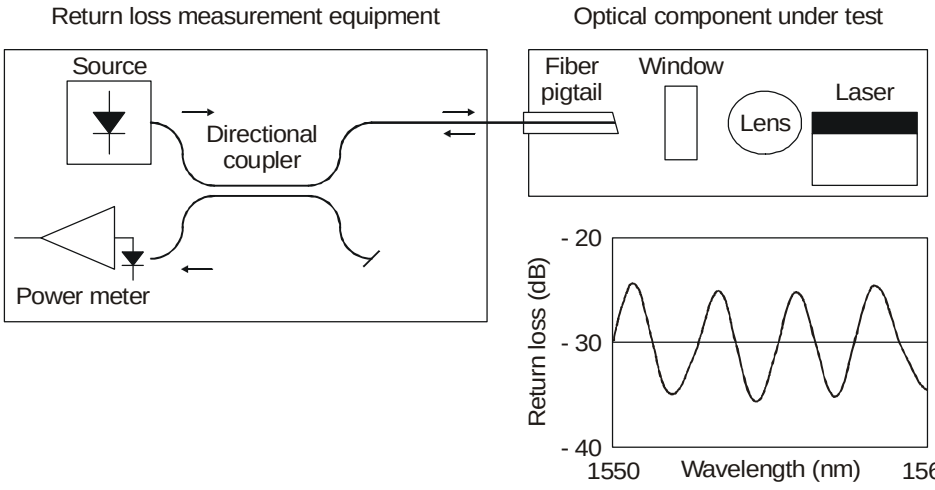
9.6.2 Optical Return Loss

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

With increasing transport data rates and WDM deployment, optical return loss (ORL) measurements have become mandatory for the assessment of fibre optic access networks. ORL is the ratio of the reflected power to the incident power at a reference point. Back reflections are caused by refractive index discontinuities along the optical path. If not controlled, they can degrade system performance through disturbing effects (e.g. increased chirp, reduced OSNR) on the operation of the optical source, or through multiple reflections which lead to additional noise at the receiver. Reflections from the optical path are taken into account often by specifying the minimum ORL of the fibre and the maximum discrete reflectance. Here, reflectance denotes the reflection from any single discrete reflection point, whereas the return loss is the total returned power from the entire fibre including both discrete reflections and distributed backscattering.

The amount of reflected power depends on the reflectance value of the discontinuity and on the distance from the optical source. For short fibre links (resulting in a low fibre loss), a non-terminated fibre e.g. due to a poorly mated connector (glass-air reflection –14 dB) may be the most important contribution to ORL (SFP transceiver usually use LC connectors with non-angled or straight faces). High backreflections can also affect the transmission performance of analogue signals. A widely used technique for measuring ORL is illustrated in Figure 9-24. The pictured return loss measurement configuration with optical source, power meter and directional coupler may also be found in commercially available equipment such as optical continuous wave reflectometers [JDSU]. Measurement methods that describe the reflection behavior of optical components are to be found in [JDSU I], [ITU-T G.957], [IEC 61300-3-7], [IEC 61931-1]



Source: Derickson

Figure 9-24: Total return loss measurement set-up and example measurement for a packed laser

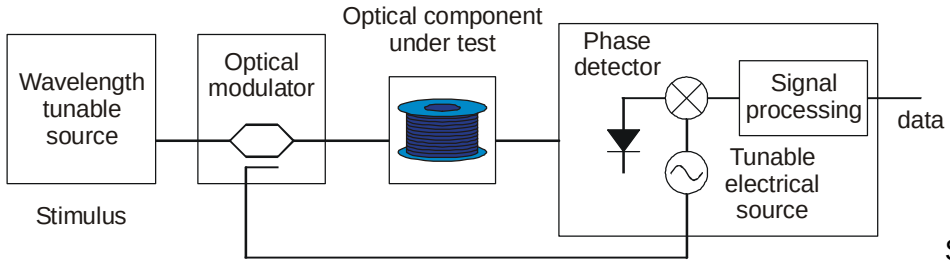
Beyond IL measurements as described in section 9.6.1, OTDR provide an alternative solution to measure the ORL of optical fibre spans. In addition to the total ORL results, this method allows to locate faults and to evaluate back reflection events. Further information may be found in [Telcordia GR-196].

9.6.3 Chromatic Dispersion

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Chromatic dispersion (CD) is the primary dispersive mechanism in SSMF. It is typically a concern for fibres but to some extent also for devices e.g. fibre bragg gratings. Full spectrum high-speed access systems often suffer from (CD) limitations inherent in SSMF cable plants. There are several CD measurement methods, [EIA-455-169], [IEC 60793 1-42], [ITU-T G.650.1]. The most common method involves measuring the variation in phase delay as a function of wavelength as is shown in Figure 9-25. A wavelength tunable source is intensity modulated as stimulus for the component under test, [Derickson]. The phase of the detected modulation signal then is compared to that of transmitted modulation. CD can be conveniently measured using commercially available equipment such as Photonic Dispersion and Loss Analyser (PDLA). An example measurement of chromatic dispersion as a function of wavelength using a PDLA is shown in Figure 9-26 for different SSMF according to [ITU-T G.652]. As a result, differences between the graphs of the fibres can be neglected. The zero-dispersion wavelength is in the range of 1310 nm and the maximum CD appears at 1610 nm.



Source: Derickson

Figure 9-25: Chromatic dispersion measurement configuration

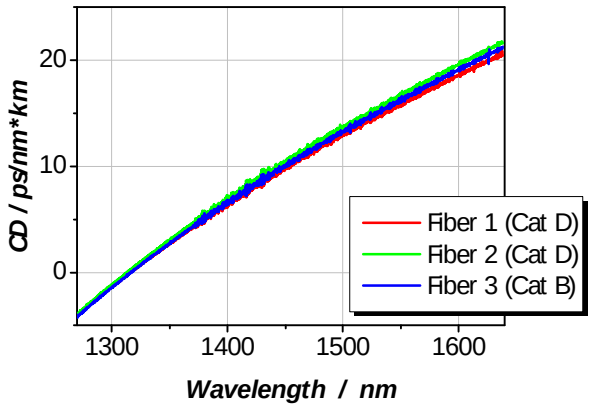


Figure 9-26: Example measurement of chromatic dispersion vs wavelength for different SSMF according to [ITU-T G.652] (external cavity lasers as optical sources and PDLA)

Fundamentally, wavelength dependent CD associated with full spectrum fibres, recommended for use in optical access networks, interact with data signals traveling through the fibre and causes pulse broadenings. Consequently, there is an increased probability that the receiver will show errors. A common way to describe impairments with chromatic dispersion effects is the dispersion power penalty, see section 9.3.3.

9.6.4 Polarization Mode Dispersion

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Polarisation Mode Dispersion (PMD) is the dispersion of a signal travelling through an optical material due to the presence of two different refractive indices which transmit polarised light at two different speeds. PMD can be present in both optical fibres and fibre optic components. It depends on the device itself and on external factors such as stress, bending conditions and temperature. Commercially available equipment is based on different measurement techniques. The Stokes parameter evaluation is a generic term for the frequency domain measurement techniques of Jones matrix eigenanalysis, [EIA-455-122]. In contrast, the fixed analyser, or wavelength scanning method is the simplest PMD measurement method optimised to characterise devices with broad transmission characteristics e.g. fibres, [EIA-455-113], [IEC 61300-3-32]. However, PMD is a limiting factor only for data rates beyond 10 Gb/s (maximum projected data rate for access networks). More information may be found in [IEC 61280-4-4].

9.6.5 Spectral Response

Applicable to following systems:

External interfaces			Architecture		Optical modulation		Number of wavelengths	
Analogue	Digital	Framed digital	P2P	P2MP	Analogue	Digital	Non-WDM	xWDM
x	x	x	x	x	x	x	x	x

Optical response refers to a two-port measurement to characterise the performance of an optical device or system. Optical access networks will require different types of wavelength dependent optical components, filters and couplers in particular, will play an important role in next generation transport systems. Important test parameters to characterise the spectral response of optical devices include central wavelength, insertion loss, filter flatness and ripple, rising and falling edge characteristics, signal-to-noise ratio, bandwidth and isolation. There are two different measurement configurations that can be applied. The first is by taking a tunable source and a broadband detector and the second is by taking a broadband source and an OSA to perform the sweeping. Further information may be found in [EXFO].

It is expected that C/DWDM systems will be widely deployed in future transmission systems to form high-capacity access networks. In particular CWDM has the potential to decrease system costs by eliminating expensive wavelength stabilising techniques. The spectral response of an 18-channel CWDM demultiplexer is shown in Figure 9-27 (central wavelengths of the grid are defined by [ITU-T 694.2]. As a result, the filter response shows a 13.5 nm wide flat passband width, a maximum insertion loss in the order of 2.5 dB and a crosstalk performance of better than –30 dB.

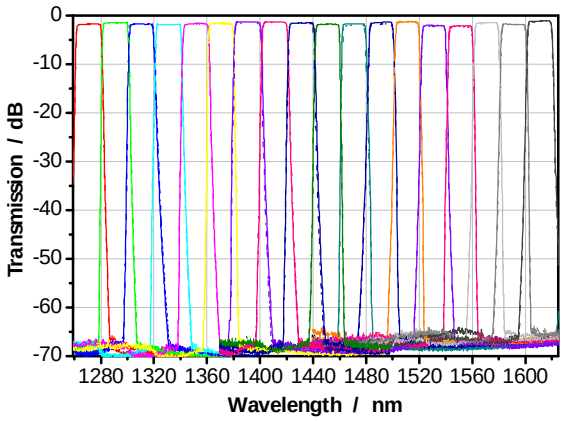


Figure 9-27: Transmission performance of a 18 channel thin film filter demultiplexer (external cavity lasers as optical sources and PDLA).

9.7 References

[Agilent I] Application Note 1550-8, Measuring Extinction Ratio of Optical Transmitters

[Agilent II] Product Note 86100-2, Measuring High Power Waveforms

[Agilent III] Application Note1340-1, Characterising High-Speed Optical Transmitters

[Derickson] Dennis, Fibre Optic Test and Measurement, ISBN 0-13-534330-5

[EIA-455-113] PMD measurement for single-mode optical fibres by the fixed analyzer method

[EIA-455-122] PMD measurement for single mode optical fibres by the Jones matrix eigenanalysis

[EIA-455-169] Chromatic Dispersion Measurement of Optical Fibres by the Phase shift Method

[EXFO] Application Note 101, CWDM and DWDM Testing in the Field Using Broadband Sources and an OSA

[Hewlett-Packard] Solution Note 815-2, Optical Power Measurement

[IEC 60793 1-42] Optical fibres – Part 1-42: Mesurement methods and test procedures – chromatic dispersion

[IEC 61280-1-3] Central Wavelength and spectral width measurement

[IEC 61280-2-1] Test procedures for digital systems – Receiver sensitivity and overload measurement

[IEC 61280-2-2] (86C/713 CD) Digital systems – Optical eye pattern, waveform, and extinction ratio measurement

[IEC 61280-4-2] Fibre optic communication subsystem basic test procedures –Part 4-2: Fibre optic cable plant – Single-mode fibre optic cable plant attenuation

[IEC 61300-3-7] Fibre optic interconnecting devices and passive components; Basic test and measurement procedures (Part 3-7: Examinations and Measurements – Wavelength Dependence of Attenuation and Return Loss)

[IEC 61300-3-32] Basic test and measurement procedures (Part 3-32: Examinations and measurements – Polarisation mode dispersion for passive optical components)

[IEC EN 60825-2]	Safety of Laser Products Part 2: Safety of Optical Fibre Communication Systems
[IEC 61931-1]	Fibre-optic Terminology, 1.34
[IEEE Std 802.3-2005]	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications
[ITU-T O.201]	Q-factor test equipment to estimate the transmission performance of optical channels
[ITU-T G.650.1]	Definition and test methods for linear, deterministic attributes of singlemode fibre and cable
[ITU-T G.652]	Characteristics of single-mode optical fibre and cable
[ITU-T 694.2]	Recommendation: Spectral grids for WDM applications: CWDM wavelength grid, 06/ 2002
[ITU-T G.695]	Optical interfaces for Coarse Wavelength Division Multiplexing applications
[ITU-T G.957]	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
[ITU-T G.Sup39]	Optical system design and engineering considerations
[JDSU I]	White Paper, Optical Return Loss Management
[Tektronix I]	Application Note Measurements on IEEE 802.3ae 10 Gb/s Ethernet
[Telcordia GR-196]	Generic Requirements for Optical Time Domain Reflectometer (OTDR) Type Equipment
[TIA 526-3]	(OFSTP-3) Fibre Optic Terminal Equipment Receiver Sensitivity and Maximum Receiver Input
[TIA/EIA -455-127]	(OFSTP-5) Data Analysis of Bit Error Ratio versus Received Power for Digital Fibre Optic Systems.
[TIA/EIA 455-180-A]	Measurement of Optical Transfer Coefficient of a Passive Branching Device (Coupler)
[TIA/EIA -455-61A]	FOTP-61 Measurement of fibre or cable attenuation using an OTDR
[TIA/EIA -526-5]	(OFSTP 5) Data Analysis of Bit Error Ratio versus Received Power for Digital Fibre Optic Systems
[TIA/EIA-455-95]	(FOTP-95) Absolute optical power test for optical fibres and cables
[TIA/EIA-526-4A]	OFSTP-4 Optical eye pattern measurement procedure
[TIA-526-10]	(OFSTP 10) Measurement of Dispersion Power Penalty in Digital Single-Mode Systems
[TIA-526-7]	(OFSTP-7) Measurement of Optical power Loss of installed Single-mode Fibre Cable Plant