

Access and Terminals (AT); Analysis and scoping of IPCablecom interfaces and interactions for testing



Reference

DTR/AT-020037

Keywords

access, broadband, cable, IP, IPCable, testing,
TTCN,

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, send your comment to:

editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	5
Foreword.....	5
1 Scope	6
2 References	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	8
4 Overview	10
4.1 General objectives	10
4.2 Business objectives.....	10
5 Analysis of the IPCablecom architecture	11
5.1 Analysis of reference architectures for testing	11
5.1.1 Analysis of the NCS - CMS reference architecture for testing	11
5.1.2 Analysis of the LCS - IPAT reference architecture for testing	12
5.2 Analysis of signalling interface-interactions	13
6 Analysis of individual IPCablecom system elements	18
6.1 Structure and basis for analysis	18
6.2 MTA/CM Framework	18
6.2.1 General.....	18
6.2.2 Description of the MTA/CM (E-MTA) interfaces and functions	19
6.2.3 Interface interaction	22
6.2.3.1 Interface-interactions for test consideration	22
6.2.3.2 CM CMTS Interface-interactions.....	23
6.3 CMTS (AN) Framework	23
6.3.1 General.....	23
6.3.2 Description of the CMTS interfaces and functions.....	23
6.3.3 Interface interaction	25
6.4 IPAT MTA Framework.....	26
6.4.1 General.....	26
6.4.2 Description of the IPAT interfaces and functions.....	26
6.4.3 Interface interaction	28
6.4.3.1 Interface-interactions for test consideration	28
6.5 CMS Framework	30
6.5.1 General.....	30
6.5.2 Description of the CMS interfaces and functions	30
6.5.3 Interface Interactions	32
7 Summary and guidance to development of Test Suite Structure and Test Purposes (TSS&TP)	33
7.1 Interoperability - vs. - conformance	33
7.2 Observations.....	34
7.3 General guidance in the production of PICS/test purposes	34
7.4 Focus on interoperability/ETSI Plugtest TM service	35
7.5 Focus on conformance testing	35
7.6 Availability of commercial test systems.....	36
8 Considerations to the development of testing specifications	37
Annex A: Test framework for MTA/CM.....	38
Annex B: Test framework for CMTS (AN)	39
Annex C: Test framework for IPAT MTA	40
Annex D: Test framework for CMS	41

Annex E: Bibliography	43
History	45

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Access and Terminals (AT).

1 Scope

The present document is the result of a study of the functional technical characteristics of the IPCablecom system based upon the current series of TS 101 909 specifications that cover Network Call-based Signalling (NCS), Internet Signalling Transport Protocol (ISTP), Trunking Gateway Control Protocol (TGCP) and Internet Protocol Access Terminal - Line Control Signalling (IPAT-LCS), it therefore specifically excludes implementation based upon the Distributed Control Signalling (DCS) model and ITU-T Recommendation H.248 [31] options. Generally the present document does not cover:

- the Euro-DOCSIS protocol between CM and CMTS (AN);
- mechanisms that are used in the IP-cloud including but not limited to the IP-routing and backbone QoS-mechanism (e.g. MPLS, RSVP);
- interfaces for connection to the PSTN network as far as these interfaces are covered in other test specifications. IPCablecom.

2 References

For the purposes of this Technical Report (TR) the following references apply:

- [1] Void.
- [2] Void.
- [3] Void.
- [4] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol".
- [5] ETSI TS 101 909-5: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems".
- [6] Void.
- [7] Void.
- [8] Void.
- [9] Void.
- [10] ETSI TS 101 909-10: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 10: Event Message Requirements for the Provision of Real Time Services over Cable Television Networks using Cable Modems".
- [11] ETSI TS 101 909-11: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".
- [12] ETSI TS 101 909-13: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol".
- [13] Void.
- [14] ETSI TS 101 909-23: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 23: Internet Protocol Access Terminal - Line Control Signalling (IPAT - LCS)".
- [15] Void.

- [16] Void.
- [17] Void.
- [18] ETSI ES 201 488: "Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification".
- [19] ETSI EN 300 324-1: "V interfaces at the digital Local Exchange (LE); V5.1 interface for the support of Access Network (AN); Part 1: V5.1 interface specification".
- [20] ETSI ETS 300 347 (series): "V interfaces at the digital Local Exchange (LE); V5.2 interface for the support of Access Network (AN)".
- [21] ETSI EG 201 188: "Public Switched Telephone Network (PSTN); Network Termination Point (NTP) analogue interface; Specification of physical and electrical characteristics at a 2-wire analogue presented NTP for short to medium length loop applications".
- [22] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".
- [23] IETF RFC 2749: "COPS usage for RSVP".
- [24] IETF RFC 2750: "RSVP Extensions for Policy Control".
- [25] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".
- [26] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".
- [27] ISO 9646 (series): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework".
- [28] Void.
- [29] Void.
- [30] Void.
- [31] ITU-T Recommendation H.248: "Implementors' Guide".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

conformance testing: ability to demonstrate that components developed independently meet a common interface standard; it does not guarantee that components will work together to perform a system function

Call Management Services (CMS): this device performs the ITU-T Recommendation E.164 [25] to IP address translation and call control management functions within the network

NOTE: It is sometimes referred to as a "Soft Switch"

Cable Modem Termination System (CMTS): the device at a cable head-end which implements the Euro-DOCSIS RFI MAC protocol and connects to CMs over an HFC network

Embedded Multimedia Terminal Adapter (E-TMA): single node which contains both an MTA and a cable modem (CM)

IKE-: IKE with pre-shared keys for authentication

IKE+: notation defined to refer to the use of IKE, which requires digital certificates for authentication

integration test run: complete set of test cases; the regression test of the software

interoperability: where one component, from one manufacturer, can be replaced with another, and the basic operation of the system remains unaffected

interworking: ability of two (or more) systems to connect and pass signalling and communication content seamlessly

Internet Protocol Access Terminal (IPAT): essentially a protocol converter, mapping V5.2 events messages to those corresponding within the NCS protocol

KERBEROS: Secret key network authentication protocol that uses a choice of cryptographic algorithms for every phone and a centralized key database for authorisation

Standalone Multimedia Terminal Adapter (S-MTA): single node which contains an MTA and a non Euro-DOCSIS MAC (e.g. ethernet)

test case: specific set of test data applied to a script that test one successful or unsuccessful scenario

test data: input data of to a test, or the expected output data from the test execution

test script: file or manual instruction document that defines a set of stimuli and expected responses intended to test some part of the system; a test script may be a template to which a number of different test data input

test result: a successful conclusion occurs when the expected results match the results generated by test execution; failure occurs when they do not

test run: execution of one or more test cases with their test results

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AN	Access Node (see CMTS)
ANC	ANnouncement Controller
ANP	ANnouncement Player
ANS	ANnouncement Server
API	Application Programming Interface
ATS	Abstract Test Scripts
BPI+	Baseline Privacy Interface Plus
CA	Call Agent
CATV	Cable Access Television
CDR	Call Detail Records
CM	Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Termination System (see AN)
COPS	Common Open Policy Service
CPE	Customer Premise Equipment
DCS	Distributed Call/Control Signalling
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data Over Cable Service Interface Specification
DNS	Domain Name System
DQoS	Dynamic Quality of Service
DTMF	Dual Tone Multi-Frequency
EBP	Exterior Border Proxies
E-MTA	Embedded Multimedia Terminal Adapter
FQDN	Fully Qualified Domain Name
GC	Gate Controller
HFC	Hybrid Fibre/Coax
HI	Handover Interface (Lawful Interception)
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPAT	Internet Protocol Access Terminal

ISDN-BRI	Integrated Services Digital Network - Basic Rate Interface
IPsec	IP security
ISO	International Organization for Standards
ISTP	Internet Signalling Transport Protocol
ISUP	Integrated Services Digital Network User Part
KDC	Key Distribution Certificate
LAN	Local Area Network
LCS	Line Control Signalling
LE	Local Exchange
LEMF	Law Enforcement Monitoring Function
LI	Lawful Interception
MAC	Media Access Control
MF	Multi-Frequency or Mediation Function
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
MMH	Multilinear Modular Hash
MPLS	Multiprotocol Label Switching
MTA	Multimedia Terminal Adapter
MTP	Message Transfer Part
NCS	Network Based Call Signalling
NTP	Network Termination Point
OSS	Operational Support System
PHB	Per Hop Behaviour
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography Initial Authentication
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in IPCablecom
RFI	Radio Frequency Interface
RKS	Record Keeping Server
RSVP	Resource reSerVation Protocol
RSVP+	Resource reSerVation Protocol Plus
RTCP	Real-Time Control Protocol
RTP	Real-Time Transfer Protocol
SA	Source Address
SCCP	Signalling Connection Control Part
SCN	Switched Circuit Network
SEC	Security
SG	Signalling Gateway
SID	System IDentification number
S-MTA	Standalone Multimedia Terminal Adapter
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SS7	ITU-T Signalling System Number 7
TCAP	Transaction Capabilities Application Part
TFTP	Trivial File Transfer Protocol
TGCP	Trunking Gateway Control Protocol
TGS	Ticket Granting Server
ToS	Type of Service
TP	Test Purpose
TSS	Test Suite Structure
UDP	User Datagram Protocol
USB	Universal Serial Bus
VoIP	Voice over IP
V5	general description used to reference V.5.1/V.5.2 signalling protocols at the digital local exchange

4 Overview

The purpose of the present document is to define the size of the task for producing a test plan or strategy for the IPCablecom system. It will describe the elements of the system under test, the interfaces that may be tested and potential functional requirements for validation. Currently it is expected that testing will focus on two objectives: conformance testing to prove a component implements a particular protocol property and interoperability testing to prove a component from one vendor can seamlessly replace another vendor. The large body of specifications are analysed to examine areas that are affected by these two testing objectives, in the context of the business objectives of the cable TV industry.

The present document only scopes the size of the task so that the next step (generation of a system test plan or strategy specification) can be assigned adequate resources. Thus it focuses on identifying critical components and interfaces for testing, sets priority for testing activities and examines availability of commercial test systems. The present document does not define test environments, test cases, test scripts, test tools, test scenarios, test sequences, etc; that is the purpose of the test strategy. However, it should be noted that the job of designing a test plan should not be underestimated. The PacketCable architecture is similar to IPCablecom, except that IPCablecom defines in addition to PacketCable a V5.2 interface on an IPAT, ISDN-BRI interface on the E-MTA, NCS European analogue line package relevant to European PSTN line characteristics and lawful interception interfaces specific to European needs. As of 2001, the Cable Labs' Forum under their project, PacketCable, had defined interoperability tests for 8 out of 11 areas (TGCP, ISTP, and security are still in definition), clearly such interoperability testing of functional requirements is beyond the scope of the ETSI intent. It is important to carefully narrow the nature of the testing intended for IPCablecom to conformance test requirements, defining a PICS, TP&TSS and ATs in accordance with the ISO 9646 [27] testing requirements.

The present document thus is a transient document intended to demonstrate the size of the testing task least it get out of hand, and discuss ways to narrow the testing scope while meeting important business and technical objectives of IPCablecom. It is expected that the next step, the creation of a test plan or strategy, will identify a set of Plugtest™ plans covering major interfaces of IPCablecom and assist in the development of conformance testing specifications in accordance with ISO 9646 [27].

4.1 General objectives

The general objectives of this STF effort are to:

- identify critical areas of the IPCablecom architecture and component interfaces for testing;
- define which areas are more applicable to be conformance tested and those which would be best tested by interoperability events (Plugtests™);
- set an order of priority for testing activities;
- examine the availability of commercial "off-the-shelf" test systems;
- produce input for development of TS 101 909 parts 25, 26 and 27.

4.2 Business objectives

The identified business objectives of developing the testing effort are:

- to identify critical areas and interfaces for testing;
- interoperable components (products);
- stimulate market by providing systems with components from different vendors;
- create stability in marketplace by defining a common fixed set of interfaces;
- reduced time and costs for system deployment;
- feedback into standardization process.

5 Analysis of the IPCablecom architecture

5.1 Analysis of reference architectures for testing

IPCablecom has been conceived as a series of upward compatible architectures, LCS, NCS, and DCS, each of which can be deployed to meet the timeframes and business objectives of operators. While DCS has been briefly discussed in committees, it is not yet at a level suitable for deployment. However, NCS is fully defined and LCS is expected to be released by ETSI by the end of 2002, so these two architectures are described below.

5.1.1 Analysis of the NCS - CMS reference architecture for testing

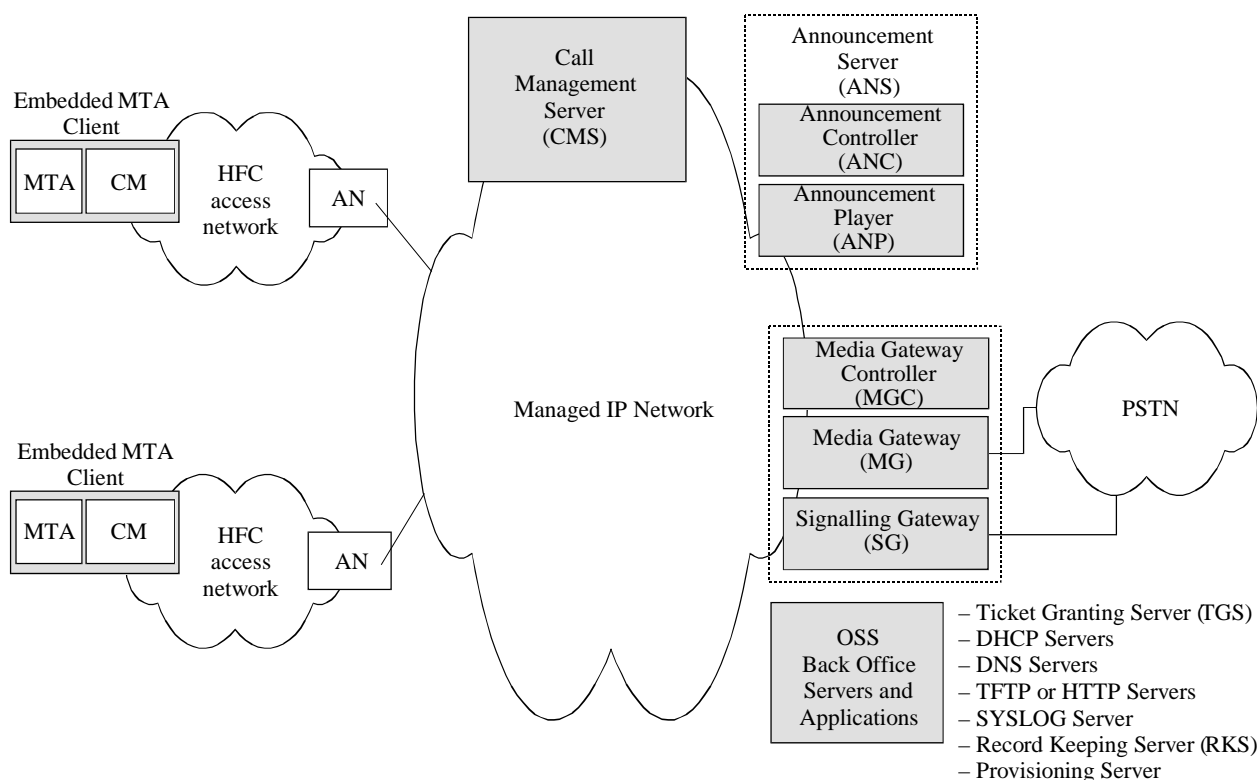


Figure 1: IPCablecom NCS reference architecture

Figure 1 provides a high level overview of the architecture defined in TS 101 909-2. The initial phase of the analysis of the IPCablecom system focussed solely upon the LCS and NCS architecture implementation and excluded the DCS model. The current edition of the document focuses on simplifying and breaking down the relationships between the various functions.

Figure 3 illustrates the critical elements of the IPCablecom system and identifies the key protocols considered within the scope of the conformance testing activity and production of deliverables TS 101 909 parts 25, 26 and 27.

Building upon the initial structure given in Figure 3, the signalling interactions between the functional elements as given by the TS 101 909 series are identified.

5.1.2 Analysis of the LCS - IPAT reference architecture for testing

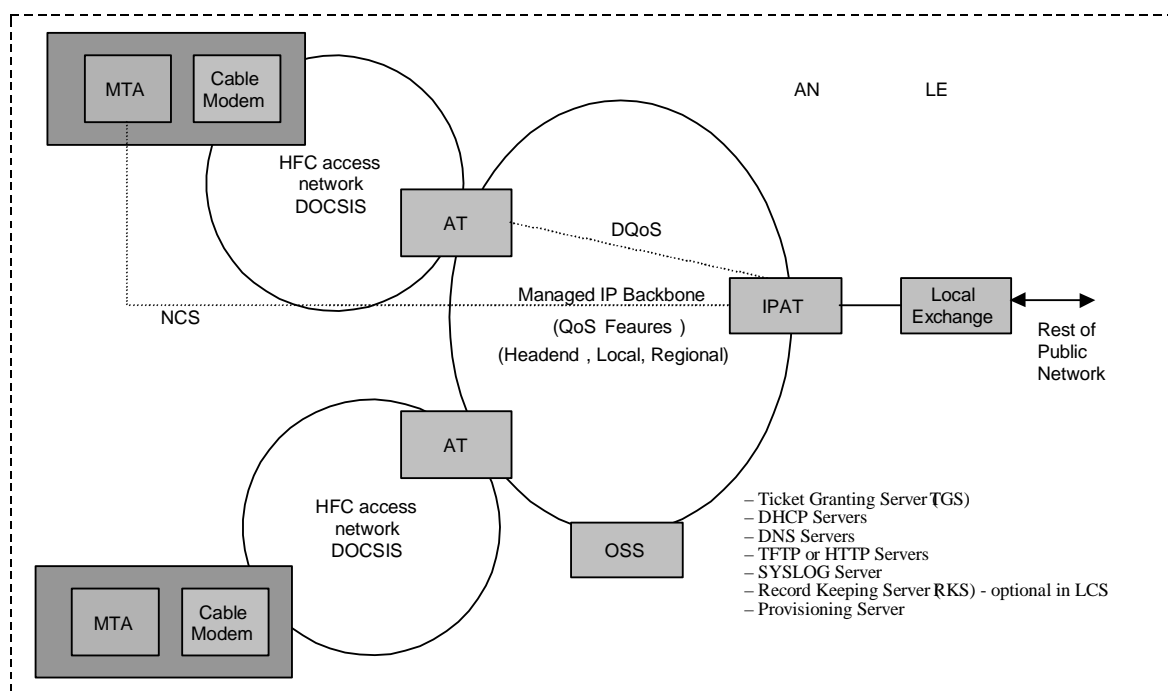


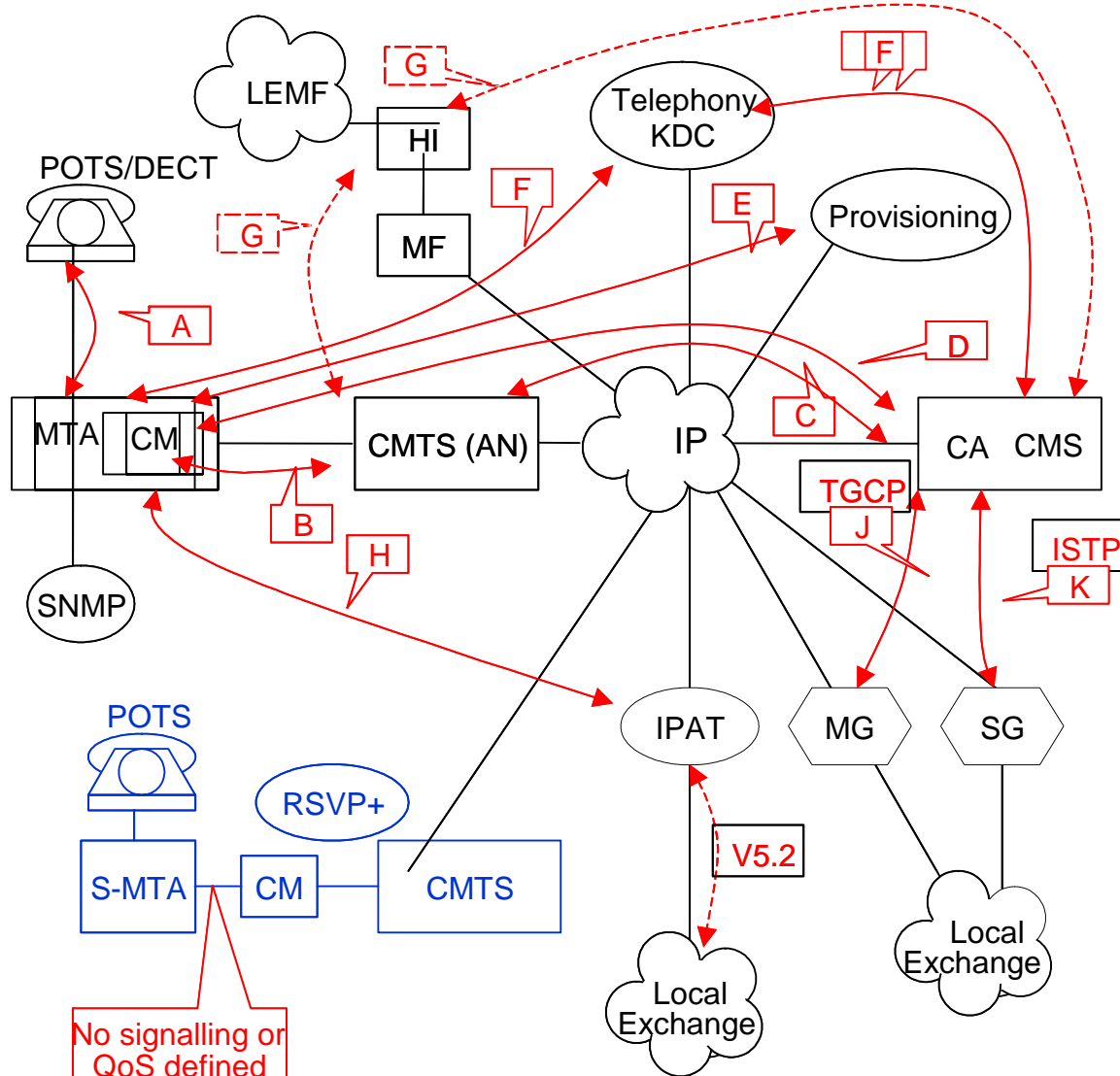
Figure 2: IPAT reference LCS architecture

Figure 2 provides a high level overview of the architecture defined in TS 101 909-23 [14].

The Line Control Signalling architecture identifies a component called the Internet Protocol Access Terminal (IPAT) which acts as the interface between the managed IP network and the Local Exchange. The IPAT provides the inter-working function of mapping the V5.2 call signalling from the LE to the NCS call signalling carried over the managed IP network. In the LCS architecture, the LE performs many of the functions, which the NCS architecture assigns to the IPAT. This includes keeping track of call state, generating billing records, providing advanced call features and lawful interception.

Four interfaces are associated with the IPAT:

- Pkt-c1 and Pkt-c10, between the IPAT and the MTA; and
- Pkt-c8 and Pkt-c9, between the IPAT and the LE.



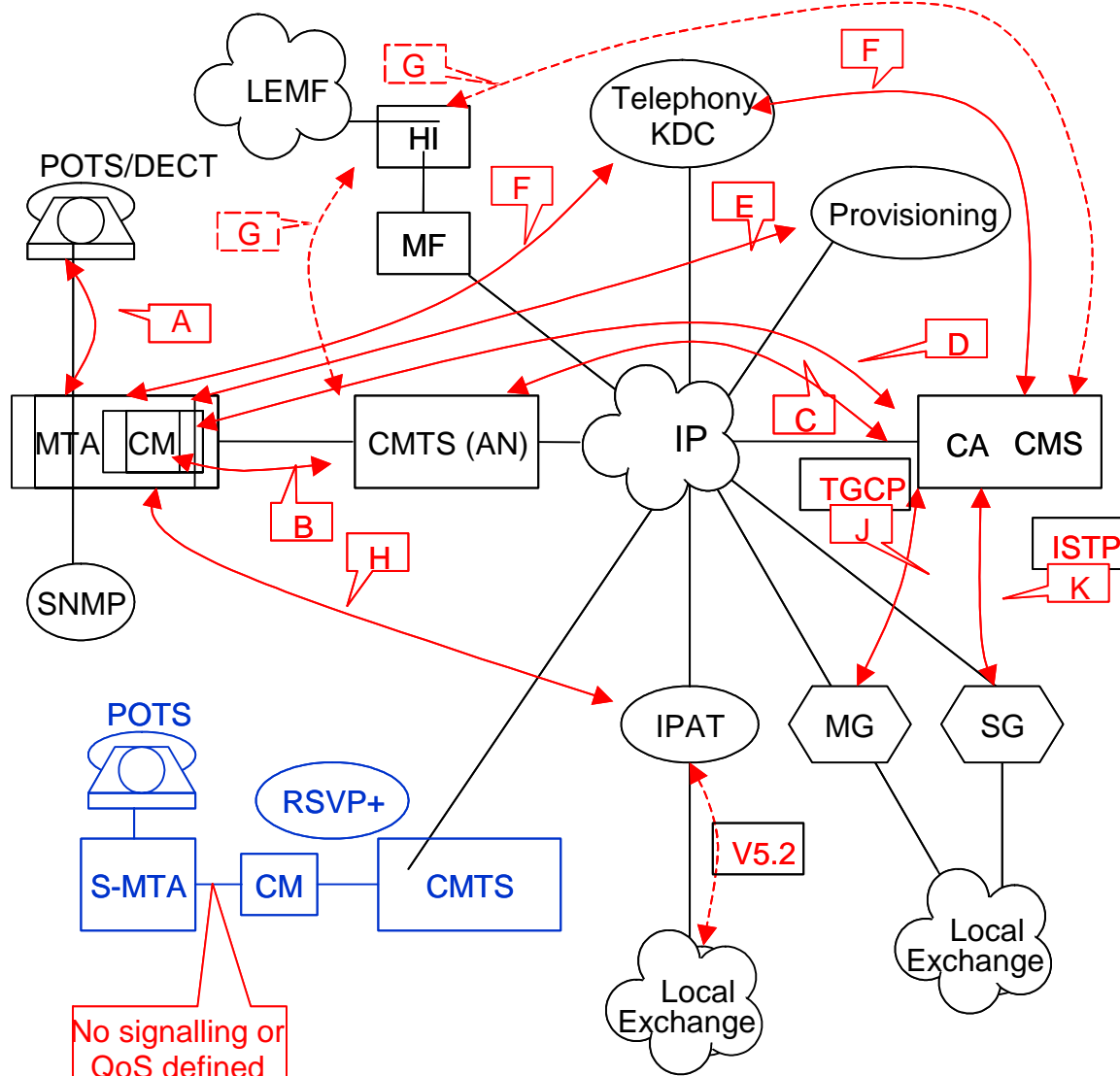
NOTE: This approach not currently standardized

Figure 3: IPCablecom reference functions/interfaces

5.2 Analysis of signalling interface-interactions

IPCablecom is conceived as an integrated distributed system of co-operating and current elements with multi-layered multi-media protocols and end-to-end service support. Thus the structure of the IPCablecom technical specifications do not by nature lend themselves to defining the individual elements of the system as isolated parts, which request that interfaces be clearly and independently identified for conformance testing purposes. Consequently, prior to performing any analysis of the complex signalling interactions that take place within the system, as graphically depicted in figure 3, each of the physical and logical interfaces are identified for each critical element.

Based upon the identification of the various interface interactions, the signalling interactions that are to be the subject of further study in respect of testing requirements are identified.



NOTE: This approach not currently standardized

Figure 4: IPCablecom interface-interactions

An analysis of the overall system is made by mapping the structure of the requirements as given in the series of TS 101 909 IPCablecom Specifications against each interface. The critical elements for further future study were identified from the analysis of the signalling interactions as illustrated in figure 5.

Figure 7 provides an outline of the primary signalling interactions considered.

Figures 8, 9, 10 and 11 identify the various elements of the IPCablecom system involved in the following signalling and requirements aspects:

- security mechanisms;
- lawful interception;
- provisioning;
- Dynamic Quality of Service (DQoS).

CM/MTA	Test Specification	B
CMTS	Test Specification	B
IPAT	IPAT <> MTA (NCS)	H
MTA	POTS Functional Testing	A
CMS	COPS : CMS – CMTS	C
	MGC – MG (TGCP)	J
	MGC – SG (ISTP)	K
	CA / MTA (NCS)	D
Provisioning	MTA – Provisioning Server	E
Security	Test Specification	F
	Lawful Intercept Test Specification	G

Figure 5: Key to signalling interactions

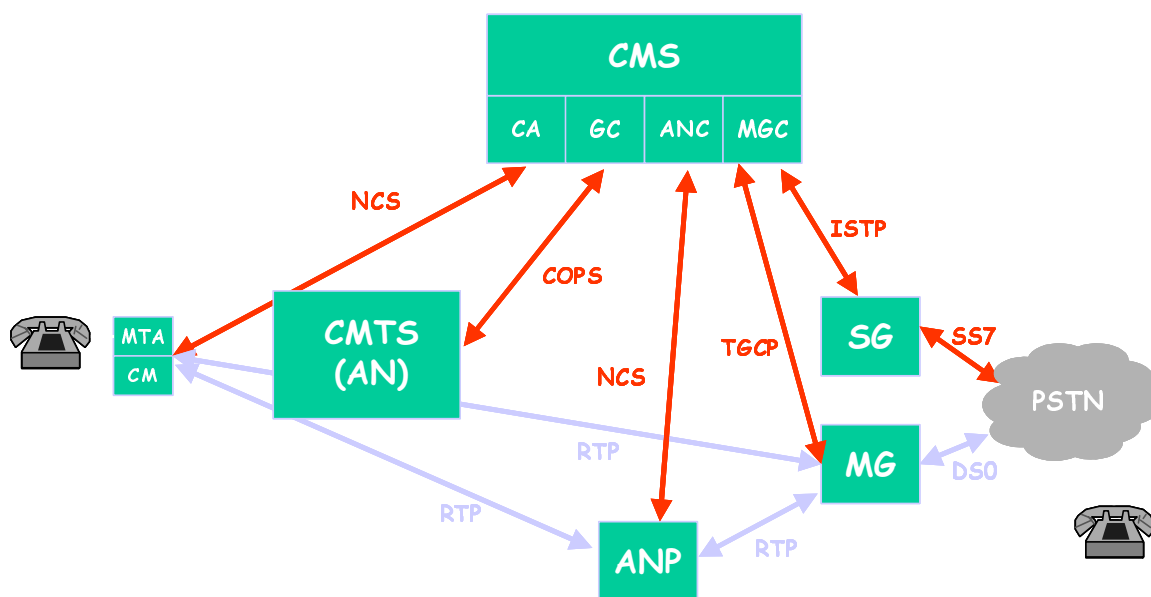


Figure 6: Overview of signalling protocol interactions

Figure 6 is an illustration of the signalling protocol interactions between the IPCablecom elements.

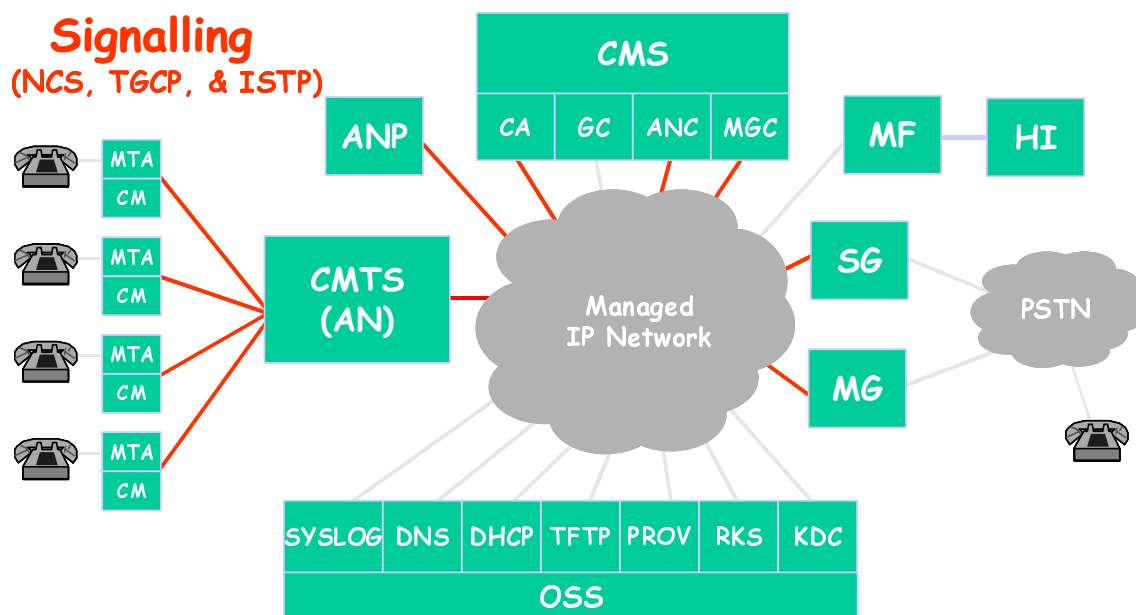


Figure 7: Outline of the primary signalling interactions

Figure 7 is an illustration of the access and trunking signalling protocol interactions between the associated IPCablecom elements.

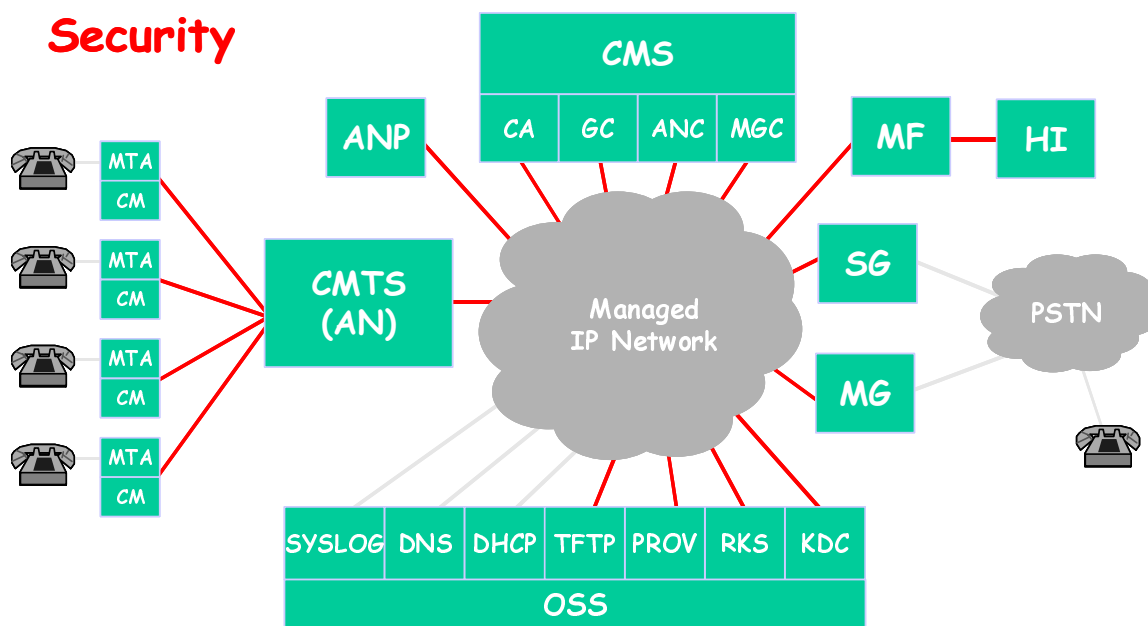


Figure 8: Outline of the security mechanisms and signalling interactions

Figure 8 illustrates the security requirements that are applied to the various IPCablecom interfaces.

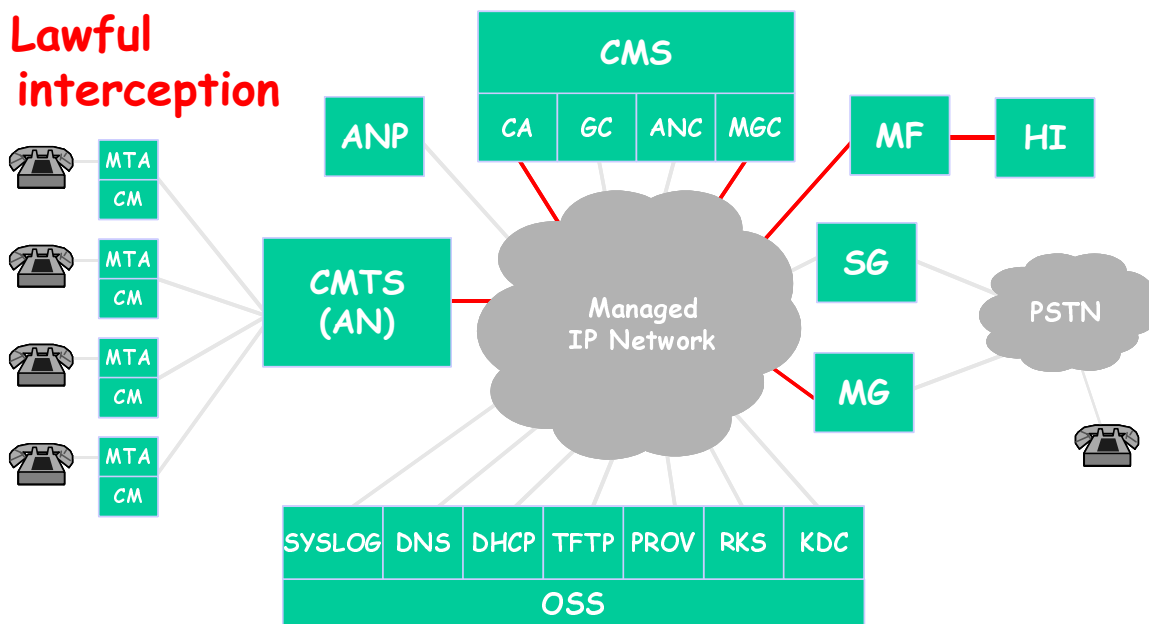


Figure 9: Outline of the elements involved in lawful intercept interactions

Figure 9 illustrates the various IPCablecom interfaces for lawful interception.

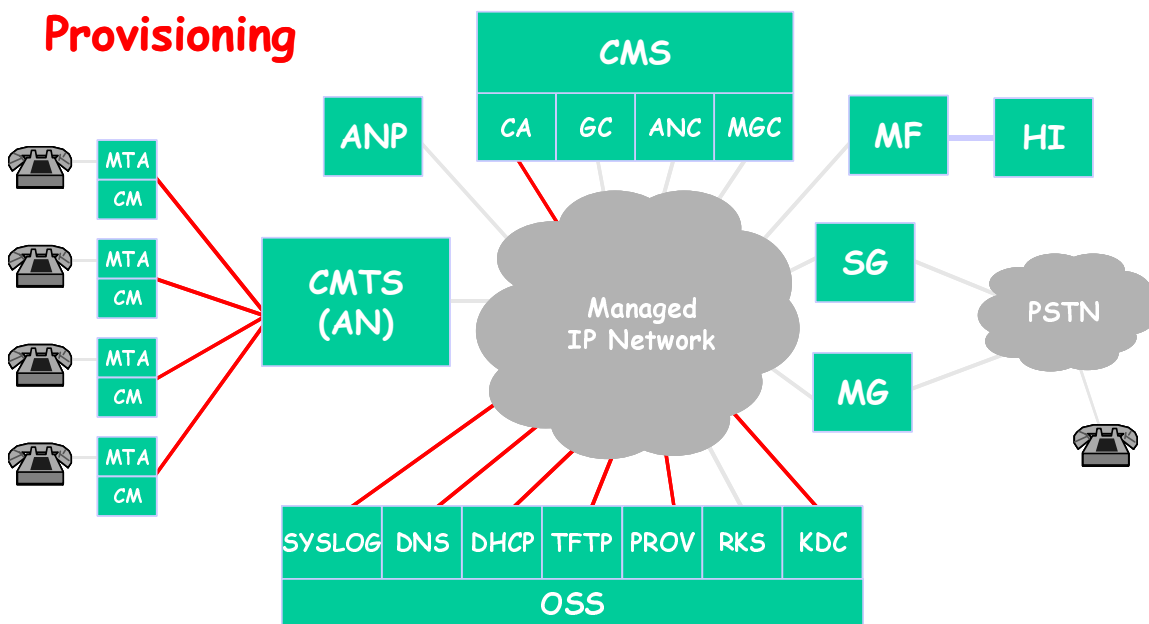


Figure 10: Outline of the elements involved in provisioning

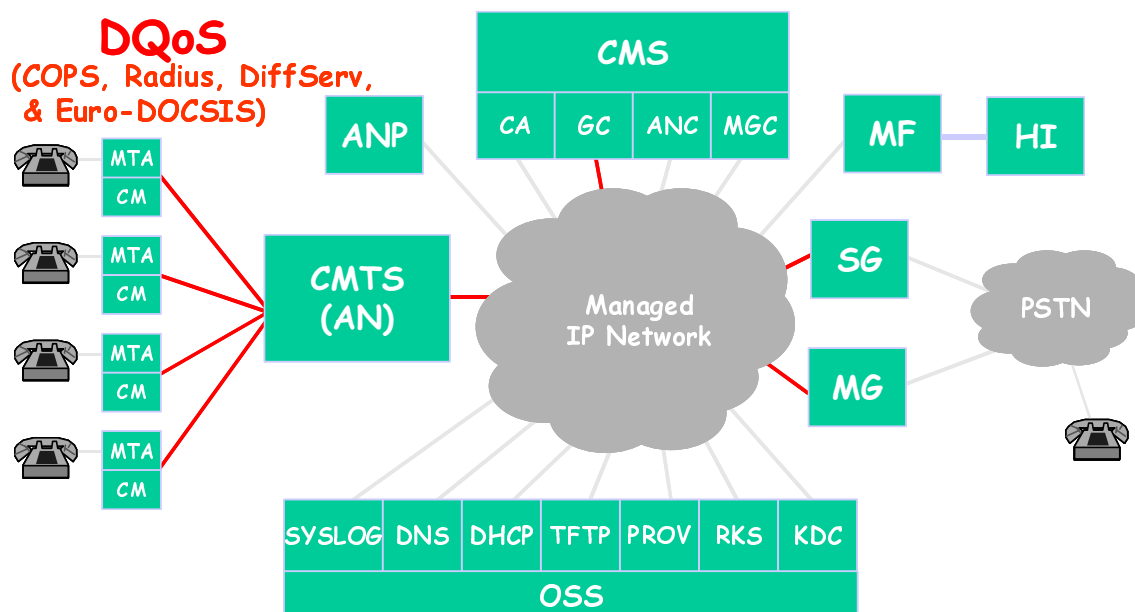


Figure 11: Outline of the elements involved in providing DQoS

6 Analysis of individual IPCablecom system elements

6.1 Structure and basis for analysis

The IPCablecom requirements as defined in the TS 101 909 series define both functional and physical requirements upon the various elements of the overall system. In an attempt to capture this in meaningful terms that can be identified and assessed from the point of developing test purposes and test cases, the various interfaces referred to in the TS 101 909 series are evaluated as being either Logical or Physical.

For instance, DQoS places requirements upon the stream interface, likewise Security specifies a requirement on the stream and NCS interfaces where these are tagged as Logical Interfaces. An example of a Physical interface is the HFC connection between a Cable Modem and the CMTS.

6.2 MTA/CM Framework

6.2.1 General

The MTA/CM is the end-user component in the IPCablecom system. Any operational problem related to a specific MTA in the field results in a high cost to an operator. Additionally a customer demands high availability and reliability of the voice-service.

The objectives for creating a test specification addressing the CM/MTA are to:

- ensure the NCS protocol has been implemented correctly by a CM/MTA;
- validate the operation/adherence with respect to IPCablecom call flows;
- create finer granularity of testing instead of one monolithic test case;
- assess conformance to the TS 101 909 series;
- ensure interoperability across different manufacturers' platforms;
- verify that the requirements within the TS 101 909 series can be tested;

- identify errors/changes in the requirements specifications and provide feedback for update of the TS 101 909 series;
- protection against theft-of-service is a critical area for CATV operators and needs to be studied;
- verify media stream adherence to RTP, UDP, and IP standards, and the IPCablecom QoS and CODEC selection options;
- adherence to DOCSIS is out of the scope of the present document.

6.2.2 Description of the MTA/CM (E-MTA) interfaces and functions

Based upon the analysis conducted and outlined earlier in clause 5, the functions of the CM/MTA interfaces can be identified to ensure the interoperability between the various elements of the IPCablecom system.

With regards to figure 12, the E-MTA is the network termination point that contains a subscriber-side interface to the subscriber's CPE through the POTS (P9) or Air interface (e.g. DECT) (P8) interfaces. Additionally, it will in most cases also have a data-port (P10) (e.g. USB or 10 BaseT) that allows the subscriber to connect to the Internet. The MTA uses the IP-protocol to communicate to elements at the network-side of the MTA, using Euro-DOCSIS 1.1 (P11) as the layer 2 protocol. The Euro-DOCSIS functionality is provided by an embedded cable modem in the MTA. This cable modem handles all layer 1 and 2 functionality for connectivity over the HFC network. Additionally the cable modem has features that enable Quality of Service across the HFC network. The voice-stream (L1) of the MTA is sent over RTP/RTCP that runs over IP to the other endpoint. This endpoint can either be a terminating endpoint (e.g. another MTA) or some intermediate device (media gateway). Voice signals are converted to a digital stream using the CODEC (L7).

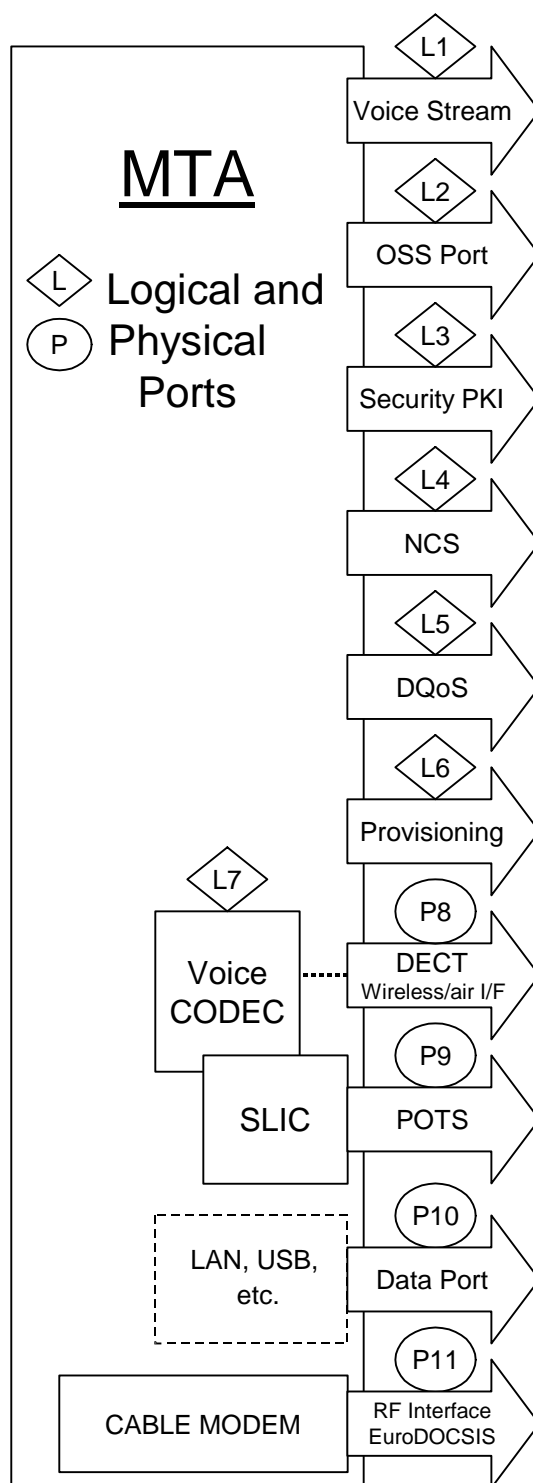


Figure 12: MTA/CM framework

The MTA uses the NCS protocol (L4) as the means of signalling to the network and specifically to the Call Agent (CA) (refer to figure 6). The DQoS (L5) (dynamic quality of service) interface specifies the mechanism used to establish QoS between the MTA and the CMTS over the Euro-DOCSIS 1.1 system. Security (L3) is applied to all signalling and stream interfaces, it consists of the authentication of MTAs to prevent theft of service, used encryption algorithms and mechanism to distribute the different encryption and authentication keys to the MTA. A Public Key Infrastructure is used to authenticate the MTA to the system.

The provisioning logical port (L6) identifies the different mechanism and protocols used to provision an MTA to become operational in an IPCablecom system. It uses a number of well-known protocols that run on top of IP, like DHCP, TFTP, DNS and SNMP. The provisioning process also covers the processing of the received configuration file for the MTA. The Operations System Support Interface (OSS) (L2) uses SNMP as the protocol to access management information in the MTA, this interface not only covers the SNMP-protocol but also the MIBs that are present in an MTA.

POTS/DECT interface: The interaction between the POTS/DECT terminal and the MTA need to be verified together with the functions and features supported. Conformity of these interfaces to existing ETSI specifications (TBR 021/TBR 010) would be deemed as providing essential interworking criteria. However, there are numerous signalling interactions that are not covered by these standards that are supported within the IPCablecom system. For example, the interactions between the MTA and CA that require verification (refer to TS 101 909-4 [4] annex A for the European Analogue Line Package). For POTS-interfaces no test-specification is available at this point in time. EG 201 188 [21] is a guide to the requirements of this interface. For DECT-interfaces, the applicable DECT test specifications should be consulted. The specification of how the POTS-interface and DECT interface need to be tested is outside of the scope of this work.

RTP/RTCP: The media stream in the MTA is carried using RTP as the underlying protocol; RTCP accompanies RTP for feedback control. There are specific problems testing the RTP/RTCP, associated with the fact that a stream cipher is used for encryption. Analysis needs to be performed if there is a need to specify the delay introduced by using encryption on the media stream. The media stream is the only stream for which QoS-parameters are very important.

DQoS: DQoS involves the process of establishing the needed messaging to be able to specify the QoS-resources needed for a voice-call. Specific relation to ES 201 488 [18] (Euro-DOCSIS) modem will need to be tested.

Euro-DOCSIS 1.1 or higher: Euro-DOCSIS 1.1 is an essential requirement on the MTA to be able to have QoS over the cable-access network. Although Euro-DOCSIS 1.1 is a separate testing process, specific items related to the Euro-DOCSIS specification need to be incorporated in the testing as the MTA is embedded within a cable modem. The interface-interactions that need to be tested are the messaging for DQoS and the classification of the RTP-streams to the right Euro-DOCSIS 1.1 Service Flow. There are no ETSI test specifications covering Euro-DOCSIS 1.1 [18], however, the testing of the physical layer of cable modems, together with the full MAC-functionality, encryption and authentication requirements and the data-interfaces towards the customer should be considered. The OSS-stack of the cable modem is also tested. The mechanism to support different QoS across the HFC-network is covered in the Euro-DOCSIS 1.1 [18] Service Flow testing also needs to be considered. The interface between MTA and embedded CM is an internal interface, therefore part of the testing of the Security and DQoS-functionality will be based on the interactions at the DOCSIS 1.1 [18] MAC layer to identify the correct behaviour for Security, Privacy and DqoS mechanisms. The testing of Euro-DOCSIS 1.1 is outside the scope of this study, however, before evaluating an IPCablecom Euro-DOCSIS 1.1 device such as an E-MTA or CMTS the device would need to be first identified to comply with the requirements of DOCSIS 1.1 [18] base standard prior to conformance testing of IPCablecom.

A DOCSIS 1.1 [18] device would need to demonstrate conformity to the Testing Specifications being developed as given by deliverables DTS/AT-020042-01, DTS/AT-020042-02 and DTS/AT-020042-03 prior to demonstrating conformity to TS 101 909-25, TS 101909-26 and TS 101909-27.

NCS: The Network Call Signalling protocol is an essential component in the whole system. It establishes the needed signalling so the Call Management Server can start the needed messaging and give the needed information to the MTA to set up a voice call. The MTA acts as a slave to the Call Agent (Master) in respect that it is instructed by the CA to monitor events at the end-point, e.g. detect Off-Hook and notify the CA, which then sends further instructions. These NCS signals and events, as given in TS 101 909-4 [4], are interactions at the MTA interface that should be verified.

Provisioning interface: The provisioning interface is a broad term related to a set of interactions using different protocols. The first step is related to the provisioning of the CM-part. Protocols involved are DHCP, TFTP, ToD, DNS, KERBEROS and SNMPv3. Another part is mainly related to getting the security information needed for the MTA.

Security: The MTA needs to get and refresh the needed security information. Lack of the needed security information generates potentially high problems in an operational network that are difficult to debug.

OSS: Operations systems support is a broad term to cover a whole set of management-related functionality. It is mainly related to implementing the MIBs correctly. Some of these MIBs are essential in the whole system, while others are of minor importance. One essential item is the fact that the protocol used to manage the MIBs (SNMP) is correctly implemented and also that the limitation of access to management-information is working correctly. It is also important to note that some management information (MIBs) can be configured or through SNMP or by config-file, the resulting behaviour should be independent from the used mechanism. Note that the very important feature of software upgrade is tested as part of the Euro-DOCSIS testing.

6.2.3 Interface interaction

It was considered that the scope for any future testing of the IPCablecom system should not be limited to individual interfaces, but includes the associated interface interactions.

6.2.3.1 Interface-interactions for test consideration

The following interface-interactions need to be considered for testing:

- **POTS/DECT-RTP:** The interaction that needs to be considered is verifying that the right CODEC is used and the corresponding RTP-stream is correctly encoded/decoded. Part of this testing also involves the analysis of the jitter of the generated media-stream. Not that this last verification needs to be performed after the stream is put on the Euro-DOCSIS service flow as there is no internal interface accessible for verification;
- **RTP/RTCP-Euro-DOCSIS:** Verification is needed that the RTP-stream is classified to the right Euro-DOCSIS Service Flow. Furthermore analysis on the CODED implementation is part of this (this is of relevance to the previous bullet);
- **Prov-OSS:** By provisioning (config-file) management information can be configured in the MTA. As part of the provisioning process the MTA will also receive specific information where to send syslogs. Part of the provisioning information needs to be reported in the correct MIBs;
- **NCS:** Verification of the correct signalling interpretation, as per the associated call flows, is a critical element to ensuring the E-MTA can be integrated within the system;
- **DQoS:** Dynamic Quality of Service places requirements upon the stream interfaces and should be considered as a critical area of further study when developing conformance test purposes. The following interface-interactions may be considered in this study:
 - **CMTS to MTA:** The MTA makes dynamic requests for modification of QoS traffic parameters. When the CMTS receives the request it makes an authorization check to find out whether the requested characteristics are within the authorized QoS envelope and also whether the media stream endpoints are authorized. Then it provisions the QoS attributes for the RFI link on the CMTS and activates the appropriate QoS traffic parameters via signalling with the CM. When all the provisioning and authorization checks succeed the CMTS sends a success message to the GC/CMS indicating that MTA and CMTS are engaged in a Service Level Agreement;
 - **CMTS to CM:** The CMTS is responsible of setting up and tearing down service flows in such a way that the service level agreement it made with the MTA is met. In as much as the CMTS does not trust the CM it polices the traffic from the CM such that the CM works in the way CMTS requested;
 - **Cable Modem (CM):** Even though the CM is an untrusted entity the CM is responsible for the correct operation of the QoS link between itself and the CMTS. The CMTS makes sure that the CM cannot abuse the RFI link, but it is the responsibility of the CM to utilize the RFI link to provide services that are defined by ITU-T Recommendation J.112 [26];
 - **MTA:** The MTA is the entity to which the Service Level Agreement is provided by the access network. The MTA is responsible for the proper use of the QoS link. If it exceeds the traffic authorized by the SLA than it the MTA will not receive the QoS characteristics that it requested. The MTA uses two stage QoS bandwidth allocation - while the call origination is proceeding the QoS resources are admitted, then when the call is answered the resources are activated.

6.2.3.2 CM CMTS Interface-interactions

With reference to figure 4, the following interface-interactions (labelled [B]) are considered as being outside the scope of the present document as these are not specified within any of the TS 101 909 series.

- cable modem initialization - covered by Euro-DOCSIS;
- interactions for initialization sequences;
- security mechanisms:
 - encryption:
 - i) 3DES;
 - ii) PKI.
 - manufacturers' digital certificates;
 - unique MAC address.
- MAC layer QoS requirements;
- base line privacy (BPI+).

6.3 CMTS (AN) Framework

6.3.1 General

The objectives for creating a test specification addressing the CMTS are to:

- validate the operation/adherence with respect to IPCablecom call flows;
- create finer granularity of testing instead of one monolithic test case;
- assess conformance to the TS 101 909 series;
- ensure interoperability across different manufacturers' platforms;
- verify that the requirements within the TS 101 909 series can be tested;
- identify errors/changes in the requirements specifications and provide feedback for update of the TS 101 909 series.

6.3.2 Description of the CMTS interfaces and functions

The CMTS provides data connectivity and complimentary functionality to Cable Modems over the HFC access network. It also provides connectivity to wide area networks. The AN is located at the cable television system head-end or distribution hub.

L20: Record Keeping Server (RKS):

The RKS is a trusted network element component that receives IPCablecom Event Messages from other trusted IPCablecom network elements such as the CMS, CMTS, and MGC. The RKS also, at a minimum, is a short-term repository for IPCablecom Event Messages. The RKS may assemble the Event Messages into coherent sets or Call Detail Records (CDRs), which are then made available to other back office systems such as billing, fraud detection and other systems.

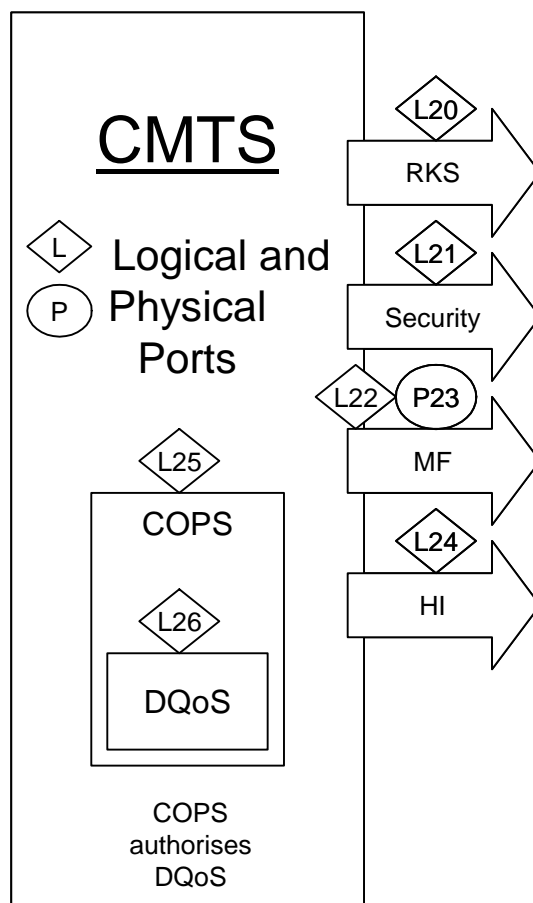


Figure 13: CMTS (AN) framework

L21: Security:

The security reference TS 101 909-11 [11] imposes requirements upon the CMTS (AN) to:

- enable residential voice capabilities with the same or higher level of perceived privacy as in the PSTN;
- provide protection against attacks on the MTA;
- protect the cable operator from various denial of service, network disruption and theft of service attacks.

Design considerations must include confidentiality, authentication, integrity, non-repudiation and access control.

L22 and P23: Mediation function (MF):

This subject is dealt with in TS 101 909 part 20; however, this specification is still under development.

NOTE: Further analysis will need to be performed once this specification is available.

L24: Handover Interface for LI (HI):

This subject is dealt with in TS 101 909 part 20; however, this specification is still under development.

NOTE: Further analysis will need to be performed once this specification is available.

L25: COPS:

COPS is specified in RFC 2748 [22], with additional information that could be useful in RFC 2749 [23] and RFC 2750 [24]. Within the IPCablecom system the COPS protocol is used to provide the CMTS information on what service flows and which classifiers the CM is allowed to use for a particular session. The COPS protocol is used between the gate-co-ordination element of the CMS to the CMTS. COPS is used for both types of setting up service flows in the Euro-DOCSIS, when RSVP signalling is used, the COPS-protocol is used to verify that the CM does not ask for too much resources or for the wrong classifiers in the RSVP messaging. When the DSx-mechanism is used, the Service Flow and Classifiers parameters are authorized using the COPS-protocol.

L26: Dynamic Quality of Service (DQoS):

IPCablecom Dynamic QoS (DQoS) utilizes the call signalling information at the time that the call is made to dynamically authorize resources for the call. Dynamic QoS prevents various theft of service attack types by integrating the QoS messaging with other protocols and network elements.

6.3.3 Interface interaction

The function within the CMTS that performs traffic classification and enforces QoS policy on media streams is called a Gate. The Gate Controller element manages Gates for IPCablecom media streams.

The following key information is included in signalling between the GC and the CMTS:

Maximum Allowed QoS Envelope:

The maximum allowed QoS envelope enumerates the maximum QoS resource (e.g., "2 grants of 160 bytes per 10 ms") the MTA is allowed to admit for a given media stream bearer flow. If the MTA requests a value greater than the parameters contained within the envelope the request will be denied.

Identity of the media stream endpoints:

The GC/CMS authorizes the parties that are involved in a media stream bearer flow. Using this information the CMTS can police the data stream to ensure that the data stream is destined and originated from the parties that are authorized.

Billing Information:

The GC/CMS creates opaque billing information that the CMTS does not have to decode. The information might be as simple as billing identity or the nature of the call. The CMTS forwards this billing information to the RKS as the call is activated or terminated.

The role of each of the IPCablecom elements in implementing DQoS is as follows:

Call Management Server/Gate Controller:

The CMS/GC is responsible for QoS authorization. The QoS authorization might depend on the type of call, type of user or other parameters defined by policy.

CMTS:

Using information supplied by the GC/CMS the CMTS performs admission control on the QoS requests and at the same time polices the data stream to make sure that the data stream is originated and sent to authorized-media stream parties. The CMTS interacts with CM, RKS, MTA, and Terminating CMTS. The responsibilities of CMTS with respect to each of these elements are:

- CMTS to Record Keeping Server: The CMTS updates the Record Keeping Server (RKS) each time there is a change in the QoS Service Level Agreement between CMTS and MTA. It uses the Billing Information that is given by GC/CMS to identify each authorized QoS link. The CMTS puts timing information in the message it sends and also buffers the messages if the connection to RKS is severed;
- CMTS to Terminating CMTS: The CMTS sends messages to the terminating end CMTS (or other terminating access networking device) to ensure that the committed bandwidth on both sides is the same. If the committed bandwidth is not the same then both sides close the connection.

Record Keeping Server (RKS):

The RKS acts as a database and stores each event as sent by the CMTS. The RKS stores the messages by attaching received time and network element information. The RKS has to have sufficient interface and/or processing power to allow additional processing to be done.

6.4 IPAT MTA Framework

6.4.1 General

The objectives for creating a test specification addressing the IPAT - MTA are to:

- ensure the NCS protocol has been implemented correctly within a IPAT;
- validate the operation/adherence with respect to IPCablecom call flows;
- create finer granularity of testing instead of one monolithic test case;
- assess conformance to the specification(s);
- ensure interoperability across different manufacturers' platforms;
- verify that the requirements within the TS 101 909 series can be tested;
- identify errors/changes in the requirements specifications and provide feedback for update of the TS 101 909 series;
- verify the QoS, security and provisioning capabilities as per the TS 101 909 series;
- verify performance and scalability of the IPAT.

6.4.2 Description of the IPAT interfaces and functions

The test framework covering the IPAT functionality is studied based on the currently available documentation. The analysis of the IPAT is based on the first edition of TS 101 909-23 [14]. The European Cable Operators deploying IPCablecom services connect to the PSTN using the architectures described by the TS 101 909 series of specifications. Interconnection between the Cable Administration and the SCN is either via the Signalling SS7 Gateway or the IPAT-LCS Local Exchange (LE) V5 interface access. This clause covers the latter case, which is known as the Line Control Signalling (LCS) architecture. Note that the development of test framework covering the IPAT interface interactions is considered to be an essential requirement by European Cable Operators for the purpose of demonstrating a basic level of interoperability.

The following should be considered:

- develop test purposes covering the MTA including the NCS - V5.2 mapping as per TS 101 909-4 [4] annex B;
- develop test purposes covering the provisioning of the MTA for the LCS architecture;
- develop test purposes covering the provisioning of the IPAT;
- develop test purposes to ensure the correct implementation of security and QoS mechanisms;
- develop test purposes covering the interactions between the LE Call control and the MTA via the IPAT based on the subset functionality defined in TS 101 909-4 [4] annex B;
- develop or reference existing V5.2 test purposes for the V5.2 Network side: Reference may be made to existing V5.2 test protocols.

The test requirements covering the interactions between the IPAT and V5 LE should not be covered as far as these interfaces are covered in other ETSI test-specifications, except for abnormal call handling.

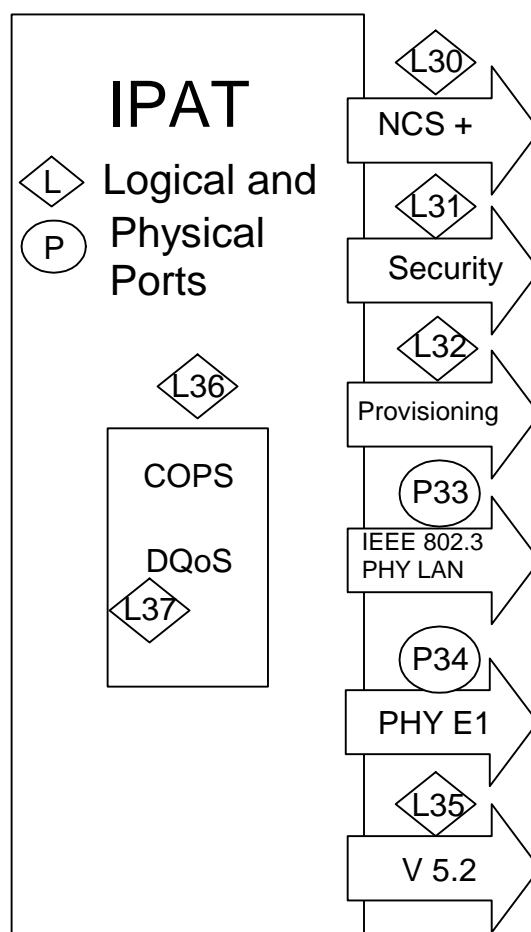


Figure 14: IPAT framework

L30: Network-based Call Signalling (NCS):

The Pkt-c1 interface uses the Network Call Signalling (NCS) protocol as used in the IPCablecom architecture and identified as signalling interaction [H] in figure 15. Commands of the NCS protocol are used to establish and tear down bandwidth across the HFC and managed IP networks, and to carry messages concerning such things as hook state and ringing cadence.

The Pkt-c8 interface defines bearer channel connectivity to the LE. There is no signalling over this interface in the LCS architecture.

L31: Security

This is identified as signalling interaction [L] in figure 15.

NOTE: This clause to be developed further based on edition 2 of TS 101 909-23 that is currently under development.

L32: Provisioning

IPAT Provisioning is identified as signalling interaction [M] in figure 15.

NOTE This clause to be developed further based on edition 2 of TS 101 909-23 that is currently under development.

P33: IEEE 802.3:

This is the physical connection of the IPAT to the IP backbone network. All signalling is carried over this interface to the rest of the IPCablecom components identified in figure 2 and is identified as signalling interaction [N] in figure 15.

P34: E1:

This is the physical connection of the IPAT to the Local Exchange. All V5.2 signalling is carried over this interface to the LE, as explained in L35.

L35: V5.2:

The Pkt-c9 interface uses the V5.2 PSTN call signalling protocol specified in EN 300 324-1 [19] and the BCC protocol specified in EN 300 347 [20]. The BCC protocol provides the information that the IPAT needs to allocate bandwidth on the TDM parts of the call. The PSTN protocol messages contain signalling information which the IPAT must translate to NCS messages. In addition to terminating the PSTN and BCC message flows from the LE, the IPAT also terminates three more LE message flows. These flows are the Control Channel, the Protection Channel and the Link Control Channel and optionally ISDN D channel. These three protocols all control some aspect of the V5.2 interface. There is no need to translate these protocol messages toward the IP network.

L36: COPS:

COPS is specified in RFC 2748 [22], with additional information that could be useful in RFC 2749 [23] and RFC 2750 [24]. Within the IPCablecom system the COPS protocol is used to provide the CMTS information on what Service Flows and which classifiers the CM is allowed to use for a particular session. The COPS protocol is used between the Gate-Coordination element of the CMS to the CMTS. COPS is used for both types of setting up service flows in the Euro-DOCSIS, when RSVP signalling is used, the COPS-protocol is used to verify that the CM does not ask for too much resources or for the wrong classifiers in the RSVP messaging. When the DSx-mechanism is used, the Service Flow and Classifiers parameters are authorized using the COPS-protocol.

L37: DQoS:

IPCablecom LCS provides guaranteed Quality of Service (QoS) for each voice communication within a single zone with Dynamic QoS, TS 101 909-5 [5].

DQoS is controlled by the Gate Controller function within the IPAT and can guarantee Quality of Service within a single zone. The IPAT Gate Controller uses the COPS protocol to download QoS policy into the AN. Should Gate Coordination be used, the IPAT Gate Controller uses the Radius protocol to coordinate the QoS reservation. The E-MTA utilizes the ITU-T Recommendation J.112 [26] QoS or/and the RSVP protocol to establish the QoS to the AN. QoS reservations are also forwarded to the IP Backbone between the ANs and the IPAT. DiffServ allows IP traffic to be marked with different DiffServ Code Points (DSCP) to obtain different queuing treatment on routers. Different queuing treatments in each router are called Per-Hop Behaviour (PHB), which is a mechanism for enforcing QoS for different flows in the IP Backbone.

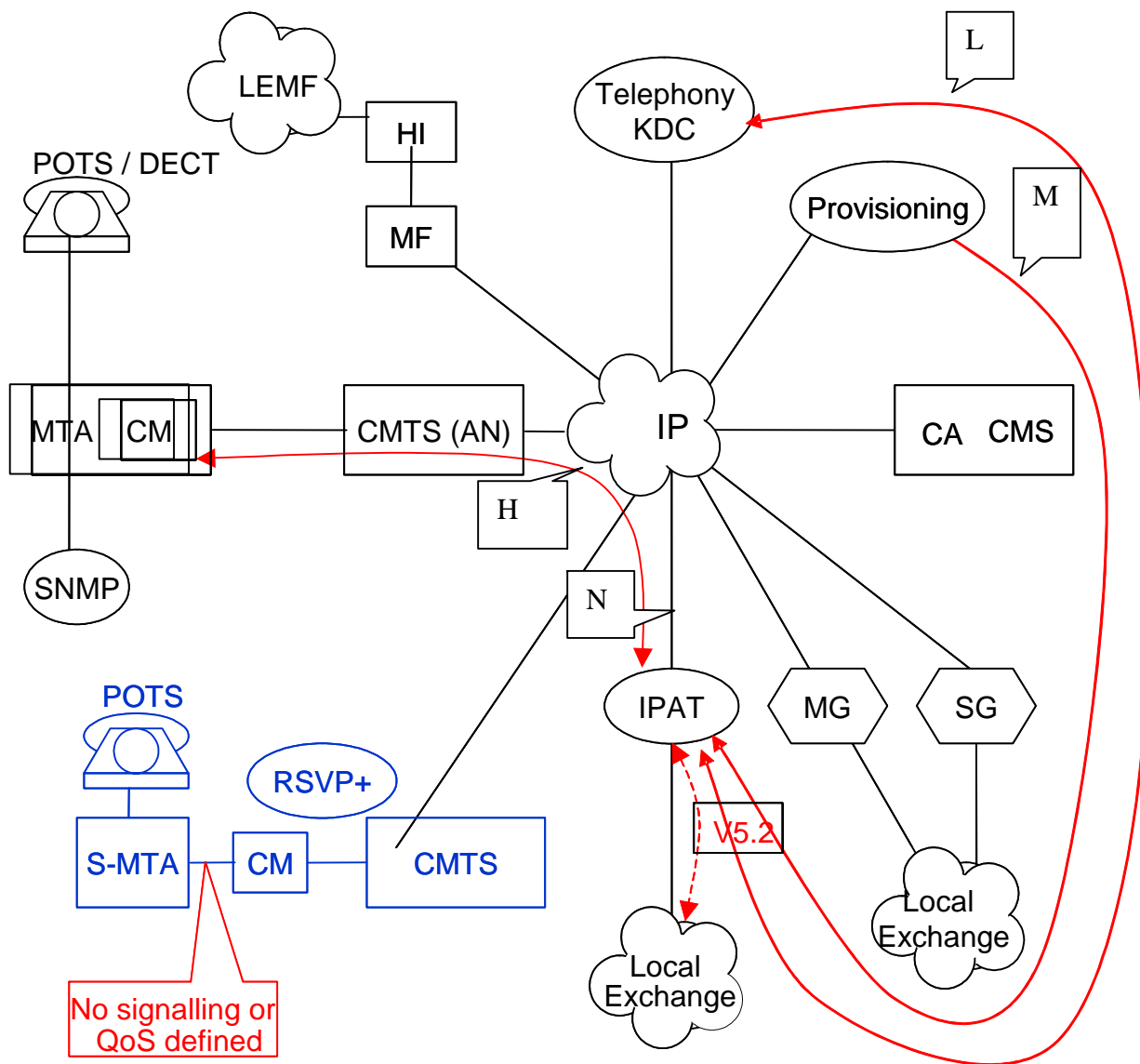
NOTE: This clause to be developed further based on edition 2 of TS 101 909-23 that is currently under development.

6.4.3 Interface interaction

It was considered that the scope for any future testing of the IPCablecom system should not be limited to individual interfaces, but includes the associated interface interactions.

6.4.3.1 Interface-interactions for test consideration

The following interface-interactions need to be considered for testing:



NOTE: This approach is not currently standardized

Figure 15: LCS architecture's impact on NCS

IPAT/CMTS	NCS & LCS	N
IPAT	IPAT MTA (NCS)	H
MTA	Security	L
Provisioning	IPAT - Provisioning Server	M

Figure 16: Key to IPAT - LCS signalling interactions

6.5 CMS Framework

6.5.1 General

The objectives for creating a test specification addressing the CMS are to:

- ensure the NCS protocol has been implemented correctly within a CMS;
- validate the operation/adherence with respect to IPCablecom call flows;
- create finer granularity of testing instead of one monolithic test case;
- assess conformance to the TS 101 909 series;
- ensure interoperability across different manufacturers' platforms;
- verify that the requirements within the TS 101 909 series can be tested and identify errors/changes in the requirements specifications and provide feedback for update of the TS 101 909 series.

6.5.2 Description of the CMS interfaces and functions

The CMS is described within the TS 101 909 series with an architecture that is decomposed giving a description of each of the CMS elements (see figure 6). The interface interactions require further study, however, it should be recognized that manufacturers may "bundle" the separate elements into a single equipment and therefore testing of these "internal" interface-interactions may not be possible.

L40: Telephony KDC:

This is the interface to the Key Distribution Certificate server, which issues KERBEROS tickets to enable the CA to authorize an MTA voice call.

P41: Record-Keeping Server (RKS):

The RKS is a trusted network element component that receives IPCablecom Event Messages from the CMS and other trusted network elements such as the CMTS and MGC. The RKS also, at a minimum, is a short-term repository for IPCablecom Event Messages. The RKS may assemble the Event Messages into coherent sets or Call Detail Records (CDRs), which are then made available to other back office systems such as billing, fraud detection, and other systems

L42 and P43: Mediation Function (MF):

This subject is dealt with in TS 101 909-20.

L44: Multimedia Terminal Adapter (MTA):

The logical interface connection to the MTA is established with the Call Agent function using the NCS protocol. In brief, this connection is then used to send the required event messages and other call signalling information to the MTA to set up a voice call.

P45: Edge Router:

This is the physical connection to the Edge Router; it is over this physical connection that RSVP is passed to the CMTS to ensure sufficient bandwidth is allocated. It should be acknowledged that in some instances the Edge Router may be embedded within the CMTS.

P46: Signalling Gateway (SG):

P46 is the physical connection between the Media Gateway Controller (MGC) function of the CMS and the Signalling Gateway. This connection uses ISTP to pass call-signalling information for OFF-NET calls, this call signalling is then converted to SS7 by the SG for its connection to the PSTN.

L47: Media Gateway (MG):

L47 is the logical connection between the Media Gateway Controller (MGC) function of the CMS and the Media Gateway. The MGC interface is effectively an Application Programming Interface (API) running on the CMS and together with the TGCP protocol (TS 101 909-13 [12] annex A) is used for controlling VoIP PSTN Gateways from external control elements.

P48: Exterior Border Proxies (EBP):

This interface is identified for the completeness of the analysis of the CMS, however, this element is involved in the inter-domain signalling between Call Management Servers and as such is outside the scope of this study.

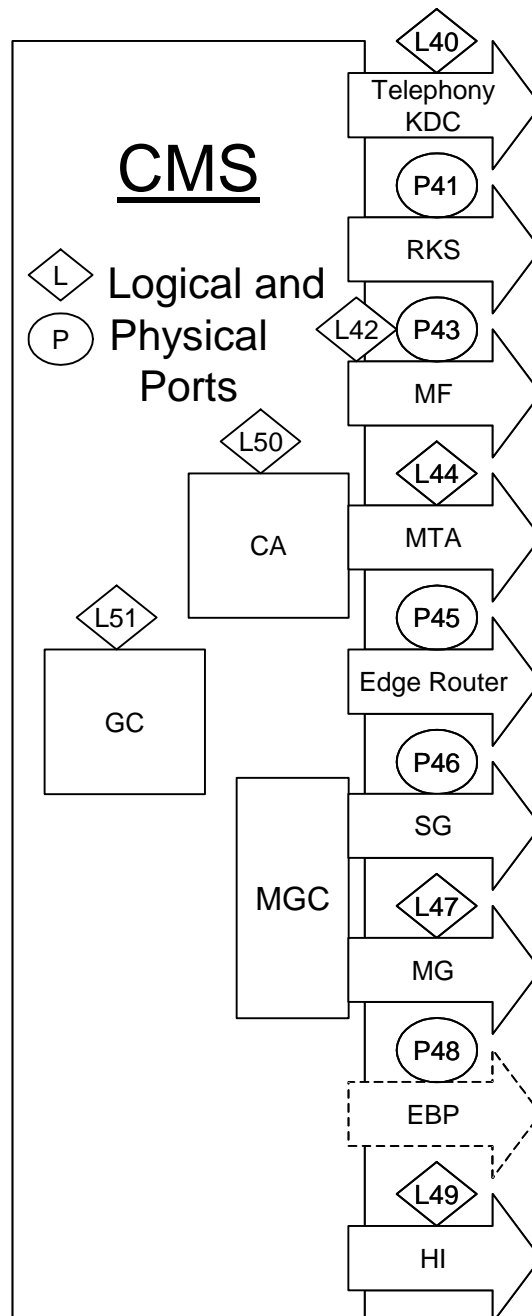


Figure 17: CMS framework

L49: Handover Interface for Lawful Interception (HI)

This subject is dealt with in TS 101 909-20.

NOTE: This clause to be developed further following the evaluation of TS 101 909-20 that is currently under development.

L50: Call Agent (CA):

The Call Agent function is often an embedded part of the physical CMS equipment and therefore the interface between the CMS and CA may not always be accessible for testing purposes. However, the CA performs the essential role in the call set-up and all call control mechanisms with the MTA.

L51: Gate Controller (GC):

The Gate Control function is often an embedded part of the physical CMS equipment and therefore the interface between the CMS and CA may not always be accessible for testing purposes. However, the CMS/GC connects to the CMTS using COPS and is responsible for QoS authorization. The QoS authorization might depend on the type of call, type of user or other parameters defined by policy.

6.5.3 Interface Interactions

The interactions between the various system elements and the CMS cover several aspects, where these are outlined in figure 18 and defined within several ETSI IPCablecom Technical Specifications. The analysis of the NCS protocol interaction with the CMS is critical to meeting the identified objectives.

Due to the complexity of the CMS the interface-interactions were addressed in stages as follows:

- signalling (NCS, TGCP and ISTP): Figure 7 depicts the involvement of the Call Agent, Announcement Controller and Media Gateway Controller. For the MG interface, the Architecture (as noted in the referenced documents) supports either a TGCP interface which is a profile of MGCP, or an interface based on ITU-T Recommendation H.248 [31], and the discussion of the TGCP interface in this clause is taken to refer to either or both interfaces;
- security: Figure 8 depicts the involvement of the Call Agent, Announcement Controller, Media Gateway Controller and Gate Controller;
- Lawful interception: Figure 9 depicts the involvement of the Call Agent and Media Gateway Controller;
- provisioning: Figure 10 depicts the involvement of the Call Agent;
- Dynamic Quality of Service: Figure 11 depicts the involvement of the Gate Controller.

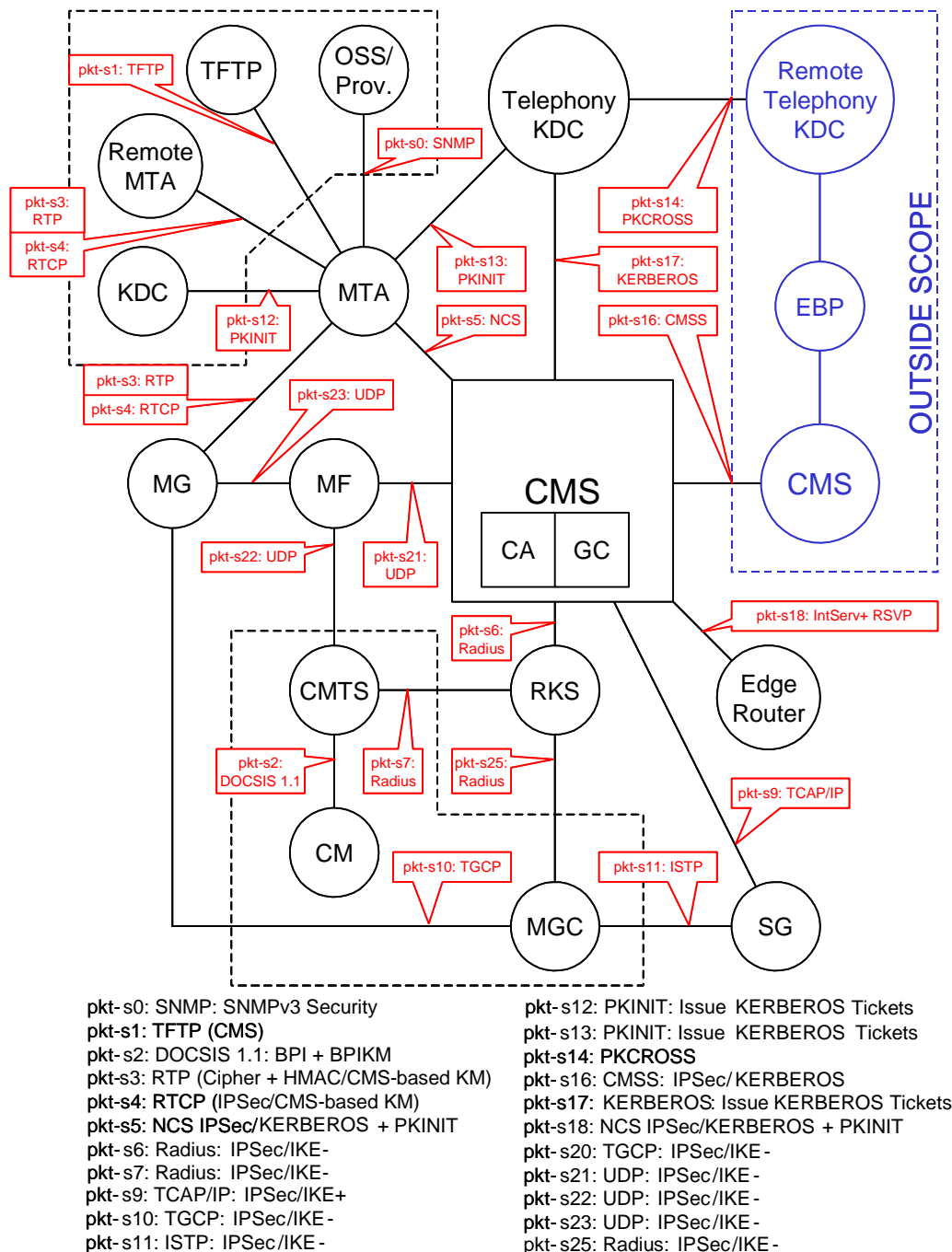


Figure 18: CMS interface-interactions

7 Summary and guidance to development of Test Suite Structure and Test Purposes (TSS&TP)

7.1 Interoperability - vs. - conformance

The IPCablecom system is a large and complex system and therefore the present document highlights what is feasible and that which is not.

It also assists in the determination of those elements of the system that could easily be subjected to a "PlugTest".

The goal of conformance testing is to demonstrate that components developed independently meet a common interface standard; it does not guarantee that components will work together to perform a system function. However, it does provide a level of confidence that devices conform to the base standard will interoperate.

Interoperability is a higher degree of testing, in that it must show that independently developed components can work together to perform a task or set of tasks seamlessly in an aggregate system. In such a case, one component, from one manufacturer, can be replaced with another, and basic operation of the system will be unaffected. In ETSI this approach has been followed to varying degrees under the PlugtestTM service.

7.2 Observations

The IPCablecom Architectural Framework TS 101 909-2 [2] defines a decomposed Architecture. However, the architecture allows for the various functional elements to be "bundled" and consequently the implementation of some interfaces will often be internal to physical equipment. This affects the number and kind of interfaces that can be tested.

IPCablecom call set-up times and scenarios will vary between manufacturers; these will need to be reflected in the PICS advisory clause.

The scope of this analysis has been limited to the single domain zone; multi zone systems are for further study.

7.3 General guidance in the production of PICS/test purposes

Currently the ETSI IPCablecom requirements TS 101 909 series, although published, are widely considered unstable for use in the development of equipment.

Test specifications should not specify additional requirements to those already specified in the IPCablecom Technical Specifications (base specifications). However, during the development of IPCablecom PICS and TSS&TP, test requirements not specifically identified within the source TS 101 909 series may be identified. In this instance the development of testing specifications may assist in the updating of the base series of TS 101 909 as they develop towards stable ES versions to accommodate deficiencies identified during the development of the testing specifications.

These are not restrictive as the TS 101 909 series is evolving.

Testing of individual elements can be subdivided into three aspects:

- valid: normal standard call-flow with all resources available and correct procedures adhered to as per the specified protocol;
- invalid: testing for an error situation e.g. incorrect syntax;
- provocative: testing and results from an out-of-sequence scenario in the specified protocol e.g. incomplete CMS call flows.

Table 1: Test priority levels used within the present document

Priority Level	Description
Critical	Required for deployment of an IPCablecom system with no deviation permitted
High	Very important for successful deployment. An IPCablecom system could be deployed without this functionality, but would result in operational problems and is therefore not recommended
Medium	Implementation is needed and may result in operational problems, but is not critical
Low	Minor, not required for successful deployment but would be "nice to have"

7.4 Focus on interoperability/ETSI Plugtest™ service

An analysis of the various functional components and interfaces lead to the recommendation that an initial set of Plugtest™ plans should be considered to promote the development of interoperable interfaces.

Table 2: Recommendations for future work on Plugtest™ plans

Description	Priority
NCS MTA	Critical
NCS CMS and call flows	Critical
Event Messaging	Critical
Provisioning	Critical
Voice CODEC (see note 1)	Critical
IPAT [V5.2] (see note 2)	Critical
Security	High
Dynamic Quality of Service	High
Trunking Gateway Control Protocol (TGCP)	High
Internet Signalling Transport Protocol (ISTP)	High
<p>NOTE 1: It is only possible to conduct subjective voice quality tests (bit exact coding) based upon a manufacturers implementation of the voice CODEC.</p> <p>NOTE 2: The edition 2 of the IPAT V5.2 requirements specification (TS 101 909-23 [14]) has yet to be completed and therefore detailed analysis performed on the interfaces suitable for testing will need to be based on the edition 1 of the specification that may need to be developed further based on enhancements given by edition 2 of the specification.</p> <p>NOTE 3: It should be noted that implementation of the IPAT within the IPCablecom architecture is an alternative to deploying a CMS (soft switch). In recognition of market demand, the reality is that most CATV networks will implement the IPAT alternative before migrating to full integration of the CMS. Further analysis of the IPAT should therefore be included in subsequent editions of the present document.</p>	

7.5 Focus on conformance testing

Table 3 provides a summary of the various logical and physical interfaces identified. The purpose of table 3 is to assist in focussing the next phase i.e. developing test purposes and plans, production of the PICS, TSS&TP and creation of ATSSs.

The current document identifies priorities in the development of test purposes for the various IPCablecom interfaces and interactions. Subsequent editions of the present document may identify changes to these priorities based on changing market conditions.

Table 3: Summary of logical and physical interface conformance test priorities

Interface		Description	Priority
No.	Name		
L1	Voice Stream	MTA/CM Voice Stream Interface	High
L2	OSS Part	MTA/CM OSS Interface	High
L3	Security PKI	MTA/CM Security Public Key Infrastructure Logical Interface	High
L4	NCS	MTA/CM Network-based Call Signalling Logical Interface	Critical
L5	DQoS	MTA/CM Dynamic Quality of Service Logical Interface	Critical
L6	Provisioning	MTA/CM Provisioning Logical Interface	Critical
L7	Voice Codec	MTA/CM Voice Codec Logical Interface	Medium
P8	Wireless Air i/f	MTA/CM Physical Wireless Air Interface	Low
P9	POTS	MTA/CM Analogue Port Physical Interface	Medium
P10	Data Port	MTA/CM Data Port Physical Interface	Low
P11	RF Interface Euro-DOCSIS	MTA/CM Co-axial RF Physical Interface	Critical see note 1
L20	RKS	CMTS Record Keeping Server Logical Interface	High
L21	Security	CMTS Security Mechanisms Logical Interface	Medium
L22	MF	CMTS Mediation Function Lawful Intercept Logical Interface	High
P23	MF	CMTS Mediation Function Lawful Intercept Physical Interface	High
L24	HI	CMTS Lawful Intercept Logical Handover Interface	High
L25	COPS	CMTS Common Open Policy Service Logical Interface	Medium
L26	DQoS	CMTS Dynamic Quality of Service Logical Interface	Critical
L30	NCS+	IPAT NCS Logical Interface	Critical
L31	Security	IPAT Security logical interface.	Medium
L31	Provisioning	IPAT Provisioning Logical interface	Critical
L32	IEEE 802.3	IPAT Physical provisioning interface	Low
P41	E1	IPAT V.52 Physical Interface to Local Exchange	Low
L42	V5.2	IPAT V5.2 Logical Interface to LE	Low
L32	COPS	IPAT Common Open Policy Service Logical Interface	Medium
L33	DQOS	IPAT DQOS Logical Interface	Critical
L40	Telephony KDC	CMS Logical Interface to the Telephony KDC	High
L41	MTA	CMS Logical Interface to the MTA	High
L42	MF	CMS Mediation Function Lawful Intercept Logical Interface	High
P43	MF	CMS Mediation Function Lawful Intercept Physical Interface	High
P44	RKS	CMS Record Keeping Server Physical Interface	High
P45	SG	CMS Signalling Gateway Physical Interface	Low
P46	Edge Router	CMS Physical Interface to the Edge Router	High
L47	MG	CMS Media Gateway Logical Interface	High
P48	EBP	CMS Physical Interface to the Exterior Border Proxy	Low
L49	HI	CMS Lawful Intercept Logical Handover Interface	High
L50	CA	CMS Call Agent Logical Interface	Medium
L51	GC	CMS Gate Control Logical Interface	High
NOTE: Although the implementation of Euro-DOCSIS 1.1 is critical to the successful deployment of an IP-Cablecom system, this testing is currently conducted under the auspices of the Euro-DOCSIS Certification Board.			

7.6 Availability of commercial test systems

Proprietary test systems have and are currently being developed by Cable Labs and tComLabs to support both DOCSIS/Euro-DOCSIS and PacketCable interoperability testing. Equipment manufacturers have also developed in-house integration test solutions that in some instances are understood to go beyond the test cases specified by the PacketCable project.

To date there are no commercially available "off-the-shelf" test systems available for the IP-Cablecom Specifications. Some elements of a test scenario are commercially available, such as IP Protocol analysers and RF signal generators, almost all utilize TCL as the programmable interface.

8 Considerations to the development of testing specifications

An analysis of the IPCablecom system and its individual elements, based upon review of the individual ETSI Technical Specifications listed in clause 2 was commissioned by TC AT as undertaken by the working group digital assisted by STF 212.

The annexes to the present document give further guidance to the working group on the various test specifications that need to be developed and provide a template that may be used as the framework. Recognizing the current allocation of resource to STF 212 and the objective of only developing test purposes, the following points need to be taken into consideration:

- resources currently allocated to STF 212 will fall short of those actually required by the market:
 - it is estimated that these may only be just enough to address the MTA;
 - further resource will be needed to consider the CMTS (AN), CMS and IPAT;
 - further resource will be needed to address the various interactions covering Security, DQoS, Provisioning, Gate Control etc.
- currently no decision has been reached upon the scripting language that is best suited to IPCablecom, hence the focus of the next phase should only be to address development of the test purposes, plans and PICS, not produce any scripted tests that should be included in subsequent phases;
- the latter can only be considered once the test purposes have been fully defined. However, the cable industry should identify the scripting language to be adopted that would meet the needs of the cable industry and facilitate the introduction of test tools in the shortest time;
- the interactions between each of the elements of the IPCablecom system are extremely complex and is new territory in ETSI - consequently, it is clearly recognized that expertise of the IPCablecom system, architecture and functions together with the interaction between each component is an essential criteria for any individual endeavouring to develop such test purposes. In addition to this knowledge of product engineering integration and deployment are to be considered as essential attributes.

Due to the complexity of the IPCablecom System and the inter-relationship between the IPCablecom series of TS 101 909, i.e. IPCablecom is a series of interwoven specifications where a change to one has a ripple effect to the others and no one specification covers the full requirements for specific component. The initial study in the development of PICS, TSS&TP should be undertaken by a team of IPCablecom specialists that have general testing experience. This team would need to be able to focus on the further system analysis and generation of the PICS and test purposes. The development of the ATS should follow the completion of the PICS and TSS&TP undertaken by specialists in the scripting language to be used for scripting the IPCablecom tests cases.

Test specifications covering ES 201 488 [18] should be developed by ETSI to verify the conformity of devices to the base standard, this work should consider the MAC layer only therefore covering the layer 2 aspects of the MAC that have a direct implication to the IPCablecom layer.

Annex A: Test framework for MTA/CM

Further study will be required to assess the test feasibility of the following MTA/CM-NCS interactions:

- identify the detailed requirements put on the requirements for every single protocol, interface and interface-interaction identified in the above two clauses. A PICS needs to be produced that identifies the requirements. Every item should be referenced to a specific item in the specification. More specifically a PICS-list needs to be developed for the requirements on the MTA regarding:
 - provisioning system, including the required behaviour for error and lack-of-resources scenarios;
 - NCS, including all possible protocol interaction, legal and illegal, of the NCS-protocol, including the testing of the influence of packet-loss as NCS uses UDP as the transport protocol. It must also be identified what possible combinations of messages and messages-format need to be tested for;
 - DQoS, verifying the MTA signals the modem the correct set of QoS-parameters, and frees up the bandwidth after the call has ended. This also includes the requirements put on the MTA to classify the packets on the right service-flow. This signalling to the CMTS can be done either by using the DSx-mechanism on the CM (internal signalling from MTA to CM) or using RSVP-signalling;
 - identifying the requirements put on the OSS-system, covering the implementation of each MIB in relation to conformance to the MIB-definition and in conformance with the other protocols;
 - identifying all the signalling related to messaging for the security interfaces. This should also cover the requirements put on resistance to hacking or denial-of-service attacks;
 - requirements on POTS/DECT interfaces are outside the scope of this work;
 - requirements on the data-port is outside the scope of this work, the only tested functionality should be that there is no harmful interference from the data-port to the IPCablecom compliance behaviour;
 - the requirements put on the Euro-DOCSIS compliance are outside the scope of this work, please refer to DQoS for input on the functionality that does need to be tested for.
- identifying test-groups that group the testing specific functionality. Most test-groups will isolate a particular protocol or interface, but some test-cases will need to be written that are crossing multiple protocols and interfaces. Especially all items related to security will interfere with the other protocols, these interactions will need to be tested for. Another item of interaction is the POTS interface to the NCS-protocol. It needs to be identified that the right NCS-messages are generated when the corresponding signals on the POTS-port are generated;
- write test plans that cover the set of identified PICS, a test plan should be unambiguous, take into account different options (if needed a specific test-plan is written for each option) and define exactly the tested PICS.

Annex B:

Test framework for CMTS (AN)

The CMTS/AN provides data connectivity and complimentary functionality to CMs over the HFC access network. It also provides connectivity to wide area networks. The AN is located at the cable television system head-end or distribution hub.

Further study will be required to assess the test feasibility of the following CMTS signalling interactions:

- providing the required QoS to the CM based upon policy configuration;
- allocating upstream bandwidth in accordance to CM requests and network QoS policies;
- classifying each arriving packet from the network side interface and assigning it to a QoS level based on defined filter specifications;
- policing the TOS field in received packets from the cable network to enforce TOS field settings per network operator policy;
- altering the TOS field in the downstream IP headers based on the network operator's policy;
- performing traffic shaping and policing as required by the flow specification;
- forwarding downstream packets to the DOCSIS network using the assigned QoS;
- forwarding upstream packets to the backbone network devices using the assigned QoS;
- converting and classifying QoS Gate parameters into ITU-T Recommendation J.112 [26] QoS parameters;
- signalling and reserving any backbone QoS necessary to complete the service reservation;
- recording usage of resources per call using IPCablecom Event Messages.

Annex C: Test framework for IPAT MTA

Further study will be required to assess the test feasibility of the IPAT signalling interactions based on the development of TS 101 909-23 to include requirements for handling abnormal call conditions and update to signalling codes to increase performance.

The V5.2 conforms to existing specifications that support analogue capabilities. Support of ISDN capabilities is for further study. Also only a subset of analogue services are mapped between V5.2 and NCS, hence as the specification develops to add further analogue service capabilities and support for ISDN capabilities, the IPAT clause in the present document and corresponding test cases would also need to be developed further accordingly.

Annex B of the NCS specification contains a mapping between V5.2 messages and NCS messages, and can be tested in a manner similar to the NCS specification (see annex A). Ideally, it should be transparent to an end user whether a NCS or LCS architecture is deployed, that is whether a MTA is communicating with a CMS or a IPAT

This area must be revisited when the LCS specification is enhanced further to support a wider set of analogue capabilities as well as ISDN capabilities.

Annex D: Test framework for CMS

Further study will be required to assess the test feasibility of the following CMS-NCS interactions:

- model and naming conventions:
 - CMS response to all MTA related endpoint naming conventions (Test Purposes to be developed);
 - correct validation of the Connection_Id parameter (Test Purposes to be developed);
 - unique Call Identifier (CallId) verification, with respect to Call Agents controlling the same gateways (Test Purposes to be developed);
 - correct handling of an incompatible protocol version (Test Purposes to be developed);
 - correct handling of an unrecognized extension connection parameter name (Test Purposes to be developed);
 - ensuring case insensitivity to command header(s) (Test Purposes to be developed).
- connection control (create, modify and delete);

EXAMPLE 1: NCS parameters - CreateConnection

- in order to validate the correct use of NCS parameters in the CreateConnection command test purposes will need to be developed in the following areas:
 - EndpointId parameter (Test Purposes to be developed);
 - packetization period (Test Purposes to be developed);
 - compression algorithm (Test Purposes to be developed);
 - embedded NotifyRequest (Notify Request) (Test Purposes to be developed).
- in order to validate the correct use of NCS parameters in the ModifyConnection command test purposes will need to be developed in the following areas:
 - EndpointId parameter (Test Purposes to be developed);
 - embedded NotifyRequest (Notify Request) (Test Purposes to be developed).
- in order to validate the correct use of NCS parameters in the DeleteConnection command test purposes will need to be developed in the following areas:
 - EndpointId parameter (Test Purposes to be developed).
 - embedded NotifyRequest (Notify Request) (Test Purposes to be developed).
- verify the implementation of NCS parameters including:
 - response ACK (acknowledgement) (Test Purposes to be developed);
 - retransmission timeouts (Test Purposes to be developed);
 - encoding of session descriptions (SDP profile) (Test Purposes to be developed).
- auditing;

EXAMPLE 2: NCS parameters - AuditEndpoint

- validate the correct use of NCS parameters in the AuditEndpoint command:
 - EndpointId parameter (Test Purposes to be developed);
 - SpecificEndPointID parameter (Test Purposes to be developed);
 - MaxEndPointID parameter (Test Purposes to be developed);

EXAMPLE 3: NCS parameters - AuditConnection.

- validate the correct use of NCS parameters in the AuditConnection command:
 - EndPointId parameter (Test Purposes to be developed).
- initialization;
- RSIP response and subsequent interaction with remote MTA (Test Purposes to be developed):
 - fail over;
 - dynamic provisioning and fault correction;
 - error detection and recovery;
 - incomplete calls as part of call flows.

Annex E: Bibliography

- ETSI ES 201 970-1: "Access and Terminals (AT); Public Switched Telephone Network (PSTN); Network Termination Point (NTP) analogue interface: Harmonized specification of physical and electrical characteristics at a 2-wire analogue presented NTP. part 01: Common Requirements".
- Draft ETSI ES 201 970-2: "Access and Terminals (AT); Public Switched Telephone Network (PSTN); Network Termination Point (NTP) analogue interface: Harmonized specification of physical and electrical characteristics at a 2-wire analogue presented NTP. Part 02: Requirements specific to a very short line installation".
- ETSI TS 101 909-12: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 12: Internet Signalling Transport Protocol".
- Draft ETSI TS 101 909-14: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 14: Operation System Support".
- Draft ETSI TS 101 909-15: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 15: Capability sets for delivery of service".
- Draft ETSI TS 101 909-16: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 16: Signalling for Call Management Server".
- ETSI TS 101 909-17: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 17: Inter-domain Quality of Service".
- ETSI TS 101 909-18: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 18: Embedded media terminal adapter (MTA) Primary Line Support".
- ETSI TS 101 909-19: "Access and Terminals (AT); Digital Broadband Cable access to the public telecommunications network; IP Multimedia Time Critical Services; Part 19: IP Cablecom Audio Server Protocol Specification Sub-part 2: J.162 option".
- Draft ETSI TS 101 909-20: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception".
- Draft ETSI TS 101 909-21: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 22: Management Event Messages".
- Draft ETSI TS 101 909-23: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 23: Gateway Access Interface V5.2".
- Draft ETSI TS 101 909-24: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 24: MTA Basic Access ISDN Interface".
- Draft ETSI TS 101 909-25: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 25: Test Suite Structure and Test Purposes".
- Draft ETSI TS 101 909-26: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 26: PICS Proforma for Conformance Test Suites".

- Draft ETSI TS 101 909-27: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 27: Abstract Test Suite (ATS) and PIXIT for conformance assessment of IP Cable Communication products".
- ETSI TBR 021: "Terminal Equipment (TE); Attachment requirements for pan-European approval for connection to the analogue Public Switched Telephone Networks (PSTNs) of TE (excluding TE supporting the voice telephony service) in which network addressing, if provided, is by means of Dual Tone Multi Frequency (DTMF) signalling".
- ETSI TBR 010: "Digital Enhanced Cordless Telecommunications (DECT); General Terminal Attachment Requirements; Telephony Applications".
- ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General".
- ETSI TS 101 909-2 V1.1.1: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".
- ETSI TS 101 909-3: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 3: Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems".
- ETSI TS 101 909-6: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 6: Media Terminal Adapter (MTA) device provisioning".
- ETSI TS 101 909-7: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 7: Management Information Base (MIB) Framework".
- ETSI TS 101 909-8: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 8: Media Terminal Adapter (MTA) Management Information Base (MIB)".
- ETSI TS 101 909-9: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 9: Network Call Signalling (NCS) MIB Requirements".
- ETSI TS 101 909-10: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 10: Event Message Requirements for the Provision of Real Time Services over Cable Television Networks using Cable Modems".
- ETSI TS 101 909-20: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 01: E.164 Voice Service".
- DTS/AT-020042-01: "Access and Terminals (AT); Digital Broadband Cable access to the public telecommunications network; Euro-DOCSIS; Part 1: Test Suite Structure and Test Purposes (TSS&TP)".
- DTS/AT-020042-02: "Access and Terminals (AT); Digital Broadband Cable access to the public telecommunications network; Euro-DOCSIS; Part 2: Protocol Implementation Conformance Statement (PICS) proforma specification".
- DTS/AT-020042-03: "Access and Terminals (AT); Digital Broadband Cable access to the public telecommunications network; Euro-DOCSIS; Part 3: Abstract Test Suite".

History

Document history		
V1.1.1	May 2003	Publication