ETSI TS 101 909-23 V1.1.1 (2002-12)

Technical Specification

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)

Reference

DTS/AT-020020-23

Keywords

broadband, IPCable, multimedia, gateway,
V5interface

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

Contents

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 Specification (TS) has been produced by ETSI Technical Committee Access and Terminals (AT).

The present document is part 23 of a multi-part deliverable covering Digital Broadband Cable Access to the Public Telecomunications Network; IP Multimedia Time Critical Services. Full details of the entire series can be found in part 1 [1].

The present document describes the Internet Protocols Access Terminal (IPAT) architecture and protocols for an Internet Protocol (IP)-based Cable Telephony access service, referred to as the Line Control Signalling (LCS) architecture.

NOTE 1: The choice of a multi-part format for the present document is to facilitate maintenance and future enhancements.

NOTE 2: The term **MUST** or **MUST NOT** is used as a convention in the present document to denote an absolutely mandatory aspect of the specification.

Introduction

The cable industry in Europe and across other Global regions has already deployed broadband cable television Hybrid Fibre/Coaxial (HFC) data networks running a standard Cable Modem Protocol. The Cable Industry is in the rapid stages of deploying IP Voice and other time critical multimedia services over these broadband cable television networks.

The Cable Industry has recognized the urgent need to develop ETSI Technical Specifications aimed at developing interoperable interface specifications and mechanisms for the delivery of end to end advanced real time IP multimedia time critical services over bi-directional broadband cable networks.

IPCablecom is a set of protocols and associated element functional requirements developed to deliver Quality of Service (QoS) enhanced secure IP multimedia time critical communications services using packetized data transmission technology to a consumer's home over the broadband cable television Hybrid Fibre/Coaxial (HFC) data network running the Cable Modem protocol. IPCablecom utilizes a network superstructure that overlays the two-way data-ready cable television network. While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice, the long-term project vision encompasses packet video and a large family of other packet-based services.

The Cable Industry is a global market and therefore the ETSI standards are developed to align with standards either already developed or under development in other regions. The ETSI Specifications are consistent with the CableLabs/PacketCable set of specifications as published by the SCTE. An agreement has been established between ETSI and SCTE in the US to ensure, where appropriate, that the release of PacketCable and IPCablecom set of specifications are aligned and to avoid unnecessary duplication. The set of IPCablecom ETSI specifications also refers to ITU-SG9 draft and published recommendations relating to IP Cable Communication.

The whole set of multi-part ETSI deliverables to which the present document belongs specify a Cable Communication Service for the delivery of IP Multimedia Time Critical Services over a HFC Broadband Cable Network to the consumers home cable telecom terminal. "IPCablecom" also refers to the ETSI TC AT working group program that shall define and develop these ETSI deliverables.

Certain matters that are included in the present document as informative may be specifically required under regional EU Directives, as transposed into national laws in some member states. Outside the EU region national law may also specify as normative that certain additional capabilities must be supported.

1 Scope

The present set of documents specifies IPCablecom, a set of protocols and associated element functional requirements. These have been developed to deliver Quality of Service (QoS), enhanced secure IP multimedia time critical communication services, using packetized data transmission technology to a consumer's home over a cable television Hybrid Fibre/Coaxial (HFC) data network.

To facilitate maintenance and future enhancements to support other real-time multimedia services the TS 101 909 document series consist of multi-parts as detailed in TS 101 909-1 [1].

The present document is part 23: Internet Protocol Access Terminal-Line Control Signalling (IPAT-LCS) providing a technical description of this architecture, and where appropriate, identify the portions of the IPCablecom specifications that apply to this architecture and their use. The present document contains a description of modifications to the NCS architecture to support a V5.2 signalling interface to a local exchange, rather than the full NCS architecture. This is a "delta" document, describing areas where the LCS architecture differs from the NCS.

In the present document, protocol extension to NCS are not included as they are in annexes A and B of TS 101 909-4 [4].

NOTE 1: To avoid confusion between the V5.2 reference Access Network (AN) and the IPCablecom Access Node (AN), the present document uses the DOCSIS nomenclature for the Cable Modem Termination System (CMTS) to designate the interface between the HFC cable plant and the IP Network.

NOTE 2: To be clear throughout the present document, the term *"CM/MTA"* will be used to denote an E-MTA.

While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services. This may require in the future, not only careful maintenance control, but also an extension of the present set of documents.

The present document assumes familiarity with the IPCablecom architecture, specifically with DQoS, Security and call signalling.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General".

[2] ETSI TS 101 909-2: "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".

[3] 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".

[4] ETSI TS 101 909-4: "Access and Terminals (AT); 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] 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".

[7] ETSI TS 101 909-11: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[8] ETSI TS 101 909-18: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 18: Embedded Media Terminal Adapter (e-MTA) offering an interface to analogue terminals and Cable Modem".

[9] 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".

[10] ETSI ES 201 235: " Access and Terminals (AT); Specification of Dual-Tone Multi-Frequency (DTMF) Transmitters and Receivers".

[11] ETSI ES 201 488: "Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification".

[12] 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".

[13] ETSI EN 300 347 (all parts): "V interfaces at the digital Local Exchange (LE); V5.2 interface for the support of Access Network (AN)".

[14] ETSI EN 300 659: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services".

[15] IETF RFC 1889: "RTP: A Transport Protocol for Real-Time Applications".

[16] IETF RFC 1890: "RTP Profile for Audio and Video Conferences with Minimal Control".

[17] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[18] IETF RFC 2833: "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[19] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[20] IEEE 802.3: "Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications".

[21] ETSI EN 300 324: "V interfaces at the digital Local Exchange (LE); V5.1 interface for the support of Access Network (AN)".

[22] ETSI ETS 300 102-1: "Integrated Services Digital Network (ISDN); User-network interface layer 3; Specifications for basic call control".

[23] ETSI ETS 300 327: "Satellite Earth Stations and Systems (SES); Satellite News Gathering (SNG) Transportable Earth Stations (TES) (13-14/11-12 GHz)".

[24] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

3 Definitions and abbreviations

3.1 Definitions

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

cable modem: layer two termination device that terminates the customer end of the ITU-T Recommendation J.112 connection

Cable Modem Termination System (CMTS): located at the cable television system headend or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network

NOTE: With reference to ES 201 488 [11] this is the AN device in the IPCablecom Architecture when using the DOCSIS RF Interface Protocol.

CNAME: a unique identifier of the sender of RTP packets

Data Over Cable System Interface Specification (DOCSIS): 6 MHz channel width with 5 MHz to 42 MHz upstream frequency plan. DOCSIS is a trade mark of CableLabs

endpoint: terminal, gateway or MCU

EuroDOCSIS: european DOCSIS provides a 8 MHz channel width with 5 MHz to 65 MHz upstream frequency plan

Flow [IP Flow]: unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information

NOTE: This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.

Flow [J.112 Flow]: unidirectional sequence of packets associated with a SID and a QoS

NOTE: Multiple multimedia streams may be carried in a single J.112 Flow

Gateway: devices bridging between the IPCablecom IP Voice Communication world and the PSTN

NOTE: Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signalling Gateway which sends and receives circuit switched network signalling tot he edge of the IPCablecom network.

IPCablecom: architecture and a series of specifications that enable the delivery of real time services (such as telephony) over the cable television networks using cable modems

latency: time, expressed in quantity of symbols, taken for a signal element to pass through a device

proxy: facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves

trunk: analogue or digital connection from a circuit switch which carries user media content and may carry voice signalling (MF, R2, etc.)

3.2 Abbreviations

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

AF	Assured Forwarding
AN	Access Node
ATM	Asynchronous Transfer Mode
CDR	Call Detail Record
CID	Caller ID
CM	Cable Modem
CMS	Call Management Server
CMTS	Cable Modem Termination System

CRCX	CReeate ConneXion
COPS	Common Open Policy Service Protocol
DCS	Distributed Call Signalling
DCR	Detailed Call Record
DF	Delivery Fonction
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOCSIS	Data Over Cable System Interface Specification
DQoS	Dynamic Quality of Service
DTMF	Dual Tone Multi-Frequency
DSCP	Diffserv Code Point
EF	Expedited Forwarding
E-MTA	Embedded Multimedia Terminal Adapter
ER	Edge Router
FE	Function Element
FSK	Frequency Shift Keying
FSM	Finite State Machine
GC	Gate controler
HFC	Hybrid Fibre/Coaxial
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
IPAT	Internet Protocol Access Terminal
LCS	Line Control Signalling
LE	Local Exchange
LI	Lawful Interception
MDCX	MoDify Connexion
MG	Media Gateway
MGC	Media Gateway Controller
MP	Media Player
MPC	Media Player Controller
MPLS	Multiprotocol Label Switching
MTA	Multimedia Terminal Adapter
NCS	Network Call Signalling
OSS	Operational Support System
PHB	Per Hop Behaviour
PHS	Payload Header Suppression
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RKS	Record Keeping Service
RSVP	Resource reSerVation Protocol
RTCP	RealTime Control Protocol
SCP	Signal Code Power
SG	Signalling Gateway
SLA	Service Level Agreement
SSP	Signalling Switch Point
STP	Signalling Transfer Point
TFTP	Trivial File Transfer Protocol
TKS	Tucana Knowledge Store
UDP	User Datagram Protocol
VoIP	Voice over IP

4 System architecture

The present document describes the architecture and protocols for an Internet Protocol (IP)-based Cable Telephony access service, referred to as the Line Control Signalling (LCS) architecture. The intent of the present document is to provide a technical description of this architecture, and where appropriate, identify the portions of the IPCablecom specifications that apply to this architecture and their use.

The objective of the LCS architecture is to allow a Public Switched Telephone Network (PSTN) Local Exchange (LE) to perform as much call processing as possible, while providing IP-based transport in the local access cable network. This is accomplished through a V5.2 interface between IPCablecom Access Network (AN) and the PSTN LE. Unlike the full IPCablecom architecture the LCS architecture uses a Local Exchange (LE) for call control, services, announcements and charging.

The LCS architecture is an interim step toward the IPCablecom end-to-end IP architecture. Operators have the opportunity to use the LCS architecture to make IP access available for telephony prior to the full availability of CMS/MGC/MG/SG/TKS/AS based architectures. While the IPCablecom architecture has the potential to support multiple applications with telephony being the initial application, LCS is only intended to support the telephony application. The LCS architecture must be such that early deployments of terminal equipment are able to migrate to the full IPCablecom architecture.

4.1 Line control signalling system architecture

The LCS System Architecture comprises a DOCSIS 1.1 Hybrid Fibre/Coaxial (HFC) access network interworking with PSTN local exchanges (LE) through an Internet Protocol Access Terminal (IPAT).

This system is illustrated by physical, data link, and transport layers between components in figure 3. The HFC access network includes all of the system components required to support IPCablecom Voice-over-IP (VoIP) telephony; in the LCS application, and for future full VoIP system operations. The IP Access Terminal (IPAT) together with the LE provide all the functions of a Media Gateway Controller (MGC), Signalling Gateway (SG), Media Gateway (MG), and a partial replacement of the Call Management Server (CMS) and Record Keeping Service (RKS).

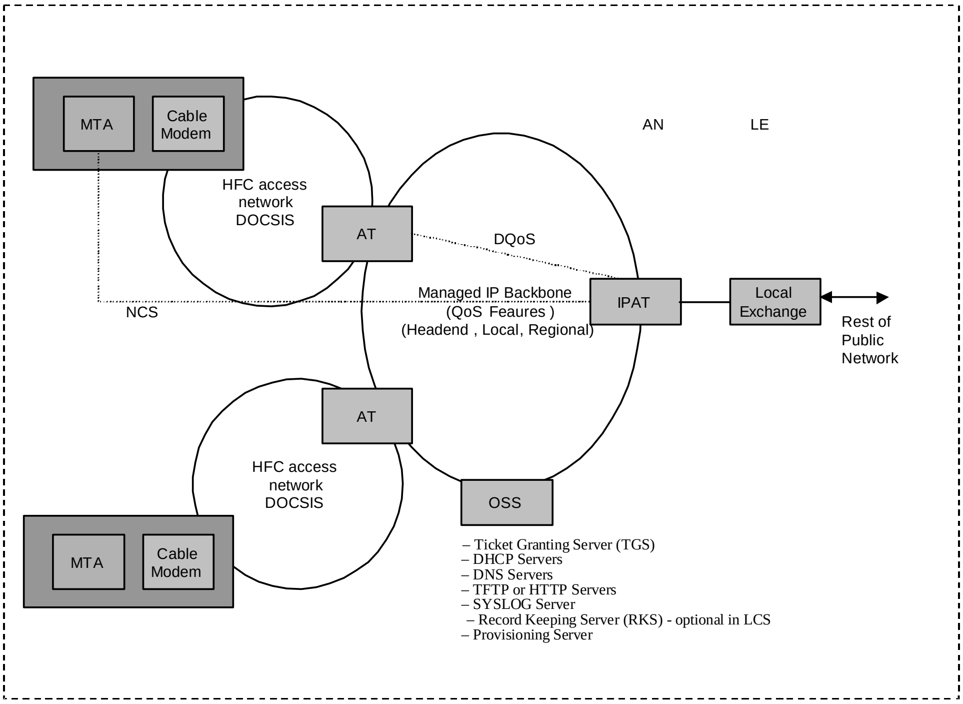


Figure 1: LCS architecture

4.2 IPAT/LE interworking: the V5.2 interface

The V5.2 interfaces are defined by two documents: EN 300 324-1 [12] and ETS 300 347 [13].

The V5.2 interface may have between one and sixteen 2 048 kbit/s links, as required. Two interface presentation alternatives are defined: the balanced interface pair type and the coaxial type. According to the two alternatives of interface applications shown in figure 1, it is left to the network operator to request the interface presentation required.

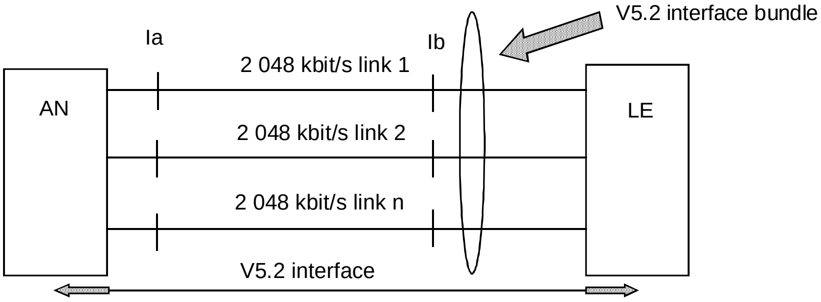


Figure 2a: Association of 2 048 kbit/s links with a V5.2 interface

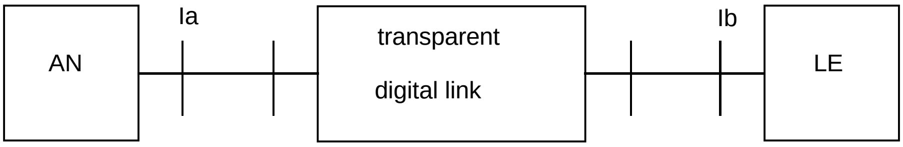


Figure 2b: transparent digital link

NOTE 1: Interfaces at the digital Local Exchange (LE);V5.2 interface for the support of Access Network (AN)
NOTE 2: n 2 048 kbit/s links are shown (n = 1..16).
NOTE 3: Any/all 2 048 kbit/s links may use a transparent digital link.
NOTE 4: Ia = interface point at the AN side; Ib = interface point at the LE side.

Figure 2: V5.2 application with and without transparent digital link

For more information, see EN 300 347 [13].

4.3 Migration to full VoIP

The LCS architecture is designed to be an *interim* and *transitional* architecture. This architecture has been developed to enable early deployment of IP telephony capability in the HFC access network. This allows cable system operators a path of entry into the evolving IP telephony marketplace, and an opportunity to gain market share and start generating revenue, offering telephone service to their subscribers without having to wait for availability of complete IPCablecom systems.

The architecture has been developed to take advantage of IPCablecom member investment in equipment. The system components migrate naturally from the switched IP architecture to IPCablecom's full VoIP architecture by transforming the IPAT into a Media Gateway.

5 System components

This clause will describe at a high level the capabilities of logical components of the Line Control Signalling Architecture required to support the V5.2 interface to a Local Exchange. Each component may physically be a single piece of equipment existing as a node on a network, a set of distributed network nodes, or it may be co-located or bundled with another components. IPCablecom architecture as described in TS 101 909-2 [2] is assumed as baseline architecture.

The major change to the components from the framework architecture is the addition of one new IPCablecom component: the IP Access Terminal (IPAT). Other components are either not required by the Line Control Signalling architecture, or have reduced capabilities since some functionality is no longer needed. Some additional provisioning is required to support V5.2 in the new IPAT component.

In addition, the change from a PSTN interface and its intelligent network equipment (SSP, STP, SCP, etc.) to a Local Exchange (LE) has a major impact on IPCablecom goals and objectives. The IPCablecom NCS architecture assumed unfettered access to the PSTN network, while LCS restricts the cable system to working as a remote device to a local switch for telephony features. For this reason, the LE is briefly described.

5.1 Local Exchange

The Local Exchange (LE) is an component external to the LCS architecture that provides line side call features and interfaces to the PSTN. It is a digital switch equipped with an interface supporting subscriber lines remoted over digital trunks. These digital trunks, or "digital loop carriers", normally terminate in a Access Network that concentrates the analogue line traffic, converts analogue line signalling into digital signals, and performs remote line maintenance. This integrated digital line system has been long deployed to reduce operating, installation, and capital equipment costs while delivering an equivalent range of telecommunications services to a direct analogue line interface; it is capable of supporting ISDN CPE terminals as well. A large percentage of subscriber lines in Europe today are connected to the Local Exchange over these remote concentrated digital interfaces instead of direct analogue lines.

The basic idea of LCS is to reuse the existing subscriber line related features capabilities of the LE by mimicking the AN-LE digital loop interface. To simulate this interface to the LE, the LCS architecture will use some existing components of the IPCablecom NCS architecture (E-MTA, CMTS, OSS), and an additional gateway component called the IP Access Terminal (IPAT). There are a number of consequences of this approach:

1) The Local Exchange combined with the IPCablecom IPAT will replace a number of NCS components that provide line side (local) call services. This includes a number of IPCablecom NCS components as defined in the architecture framework: CMS, MGC, SG, MG, RKS, and AS.

2) Some line and billing related OSS functions are not needed in the LCS architecture. These will be handled by the LE's operator support system instead of the IPCablecom OSS and RKS. However, the full OSS system is needed, including the various servers, including the TKS, DNS, DHCP, TFTP, HTTP, SYSLOG, and provisioning servers.

3) The subscriber line features are determined by the LE feature set, and not necessarily by IPCablecom requirements. At this time, most LE's support all the IPCablecom call features needed in the initial release, and even many not specified in IPCablecom ; however LE's do not typically support internet, web, or IP-based multi-media features, which must be considered beyond the scope of LCS. Since the LCS architecture is considered to be a transient step in an evolution to NCS, it may be important for the cable operating company to restrict the subscriber line call features allowed in the LE to those defined by IPCablecom to avoid backward compatibility issues in the future, since many existing LE features may prove difficult or impracticable to implement in the IPCablecom Architecture.

4) The LE OSS has certain provisioning expectations and will manage some line and subscriber features although not the full scope of line related calling features. The LCS OSS also has its requirements on provisioning, many of which are subscriber related and call feature related. These two provisioning systems will have to by synchronized, if not integrated. There will also be some additional requirements on LCS provisioning to handle the requirements of the IPAT gateway and digital loop trunk provisioning.

5) There is a testing "mismatch" between the maintenance expectations of the LE and IPCablecom in the area of line testing. V5.2 was designed to remotely control and test analog lines using digital loop carriers. The cable architecture controls and tests lines over CMTS/MTA using HFC networks. The LCS will not manage the testing of IPCablecom components and lines; instead IPCablecom testing procedures are used.

5.2 IP Access Terminal

The IP Access Terminal (IPAT) provides the interworking between the LE and the IPCablecom network. It interfaces to the LE over digital trunks which carry signalling and voice traffic. It interfaces to other components (CMTS, OSS, and, indirectly, the MTA) of the IPCablecom architecture over an IP network, which carries signalling and voice traffic. From the LE side, it simulates a remote digital loop carrier CMTS interface. From the IPCablecom IP network side, it replaces the subscriber line call related functions and voice to packet translation functions. Thus it will:

1) Convert outgoing IPCablecom voice packets into digital circuit voice traffic and pass it to the LE over digital trunks. Thus, the IPAT replaces some functions of the MG.

2) Convert incoming voice circuit traffic on digital trunks from LE into IPCablecom packet traffic.

3) Convert NCS protocol call control signalling into digital line interface signalling (V5.2) required by the LE.

4) Convert digital line interface signalling from the LE (V5.2) into IPCablecom NCS protocol call control signalling.

5) Manage its end of the digital trunks, including alarms, initialization, and maintenance.

6) Manage its own provisioning information as needed to support the interworking (mapping between LCS and LE numbering, trunk identities, etc.).

7) Manage the gates in the CMTS, i.e. implement the CMS Gate Controller functions to provide DQoS functions.

The IPAT itself does not perform call processing, call feature related line provisioning, or billing functions- these are handled by the LE.

5.3 Cable Modem Termination System

The Cable Modem Termination System (CMTS) is the component that terminates one or more DOCSIS 1.1 based Hybrid Fibre/Coax (HFC) access links and provides connectivity to one or more wide area networks (typically IP). It is located at the cable television system head-end or distribution hub.

On the HFC network side, it supports several layers of interface protocols to manage the population of MTAs as defined by DOCSIS. On IPCablecom managed IP network side, it supports the transport of RTP voice packets with appropriate priority and quality-of-service constraints.

For LCS, its functions are identical to the IPCablecom functions.

5.4 Embedded MTA

An embedded MTA (E-MTA) is a hardware device that incorporates a DOCSIS 1.1 cable modem as well as a IPCablecom multi-media terminal adapter component. Following this, the E-MTA has two logical parts, which are physically combined into one device: a Cable Modem (CM), and a Multimedia Terminal Adapter (MTA). Every home using IPCablecom services has at least one such device. On the subscriber side, it supports one or more phone lines, and optionally includes one or more ports for high-speed data access such as a local 10BaseT or 100BaseT interface. On the network side it supports the IPCablecom /DOCSIS 1.1/HFC network requirements.

The cable modem is a modulator that provides data transmission over the cable network using the DOCSIS 1.1 protocol. In IPCablecom, the CM plays a key role in handling the media stream and provides services such as classification of traffic into service flows, rate shaping, and prioritized queuing.

The MTA is a IPCablecom client device that contains a subscriber-side interface to the subscriber's CPE (e.g. telephone) and a network-side voice and signalling interface to elements in the network. It basically handles the two-way translation of voice to IP packets, and two wayPOTS telephone to IP based signalling conversion. It provides codecs and all signalling and encapsulation functions required for media transport and call signalling. IPCablecom MTAs are required to support the Network Call Signalling (NCS) protocol.

Compared to the IPCablecom 1.0 NCS architecture, the LCS E-MTA has the following changes:

1) The E-MTA is still required to support only a subset of the NCS signalling; however since LCS E-MTAs are expected to migrate to a full NCS architectures, this should not be construed as a guideline for MTA development.

2) Only ITU-T Recommendation G.711 [24] codec translation and compression is supported. Minimum requirements to support ITU-T Recommendation G.711 [24] are given in the Codec Specification TS 101 909-3 [3].

3) The E-MTA interfaces at the DOCSIS physical and logical level with the CMTS, but the LCS Architecture suggests two architecture changes (which are transparent to the E-MTA):

   - the telephone signalling interface is with IPAT instead of the MGC/CMS;

   - the voice to packet translations are handled by the IPAT instead of the MG.

5.5 Operational support systems

The Operational Support System components are typically used as part of the network's "back office" to manage, administer, and provision the IPCablecom systems. They provide fault management, performance management, security management, accounting management, and configuration management for all devices and equipment in the IPCablecom system. The OSS components for LCS are mostly unchanged from the NCS IPCablecom architecture. The main impact of LCS on the OSS components are:

1) Additional management is required for the IPAT, including:

   - V5.2 trunk (digital line) provisioning and management;

   - V5.2 trunk (digital line) numbering mapping to NCS trunk numbering mapping;

   - subscriber data required for NCS to V5.2 translation.

2) Less management is required for features in the CMS, MGC, SG, MG, RKS, and AS components that have been replaced by the LE.

3) The Record Keeping Server (RKS) will not be used to keep billing (CDR) related data, as the LE will keep its own records.

6 System interfaces

Protocol specifications have been or are currently being defined for most component interfaces within the IPCablecom architecture. An overview of these component interfaces is provided in the TS 101 909-2 [2]. The individual IPCablecom protocol specifications should be consulted for complete requirements of each component interface.

New interfaces pertaining to the support Line Control Signalling have been added to the IPCablecom architecture. These will be detailed in the following clauses. Additionally, several interfaces defined for the IPCablecom architecture do not exist in the IPCablecom LCS system architecture. Since an IP Access Terminal (IPAT) integrates part of the functionality of a Call Management Server (CMS) with that of a Signalling Gateway (SG), Media Gateway Controller (MGC) and Media Gateway (MG); none of the interfaces between these components is considered an defined interface in the LSC system. Also, an IPAT uses the V5.2 interface and a Local Exchange Switch (LE) to provide feature functionality, subscriber and PSTN connectivity; thus IPCablecom's inter-domain signalling and audio server interfaces do not apply either.

The following clauses overview the use of the existing and new IPCablecom component interfaces within the LSC system.

6.1 Physical and data link layer interfaces

The lower layer interfaces supported between the components used in the V5.2 sub-system of the IPCablecom architecture are as shown in table 1.

Table 1: Physical Interfaces

Component interface	Network interface
CMTS-to-HFC Network and HFC Network-to-MTA	DOCSIS 1.1
LE-to-IPAT	E1
CMTS-to-IPAT	IEEE 802.3 [20]
MTA-to-IPAT	No direct physical interface exists
MTA-to-CPE	Refer to TS 101 909-18 [8].
CMTS-to-Network Servers and IPAT-to-Network Servers	IEEE 802.3 [20]
CMTS-to-EMS and IPAT-to-EMS	IEEE 802.3 [20]

6.2 Call signalling interfaces

Line control signalling is implemented across four call signalling interfaces. These are shown in figure 3. Each interface in the figures is labelled and further described in table 2.

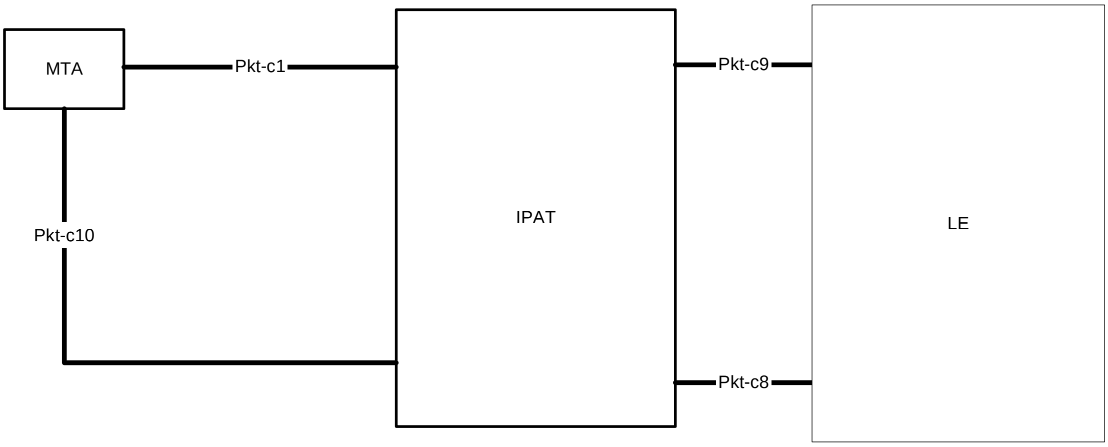
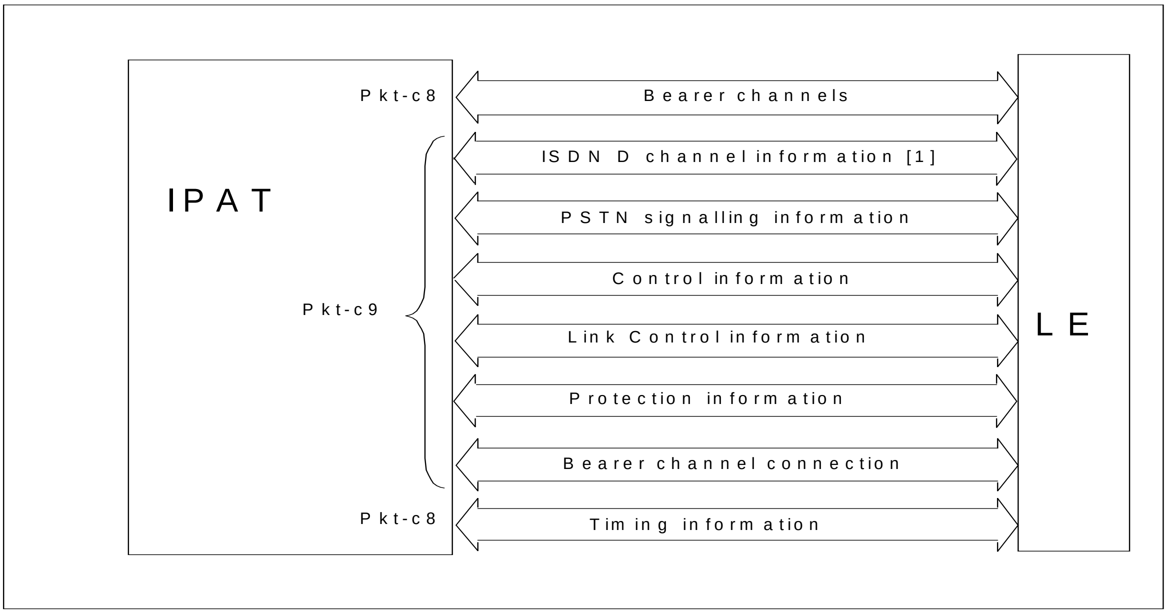


Figure 3: Call Signalling Interfaces

Table 2

Interface	IPCablecom Functional Components	Description
Pkt-c1	MTA-IPAT	Call signalling messages exchanged between the MTA and IPAT using the NCS protocol. This interface exists in packet cable. A subset of the interface is used in the V5.2 to NCS mapping.
Pkt-c8	IPAT-LE	This interface defines bearer channel connectivity from the IPAT to the LE via the V5.2 interface and supports the following call signalling protocols: • In-Band DTMF Signalling towards the Local Exchange ES 201 235 [10]. • Receipt of call progress tones and announcements from the Local Exchange EG 201 188 [9]. • Receipt of display services protocols from the Local Exchange EN 300 659 [14].
Pkt-c9	IPAT-LE	The IPAT terminates the signalling functions of the V5.2 interface (EN 300 347-1 [13]) from the Local Exchange (LE). The IPAT supports the following Access Network (AN) functionality of the V5.2 interface: • AN Data Link Layer Protocols • AN PSTN Protocol • AN BCC Protocol • AN Link Control Protocol • AN Control Protocol • AN Protection Protocol
Pkt-c10	IPAT-MTA	Packetized PSTN media flows transmitted and managed using the RTP and RTCP protocols with QoS and security as defined in IPCablecom This may include for example, tones, announcements and voice.



NOTE: ISDN support is optional. It is shown here for completeness.

Figure 4: V5.2 interface between IPAT and LE

6.2.1 The IPAT and the line control signalling Interfaces

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 interworking function of mapping the V5.2 call signalling from the LE to the NCS call signalling of the 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, etc. Four interfaces are associated with the IPAT: Pkt-c1 and Pkt-c10, between the IPAT and the MTA; Pkt-c8 and Pkt-c9, between the IPAT and the LE.

The Pkt-c1 interface uses the Network Call Signalling (NCS) protocol as used in the IPCablecom architecture 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. In band Call Progress (Call Supervision) signalling tones (e.g. dial tone, ring back, DTMF, CID FSK, etc.) exist in the LCS architecture.

The Pkt-c9 interface uses the V5.2 PSTN call signalling protocol specified in EN 300 324-1 [12] and the BCC protocol specified in EN 300 347 [13]. 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. There are other control protocols across this interface and these are covered in clause 6.2.2.

The Pkt-c10 interface uses the RTP and RTCP protocols to transport voice band information. Dial tone and call progress tones are transmitted in this flow by the LE to the end-user; the end-user sends DTMF digits to the LE in this flow. It also follows the QoS and Security requirements of IPCablecom.

6.2.2 The IPAT and the LE

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. However, the IPAT must handle the control requirements as defined in EN 300 347 [13].

6.3 Media streams

IPCableCom identifies the IETF RFC 1899 [15] as the means to transport all media streams in the network. IPCableCom utilizes the RTP profile for audio and video streams as defined in IETF RFC 1890 [16].

The Pkt-rtp3 interface uses the RTP and RTCP protocols . Dial tone, alerting tones, announcements, and media content -- all supplied by the LE are sent from the IPAT to the MTA across this interface. The MTA sends DTMF digits as well as media content to the IPAT across this interface.

RTP encodes a single channel of multimedia information in a single direction. RTP sessions are established dynamically by the endpoints involved, so there is no "well-known" UDP port number. The Session Description Protocol (SDP) is used to communicate the particular IP address and UDP port an RTP session is using.

The packet header overhead of Ethernet, IP, UDP, and RTP is significant when compared to a typical RTP Payload size, which can be as small as 10 bytes for packetized voice. The DOCSIS 1.1 specification addresses this issue with a Payload Header Suppression feature for abbreviating common headers.

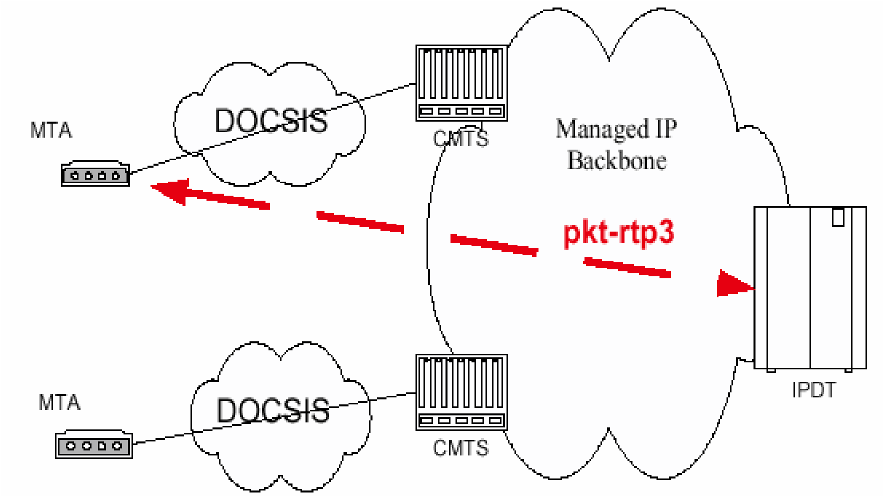
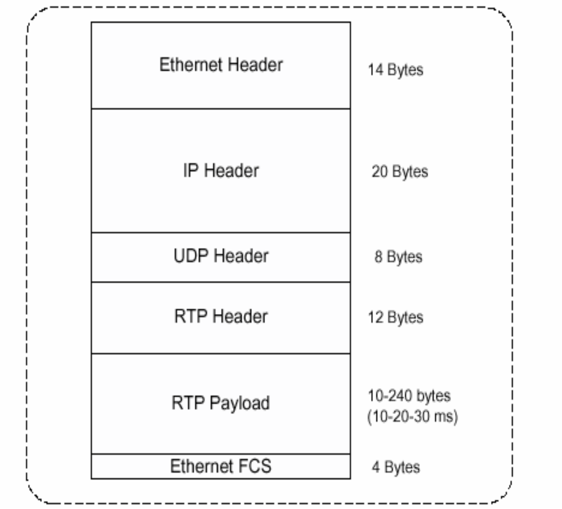


Figure 5: RTP Media Stream Flows in a IPCableCom Network

pkt-rtp3: Media flow between the IPAT MG function and the MTA. Includes, for example, tones, announcements, and PSTN media flow sent to the MTA from the IPAT MG function . Also includes upstream media flow between the MTA and IPAT MG function . RTP encodes a single channel of multimedia information in a single direction. The standard calls for a 12-byte header with each packet. An 8-bit RTP Payload Type (PT) is defined to indicate which encoding algorithm is used. Most of the standard audio and video algorithms are assigned to particular PT values in the range 0 through 95. The range 96 through 127 is reserved for "dynamic" RTP payload types. The range 128 through 255 is reserved for private administration.

The packet format for RTP data transmitted over IP over Ethernet is depicted in figure 6.



Ethernet Header	14 Bytes
IP Header	20 Bytes
UDP Header	8 Bytes
RTP Header	12 Bytes
RTP Payload	10-240 bytes (10-20-30 ms)
Ethernet FCS	4 Bytes

Figure 6: RTP Packet Format

The length of the RTP Payload as well as the frequency with which packets are transmitted depends on the algorithm as defined by the Payload Type field.

RTP sessions are established dynamically by the endpoints involved, so there is no "well-known" UDP port number. The Session Description Protocol (SDP) was developed by the IETF to communicate the particular IP address and UDP port an RTP session is using.

The packet header overhead of Ethernet, IP, UDP, and RTP is significant when compared to a typical RTP Payload size, which can be as small as 10 bytes for packetized voice. The DOCSIS 1.1 specification addresses this issue with a Payload Header Suppression feature for abbreviating common headers. To support transparent use of DOCSIS 1.1 Payload Header Suppression, IETF RFC 2833 [18] event packets should be padded to match the length of the corresponding RTP voice packet that would have otherwise been sent upstream or downstream. The padding value is undefined.

6.4 MTA device provisioning

The LCS Architecture does not impact MTA device provisioning. A description of MTA device provisioning can be found in the IPCablecom MTA Device Provisioning Specification, TS 101 909-6 [6].

6.5 Event messages interfaces

A IPCablecom Event Message is a data record containing information about network usage and activities. A single Event Message may contain a complete set of data regarding usage or it may only contain part of the total usage information. When correlated by the Record Keeping System (RKS), information contained in multiple Event Messages provides a complete record of the service. This complete record of the service is often referred to as a Call Detail Record (CDR). Event Messages or CDRs may be sent to one or more back office applications such as a billing system, fraud detection system, or pre-paid services processor.

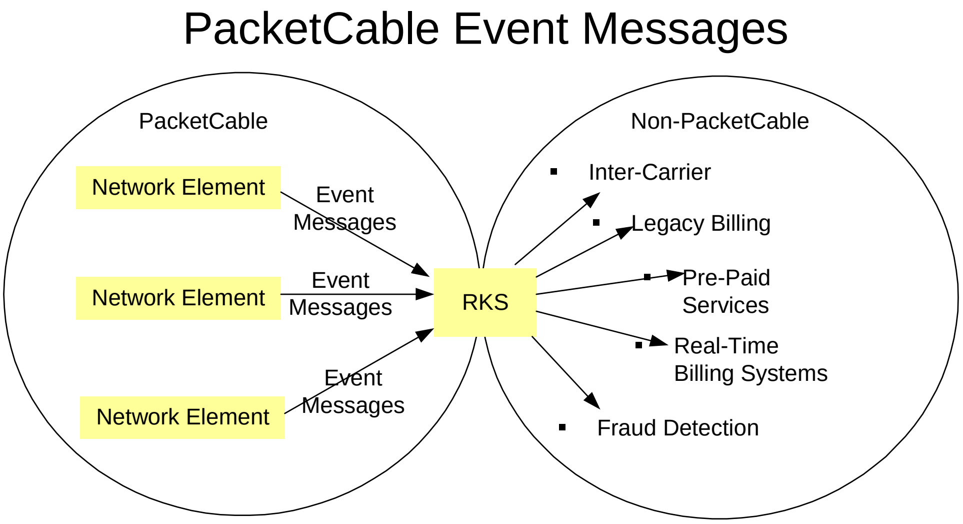


Figure 7: Representative event messages architecture

IPCablecom Event Message generation for subscriber billing is not required for services provided by the LCS system. In an LCS system, all CDRs for subscriber billing are generated by the LE. The IPAT functional component of an LCS system supports minimal CMS and MGC functionality and does not contain sufficient information to generate IPCablecom Event Messages, therefore the IPAT does not generate IPCablecom Event Messages for services provided by the LCS system. Although the IPAT communicates with the CMTS, the IPAT does not send the Event-Generation-Info object in the GATE-SET message therefore the CMTS is unable to generate Event Messages for services provided by the LCS system.

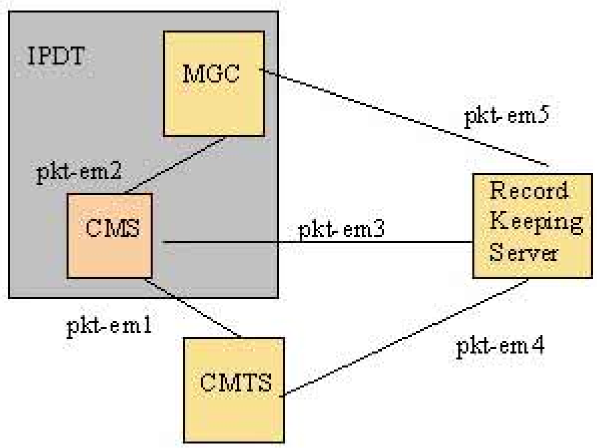


Figure 8: Event Message Interfaces

It should be noted here that the LSC system makes optional the previously mandatory Event Message interfaces between a CMS and an RKS, between an MGC and an RKS, and between a CMTS and an RKS.

The table 3 describes the Event Message interfaces shown in figure 8.

Table 3: Event Message Interfaces

Interface	IPCablecom Functional Component	Description
pkt-em1	CMS-CMTS	DQoS Gate-Set message carrying Billing Correlation ID and other data required for CMTS to send Event Messages to an RKS. (see note 1)
Pkt-em2	CMS-MGC	Vendor-proprietary interface carrying Billing Correlation ID and other data required billing data. Either the CMS or MGC may originate a call and therefore need to create the Billing Correlation ID and send this data to the other. (see note 2)
Pkt-em3	CMS-RKS	RADIUS protocol carrying IPCablecom Event Messages. (see note 3)
Pkt-em4	CMTS-RKS	RADIUS protocol carrying IPCablecom Event Messages. (see note 4)
Pkt-em5	MGC-RKS	RADIUS protocol carrying IPCablecom Event Messages. (see note 5)
NOTE 1: This existing IPCablecom interface is not used by the LSC system. DQoS signalling between and IPDT CMS and the CMTS will not include Event-Generation-Info objects. NOTE 2: Not an open interface in the LSC system; CMS and MGC are integrated within a single physical IPAT entity. NOTE 3: This existing IPCablecom interface is not used by the LCS system. NOTE 4: This existing IPCablecom interface is not used by the LCS system. DQoS signalling between and IPAT CMS and the CMTS will not include Event-Generation-Info objects. This omission will indicate to the CMTS to not send Event Messages to the RKS for calls so signalled. NOTE 5: This existing IPCablecom interface is not used by the LCS system.		

6.6 Quality of service

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

The LCS System is defined over ES 201 488 [11] only, based on, Dynamic QoS control Specification, TS 101 909-5 [5].

There are two options for DQoS, one called "with Gate Coordination", and one called "without Gate Coordination". The difference is primarily in the choice of whether to use the full Gate Coordination function of the CMS inside the IPAT, or to use a reduced version. It should be noted the PacketCable GR303 IPDT uses the "without Gate Coordination" option, and some may prefer to retain commonality between PacketCable and IPCablecom where possible.

Gate coordination (GC) is the process by which gates in the CMTS are managed by the CMS; gates are the mechanism used to dynamically authorize quality of service resources while providing security to prevent theft and loss of service attacks on the network. The GC function is essentially a policy decision maker. DOCSIS QoS is based upon the objects which describe traffic and flow specifications, similar to the TSpec and RSpec objects as defined in the IETF Resource reSerVation Protocol (RSVP). This allows QoS resource reservations to be defined on a per flow basis.

The two options require different provisoing choices in the IPAT and the CMTS gate object, differences in RADIUS support, differences in the use of the either "get close" or the "get info" messages to validate gate closure, and differences in the monitoring of the RTP stream.

1) In the CMTS, the remote gate info object can be provisioned in one of three ways: with a local CMS IP address, with a remote proxy CMS address for interdomain cases, or a null address. In the "with coordination" case, the IPAT's IP address should be provisioned into the info object; this will cause the CMTS to operate as if there were a full CMS involved for gate functions. In the "without coordination" case, the field should be null; the CMTS will then take no proactive action.

2) In the CMTS both options require provisiong using the Gate Set command to enfore the omission of the "Event-Generation-Info" object; this will indicate that no event generation should be done for this Gate and the CMTS should not communicate with the RKS.

3) In the CMTS the "without Gate coordination" case requires that a flag must be set in the Gate Set command and the "Remote Gate Info" object is omitted; this will stop the CMTS from sending or receiving the Radius "Gate close" or "Gate Open" commands from the IPAT. Thus in the IPAT, the "without Gate coordination" option does not use the Gate coordination message, but the info message which is sent as message after every call release from the IPAT.

4) In the "with Gate Coordination" option, the IPAT requires RADIUS protocol support.

6.6.1 Application of TS 101 909-5 to Dynamic Quality of Service

IPCablecom Dynamic QoS (DQoS) uses the call signalling information at the time that the call is made to dynamically authorize resources for the call. Dynamic QoS prevents various thefts of service attack types by integrating QoS messaging with other protocols and network elements. The network elements that are necessary for LCS Architecture Dynamic QoS control based on TS 101 909-5 [5] are shown in figure 1.

NOTE 1: Pkt-q7, CMTS to RKS interface is not used in the LCS Architecture since billing is handled completely by the LE.

NOTE 2: In the "without Gate coordination" option, the IPAT/CMTS proxy and the Pkt-q8 interface are not needed.

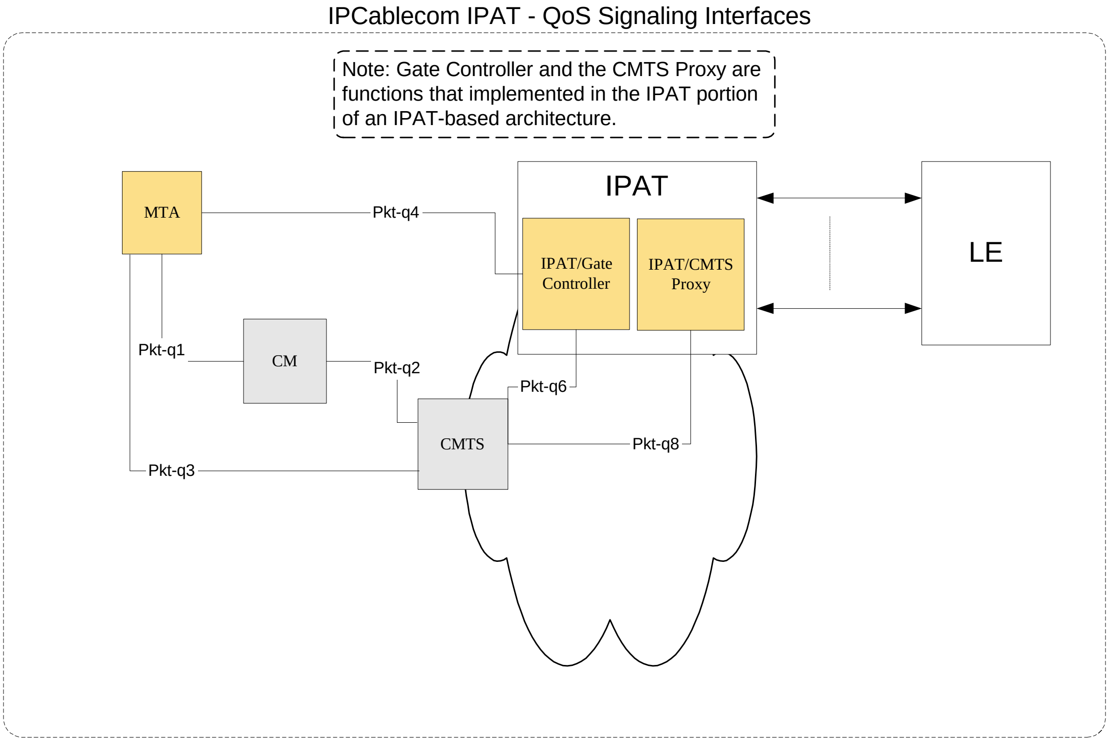

IPCablecom IPAT - QoS Signaling Interfaces
Note: Gate Controller and the CMTS Proxy are functions that implemented in the IPAT portion of an IPAT-based architecture.
MTA
Pkt-q4
IPAT
IPAT/Gate Controller
IPAT/CMTS Proxy
LE
Pkt-q1
CM
Pkt-q2
Pkt-q6
CMTS
Pkt-q8
Pkt-q3

Figure 9: IPCablecom IPAT - QoS Signalling Interface

Interfaces pkt-q1 through pkt-q8 are available for controlling and processing QoS. Not all interfaces are used in LCS system. Table 4 identifies the component interfaces and how each interface is used in the Dynamic QoS Specification (DQoS - TS 101 909-5 [5]).

Two alternatives are shown for the present document: first a general interface that is applicable to either embedded or standalone MTAs; and second, an optional interface that is available only to embedded MTAs.

Table 4: QoS Interfaces for Standalone and Embedded MTAs

Interface	IPCablecom Functional Components	DQoS Embedded/ Standalone MTA	D-QoS Embedded MTA
Pkt-q1	MTA - CM	N/A	E-MTA, J.112 [19] MAC Control Service Interface
Pkt-q2	CM - CMTS (DOCSIS)	ES 201 488 [11] , CMTS-initiated	ES 201 488 [11], CM-initiated
Pkt-q3	MTA - CMTS	RSVP+	N/A
Pkt-q4	MTA - IPAT	NCS	NCS
Pkt-q6	IPAT - CMTS	Gate Management	Gate Management
Pkt-q8 (see note)	CMTS - IPAT/CMTS-Proxy (see note)	Gate Management (see note)	Gate Management (see note)
NOTE: Not needed in "without gate coordiatnion option".			

6.6.2 LCS Dynamic Quality of Service architecture

Should Gate Coordination be used, the functions of each QoS interface in CMS System and the migration to the LCS Architecture are described in table 5 (according to TS 101 909-5 [5]).

Table 5: DQoS Interfaces migration to LCS System

Interface	Functional Components	Description
Pkt-q1	MTA - CM	This interface is only defined for the embedded MTA. The interface decomposes into three sub-interfaces: *Control*: used to manage ES 201 488 [11] MAC service-flows and their associated QoS traffic parameters and classification rules. *Synchronization*: used to synchronize packet and scheduling for minimization of latency and jitter. *Transport*: used to process packets in the media stream and perform appropriate per-packet QoS processing. The MTA/CM interface is conceptually defined in appendix B.IV of ITU-T Recommendation J.112 [19]. For standalone MTAs no instance of this interface is defined.
Pkt-q2	CM - CMTS	This is the ES 201 488 [11] QoS interface (control, scheduling, and transport). Control functions can be initiated from either the CM or the CMTS. However the CMTS is the final policy arbiter and granter of resources by performing admission control for the IPCablecom network. This interface is defined in the ES 201 488 [11].
Pkt-q3	MTA - CMTS	The interface is used to request bandwidth and QoS in terms of delay using standard RSVP and extensions specified in TS 101 909-5 [5]. As a result of message exchanges between the MTA and CMTS, service flows are activated using the CMTS-originated signalling on interface Pkt-q2.
Pkt-q4	MTA -IPAT	Many parameters are signalled across this interface such as media stream, IP addresses, port numbers, and the selection of codec and packetization characteristics. NCS also provides specific parameters for signalling DQoS protocol information like GateID and IPv4 TOS byte.

Interface	Functional Components	Description
Pkt-q6	IPAT - CMTS	This interface is used to manage the dynamic Gates for media stream sessions. This interface enables the IPCablecom network to request and authorize QoS.
Pkt-q8	CMTS-IPAT/CMTS-Proxy	This interface is used for coordination of resources between the CMTS of the local MTA and the CMTS of the remote MTA. The CMTS is responsible for the allocation and policing of local QoS resources. The IPAT acts as a CMTS proxy - identifying instances when the media stream is cut off and stopping the billing at those times (see note).
NOTE: In the "without Gate Coordination" case, this interface is not needed.		

The function within the CMTS that performs traffic classification and enforces QoS policy on media streams is called a Gate. The Gate Controller (GC) element manages Gates for IPCablecom media streams. The following key information is included in signalling between the IPAT/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 10ms") 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 IPAT/GC 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 authorized parties.

Identity of the DiffServ Code Point (DSCP): The CMTS needs to police received packets to ensure that correct DSCP is being used and that the volume of packets in a given class is within authorized bounds.

Identity of the media stream cut off: The CMTS is monitoring the data stream to ensure that when the session is terminated unnaturally (because of RF problems), all QoS resources allocated will be released. The CMTS will notify the IPAT of the release of the QoS resources and the IPAT will respond by sending an appropriate V 5.2 message to the LE to cause billing to cease. In the "without coordination option", the IPAT must perform this function, since it does not receive the "get close" message.

Billing Information: In the V 5.2 sub-system all billing information is collected at the LE and the IPAT does not get any indication from the LE on the call start time. Consequently there is no need for the IPAT to create opaque billing information that the CMTS would need to forward to the RKS.

In IPCablecom LCS systems, the LE should manage the billing.

The role of each of the IPCablecom LCS System components implementing DQoS is as follows:

IPAT/Gate Controller: The IPAT/GC is responsible for QoS authorization.

In the LCS application, the IPAT /GC will authorize QoS on a per-call basis when the LE first authorizes the call attempt. Once a call attempt has been authorized by the LE, the IPAT /GC will establish a Gate for the call with the CMTS and will signal DQoS parameters (e.g., Gate ID, DSCP) via NCS to the MTA involved in the call.

At the end of the call, the LE will initiate call disconnect. As a result the IPAT will control the release of resources by signalling to the MTA (i.e. via NCS), and the MTA will respond by signalling to the CMTS (i.e. via ES 201 488 [11] MAC layer or RSVP+). The CMTS will then ensure that the access network resources are properly released through interaction with the CM associated with the MTA involved in the call and it will report back to the IPAT/GC.

The IPAT must verify at the completion of all calls that the CMTS has reported that QoS resources were released, otherwise it must release them by itself.

When the CMTS reports that QoS resources were released as a result of any problem in the network (e.g. the LE did not initiate the release command).

In the case of abnormal disconnection as described in clause B.1.2, the IPAT must report to the LE (via the V 5.2 interface) to stop the billing and release all LE resources of the MTA involved in the call.

CMTS: Using information supplied by the IPAT/GC, 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 is monitoring the data stream, and when the session is terminated the CMTS releases the QoS resources and reports it to the IPAT/GC. The CMTS interacts with CM, MTA and IPAT/GC.

The responsibilities of CMTS with respect to each of these elements are:

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. Inasmuch 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.

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 IPAT/GC indicating that MTA and CMTS are engaged in a Service Level Agreement (SLA).

CMTS to IPAT: The CMTS responds to requests from an IPAT to authorize voice call bandwidth for an MTA endpoint. It does so by creating a Gate for the call and by returning the Gate ID to the IPAT for subsequent use in signalling with the MTA (i.e. via NCS). The CMTS is monitoring the data stream, and when the session is terminated it closes the Gate and sends Gate-Close message to the IPAT/CMTS Proxy. The CMTS also responds to requests by the IPAT/GC for Gate information and will close Gates at the request of the IPAT during certain abnormal situations. In the "without coordination option", the IPAT must perform this function, since it does not receive the "get close" message.

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 the ES 201 488 [11].

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 then the MTA will not receive the QoS characteristics that it requested.

For the LCS application, the MTA uses single stage QoS bandwidth allocation - when an originating or terminating call is processed the QoS resources are reserved and committed in a single step.

6.6.3 Layer-two vs. layer-four MTA QoS signalling

QoS signalling from the MTA may be required at both layer two (ES 201 488 [11] and layer four (RSVP)). Layer-two signalling is accessible to CM and CMTS devices that exist at the RF boundary of the ES 201 488 [11] access network. Layer-four signalling is required for devices that are one or more hops removed from the RF boundary of the ES 201 488 [11] access network.

Layer-two QoS signalling is initiated by an embedded MTA. The MTA utilizes the implicit interface for controlling the ES 201 488 [11] MAC Layer service flows as suggested by appendix B.IV of ITU-T Recommendation J.112 [19].

Layer-four QoS signalling is usually initiated by a standalone MTA. Enhanced RSVP is used for this signalling and is intercepted by the CMTS. The CMTS utilizes layer-two QoS signalling to communicate QoS signalling changes to the CM.

6.6.4 LCS system Dynamic Quality of Service implementation

A minimal sub-set of the IPCablecom Dynamic Quality of Service (DQoS) specification will need to be implemented in order to mitigate theft and denial of service within the LCS system. Capabilities already existing in DQoS TS 101 909-5 [5] will be used with provisioning options set to enforce CMTS behavior (see clause 6.6.1) to meet the needs of the LCS architecure.

6.6.4.1 Dynamic Quality of Service functional requirements

6.6.4.1.1 Gate establishment

The IPATs must establish DQoS Gates for every voice call by initiating DQoS *GATE-SET* message exchanges with the CMTS. The IPAT then may signal the GateID returned in the *GATE-SET-ACK* by the CMTS via NCS connection commands (e.g., CRCX) to the MTA associated with that call.

MTAs must use the GateID signalled in NCS connection commands received from the IPAT in subsequent resource reservation and committal message exchanges (e.g. ES 201 488 [11] E-MTA MAC DSA-REQ/RSP/ACK) with the CMTS.

Gate establishment makes use of existing DQoS (TS 101 909-5 [5]), ES 201 488 [11] E-MTA MAC and NCS (TS 101 909-4 [4]) messages and procedures.

6.6.4.1.2 Packet classification and filtering

The CMTS must perform packet classification and filtering based upon the signalled Gate Spec (i.e.from IPAT-initiated *GATE-SET* messages) and through using the parameters received via ES 201 488 [11] E-MTA MAC messaging from the MTA. The Gate Spec received from an IPAT/GC will be missing MTA upstream UDP source port and downstream UDP receive port information. The CMTS must obtain these ports via E-MTA MAC messaging and use them to populate packet classifiers for the respective upstream and downstream flows.

Packet classification and filtering is per existing DQoS (TS 101 909-5 [5]) and ES 201 488 [11] messages and procedures.

6.6.4.1.3 Setting the DiffServ Code Point (DSCP)

This architecture allows for the use of a Differentiated Services backbone, where there is adequate bandwidth to carry voice conversations, but access to this bandwidth is on a controlled basis. It is desirable to be able to set the Diffserv code point of packets that are about to enter the provider IP backbone from the CMTS. The DS field maintains backward compatibility with the present uses of the IP Precedence bits of the IPv4 TOS byte (IETF RFC 2474 [17]). The provider can configure policies in the CMTS that determine how to set the DSCP for flows that pass through the CMTS. Such policies are sent to the CMTS in the Gate-set command from the IPAT/GC.

For implementation efficiency, the call agent send to the MTA the information about the appropriate DSCP for it to use on a given session. This is done with the NCS CRCX or MDCX messages by the IPAT. The CMTS still needs to police received packets to ensure that correct DSCP is being used and that the volume of packets in a given class is within authorized bounds.

6.6.4.1.4 CMTS - IPAT/CMTS proxy gate coordination with gate coordination option

The CMTS and the IPAT/CMTS Proxy exchange messages with each other to synchronize the use of gates. These are messages that include GATE-OPEN, GATE-CLOSE and their corresponding Acknowledgments. GATE-OPEN messages are exchanged when the gate has committed resources activated or changed as the result of a command from the MTA. GATE-CLOSE messages are exchanged when those resources are released. Timers within the gate implementation impose strict controls on the length of time these exchanges may occupy.

A gate is initially created by a GATE-SET command from the IPAT/GC. The GATE-SET command will contain such information as the prototype classifiers and Flowspecs for both the local and remote gates. It also contains the IP address and port number of the IPAT/CMTS Proxy so they can implement Gate-to-Gate coordination.

Gate Coordination makes use of existing DQoS (TS 101 909-5 [5]) messages and procedures.

6.6.4.1.5 Gate Closure without Gate Coordination options

IPATs will expect the CMTS to close Gates based upon signalling from the MTA (e.g., ES 201 488 [11] E-MTA MAC DSD-REQ) or based upon service flow inactivity timeouts. The IPAT must verify that Gates have been closed in all call release scenarios and must delete Gates that have not been properly closed by the CMTS (i.e. by using the *GATE-INFO* and *GATE-DELETE* message exchanges). The IPAT will always validate the identity of Gates that it deletes to minimize the possibility of deleting valid Gates.

Gate closure makes use of existing DQoS messages and procedures.

6.6.4.1.6 Gate Closure with Gate Coordination options.

Gate coordination is also done at the time a gate is closed. The CMTS sends a GATE-CLOSE message to the IPAT/GC when it receives an explicit release message from the MTA, or when it detects that the client is no longer actively generating packets and not generating proper refreshes for the flow associated with a gate. A CMTS also closes a gate when it receives a GATE-CLOSE or GATE-DELETE message from the IPAT/GC.

The IPAT must verify the reason for the Gates Closure, in abnormal cases, when the Gate has not been closed because of an explicit disconnect message from the LE (via V 5.2 interface), the IPAT must indicate to the LE about call cut off (by sending V 5.2 AN_Fault message) in order to stop the call billing and to release all resources connected to this line (see figure 10).

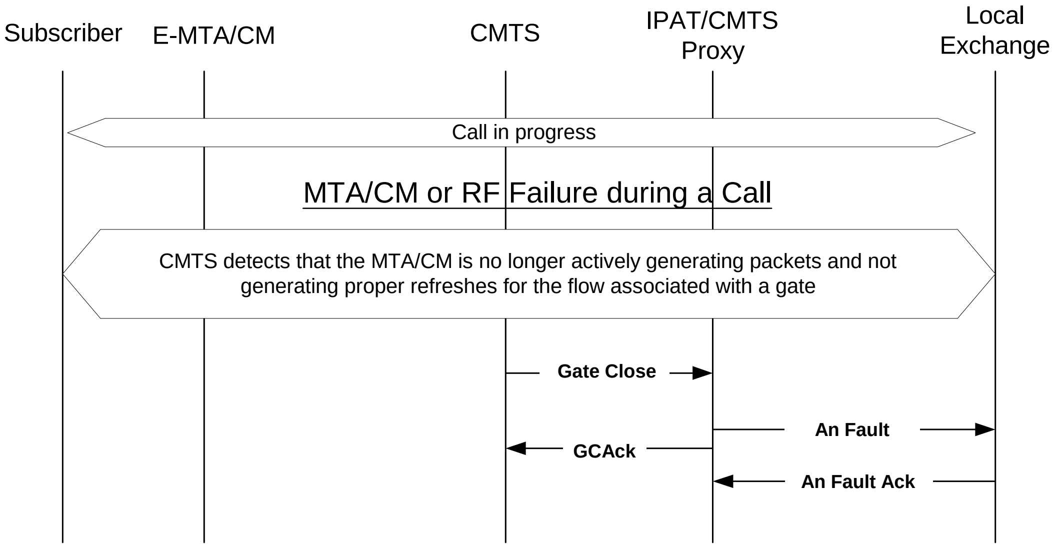

Subscriber
E-MTA/CM
CMTS
IPAT/CMTS Proxy
Local Exchange
Call in progress
MTA/CM or RF Failure during a Call
CMTS detects that the MTA/CM is no longer actively generating packets and not generating proper refreshes for the flow associated with a gate
Gate Close
An Fault
GCAck
An Fault Ack

Figure 10: MTA/CM or RF failure during a call

6.6.4.1.7 Miscellaneous

IPATs must protect against deleting valid Gates. They will do this by comparing Gate information received in *GATE-INFO-ACK* messages against what is expected to be received for the given GateID.

Note that *GATE-INFO-ACK* messages should only be returned in two situations, both of which are abnormal cases.

- The first case is where the CMTS has not already closed the Gate, which would be the case when an MTA fails to initiate resource release when signalled to do so via a DLCX (e.g. via a DSD-REQ to the CMTS).
- The second case is where the CMTS already closed the Gate associated with the IPAT's GateID but has already recycled the GateID for use in another Gate. In either case, the IPAT must be able to validate Gate information prior to sending a *GATE-DELETE* to force delete the Gate.

IPATs must try to protect against denial of service attacks brought on by a misbehaving MTA requesting many more simultaneous UGS sessions than it is entitled to. This is done systematically by not allowing unprovisioned endpoints to initiate voice calls and by limiting provisioned endpoints to a single active voice call at a time.

Additional protection may be obtained through use of the Activity-Count object available in *GATE-ALLOC* and *GATE-SET* message exchanges. However, since it is possible that different endpoints on a given MTA could be drawing service from different CMSs (e.g. IPAT and/or full IP CMS) it is not practical for a given IPAT to know the exact number of Gates to allow for an MTA. The Activity-Count object could be used to provide a practical upper bound on the number of open Gates. The IPAT may send an Activity-Count with a practical upper limit (e.g., four, eight, or sixteen Gates) or may choose to respond to received Activity-Counts that exceed this practical upper limit (i.e. by force deleting of the most recently allocated Gate).

6.6.4.2 IPAT implementation requirements

The following lists QoS implementation requirements for the IPAT component of the LCS system.

1) The IPAT must implement the TS 101 909-5 [5] DQoS Gate Control interface and shall support the messages and objects specified in the DQoS Gate Control Messaging clause of this report. In the "with Gate Coordination" option it must also implement the Gate Coordination Messaging clauses of the present document.

2) If the IPAT chooses not to support DQoS Gate Coordination then the IPAT should omit the Remote-Gate-Info and Gate-Coordination-Port objects from GATE-SET messages that it sends to the CMTS. Omission of these objects should prevent the CMTS from performing Gate Coordination for the associated Gate. In the "with Gate coordination" options, the contents of IPAT-generated Remote-Gate-Info must contain the IPAT/CMTS Proxy IP address and UDP port number (No-Gate-Open flag is set) so they can implement Gate-to-Gate co-ordination.

3) The IPAT MUST signal the CMTS that Event Messages should not be generated for IPAT-initiated voice calls. It MUST do so by omitting the Event-Generation-Info object from the GATE-SET message to indicate that Event Messaging is not to be used for this Gate.

4) The IPAT MUST establish DQoS Gates for every voice call by initiating DQoS GATE-SET message exchanges with the CMTS, and by signalling the GateID returned by the CMTS in subsequent NCS connection control messaging exchanged with the associated MTA.

5) The contents of IPAT-generated Gate-Specs MUST contain the MTA IP address and IPAT IP address in the appropriate positions for the upstream and downstream Gates. It MUST also contain the IPAT receive UDP port as the destination port of the upstream Gate, and it MUST contain the IPAT transmit UDP Port in the source port of the downstream Gate. The IPAT MUST set the UDP port of the MTA to zero in the appropriate positions for the upstream and downstream Gates.

6) The IPAT MUST ensure that DQoS Gates it established have been properly closed by the CMTS for every voice call. In the "without gate coordination" option, the IPAT MUST initiate DQoS GATE-INFO message exchanges with the CMTS, and MUST delete any Gates that have been left open. The DQoS GATE-DELETE message MUST be used for these abnormal cases. In the "with gate coordination" option, The IPAT MUST close any Gates that have been left open.

7) The IPAT MUST ensure that it minimizes the possibility of deleting any Gates that are properly open. This could occur if a CMTS has recycled a closed GateID too quickly. The IPAT MUST validate information it receives in a GATE-INFO-ACK for Gates that it expected to be closed to prevent improper deletions.

8) The IPAT SHOULD make use of the Activity-Count object to place a protective limit on the number of simultaneously active Gates an MTA can have. If this capability is used the IPAT SHOULD consider that it may not actually have knowledge of the true number of Gates that can be open simultaneously by an MTA (e.g., in cases where an MTA"s endpoints are not homed on the same IPAT).

9) The IPAT SHOULD monitor VoIP activity in the "without Gate coordination" option, or verify the reason for the Gates Closure in the "with Gate coordination" options. It SHOULD initiate a V 5.2 AN_FAULT message toward the LE whenever it detects an abnormal condition.

6.7 Audio servers

Announcements are typically needed for calls that do not complete. Additionally, they may be used to provide enhanced information services to the caller (e.g., calling card, n11 services, etc.). The signalling interfaces defined to support IPCablecom Announcement Services are not needed by the LCS system. All announcement functionality is provided by the LE for IPCablecom LCS subscribers, or by local MTA functions.

6.8 Security

This clause describes the IPAT requirements and the IPCablecom LCS architecture for supporting the security specification.

The Line Control Signalling (LCS) Security architecture is based on TS 101 909-11 [7]. It makes use of existing interfaces and security mechanisms already defined in the TS 101 909-11 [7] Security Specification for Single Zone architecture and defines two new interfaces which are outlined in figure 11 and table 6. To obtain an in-depth understanding of the security mechanisms the IPCablecom Security Specification for Single Zone must be consulted using this clause as a guide.

Certain functional elements in the full IP IPCablecom solution are removed in the LCS solution due to the Local Exchange (LE) providing the same functionality. When a functional element is removed then the protocol interfaces between the removed functional element and other elements are also removed. Hence, the need to secure those protocol interfaces is removed.

The LCS billing function is performed in the LE. The Record Keeping Server (RKS) and its interfaces to the CMS and CMTS are removed from the LCS architecture.

Audio Server services is performed in the LE. The Media Player Controller (MPC)/Media Player (MP) and their interfaces to the CMS and CMTS are removed from the LCS architecture.

The Lawful Intercept function is performed in the LE. The Delivery Function (DF) and its interfaces to the MG, CMS, and CMTS are removed from the LCS architecture.

6.8.1 Threats overview

Each of IPCablecom's LCS protocol interfaces is subject to threats that could pose security risks to both the subscriber and service provider. The TS 101 909-11 [7] addresses these threats by specifying, for each defined protocol interface, the underlying security mechanisms (such as IPSec) that provide the protocol interface with the security services it requires, e.g., authentication, integrity, confidentiality.

For example, the media stream path may traverse a potentially unknown Internet service and backbone service providers" wires. As a result, the media stream may be vulnerable to malicious eavesdropping, resulting in a loss of communications privacy. IPCablecom core security services include a mechanism for providing encryption of RTP media streams, thus substantially reducing the threat to privacy.

TS 101 909-11 [7] summarizes all security services available through IPCablecom's. Some of the outlined threats cannot be addressed purely by cryptographic means - physical security and/or fraud management should also be used. These threats may be important, but cannot be fully addressed within the scope of IPCablecom. How vendors and Cable Operators implement fraud management and physical security will differ and in this case a standard is not required for interoperability.

6.8.2 Functional categories

The LCS IPCablecom Architecture Framework identifies the following functional categories within the architecture:

- MTA device provisioning
- Quality of Service (HFC access network and managed IP backbone)
- Security (specified herein)
- Network call signalling (NCS)
- CODEC functionality and media stream mapping
- V5.2 interconnectivity

In most cases, each functional category corresponds to a particular IPCablecom document.

6.8.2.1 MTA device and service provisioning

During MTA provisioning, the MTA gets its configuration with the help of the DHCP and TFTP servers, as well as the OSS.

Provisioning interfaces need to be secured and the MTAs need to be configured with the appropriate security parameters (e.g. customer X.509 certificate signed by the Service Provider). TS 101 909-11 [7] specifies the steps in MTA provisioning, but provides detailed specifications only for the security parameters. Refer to TS 101 909-6 [6] for a full specification on MTA provisioning and customer enrollment.

6.8.2.2 Dynamic Quality of Service

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 CMTS. Should Gate Coordination be used, the IPAT Gate Controller uses the Radius protocol to coordinate the QoS reservation. The MTA utilizes the J.112 [19] QoS or/and the RSVP protocol to establish the QoS to the the CMTS. QoS reservations are also forwarded to the IP Backbone between the CMTSs 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.

6.8.2.3 Call signalling

The call signalling architecture defined within LCS is Network based Call Signalling (NCS) TS 101 909-4 [4]. The Call Agent function within the IPAT uses the MGCP protocol to control call setup, termination and most other call signalling functions.

6.8.2.4 CODEC functionality and media stream mapping

The media stream between MTA and the IPAT Media Gateways utilizes the RTP protocol. Although ITU-T Recommendation J.112 [19]/BPI+ provides for privacy over the HFC network, the potential threats within the rest of the voice communications network (over the IP Network) require that the RTP packets be encrypted.

NOTE: In LCS architecture, it is always an MTA-to-PSTN connection and this path may cross a PSTN network of several different Service Providers. In the process, all RTP packets are encrypted. The media traffic inside a PSTN network does not utilize RTP and has its own security requirements. Thus, in this case the encryption would terminate at the IPAT on both sides of the intermediate PSTN network.

In addition to RTP, there is an accompanying RTCP protocol, primarily used for reporting of RTCP statistics. In addition, RTCP packets may carry CNAME - a unique identifier of the sender of RTP packets. RTCP also defines a BYE message (see note) that can be used to terminate an RTP session. These two additional RTCP functions raise privacy and denial-of-service threats. Due to these threats, RTCP security requirements are the same as the requirements for all other signalling and are addressed in the same manner. For more information on Codec functionality, see TS 101 909-3 [3].

6.8.2.5 V 5.2 interconnectivity

The signalling and media aspects of V5.2 interface are handled by the IPAT Call Agent and Media Gateways respectively.

The V 5.2 Signalling between IPAT CA and LE and voice communications between IPAT MG and LE are fully defined in EN 300 324-1 [12] and ETS 300 347-1 [13]. Security methods are not specified on this interface.

When communications from an MTA to a PSTN phone are made, bearer channel traffic is passed directly between an MTA and the IPAT MG. The protocols used in this case are RTP and RTCP, as in the MTA-to-MTA case. Both security requirements and specifications are very similar to the MTA-to- MTA bearer requirements and are fully defined in TS 101 909-11 [7]. After a voice communication enters the PSTN, the security requirements as well as specifications are the responsibility of the PSTN.

6.8.3 LCS security architecture

IPCablecom security addresses the security requirements of each constituent protocol interface by:

1) Identifying the threat model specific to each constituent protocol interface.

2) Identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats.

3) Specifying the particular security mechanism providing the required security services.

The security mechanisms include both the security protocol (e.g., IPSec, RTP-layer security, and SNMPv3 security) and the supporting key management protocol (e.g., IKE, PKINIT/Kerberos) where applicable.

Figure 11 provides a summary of all the LCS protocol interfaces and the mechanisms used to secure those interfaces.

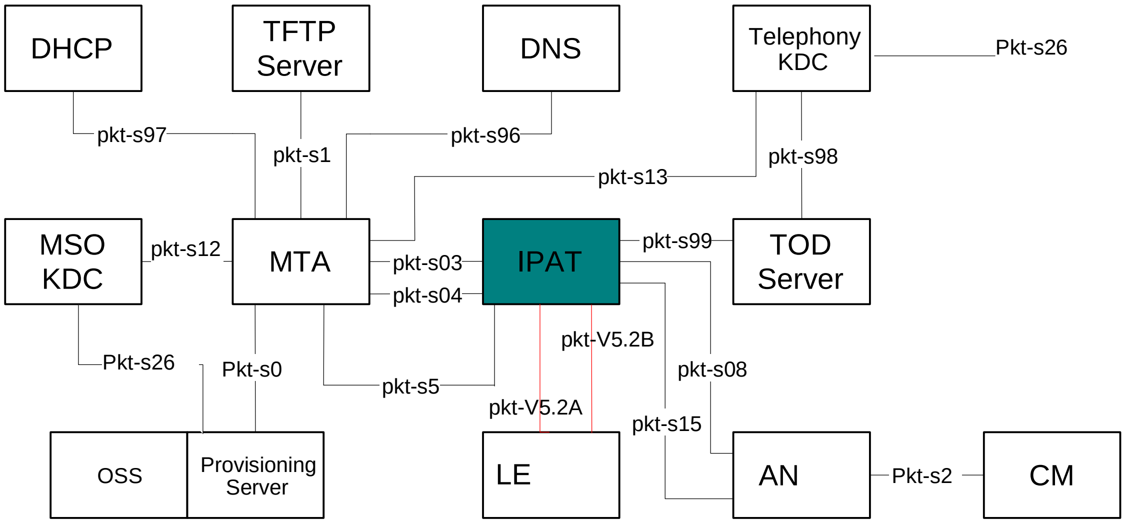


Figure 11: LCS security interface

Table 1 describes each of the interfaces shown in figure 11.

The inteface labelling in table 6 is the same as those from the TS 101 909-11 [7] security specification except where noted here. Certain interfaces present in the Security Specification are not present in the LCS architecture, therefore, they are not included here (i.e. pkt-s6, pkt-s7, etc.). Certain interfaces are described in the LCS architecture but are not included in the corresponding TS 101 909-11 [7] interface table. These interfaces are labeled in the 9x range (i.e. pkt-s99, pkt-s98, etc.). New interfaces added by the LCS architecture are labeled in the form pkt-V5.2x where x is a letter of the alphabet (i.e. pkt-V5.2A, pkt-V5.2B, etc.). These interfaces are represented by solid red lines in figure 11.

The description in Table 1 is the same as those in the TS 101 909-11 [7] security specification except where noted.

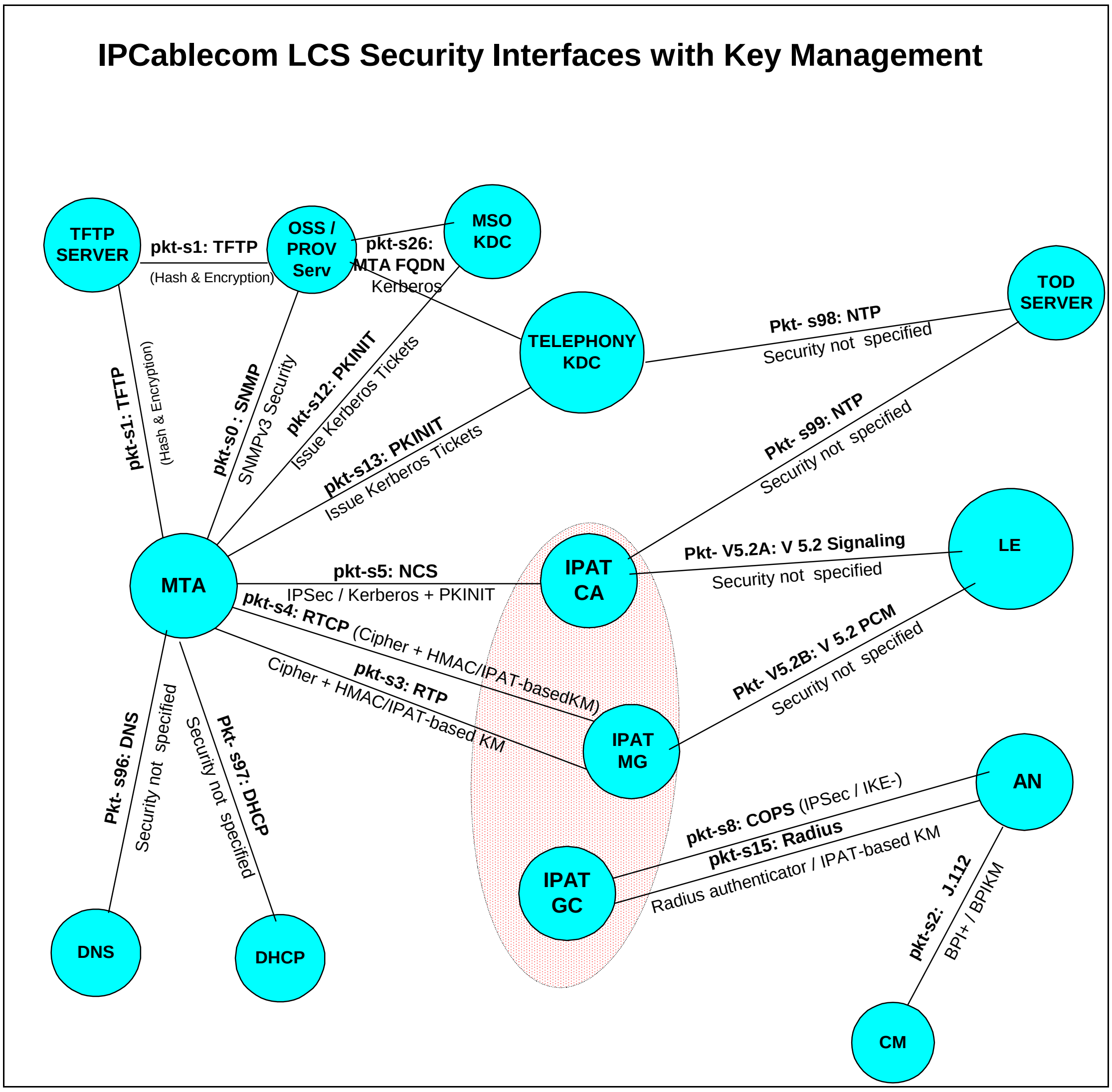
Table 6: Security Interfaces

Interface	IPCablecom Functional Components	Description
pkt-s0	MTA - PS/OSS	**SNMPv3:** The initial SNMPv3 INFORM from the MTA to the Provisioning Server, followed by optional SNMP GET(s) by the SNMP Manager, is used to query MTA device capabilities. This occurs at the time where SNMPv3 keys may not be available, and security is provided with an RSA signature, formatted according to Cryptographic Message Syntax. Later, standard SNMPv3 security is enabled to the OSS.
pkt-s1	MTA - TFTP	**TFTP:** MTA Configuration file download. The MTA downloads a secure configuration file (with TFTP-get) that is signed by the TFTP server and sealed with the MTA public key, with a Cryptographic Message Syntax wrapper.
pkt-s2	CM - CMTS	**ITU-T Recommendation J.112 [19]:** Secured with BPI+ using BPI Key-Management. BPI+ privacy layer on the HFC link.
pkt-s3	MTA - IPAT Media Gateway	**RTP:** End-to-end media packets between MTA and IPAT MG. Note that the MTA to MTA interface is not part of the LCS solution. RTP packets are encrypted directly with the chosen cipher. Message integrity is optionally provided by an HMAC (Hashed Message Authentication Code). Keys are randomly generated and exchanged by the two endpoints inside the signalling messages via the IPAT CA.
pkt-s4	MTA - IPAT Media Gateway	**RTCP:** RTCP control protocl for RTP. Message integrity and encrypted by selected cipher. The RTCP keys are derived using the same secret negotiated during the RTP key management. No additional key management messages are needed or utilized.
Pkt-s5	MTA - IPAT Call Agent	**NCS:** Message integrity and privacy via IPSec. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
Pkt-s8	IPAT Gate Controller-CMTS	**COPS:** Gate Control protocol between the IPAT GC and the CMTS, used to download QoS authorization to the CMTS. Message integrity and privacy provided with IPSEC. Key management is IKE with preshared keys (IKE-).
pkt-s12	MTA - MSO KDC	**PKINIT:** An AS-REQ message is sent to the KDC as before, except public key cryptography is used in the initial authentication step. The KDC verifies the certificate and issues a ticket granting ticket (TGT). The KDC authenticates the message using its public key signature.
Pkt-s13	MTA - Tel KDC	**PKINIT:** See pkt-s12 above.
Pkt-s15	IPAT Gate Controller-CMTS	**Radius:** For DQoS Gate Coordination (optional). Message integrity is provided with an application-layer (Radius) authenticator. Keys are distributed by the IPAT GC over COPS. This protocol interface is optional and not recommended for use in the LCS architecture.
Pkt-s26	OSS/Prov Server - MSO KDC OSS/Prov Server-Telephony KDC	The KDC uses Kerberos to map the MTA's MAC address to its FQDN for the purpose of authenticating the MTA before issuing it a ticket.
Pkt-s96	MTA - DNS	**DNS:** Used by the MTA to obtain IP addresses for KDC and TFTP servers. Cryptographic methods are not specified on this interface for all IPCablecom architectures. Securing this interface is at the discretion of the system operator.

Interface	IPCablecom Functional Components	Description
Pkt-s97	MTA - DHCP	**DHCP:** used by the various network elements to obtain an IP address. Cryptographic methods are not specified on this interface for all IPCablecom architectures. Securing this interface is at the discretion of the system operator.
Pkt-s98	Telephony KDC - TOD Server	**Network Time Protocol (NTP):** used by the Telephony KDC to obtain time from the Time Of Day (TOD) server. The method to security this protocol has not been determined yet.
Pkt-s99	IPAT CA - TOD Server	**Network Time Protocol (NTP):** used by the IPAT CA to obtain time from the Time Of Day (TOD) server. The method to security this protocol has not been determined yet.
Pkt-V5.2A	IPAT CA - LE	**V 5.2 Signalling:** Used to send signalling and control information between the LE and IPAT, containing the following V 5.2 protocols: Comman Control, Port Control, Link Control, BCC, Protection, PSTN and ISDN. New interface specified by the LCS. Cryptographic methods are not specified on this interface to secure it. Securing this interface is at the discretion of the system operator.
Pkt-V5.2B	IPAT MG - LE	**V 5.2 PCM:** Used to send voice between the LE and the IPAT GW. New interface specified by the LCS. Cryptographic methods are not specified on this interface to secure it. Securing this interface is at the discretion of the system operator.

6.8.3.1 LCS security interfaces summary

Figure 12 summarizes all of the IPCablecom LCS security interfaces, including key management.



NOTE: The following abbreviations are used in figure 12:

IKE-	IKE with pre-shared keys
IPAT - based KM	Keys randomly generated and exchanged inside signalling messages

Figure 12: IPCablecom LCS Security Interfaces with Key-Management

In figure 12, each interface label is of the form:

<label>: **<protocol> { <security protocol> / <key management protocol> }**

If the key management protocol is missing, it is not needed for that interface.

6.9 Lawful Interception

Most of the function of Lawful Interception (LI) will be supplied by the LE. However, the extent of Lawful Intercept requirements on local MTA functions and on provisioning information are currently a matter of debate, and some event messages and QoS information may also be subject to LI collection requirements in the future. Thus this is an area that might have to be revisited in the future.

6.10 Caller Identification provisioning and Detailed Call Record

The IPAT must provide (via provisioning) an internal address translation table from the V5 User Port Identification Value to the associated IP/Line ID address of the CM/MTA that is associated with that line number. This translation table must be available through a provisioning system interface.

The IPAT Detailed Call Record (DCR) must include the User Port Identification Value and the IP/Line ID address values for each call processed by the IPAT.

Annex A (informative): Protocol mapping framework between V5 interface and NCS TS 101 909-4 annexes A and B for analogue telephone access

This annex is based on the reference documents EN 300 324 [21] and ETS 300 327[23]. It is to provide a V5 interface framework to show how the NCS mapping relates in the context of the V5 interface specification. In this framework, the "AN" notation should be loosely interpreted as the "IPAT-MTA" since these elements emulate the "AN" functionality in a Switched IP architecture.

The actual Protocol mapping begins at clause 13 of EN 300 324 [21]. For clarity of the NCS to V5 protocol mapping some of the body of EN 300 324 [21] is duplicated here solely to demonstrate the mapping of the V5 bit oriented protocol to the NCS Text based protocol.

In reviewing the present document it will become apparent that a number of V5 signals are not defined in the NCS signalling set. This is because the NCS signal set was specifically selected to support a 2-wire analog, loop start POTS interface. If any of the currently undefined V5 messages are deemed necessary for this type of POTS interface, then additional NCS messages will need to be defined and are reserved for future study.

ISDN is for future study.

A.1 PSTN signalling protocol specification and layer 3 multiplexing

A.1.1 General

In this framework, the "AN" notation should be loosely interpreted as the "IPAT-MTA" since these elements emulate the "AN" functionality in a Switched IP architecture.

A.1.2 Overview

The PSTN protocol on the V5.2 interface is basically a stimulus protocol; i.e. it does not control the call procedures in the AN rather it transfers information about the analogue line state over the V5.2 interface. The V5.2 PSTN protocol shall be used in conjunction with the national protocol entity in the LE (see figure A.1). The national protocol entity in the LE, which is used for customer lines which are connected directly to the LE, will also be used to control calls on customer lines which are connected via the V5.2 interface. For time critical sequences it is also required to extract certain signalling sequences (e.g. compelled sequences) from the national protocol entity into an "AN part" of the national protocol entity.

However, the V5.2 PSTN protocol has a relatively small functional part which is concerned with path setup, release of the path on the V5.2 interface, call collision resolution on the V5.2 interface and handling of new calls in case of overload conditions in the LE. The majority of line signals will not be interpreted by the V5.2 PSTN protocol, but simply transferred transparently between the user port in the AN and national protocol entity in the LE.

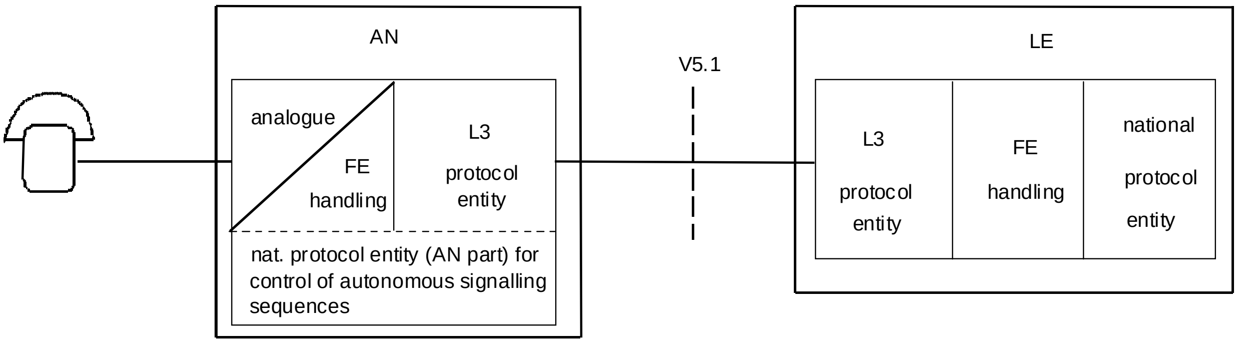


Figure A.1: PSTN user port functional model

A.1.3 Separation of responsibilities

The LE shall be responsible for providing the service (call control, supplementary services). DTMF senders, receivers, tone generators and announcements shall be located in the LE. This implies that address information using DTMF shall be carried transparently between user port and LE whereas line state signalling shall be interpreted in the AN and then carried over the V5.2 interface by means of layer 3 messages.

It shall be the responsibility of the AN to handle access specific parameters related to the protocol such as recognition times of analogue signals, duration, voltage and frequency of meter pulses, ringing current or the specific details of a signalling sequence (AN part of the national protocol entity). These parameters shall be set either in hardware, software or in data. In the latter case this data shall be pre-defined but some of the data may be overruled by "protocol parameter" messages via the V5.2 interface for a call.

For time critical responses to customer signalling it is necessary for the AN to respond autonomously. This shall be explicitly required for ring trip and dial tone suppression. There may be other time critical responses required in national PSTN protocols which shall be defined in the national PSTN protocol mapping specification.

For time critical signalling sequences (e.g. autonomous seizure acknowledge for ground start PBXs) it shall also be necessary for the AN to control the time-critical part of the signalling sequence autonomously. In this case, the autonomous signalling sequence shall be triggered by the national protocol entity in the LE. After executing the autonomous signalling sequence, the AN may return a response to the LE.

The protocol definition is provided in this annex. Background information and flow diagrams are provided in EN 300 324-1 [12] annex H. The SDL diagrams are given in EN 300 324-1 [12], annex L. Annex D provides additional information for the use of the information elements to define the national PSTN protocol mapping.

A.1.4 National specific PSTN signal information elements

ETS 300 327 [23] gives the complete set of PSTN signalling information elements that may be sent over a V5.2 interface in order to cope with all the national PSTN protocols identified to date. It is unlikely that the full set of PSTN signal information elements will be required by any network provider and therefore it is not expected that the full set will be utilized over any individual V5.2 interface. Optionally an equipment may support more PSTN signal information elements than required by a particular network provider. In this case, only those PSTN signal information elements required in order to correctly support that particular national PSTN protocol shall appear on the interface.

It will be the responsibility of the individual equipment providers to ensure that their equipment contains at least the ability to recognize and utilize the correct PSTN signal information elements for the national PSTN protocols to be supported by the local network provider.

It shall be the responsibility of the equipment providers to ensure that the PSTN signal information elements are provided in accordance with the national PSTN protocols.

PSTN signal information elements not required for the required national PSTN protocol shall be treated as unrecognized information elements as specified under clause 13.5.2.7, if they occur.

The full set of PSTN messages, information elements, and coding, may not be required to support a specific national protocol. Only those PSTN messages, information elements, and coding that apply to the protocol shall be used over the V5.2 interface.

A.2 PSTN protocol entity definition

A.2.1 Definition of PSTN path states and explanation

A.2.1.1 Path states in the AN (AN(PSTN))

Out of service state (AN0): This state shall be entered when the restart procedure has been initiated by the system management and is applicable to all PSTN ports simultaneously.

Null state (AN1): The port is inactive and there is no call in progress. This shall be the rest state for the port interface. When the PSTN protocol entity in the AN returns to the NULL state, it shall be capable to detect and report a (may be already present) subscriber seizure.

Path initiated by AN state (AN2): A seizure has been detected within the AN and an ESTABLISH message has been sent to the LE. The AN is now waiting for a ESTABLISH-ACK back from the LE. In the event of no response from the LE, for example in the case of an LE overload, the ESTABLISH message will be repeated at a low repetition rate (Timer T1). Call collision resolution shall be achieved by the AN and LE during this phase of the call.

Path abort request state (AN3): ESTABLISH message was sent to the LE but no ESTABLISH-ACK has yet been received. The subscriber has released (e.g. on-hook). This state shall be used to regulate the number of ESTABLISH messages that may be sent to the possibly overloaded LE, if the port is seized again. After a guard period the AN will go back to the NULL state.

Line information state (AN4): This state shall only be entered into whilst a line information from the PSTN port is being processed by the LE. This state may only be entered or exited from/to the NULL state.

Path active (AN5): The active state shall be the state during which normal PSTN signalling functions are active for that port. During this state a user may proceed with call establishment, communication or call clearing.

Port blocked state (AN6): This state can be entered from any state. Once entered, the only state that the port may proceed to shall be the NULL state when the port is again available for service.

Once the blocked state has been entered all call activity for that port shall be halted and the port may be deactivated, e.g. power down.

Disconnect request state (AN7): The AN requests the LE to disconnect the path. This state shall be exited when the LE has successfully acknowledged the DISCONNECT. If this does not happen, the maintenance entity shall be informed.

A.2.1.2 Path states in the LE (LE(PSTN))

Out of service state (LE0): This state shall be entered when the restart procedure has been initiated by the system management and is applicable to all PSTN ports simultaneously.

Null state (LE1): The port is inactive and there is no call in progress. This shall be the rest state for the port interface.

Path initiated by LE state (LE2): The port is seized. The LE has sent an ESTABLISH message to the AN. Call collision resolution shall be achieved by the AN and the LE during this phase of the call.

Path initiated by AN state (LE3): The AN has sent an ESTABLISH message to the LE and is waiting for an ESTABLISH-ACK. Call collision resolution shall be achieved by the AN and the LE during this phase of the call.

Path active state (LE4): The active state shall be the state during which normal PSTN signalling functions are active for that port. During this state a user may proceed with call establishment, communication or call clearing.

Path disconnect request state (LE5): The LE requested the AN to release the path. This state shall be exited when the AN has successfully acknowledged the DISCONNECT. If this does not happen, the maintenance entity shall be informed.

Port blocked state (LE6): This state can be entered from any state. Once entered, the only state that the interface may proceed to shall be the NULL state when the port is again available for service.

Once the blocked state has been entered all call activity for that port shall be halted.

A.2.2 Definition of PSTN protocol primitives, messages and timers

Tables A.1 and A.2 define the primitives, messages and timers used for the PSTN state transitions in EN 300 324 [21], tables 29 and 30. The PSTN Function Element (FE) primitives are to be used either inside the AN between the PSTN protocol entity and the user port or inside the LE between the PSTN protocol entity and the National Protocol entity.

Table A.1: Primitives, messages and timers used in the AN (PSTN) FSM

Name	Direction	Description
FE-line_information	PSTN_AN <-- SUB	The subscriber line status has changed.
FE-line_signal	PSTN_AN <-> SUB	The subscriber has applied an electrical condition to the port or change the electrical condition of the subscriber port.
FE-subscriber_release (e.g. on hook)	PSTN_AN <-- SUB	The subscriber indicates release during initiation of the PSTN path.
FE-subscriber_seizure (e.g. off hook)	PSTN_AN <-- SUB	Subscriber wishes to originate a PSTN path.
DISCONNECT	PSTN_AN <-> PSTN_LE	Initiation of clearing the path.
DISCONNECT COMPLETE	PSTN_AN <-> PSTN_LE	Positive response to path clearing.
ESTABLISH	PSTN_AN <-> PSTN_LE	Initiation of PSTN path.
ESTABLISH ACK	PSTN_AN <-> PSTN_LE	Positive response to PSTN path initiation.
PROTOCOL PARAMETER	PSTN_AN <-- PSTN_LE	A request to change a PSTN port parameter.
SIGNAL	PSTN_AN <-> PSTN_LE	An electrical condition described in a message.
SIGNAL ACK	PSTN_AN <-> PSTN_LE	Acknowledgement of sent/received signal messages.
STATUS ENQUIRY	PSTN_AN <-- PSTN_LE	Request of PSTN port status.
STATUS	PSTN_AN --> PSTN_LE	Report of PSTN port status.
timeout T1/T2	AN internal	Timer T1 or T2 has expired.
timeout T3	AN internal	Timer T3 has expired.
timeout Tr	AN internal	Timer Tr has expired.
timeout Tt	AN internal	Timer Tt has expired.
MDU-CONTROL (port blocked)	PSTN_AN <-- SYS	The AN system management indicates to block the subscriber port in the AN.
MDU-CONTROL (port unblocked)	PSTN_AN <-- SYS	The AN system management indicates to unblock the subscriber port in the AN.
MDU-CONTROL (restart request)	PSTN_AN <-- SYS	The AN system management requests a restart of the PSTN protocol entity.
MDU-CONTROL (restart complete)	PSTN_AN <-- SYS	The AN system management indicates that the restart procedure is completed.
MDU-CONTROL (restart ack)	PSTN_AN --> SYS	Positive response to restart request.
MDU_error_indication	PSTN_AN --> SYS	Indication of error condition in AN.
NOTE: SUB = subscriber port; SYS = AN system management. PSTN_AN = PSTN protocol entity in the AN. PSTN_LE = PSTN protocol entity in the LE.		

Table A.2: Primitives, messages and timers used in the LE (PSTN) FSM

Name	Direction	Description
FE-disconnect_request	PSTN_LE <-- NAT	The national protocol requests clearing of the PSTN path.
FE-disconnect_complete_ request	PSTN_LE <-- NAT	The national protocol requests that an acknowledgement of line-information is sent.
FE-establish_acknowledge	PSTN_LE <-- NAT	Positive response from the national protocol to request for a PSTN path.
FE-establish_request	PSTN_LE <-- NAT	The national protocol requests establishment of a PSTN path.
FE-line_signal_request	PSTN_LE <-- NAT	The national protocol requests an electrical condition to be applied to the subscriber's port in the AN.
FE-protocol_parameter_ request	PSTN_LE <-- NAT	The national protocol requests that a PSTN protocol parameter is changed.
FE-disc._complete_ind.	PSTN_LE --> NAT	Indication that the PSTN path has been cleared completely.
FE-establish_indication	PSTN_LE --> NAT	Report of a request to initiate a PSTN path.
FE-establish_ack_ind.	PSTN_LE --> NAT	Positive response to a request to initiate a PSTN path.
FE-line_signal_indication	PSTN_LE --> NAT	Report that the electrical conditions have changed at the subscriber's port in the AN.
DISCONNECT	PSTN_LE <-> PSTN_AN	Initiation of clearing the PSTN path.
DISCONNECT COMPLETE	PSTN_LE <-> PSTN_AN	Positive response to a path clearing.
ESTABLISH	PSTN_LE <-> PSTN_AN	Initiation of PSTN path.
ESTABLISH ACK	PSTN_LE <-> PSTN_AN	Positive response to path initiation.
SIGNAL	PSTN_LE <-> PSTN_AN	An electrical condition described in a message.
SIGNAL ACK	PSTN_LE <-> PSTN_AN	Acknowledgement of sent/received signal messages.
STATUS	PSTN_LE <-- PSTN_AN	Report of PSTN status.
STATUS ENQUIRY	PSTN_LE --> PSTN_AN	A request for a report of PSTN port state.
PROTOCOL PARAMETER	PSTN_LE --> PSTN_AN	A request to change a PSTN port parameter.
timeout T1	LE internal	Timer T1 has expired.
timeout T3	LE internal	Timer T3 has expired.
timeout T4	LE internal	Timer T4 has expired.
timeout Tr	LE internal	Timer Tr has expired.
timeout Tt	LE internal	Timer Tt has expired.
MDU-CONTROL (port blocked)	PSTN_LE <-- SYS	The LE system management indicates to block a PSTN port in the LE.
MDU-CONTROL (port unblocked)	PSTN_LE <-- SYS	The LE system management indicates to unblock a PSTN port in the LE.
MDU-CONTROL (restart request)	PSTN_LE <-- SYS	The LE system management requests a restart of the PSTN protocol entity.
MDU-CONTROL (restart complete)	PSTN_LE <-- SYS	The LE system management indicates that the restart procedure is completed.
MDU-CONTROL (restart ack)	PSTN_LE --> SYS	Positive response to a restart request.
MDU-error_indication	PSTN_LE --> SYS	Indication of error condition at the LE.
NOTE: NAT = national Protocol; SYS = LE system management. PSTN_AN = PSTN protocol entity in the AN. PSTN_LE = PSTN protocol entity in the LE.		

A.3 PSTN protocol message definition and content

A complete set of messages for the PSTN protocol is given in table A.3.

Table A.3: Messages for PSTN protocol control

Message type	Reference
ESTABLISH	13.3.1
ESTABLISH ACK	13.3.2
SIGNAL	13.3.3
SIGNAL ACK	13.3.4
STATUS	13.3.5
STATUS ENQUIRY	13.3.6
DISCONNECT	13.3.7
DISCONNECT COMPLETE	13.3.8
PROTOCOL PARAMETER	13.3.9

In the following clauses, the different messages are specified highlighting the functional definition and information content (i.e. semantics) of each message. Each definition includes:

a) a brief description of the message, direction and use;

b) a table listing the information elements in the order of their appearance in the message (same relative order for all message types). For each information element the table indicates:

1) the clause of EN 300 324-1 [12] describing the information element;

2) the direction in which it may be sent; i.e. AN-to-LE, LE-to-AN, or both;

3) whether inclusion is mandatory ("M") or optional ("O");

4) the length of the information element in octets.

Refer to EN 300 324-1 [12] annex G for further information about the FE primitives used in the AN and LE.

A.3.1 ESTABLISH message

The ESTABLISH message shall be used as an indication of either an originating or terminating path request.

Table A.4: ESTABLISH message content

Message Type: ESTABLISH
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Line-information	13.4.6.2	AN to LE	O	1
Autonomous-signalling-sequence	13.4.6.4	LE to AN	O	1
Cadenced-ringing	13.4.7.2	LE to AN	O	3
Pulsed-signal	13.4.7.3	LE to AN	O	3 to 5
Steady-signal	13.4.7.4	Both	O	3
NOTE: Only one of the optional information elements may be contained in the message.				

A.3.2 ESTABLISH ACK message

The ESTABLISH ACK message shall be used to acknowledge that the requested action has been performed by the entity. Reference is made to EN 300 324-1 [12], clause D.10, concerning a special procedure for the cases where a signal information element was contained in the ESTABLISH message.

Table A.5: ESTABLISH ACK message content

Message Type: ESTABLISH ACK
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Autonomous-signalling-sequence	13.4.6.4	LE to AN	O	1
Pulsed-signal	13.4.7.3	Both	O	3 to 5
Steady-signal	13.4.7.4	Both	O	3
NOTE: Only one of the optional information elements may be contained in the message.				

A.3.3 SIGNAL message

The SIGNAL message shall be used to convey the PSTN line conditions to the LE, or to instruct the AN to establish specific line conditions.

Table A.6: SIGNAL message content

Message Type: SIGNAL
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Sequence-number	13.4.7.1	Both	M	3
Pulse notification	13.4.6.1	AN to LE	O	1
Autonomous-signalling-sequence	13.4.6.4	LE to AN	O	1
Sequence-response	13.4.6.5	AN to LE	O	1
Cadenced-ringing	13.4.7.2	LE to AN	O	3
Pulsed-signal	13.4.7.3	Both	O	3 to 5
Steady-signal	13.4.7.4	Both	O	3
Digit-signal	13.4.7.5	Both	O	3
Resource-unavailable	13.4.7.10	AN to LE	O	3 to 8
NOTE: Only one optional information element shall be contained in the message and shall be handled as mandatory information element.				

A.3.4 SIGNAL ACK message

The SIGNAL ACK message shall be used to acknowledge SIGNAL and PROTOCOL PARAMETER messages.

Table A.7: SIGNAL ACK message content

Message Type: SIGNAL ACK
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Sequence-number	13.4.7.1	Both	M	3

A.3.5 STATUS message

The STATUS message shall be used to indicate the status of the V5 PSTN protocol entity in the AN. This message shall be sent either on request by a STATUS ENQUIRY message from the LE or when the AN receives an unexpected message from the LE.

Table A.8: STATUS message content

Message Type: STATUS
Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	AN to LE	M	1
L3 address	13.4.3	AN to LE	M	2
Message type	13.4.4	AN to LE	M	1
State	13.4.6.3	AN to LE	M	1
Cause	13.4.7.9	AN to LE	M	3 to 5

A.3.6 STATUS ENQUIRY message

The STATUS ENQUIRY message shall be used to request the status of the V5 PSTN protocol entity in the AN.

Table A.9: STATUS ENQUIRY message content

Message Type: STATUS ENQUIRY
Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	LE to AN	M	1
L3 address	13.4.3	LE to AN	M	2
Message type	13.4.4	LE to AN	M	1

A.3.7 DISCONNECT message

The DISCONNECT message shall be used to indicate that there is no call activity and that the protocol entity in the AN can return to the NULL state or it shall be used by the AN to indicate that the path shall be released.

Table A.10: DISCONNECT message content

Message Type: DISCONNECT
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Steady-signal	13.4.7.4	Both	O	3

A.3.8 DISCONNECT COMPLETE

This message shall be used to acknowledge that the requested action has been performed by the entity.

Table A.11: DISCONNECT COMPLETE message content

Message Type: DISCONNECT COMPLETE
Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	Both	M	1
L3 address	13.4.3	Both	M	2
Message type	13.4.4	Both	M	1
Steady-signal	13.4.7.4	LE to AN	O	3

A.3.9 PROTOCOL PARAMETER

The PROTOCOL PARAMETER message shall be used by the LE to change a protocol parameter in the AN.

Table A.12: PROTOCOL PARAMETER message content

Message Type: PROTOCOL PARAMETER
Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol discriminator	13.4.2	LE to AN	M	1
L3 address	13.4.3	LE to AN	M	2
Message type	13.4.4	LE to AN	M	1
Sequence-number	13.4.7.1	LE to AN	M	3
Recognition-time	13.4.7.6	LE to AN	O	4
Enable-autonomous-acknowledge	13.4.7.7	LE to AN	O	4 to 6
Disable-autonomous-acknowledge	13.4.7.8	LE to AN	O	3
NOTE: At least one optional information element shall be contained in the message. It is only allowed to have one of each information element in the message. When provided these information elements shall be handled as mandatory information elements.				

A.4 General message format and information element coding

This clause defines the message format and the coding of the information elements. For each of the information elements the coding of their different fields is provided. For some information elements (e.g. cadenced-ringing) the code points are not defined (e.g. cadence ringing type) and those code points are left to be nationally specified according to the requirements of the national PSTN protocols.

Within each octet, the bit designated "bit 1" shall be transmitted first, followed by bits 2, 3, 4, etc. Similarly, the octet shown at the top of each figure shall be sent first.

A.4.1 Overview

Within this protocol, every message shall consist of the following parts:

a) protocol discriminator;

b) L3 address;

c) message type;

d) other information elements, as required.

Information elements a), b) and c) are common to all the messages and shall always be present, while information element d) is specific to each message type.

This organization is illustrated in the example shown in figure A.2.

<table>
<tr><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>Octet</th></tr>
<tr><td colspan="8">Protocol discriminator</td><td>1</td></tr>
<tr><td colspan="7">Layer 3 address</td><td>1</td><td>2</td></tr>
<tr><td colspan="8">Layer 3 address (lower)</td><td>3</td></tr>
<tr><td>0</td><td colspan="7">Message type</td><td>4</td></tr>
<tr><td colspan="8">Other information element</td><td>etc.</td></tr>
</table>

Figure A.2: General message organization example

A particular information element shall be present only once in a given message.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. The least significant bit of the field shall be represented by the lowest numbered bit of the highest-numbered octet of the field.

A.4.2 Protocol discriminator

The purpose of the Protocol-discriminator information element is to distinguish messages corresponding to the protocols defined in EN 300 324-1 [12] from others corresponding to other protocols (not defined in EN 300 324-1 [12]) making use of the same data link connection.

NOTE: The Protocol-discriminator information element has been included within the protocol messages for structural compatibility with other protocols (e.g. with ETS 300 102 [6]). It provides a mechanism for being future proof, allowing the future use of the same data link connection for other layer 3 protocols not yet identified.

The protocol discriminator shall be the first element of every message.

The protocol discriminator shall be coded according to table A.13.

Table A.13: Protocol discriminator

Bits								
8	7	6	5	4	3	2	1	Octet
0	1	0	0	1	0	0	0	1
NOTE: All other values are reserved.								

A.4.3 Layer 3 address

The purpose of the L3 address is to identify the PSTN user port at the V5.2 interface to which the particular message applies. The format of the L3 address shall be according to figure A.2. The L3 address shall be coded in binary and all values from 0 to 32 767 shall be valid.

A.4.4 Message type

The purpose of the message type is to identify both, the protocol the message belongs to and the function of the message being sent. Table A.14 defines the coding rules for the various protocol message types required by EN 300 324-1 [12].

Table A.14: Protocol message types

Bits							Protocol message types	Reference
7	6	5	4	3	2	1		
0	0	0	-	-	-	-	PSTN protocol message types	13.3
0	0	1	0	-	-	-	Control protocol message types	14.4

The message type shall be the third part of every message. The PSTN protocol message types shall be coded as shown in table A.15.

Table A.15: PSTN protocol message types

Bits							Message type	Reference
7	**6**	**5**	**4**	**3**	**2**	**1**		
0	0	0	0	-	-	-	Path establishment messages	
0	0	0	0	0	0	0	ESTABLISH	13.3.1
0	0	0	0	0	0	1	ESTABLISH ACK	13.3.2
0	0	0	0	0	1	0	SIGNAL	13.3.3
0	0	0	0	0	1	1	SIGNAL ACK	13.3.4
0	0	0	1	0	-	-	Path clearing messages	
0	0	0	1	0	0	0	DISCONNECT	13.3.7
0	0	0	1	0	0	1	DISCONNECT COMPLETE	13.3.8
0	0	0	1	1	-	-	Other messages	
0	0	0	1	1	0	0	STATUS ENQUIRY	13.3.6
0	0	0	1	1	0	1	STATUS	13.3.5
0	0	0	1	1	1	0	PROTOCOL PARAMETER	13.3.9
NOTE: All other values of PSTN protocol message types are reserved.								

A.4.5 Coding of other information elements

For the coding of the information elements the same rules apply as defined in ETS 300 102-1 [22], clause 4.5.1, without the functionality of the shift information element (there shall be only one codeset).

The information elements are defined in table A.16, which also gives the coding of the information identifier bits.

EN 300 324-1 [12], annex D provides guidelines how to interpret line signals used in a national PSTN protocol into the defined information elements and their coding.

Table A.16: Information element identifier coding

Bits								Name	Reference	Length	TS 101 909 (all parts)
8	7	6	5	4	3	2	1				
1	-	-	-	x	x	x	x	SINGLE OCTET			
1	1	0	0	0	0	0	0	Pulse-notification	13.4.6.1	1	B.4.2.3 - pc
1	0	0	0	x	x	x	x	Line-information	13.4.6.2	1	
1	0	0	1	x	x	x	x	State	13.4.6.3	1	
1	0	1	0	x	x	x	x	Autonomous-signalling-sequence	13.4.6.4	1	
1	0	1	1	x	x	x	x	Sequence-response	13.4.6.5	1	
0	-	-	-	-	-	-	-	VARIABLE LENGTH			
0	0	0	0	0	0	0	0	Sequence-number	13.4.7.1	3	
0	0	0	0	0	0	0	1	Cadenced-ringing	13.4.7.2	3	B.4.1 - cr(x)
0	0	0	0	0	0	1	0	Pulsed-signal	13.4.7.3	3 to 5	B.4.2 - ps
0	0	0	0	0	0	1	1	Steady-signal	13.4.7.4	3	B.4.8 - ss
0	0	0	0	0	1	0	0	Digit-signal	13.4.7.5	3	
0	0	0	1	0	0	0	0	Recognition-time	13.4.7.6	4	
0	0	0	1	0	0	0	1	Enable-autonomous-acknowledge	13.4.7.7	4 to 6	
0	0	0	1	0	0	1	0	Disable-autonomous-acknowledge	13.4.7.8	3	
0	0	0	1	0	0	1	1	Cause	13.4.7.9	3 to 5	
0	0	0	1	0	1	0	0	Resource-unavailable	13.4.7.10	3 to 8	
NOTE: All other values are reserved.											

A.4.6 Single octet information elements

A.4.6.1 Pulse-notification

The purpose of the Pulse-notification information element is to indicate to the LE that a certain pulse at the PSTN user port requested by the LE has finished.

The Pulse-notification information element does not contain any specific identification to indicate which pulse has finished.

It is understood that the transmission of this information element shall be the result of the last request in a Pulsed-signal information element or in a digit signal information element from the LE asking the AN for notification.

The Pulse-notification information element shall be coded according to table A.17.

Table A.17: Pulse-notification information element

Bits									TS 101 909-4 [4]
8	7	6	5	4	3	2	1	Octet	
1	1	0	0	0	0	0	0	1	B.4.2.3 - pc

A.4.6.2 Line-information

The purpose of the Line-information information element is to transmit specific information on the subscriber line status from AN to LE whilst there is no signalling path.

The Line-information information element shall be coded according to figure A.2 and table A.18.

Bits								
8	7	6	5	4	3	2	1	Octet
1	0	0	0	Parameter				1

-

Figure A.3: Line-information information element

Table A.18: Coding of parameter

Bits 4 3 2 1	Meaning
0 0 0 0	Impedance marker reset
0 0 0 1	Impedance marker set
0 0 1 0	Low loop impedance
0 0 1 1	Anomalous loop impedance
0 1 0 0	Anomalous line condition received
NOTE: All other values are reserved.	

A.4.6.3 State

The purpose of the State information element is to indicate to the LE the state of the PSTN signalling protocol entity in the AN when requested by the LE.

The length of this information element shall be one octet.

The State information element shall be coded according to figure A.4 and table A.19.

			Bits					
8	7	6	5	4	3	2	1	Octet
1	0	0	1	PSTN FSM state				1

Figure A.4: State information element

Table A.19: Coding of PSTN FSM state

Bits 4 3 2 1	Meaning
0 0 0 0	AN0 - Out of Service
0 0 0 1	AN1 - Null (Idle line)
0 0 1 0	AN2 - AN line seizure - Establish Message Generated to LE
0 0 1 1	AN3 - AN line release prior to Establish Ack from LE
0 1 0 0	AN4 - Line info from AN being processed by LE
0 1 0 1	AN5 - Path active - Call Establish, communication or call clearing
0 1 1 0	AN6 - Port Blocked - Halt call activity - Port may be de-activated (pwr down)
0 1 1 1	AN7 - Disconnect Request - AN to LE
1 1 1 1	reserved

A.4.6.4 Autonomous-signalling-sequence

The purpose of the Autonomous-signalling-sequence information element is to indicate to the AN, that it has to start a particular (pre-defined) signalling sequence autonomously. The autonomous-signalling-sequence information element shall be sent in messages from the LE to the AN only. The signalling sequence to be started shall be indicated by the sequence type.

The autonomous-signalling-sequence shall be coded according to figure A.5.

The sequence type shall be coded in binary.

			Bits					
8	7	6	5	4	3	2	1	Octet
1	0	1	0	Sequence type				1

Figure A.5

Sequence type is a binary number that "points" to a table in the AN to apply a signal to a line with a pre-defined sequence. The IPAT shall establish a table to assign pre-defined Sequence types to NCS text messages.

This table represents National Deviations as defined by the V5 National Protocol Entities and therefore exact mapping between the V5 to NCS protocols cannot be defined in the present document and is left to IPAT vendor to determine based on the Operators National V5 LE Protocol Entity. The key in this mapping is to ensure that the intended V5 Autonomous-signalling-sequence is properly coded to the associated NCS autonomous line treatments.

Sequence type bits					
4	**3**	**2**	**1**	**TS 101 909 Part 4 text message**	**Part 4 reference clause**
0	0	0	0	em	B.4.2.1
0	0	0	1		
0	0	1	0		
0	0	1	1		
0	1	0	0		
0	1	0	1		
0	1	1	0		
0	1	1	1		
1	0	0	0		
1	0	0	1		
1	0	1	0		
1	0	1	1		
1	1	0	0		
1	1	0	1		
1	1	1	0		
1	1	1	1		

Figure A.6: Autonomous-signalling-sequence information element

A.4.6.5 Sequence-response

The purpose of the Sequence-response information element is to give a response back to the LE about the result of the signalling sequence. The sequence-response information element shall be sent in messages from the AN to the LE only. The Sequence-response type indicates a particular (pre-defined) response value. The sequence-response type shall be coded in binary. The sequence-response information element shall be coded according to figure A.7.

				Bits				
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Octet**
1	0	1	1	Sequence-response type				1

Figure A.7

Sequence-response type is a binary number that "points" to a table in the AN to convert a NCS Text message to a pre-defined binary sequence-response type to the LE. The IPAT shall establish a table to assign Sequence-response types to NCS text messages.

This table represents National Deviations as defined by the V5 National Protocol Entities and therefore exact mapping between the V5 to NCS protocols cannot be defined in the present document and is left to IPAT vendor to determine based on the Operators National V5 LE Protocol Entity. The key in this mapping is to ensure that the intended V5 sequence reponse types are properly coded to the associated NCS response requests.

Sequence-response type bits					
4	3	2	1	TS 101 909-4 [4] text message	Part 4 reference clause
0	0	0	0		
0	0	0	1		
0	0	1	0		
0	0	1	1		
0	1	0	0		
0	1	0	1		
0	1	1	0		
0	1	1	1		
1	0	0	0		
1	0	0	1		
1	0	1	0		
1	0	1	1		
1	1	0	0		
1	1	0	1		
1	1	1	0		
1	1	1	1		

Figure A.8: Sequence-response information element

A.4.7 Information elements with variable length format

A.4.7.1 Sequence-number

The purpose of the Sequence-number information element is to communicate a sequence number to the peer entity. The procedures which use this sequence number are specified in clause 13.5.5.

The Sequence-number information element may be sent in both directions, from the LE to the AN or vice-versa.

The Sequence-number information element shall be mandatory for SIGNAL, PROTOCOL PARAMETER and SIGNAL ACK messages and is not allowed in other messages.

The length of the Sequence-number information element shall always be 3 octets.

In SIGNAL and PROTOCOL PARAMETER messages the sequence number contains the send sequence number M(S) (see clause 13.5.5.1.4) and in SIGNAL ACK messages the sequence number contains the receive sequence number M(R) (see clause 13.5.5.1.6).

The sequence number shall be coded in binary.

The Sequence-number information element shall be coded according to figure A.9.

Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Octet**
0	0	0	0	0	0	0	0	1
Length of Sequence-number content								2
1 ext.	Sequence number							3

Figure A.9: Sequence-number information element

A.4.7.2 Cadenced-ringing

The purpose of the Cadenced-ringing information element is to indicate to the AN that ringing with a certain pre-defined cadenced-ringing type shall be started at the PSTN user port. The cadenced-ringing type shall be coded in binary.

The Cadence-ringing information element shall be sent in messages from the LE to the AN only.

The length of the Cadenced-ringing information element shall always be 3 octets.

The Cadence-ringing information element shall be coded according to figure A.10.

Bits									TS 101 909-4 [4]
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Octet**	
0	0	0	0	0	0	0	1	1	
Length of Cadenced-ringing content								2	
1 ext.	Cadenced-ringing type (binary)							3	B.4.1 cr (x) x = Decimal value of binary number

Figure A.10: Cadenced-ringing information element

A.4.7.3 Pulsed-signal

The purpose of the Pulsed-signal information element sent from LE to AN is to indicate to the AN that a certain pulsed signal shall be activated at the PSTN user port.

Table A.20: coding of pulse type (octet 3)

Bits 7 6 5 4 3 2 1	Meaning	TS 101 909 Part 4 clause B.4.2.1
1 1 1 1 1 1 1	Pulsed normal polarity	np
1 1 1 1 1 1 0	Pulsed reversed polarity	rp
1 1 1 1 1 0 1	Pulsed battery on c-wire	
1 1 1 1 1 0 0	Pulsed on hook	lo
1 1 1 1 0 1 1	Pulsed reduced battery	rb
1 1 1 1 0 1 0	Pulsed no battery	nb
1 1 1 1 0 0 1	Initial ring	ir
1 1 1 1 0 0 0	Meter pulse	mpb
1 1 1 0 1 1 1	50 Hz pulse	
1 1 1 0 1 1 0	Register recall (timed loop open)	"Annex A" R: L/hf(N)
1 1 1 0 1 0 1	Pulsed off hook (pulsed loop closed)	lc
1 1 1 0 1 0 0	Pulsed b-wire connected to earth	
1 1 1 0 0 1 1	Earth loop pulse	
1 1 1 0 0 1 0	Pulsed b-wire connected to battery	
1 1 1 0 0 0 1	Pulsed a-wire connected to earth	
1 1 1 0 0 0 0	Pulsed a-wire connected to battery	
1 1 0 1 1 1 1	Pulsed c-wire connected to earth	
1 1 0 1 1 1 0	Pulsed c-wire disconnected	
1 1 0 1 1 0 1	Pulsed normal battery	
1 1 0 1 1 0 0	Pulsed a-wire disconnected	
1 1 0 1 0 1 1	Pulsed b-wire disconnected	

The duration of that pulsed signal shall be indicated by pulse duration type. The pulse duration type points to a pre-defined description which e.g. consists of the time for the pulse in total and the duty cycle.

The suppression indicator (bit 6 and 7 in octet 4) allows the LE to indicate to the AN whether the ongoing pulsed signal shall be suppressed. See EN 300 324-1 [12], annex D and table A.17.

Table A.21: Coding of suppression indicator (octet 4)

Bits 7 6	Meaning
0 0	No suppression
0 1	Suppression allowed by pre-defined V5.2 SIGNAL message from LE
1 0	Suppression allowed by pre-defined line signal from TE
1 1	Suppression allowed by pre-defined V5.2 SIGNAL message from LE or pre-defined line signal from TE

The acknowledge request indicator (bits 6 and 7 in octet 4a) allows the LE to request that the AN notify that a pulsed signal has either begun, ended or one of a sequence of pulses has ended, see table A.22.

Upon receipt of the suppression indicators, the IPAT shall start the suppression process defined in TS 101 909-4 [4], clause B.4.2.7. This process achieves the desired suppression functionality with the appropriate NCS text message sequences.

Table A.22: Coding of acknowledge request indicator (octet 4a)

Bits 7 6	Meaning	TS 101 909-4 [4] clause B.4.2.3
0 0	No acknowledgement requested	R: <null>
0 1	Ending acknowledgement requested when finished each pulse	R: pc
1 0	Ending acknowledgement requested when finished all pulses	R: oc
1 1	Start of pulse acknowledgement requested	Apply request indicator acknowledgement towards LE upon receipt of corresponding NCS acknowledgement from MTA "200 OK".

The Number of pulses field contains a number coded in binary which indicates "how many pulses" shall be sent. The value 0 is invalid.

The length of the Pulsed-signal information element may vary from 3 to 5 octets.

If the Pulsed-signal information element is sent from the AN to the LE it corresponds to a pulsed signal at the PSTN user port generated by the subscriber's equipment.

The Pulsed-signal information element shall be coded according to figure A.11and tables 20 to A.22.

Bits									TS 101 909-4 [4]
8	7	6	5	4	3	2	1	Octet	
0	0	0	0	0	0	1	0	1	
Length of Pulsed-signal content								2	
1 ext.	Pulse type (Table A.)							3	
0/1 ext.	Suppression Indicator (table A)		Pulse duration type Binary number points to a table in the IPAT for values of pd and pr					4	B.4.2.4.1 pd B.4.2.4.2 pr Must be used if supplied by LE, otherwise these are Optional parameters per IPAT provisioning or default values will be applied
1 ext.	Acknowledge request indicator (table A)		Number of pulses (binary)					4a	B.4.3 rep=x x = decimal value of binary number

Figure A.11: Pulsed-signal information element

A.4.7.4 Steady-signal

The purpose of the Steady-signal information element is either to indicate to the AN that a certain steady signal shall be activated at the PSTN user port (generated by the AN) or that a particular steady signal transmitted by the subscriber's equipment has been detected at the PSTN user port which shall be reported to the LE.

The length of the Steady-signal information element shall always be 3 octets.

The Steady-signal information element shall be coded according to figure A.12 and table A.23.

Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Octet**
0	0	0	0	0	0	1	1	1
Length of Steady-signal content								2
1 ext.	Steady-signal type							3

Figure A.12: Steady-signal information element

Table A.23: Coding of Steady-signal type (octet 3)

Bits 7 6 5 4 3 2 1	Meaning	TS 101 909-4 [4]
0 0 0 0 0 0 0	Normal polarity	clause B.4.8.1 - np
0 0 0 0 0 0 1	Reversed polarity	clause B.4.8.1 - rp
0 0 0 0 0 1 0	Battery on c-wire	
0 0 0 0 0 1 1	No battery on c-wire	
0 0 0 0 1 0 0	Off hook (loop closed)	clause B.4.8.1 - lc
0 0 0 0 1 0 1	On hook (loop open)	clause B.4.8.1 - lo
0 0 0 0 1 1 0	Battery on a-wire	
0 0 0 0 1 1 1	A-wire on earth	
0 0 0 1 0 0 0	No battery on a-wire	
0 0 0 1 0 0 1	No battery on b-wire	
0 0 0 1 0 1 0	Reduced battery	clause B.4.8.1 - rb
0 0 0 1 0 1 1	No battery	clause B.4.8.1 - nb
0 0 0 1 1 0 0	Alternate reduced power / no power	
0 0 0 1 1 0 1	Normal battery	clause B.4.8.1 - fb
0 0 0 1 1 1 0	Stop ringing	clause B.4.5 - R:<null>
0 0 0 1 1 1 1	Start pilot frequency	
0 0 1 0 0 0 0	Stop pilot frequency	
0 0 1 0 0 0 1	Low impedance on b-wire	
0 0 1 0 0 1 0	B-wire connected to earth	
0 0 1 0 0 1 1	B-wire disconnected from earth	
0 0 1 0 1 0 0	Battery on b-wire	
0 0 1 0 1 0 1	Low loop impedance	
0 0 1 0 1 1 0	High loop impedance	
0 0 1 0 1 1 1	Anomalous loop impedance	
0 0 1 1 0 0 0	A-wire disconnected from earth	
0 0 1 1 0 0 1	C-wire on earth	
0 0 1 1 0 1 0	C-wire disconnected from earth	

A.4.7.5 Digit-signal

The purpose of the Digit-signal information element is either to indicate to the AN that a certain digit shall be sent to the subscribers equipment or that a particular digit transmitted by the subscribers equipment has been detected at the PSTN user port.

The length of the Digit-signal information element shall always be 3 octets.

Within the digit information field the number of pulses received by AN or required to be sent by AN, coded in binary, shall be transmitted. The code with bits 1 to 4 all set to ZERO is invalid.

The digit acknowledge request indicator field allows the LE to request the AN to indicate the ending of the transmission of a digit to the user port (see table A.24for coding). In the AN to LE direction this bit shall always be set to ZERO.

The Digit-signal information element shall be coded according to figure A.13and table A.24.

Bits

8	7	6	5	4	3	2	1	Octet
0	0	0	0	0	1	0	0	1
Length of Digit-signal content								2
1 ext.	Digit ack. req. ind.	Spare		Digit information				3

Figure A.13: Digit-signal information element

Table A.24: Coding of Digit acknowledge request indicator (octet 3)

Bit 7	Meaning	TS 101 909-4 [4]
0	No ending acknowledgement requested	Clause B.4.5 - R:<null>
1	Ending acknowledgement requested when digit transmission is finished	R: oc

Bits 5 and 6 of the third octet shall be set to ZERO.

A.4.7.6 Recognition-time

The purpose of the Recognition-time information element is to indicate to the AN that the recognition time of a certain signal has to be updated.

The length of the Recognition-time information element shall always be 4 octets.

The Recognition-time information element shall be sent in messages from the LE to the AN only.

In the Signal field all codings of signals as specified in table A.20 and table 23 shall be valid.

The duration type field contains an index into a pre-defined table within the AN. The table shall contain the actual value of the duration of the recognition time. The actual value shall be the time the signal shall stay active before being recognized.

The Recognition-time information element shall be coded according to figure A.14.

Bit 7 of the fourth octet shall be set to ZERO.

Bits

8	7	6	5	4	3	2	1	Octet
0	0	0	1	0	0	0	0	1
Length of Recognition-time content								2
1 ext.	Signal (table A.20 or table A.29)							3
1 ext.	Spare	Duration type						4

Figure A.14: Recognition-time information element

A.4.7.7 Enable-autonomous-acknowledge

The purpose of the Enable-autonomous-acknowledge information element is to indicate to the AN that there shall be an autonomous response to a particular line signal produced by the subscribers equipment. This shall be done to ensure that the reaction to that signal will be in time.

The Enable-autonomous-acknowledge information element shall be sent in messages from the LE to the AN only.

The length of the Enable-autonomous-acknowledge information element shall be 4 octets for steady signals or 4 to 6 octets for pulsed signals.

For the Signal field all codings of signals as specified in tables A.20 and A.23 shall be valid.

For the Response field all codings of signals as specified in tables A.20 and A.23 shall be valid.

The Enable-autonomous-acknowledge information element shall be coded according to figure A.15 for steady signal responses and figure A.16 for pulsed signal responses.

Bits 8	7	6	5	4	3	2	1	Octet
0	0	0	1	0	0	0	1	1
Length of Enable-autonomous-acknowledge content								2
1 ext.	Signal (table A.23)							3
1 ext.	Response TS 101 909-4 [4] R: oc							4

Figure A.15: Enable-autonomous-acknowledge information element (response is a steady signal)

Bits 8	7	6	5	4	3	2	1	Octet
0	0	0	1	0	0	0	1	1
Length of Enable-autonomous-acknowledge content								2
1 ext.	Signal (table A.20)							3
1 ext.	Response TS 101 909 Part 4 R: pc							4
0/1 ext.	Suppression Indicator (table A.21)		Pulse duration type (Figure A.)					5
1 ext.	Acknowledge request indicator (table A.22)		Number of pulses (Figure A.)					5a

Figure A.16: Enable-autonomous-acknowledge information element (response is a pulsed signal)

In case the response is a pulsed signal the same rules apply to the pulse duration type, suppression indicator, acknowledge request indicator and number of pulses field as specified for the Pulsed-signal information element in EN 300 324-1 [12], clause 13.4.7.3.

A.4.7.8 Disable-autonomous-acknowledge

The purpose of the Disable-autonomous-acknowledge information element is to indicate to the AN that a previously enabled autonomous acknowledge has to be disabled.

The Disable-autonomous-acknowledge information element shall be sent in messages from the LE to the AN only.

The length of the Disable-autonomous-acknowledge information element shall always be 3 octets.

For the Signal field all codings of signals as specified in tables A.20 and A.23 shall be valid.

The Disable-autonomous-acknowledge information element shall be coded according to figure A.17.

				Bits				
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Octet**
0	0	0	1	0	0	1	0	1
Length of Disable-autonomous-acknowledge content								2
1 ext.	Signal (Table A.19 or A.23)							3

Figure A.17: Disable-autonomous-acknowledge information element

A.4.7.9 Cause

The purpose of the Cause information element is to report to the LE the error condition in the AN.

The Cause information element shall be sent in messages from the AN to the LE only.

The Cause information element for some cause types shall include a diagnostic field in order to provide additional information related to these cause values. This diagnostic field shall consist of one or two octets, when present, shall be a copy of the received message type identifier that has triggered the sending of the message containing the cause and, when needed, the relevant information element identifier within that message.

The length of the Cause information element may be 3, 4 or 5 octets as indicated in table A.25.

Table A.25: Coding of cause type

Bits **7 6 5 4 3 2 1**	**Meaning**	**Length of inform. element**	**TS 101 909-4 Table 3**
0 0 0 0 0 0 0	Response to STATUS ENQUIRY	3	
0 0 0 0 0 0 1	Protocol discriminator error	3	
0 0 0 0 0 1 1	L3 address error	3	515
0 0 0 0 1 0 0	Message type unrecognized	4	518
0 0 0 0 1 0 1	Out of sequence information element	5	
0 0 0 0 1 1 0	Repeated optional information element	5	
0 0 0 0 1 1 1	Mandatory information element missing	5 (4) (see note 2)	510
0 0 0 1 0 0 0	Unrecognized information element	5	513
0 0 0 1 0 0 1	Mandatory information element content error	5	510
0 0 0 1 0 1 0	Optional information element content error	5	510
0 0 0 1 0 1 1	Message not compatible with path state	4	523
0 0 0 1 1 0 0	Repeated mandatory information element	5	
0 0 0 1 1 0 1	Too many information elements	4	
NOTE 1: All other values reserved. NOTE 2: If the missing information element is an optional one, refer to EN 300 324-1 [12], clause 13.5.2.12, the information element identifier cannot be inserted into the diagnostics. In this case the length of the Cause information element shall be 4 octets.			

When the length of the Cause information element is 3 octets, no diagnostic field shall be included.

When the length of the Cause information element is 4 octets, octet 4 of the Cause information element shall be present, as the diagnostic, specifying the message type identifier of the message triggering the cause.

When the length of the Cause information element is 5 octets, octets 4 and 4a of the Cause information element shall be present, as the diagnostic, specifying the message type identifier and the information element identifier triggering the cause.

The Cause information element shall be coded according to figure A.18 and table A.25.

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	1	0	0	1	1	1
Length of Cause content								2
1 ext.	Cause type (table A.25)							3
0	Diagnostic (message type identifier)							4
Diagnostic (information element identifier)								4a

Figure A.18: Cause information element

A.4.7.10 Resource-unavailable

The purpose of the Resource-unavailable information element is to indicate to the LE that the particular resource which had been requested by that information element copied into the returned Resource-unavailable information element is not available.

The Resource-unavailable information element shall be sent in SIGNAL messages from the AN to the LE only.

The length of the Resource-unavailable information element depends on the length of the information element returned. Therefore it may vary between 3 and 8 octets.

The copy field contains the copy of that information element for which the requested action could not be performed due to the unavailability of resources.

The Resource-unavailable information element shall be coded according to figure A.19.

Bits								
8	7	6	5	4	3	2	1	Octet
0	0	0	1	0	1	0	0	1
Length of resource unavailable content								2
Copy of information element								3
with failed request								n-1
								n

Figure A.19: Resource-unavailable information element

A.5 Caller Identification (CLID)

The IPCablecom Access Network (AN) provides connection between a remote access node (CM/MTA) and the LE over a V5 interface. In this architecture, Caller ID functionality resides in the LE with the exception of an address translation function that must reside in the IPAT/CA.

A.5.1 Caller Identification origination function

When an "On Net" end user requests system resources for an analog POTS connection (CM/MTA detects receiver "Off Hook"), the CM/MTA initiates a connection request identifying the originators IP/Line number address. The IPAT uses the IP/Line number address and an internal translation table to map this IP/Line number address to a provisioned User Port Identification Value. The IPAT sends an "ESTABLISH" message to the LE on the V5 interface. The LE then requests a V5 interface time slot assignment using the BCC Protocol. Based on the User Port Identification Value in the BCC Protocol request the serving LE can then provide Caller Identification information to the terminating terminal ("on net" or "off net") and create its Detailed Call Record (DCR).

A.5.2 Caller Identification delivery function

When an "On Net" end user subscribes to the Caller ID delivery function, the serving LE addresses the end users by using the BCC Protocol with the User Port Identification Value on the V5 interface and provides the originators Caller ID information in the form of an in-band FSK modulated data stream. In this mode the LE has knowledge of the originating call either by inter-actions with a remote LE serving the origination user ("off net" calls) or by the serving LE knowledge of the origination users line number consistent with an "on net" call origination.In this mode of Caller Identification delivery, the IPAT and CM/MTA are required to pass this in-band signalling information as supplied by the serving LE and as addressed via the V5 BCC Protocol with the User Port Identification Value

Optional:

> When an "On Net" end user subscribes to the Caller ID delivery function, the serving LE addresses the end users using the BCC Protocol with the User Port Identification Value on the V5 interface and provides the originators Caller ID information in the form of an in-band FSK modulated data stream. In this mode the LE has knowledge of the originating call either by inter-actions with a remote LE serving the origination user ("off net" calls) or by the serving LE knowledge of the origination users line number consistent with an "on net" call origination.
>
> In this mode of Caller Identification delivery, the IPAT is required to decode and translate the FSK modulated data stream as supplied by the serving LE and as addressed via the V5 BCC Protocol with the User Port Identification Value into a NCS message addressed to the subscribers CM/MTA to locally generate an FSK modulated data stream for delivery on the analog POTS line. This requires the CM/MTA to apply the appropriate line treatment (Provisioned TAS) and ring cadence (LE supplied) with the required timing automously, consistent with a full VoIP system architecture (softswitch). To avoid duplication of the CLID FSK modulation, the IPAT must also subtract the LE supplied FSK modulated data stream from the bearer channel before supplying the bearer channel to the CM/MTA.

In the Downward direction (V5 to IPAT) the following table defines the mapping to NCS from in-band CLI (EN 300 659-3 [14]) for at least the following parameters:

Parameter type	Reference to EN 300 659-3 [14] clause:
Date and Time	5.4.1
Calling Line Identity	5.4.2
Or	
(Reason for absence of Calling Line Identity)	5.4.4
Calling Party Name	5.4.5
Or	
(Reason for absence of Calling Party Name)	5.4.6
Call type	5.4.12
Number of Messages	5.4.14
Message Type	5.2

Annex B (informative): Billing accuracy

B.1 Billing accuracy

The IPCablecom Access Network (AN) provides connection between a remote access node (CM/MTA) and the LE over a V5 interface. In this architecture, Billing Services are performed as part of the LE Functionality. The Billing Call Record is the result of the reported loop state by the IPCablecom Access Network over the V5 Interface to the LE. Therefore, the IPCablecom Access Network must provide timely reporting to the LE of the loop state at the CM/MTA so as to enable accurate billing to be accomplished.

B.1.1 Normal call disconnection

Under normal call termination conditions the CM/MTA will detect the local loop state and send an NCS message to the IPAT. The IPAT must then convert this message into the appropriate loop state message on the V5 Interface.

The time from the detection from the local loop state to the finalization of the billing record is a circuit switched industry specified guidance e.g. 500 ms according to U.K national regulation.

B.1.2 Abnormal call disconnection

Abnormal call disconnection is defined as an autonomous call disconnection by the IPAT that is the result of not receiving the appropriate NCS call disconnection message but where there is reason to believe that the physical or logical connection between the CM/MTA and the IPAT has been lost and the call has been "dropped".

The method for the determination of a "dropped" call is outside of the scope of the present document However, it is necessary to recognize that in networks where redundency is implemented, there is time necessary to re-route the packet streams and during this time the User audio packets may not be delivered to the IPAT. Therefore, these calls may be momentarily interupted but not dropped. This operation defines a "minimum hold up time" to allow for automated Network Re-routing. This time must be balanced against a reasonable "inaccuracy" in the billing time ("maximum hold up time") since the call may still be maintained after the re-routing is complete.

As the result of a network or device failure that results in the loss of User audio packet delivery to the IPAT, the IPAT must send the DISCONNECT or AN FAULT message on the V5 interface no earlier than a provisional "minimum hold up time" after the loss of the User audio packet flow and no later than a provisional "maximum hold up time" after the loss of the User audio packet flow.

NOTE 1: User audio packet flow loss start time shall be defined as the moment of the first expected User audio packet that is not received in sequential order and where no additional User audio packets are received during the "minimum hold up time".

NOTE 2: Abnormal Call Disconnection is an exception event and it is believed it will be viewed as such by Regulators.

NOTE 3: In the case of abnormal call disconnect, the IPAT DISCONNECT or AN FAULT message to the LE (via the V5.2 interface) will cause the the billing record to be finalized in the LE and should initiate a release of all LE resources of the MTA involved in the call.

Annex C (informative): Call flow examples

C.1 Introduction

The following call flows identify messages that are exchanged between the subscriber (SUB), the media terminal adapter (MTA), the cable modem termination system (CMTS), the internet protocol access terminal (IPAT) and the local exchange (LE). The protocols used in these signals are identified in the first part of the message label when appropriate. For example, NCS_RQNT, means that the RQNT message is defined in the NCS protocol. The timers associated with the V5 PSTN signals are defined in EN 300 324-1 [12]. The timers associated with the V5 BCC signals are defined in ETS 300 347-1 [13].

C.2 Call origination

Call origination is the scenario in which the near-end subscriber initiates a call to a telephone user elsewhere.

C.2.1 Origination call flow

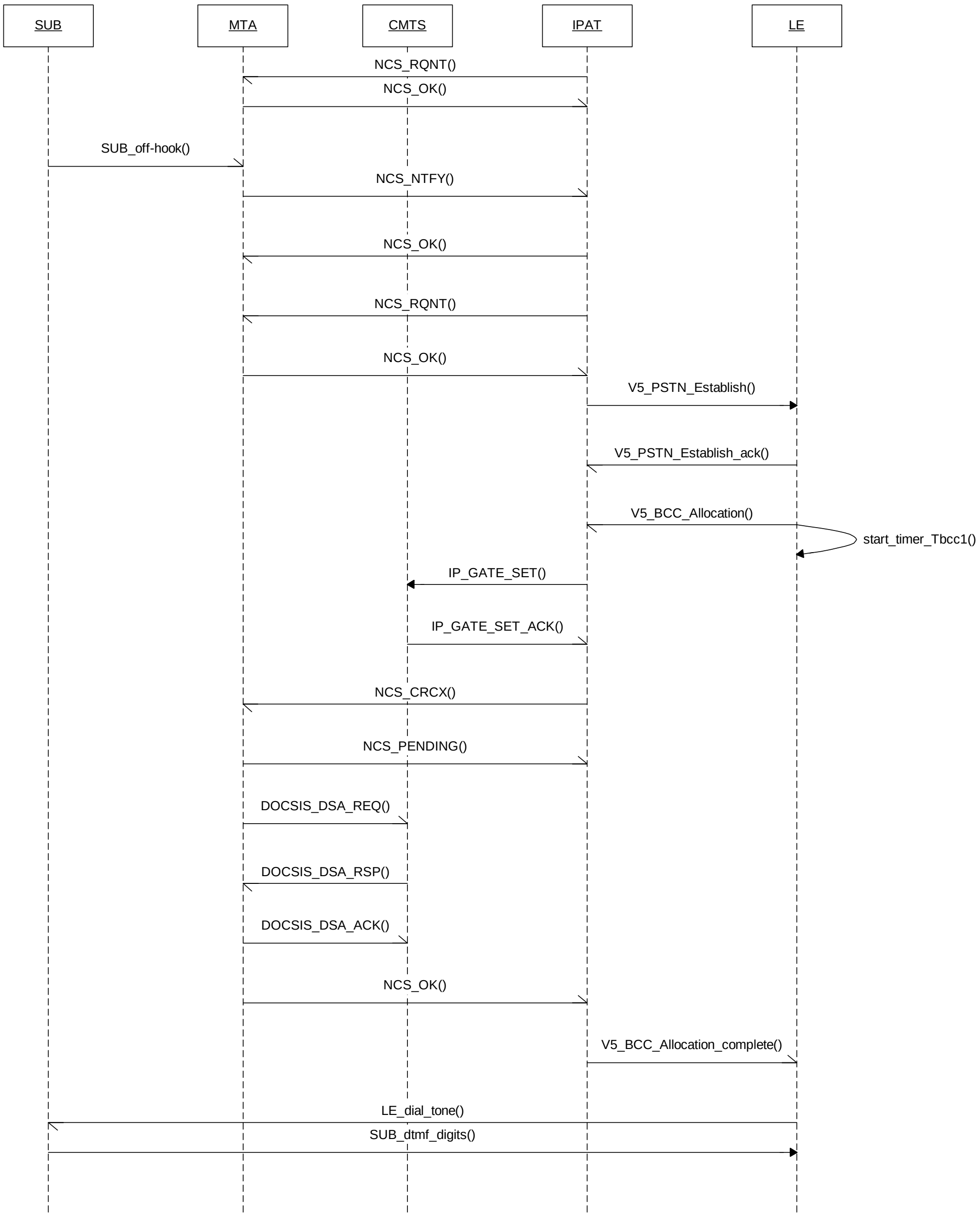


Figure C.1: Call origination

C.2.2 Origination call flow signals description

NCS_RQNT: Before the origination begins, the IPAT has sent a request notify message to the MTA telling it to report off hook signals.

NCS_OK: The MTA acknowledges the request. These first two messages may occur any time before the subscriber goes off-hook.

SUB_off_hook: The subscriber takes the phone off hook.

NCS_NTFY: The MTA sends an NCS message to the IPAT notifying it that it has observed the hang-down (off-hook) event. O: hd.

NCS_OK: The IPAT acknowledges the notification.

NCS_RQNT: The IPAT sends a request to the MTA for notification of hang-ups and of hook-flashes detected by the MTA. R: hu, hf.

NCS_OK: The MTA acknowledges the request.

V5_PSTN_Establish: The IPAT sends a V5 PSTN Establish message to the LE. The Establish message contains the L3 address of the subscriber (the calling party). The IPAT starts timer T1.

V5_PSTN_Establish_ack: The LE sends a V5 PSTN Establish ack message to the IPAT, acknowledging receipt of the Establish message.

V5_BCC_Allocation: The LE sends a V5 BCC Allocation message to the IPAT. The message identifies the bearer channel that the IPAT and LE will use for the media portion of the call. The LE starts timer Tbcc1.

IP_GATE_SET: The IPAT sends a gate_set message to the CMTS over the managed IP network. The message contains the gate ID that the IPAT and the CMTS will use for the call.

IP_GATE_SET_ACK: The CMTS acknowledges the gate_set message.

NCS_CRCX: The IPAT sends a create connection message to the MTA. The message includes the gate ID.

NCS_PENDING: The MTA sends the IPAT a pending message acknowledging that it is working on the creation of the connection.

DOCSIS_DSA_REQ: The MTA sends the CMTS a DSA request. The message includes the gate ID. It is part of the three-way handshake used in the Dynamic Service Addition process.

DOCSIS_DSA_RSP: The CMTS sends the MTA a DSA response. It is part of the three-way handshake used in the Dynamic Service Addition process.

DOCSIS_DSA_ACK: The MTA sends the CMTS a DSA acknowledgement. It is part of the three-way handshake used in the Dynamic Service Addition process.

NCS_OK: The MTA sends the IPAT an NCS OK message, indicating that the connection previously requested has been created.

V5_BCC_Allocation_complete: The IPAT sends a V5 BCC allocation complete message to the LE indicating that the bandwidth for the call has been established.

A two way voice path has now been established. The LE proceeds to send dial tone over this path, and the subscriber, upon hearing the dial tone begins to send DTMF digits toward the LE.

C.3 Call termination

Call termination is the scenario in which the subscriber receives a call which was initiated by a telephone user elsewhere.

C.3.1 Termination call flow

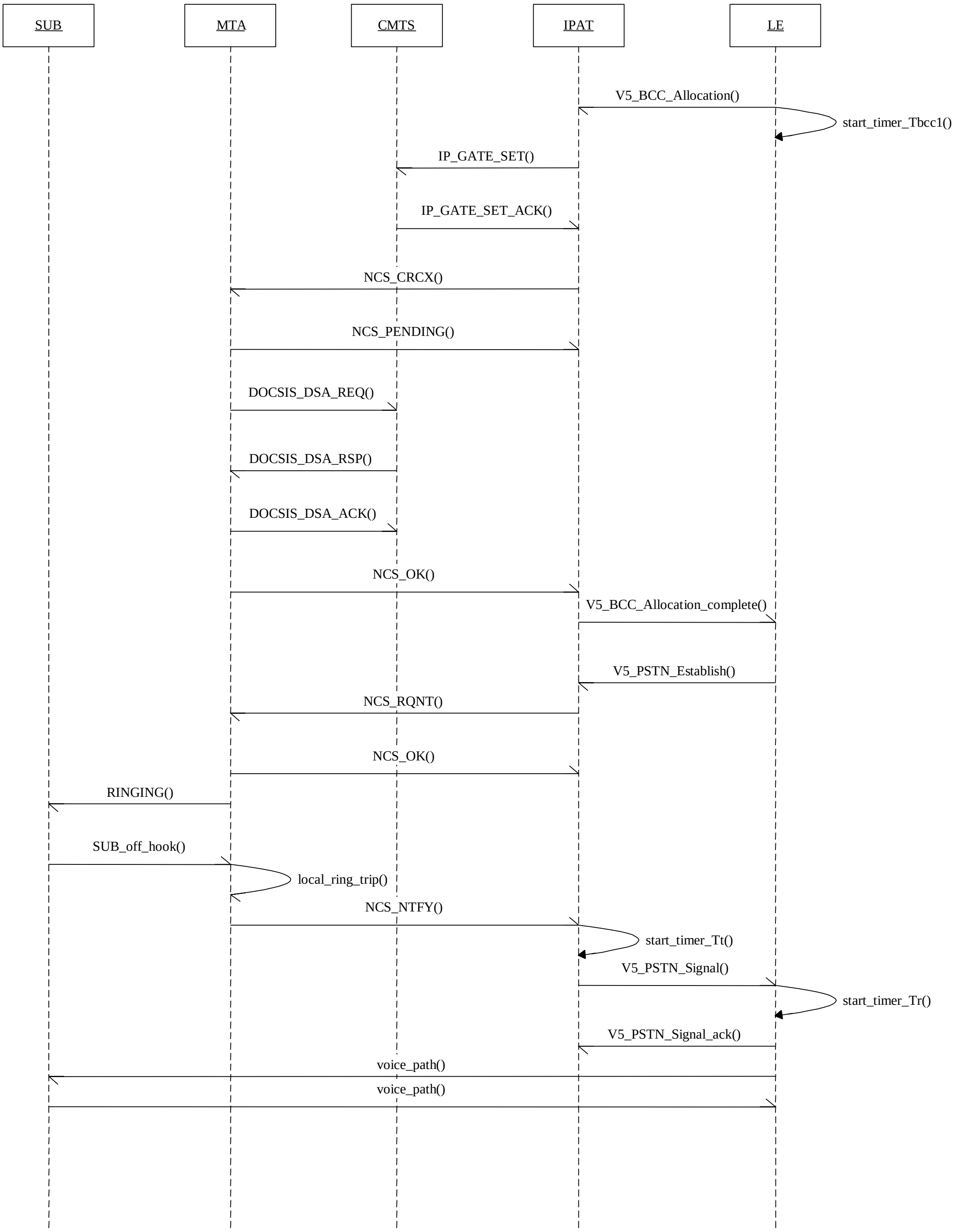


Figure C.2: Call termination

C.3.2 Call termination call flow description

V5_BCC_Allocation: In response to an incoming call from a far-end caller, the LE begins the process of allocating bandwidth for the call by sending the IPAT a V5 BCC Allocation message. The message identifies the time slot which the LE will use for the voice path. The LE also starts timer Tbcc1.

IP_GATE_SET: The IPAT sends a gate_set message to the CMTS over the managed IP network. The message contains the gate ID which the IPAT and the CMTS will use for the call.

IP_GATE_SET_ACK: The CMTS acknowledges the gate_set message.

NCS_CRCX: The IPAT sends a create connection message to the MTA. The message includes the gate ID.

NCS_PENDING: The MTA sends the IPAT a pending message acknowledging that it is working on the creation of the connection.

DOCSIS_DSA_REQ: The MTA sends the CMTS a DSA request. The message includes the gate ID. It is part of the three-way handshake used in the Dynamic Service Addition process.

DOCSIS_DSA_RSP: The CMTS sends the MTA a DSA response. It is part of the three-way handshake used in the Dynamic Service Addition process.

DOCSIS_DSA_ACK: The MTA sends the CMTS a DSA acknowledgement. It is part of the three-way handshake used in the Dynamic Service Addition process.

NCS_OK: The MTA sends the IPAT an NCS OK message, indicating that the connection previously requested has been created.

V5_PSTN_Establish: The LE sends a V5 PSTN establish message to the IPAT. The message contains the L3 address of the called party.

NCS_RQNT: The IPAT sends the MTA a request notify message. The message contains the instruction to ring the subscriber's telephone. S:< ringing signal>. The <ringing signal> used by the IPAT can be an rx signal defined in the L package or a cr(x) signal defined in the E Package. Both packages are described in Part 4 of the IPCablecom suite.

SUB_off_hook: The subscriber takes the telephone off hook. The MTA must stop ringing locally without waiting for a message from the LE.

NCS_NTFY: The MTA sends a notify message to the IPAT, indicating that it has detected the hang-down condition which it was requested to report. O:hd.

V5_PSTN_Signal: The IPAT starts timer Tt and proceeds to send a signal message to the LE. The message notifies the LE that the called party has gone off-hook. Upon receipt of this message, the switch starts timer Tr.

V5_PSTN_Signal_ack: The LE acknowledges receipt of the signal message.

At this point, a two way audio path exists between the calling and the called parties.

C.4 Call Disconnection

C.4.1 Disconnection - call flow

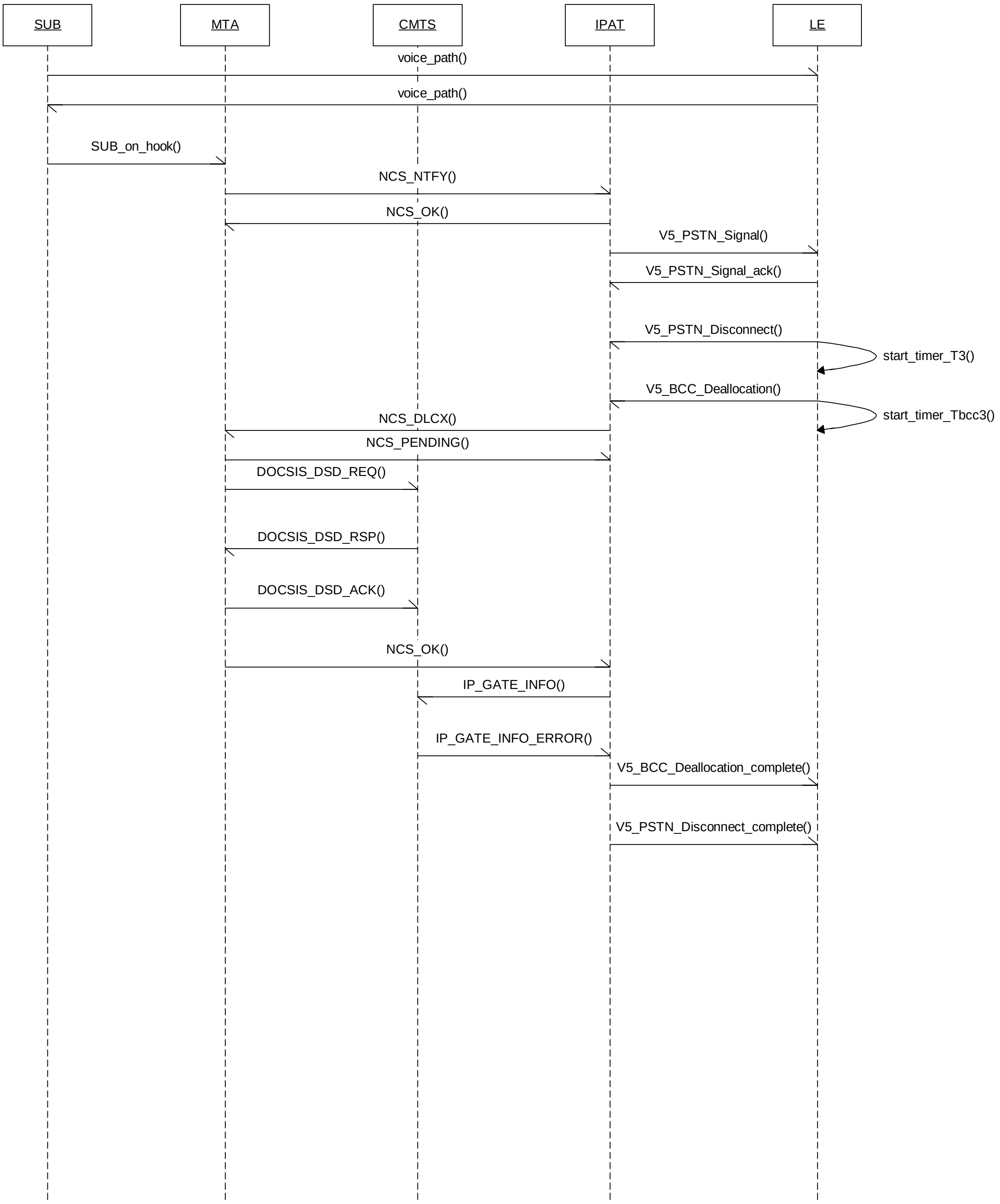


Figure C.3: Call disconnection by subscriber

C.4.2 Disconnection - call flow description

SUB_on_hook: A media path exists between the called and the calling party. The subscriber hangs up the telephone.

NCS_NTFY: The MTA detects the hang-up event and sends a notification to the IPAT as it was previously instructed to do in a RQNT message from the IPAT (not shown here). The NTFY message contains the observed event. O:hu.

NCS_OK: The IPAT acknowledges receipt of the notification.

V5_PSTN_Signal: The IPAT sends a V5.2 PSTN signal message to the LE indicating that the subscriber is on-hook. The message contains the L3 address of the subscriber.

V5_PSTN_Signal_Ack: The LE acknowledges the receipt of this indication.

V5_PSTN_Disconnect: The LE sends a PSTN message to the IPAT instructing it to disconnect the call. The message contains the L3 address of the subscriber. The LE also starts timer T3.

V5_BCC_Deallocation: The LE sends a BCC message to the IPAT instructing it to deallocate bandwidth for the call. The LE also starts timer Tbcc3.

NCS_DLCX: The IPAT sends an NCS delete connection message to the MTA.

NCS_PENDING: The MTA acknowledges receipt of the delete connection and indicates that it is in the process of de-allocating.

DOCSIS_DSD_REQ: The MTA sends a DOCSIS DSD_REQ message to the CMTS. The message identifies the DOCSIS service flow on the HFC which is to be deleted.

DOCSIS_DSD_RSP: The CMTS sends a DOCSIS DSD_RSP message to the MTA. The message is part of the three-way handshake used to delete DOCSIS service flows.

DOCSIS_DSD_ACK: The MTA sends a DOCSIS DSD_ACK to the CMTS. The message is part of the three-way handshake used to delete DOCSIS service flows.

NCS_OK: Once the gate on the DOCSIS network has been deleted, the MTA acknowledges that the delete connection requested by the IPAT has been completed.

IP_GATE_INFO: The IPAT needs to verify that the gate has been deleted. To do so, it sends a gate information request to the CMTS. The request contains the gate ID of the connection that is being deleted.

IP_GATE_INFO_ERROR: The CMTS sends a gate information error message, since it has no record of a gate with the given ID. This is expected behavior. If the IPAT does not receive the error message it will need to take steps to prevent theft of service.

V5_BCC_Deallocation_complete: The IPAT sends a V5 BCC message to the LE indicating that the time slot allocated to the call has been released.

V5_PSTN_Disconnect_complete: The IPAT sends a V5 PSTN message to the LE indicating that the state of the call has been returned to idle.

Annex D (informative): Provisioning of parameters for with and without gate coordination

This annex defines issues on provisioning relating to the Gate Coordination options of LCS.

D.1 Dynamic Quality of Service interface usage

D.1.1 DQoS gate control messaging

LCS IPATs must implement the COPS-based Gate Control interface of the DQoS TS 101 909-5 [5]. The required messages and parameters are enumerated below.

D.1.2 Required gate control messages

The IPAT must implement DQoS messages needed for COPS association initialization and keep-alive, as well as messages necessary for setting and deleting Gates and querying for Gate information. The messages required for use by the IPAT are as follows:

- COPS Association Initialization and Keep-Alive:
  - COPS CLIENT-OPEN (CMTS to IPAT)
  - COPS CLIENT-ACCEPT (IPAT to CMTS)
  - COPS REQUEST (CMTS to IPAT)
  - COPS KEEP-ALIVE (IPAT to CMTS and CMTS to IPAT)
  - DQoS Gate Control:
  - DQoS GATE-SET (IPAT to CMTS)
  - DQoS GATE-SET-ACK (CMTS to IPAT)
  - DQoS GATE-SET-ERR (CMTS to IPAT)
  - DQoS GATE-INFO (IPAT to CMTS)
  - DQoS GATE-INFO-ACK (CMTS to IPAT)
  - DQoS GATE-INFO-ERR (CMTS to IPAT)

D.1.3 Optional gate control messages

The IPAT should implement the following DQoS messages:

- DQoS Gate Control:
  - DQoS GATE-ALLOC (IPAT to CMTS)
  - DQoS GATE-ALLOC-ACK (CMTS to IPAT)
  - DQoS GATE-ALLOC-ERR (CMTS to IPAT)
  - DQoS GATE-DELETE (IPAT to CMTS) (Should Gate Coordintion be used)
  - DQoS GATE-DELETE-ACK (CMTS to IPAT) (Should Gate Coordination be used)
  - DQoS GATE-DELETE-ERR (CMTS to IPAT) (Should Gate Coordination be used)

D.1.4 Gate control object usage

The IPAT must implement the COPS and DQoS objects needed to support the COPS association initialization and keep-alive messages and also the DQoS Gate Control messages specified above. The necessary standard COPS objects must be implemented as specified in the COPS standard. Additional COPS objects specified by TS 101 909-5 [5] for Gate Control must be implemented by the IPAT. These are enumerated below:

Additional COPS Objects for Gate Control

- Transaction-ID
  - Use is per TS 101 909-5 [5]
- Subscriber-ID
  - Use is per TS 101 909-5 [5]
- Gate-ID
  - Use is per TS 101 909-5 [5]
- Activity-Count
  - When used in a GATE-ALLOC or GATE-SET message, this object specifies the number of Gates that can be simultaneously allocated to the indicated Subscriber-ID. When returned in a GATE-ALLOC-ACK or a GATE-SET-ACK it indicates the number of Gates assigned to a single subscriber. Activity-Count is useful for preventing denial of service attacks in that the number of simultaneous open Gates allowed at an MTA can be controlled.

Gate-Spec (two will exist per Gate)

- Direction
  - Use is per TS 101 909-5 [5]
- Protocol-ID
  - Use is per TS 101 909-5 [5]

Flags

- Without Gate Coordination:
    - Use per TS 101 909-5 [5]
- Should Gate Coordination be used:

    0x01 = Auto-Commit, should be set, causes resources to be committed immediately upon reservation, as per TS 101 909-5 [5].

- Session Class
    - 0x01 = Normal priority VoIP session should be used by IPATs
    - Source IP Address
        - Use is per TS 101 909-5 [5]
    - Destination IP Address
        - Use is per TS 101 909-5 [5]
    - Source Port
        - When source is an MTA this should be set to zero (wild-carded) since this information is not available to an IPAT at the time of sending GATE-SET
    - Destination Port
        - When the destination is an MTA this should be set to zero (wild-carded) since this information is not available to an IPAT at the time of sending GATE-SET
    - DS Field
        - Diffserv value as per TS 101 909-5 [5]
    - Timer-T1 value
        - Use is per TS 101 909-5 [5]
    - Timer-T2 value
        - Should be set to zero by the IPAT since T2 timing should not be done with single step reserve and commit
    - Token Bucket Rate [r]
        - Use is per TS 101 909-5 [5]
    - Token Bucket Size [b]
        - Use is per TS 101 909-5 [5]
    - Peak Data Rate [p]
        - Use is per TS 101 909-5 [5]
    - Minimum Policed Unit [m]
        - Use is per TS 101 909-5 [5]
    - Maximum Packet Size [M]
        - Use is per TS 101 909-5 [5]

- Rate [R]
    - Use is per TS 101 909-5 [5]
- Slack Term [S]
    - Use is per TS 101 909-5 [5]

Remote-Gate-Info:

Without Gate Coordination:

- This optional object will not be used for IPAT applications. Its omission implies to the CMTS that no Gate Coordination will be done for this Gate, meaning no Gate-Open or Gate-Close message exchanges should be attempted by the CMTS and the CMTS should not expect to receive such messages from the Gate Controller (i.e. the IPAT).

Should Gate Coordination be used:

- AN-IP-Address
- The IPAT/CMTS Proxy IP-Address with whom Gate Co-ordination is to be done.
- AN-Port
- The IPAT/CMTS Proxy port number for the messages sent for gate co-ordination.
- Flags:
    - 0x0002 = No-Gate-Open, should be set, causes CMTS to skip sending of the Gate-Open message when a Commit is processed

The rest are per TS 101 909-5 [5]

Event-Generation-Info:

- This optional object will not be used for IPAT applications. Omission of this object will indicate that no event generation should be done for this Gate.

NOTE 1: Since all accounting and billing are done by the LE in an IPAT environment, interaction with a Record Keeping Server (RKS) must not be done for IPAT-controlled calls.

Media-Connection-Event-Info

- This optional object will not be used for IPAT application. Its omission implies to the CMTS that Call-Answer and Call-Disconnect event messages are not to be used.

Error

- Use is per TS 101 909-5 [5]

Electronic-Surveillance-Parameters

- This optional object will not be used for IPAT applications.

NOTE 2: Since all electronic surveillance of voice calls is handled by the LE in an IPAT environment, interaction with an Electronic Surveillance Delivery Function must not be done for IPAT-controlled calls.

Session-Description-Parameters

- This optional object will not be used for IPAT applications.

NOTE 3: Since all accounting and billing are done by the LE in an IPAT environment, interaction with a RKS must not be done for IPAT-controlled calls.

Gate-Coordination-Port

- Without Gate Coordination:
    - This optional object will not be used for IPAT applications. Its omission, along with omission of the Remote-Gate-Info object implies to the CMTS that no Gate Coordination will be done for this Gate.
- Should Gate Coordination be used:
    - Use is per TS 101 909-5 [5].

D.1.5 DQoS gate coordination messaging

Without Gate Coordination:

LCS IPATs will not use the RADIUS-based Gate Coordination interface of the specification. It was determined that the functionality existing in the COPS-based Gate Control interface is sufficient for LCS IPATs to prevent all theft and denial of service scenarios that are foreseen.

This recommendation does not change the DQoS requirement on CMTS components, as they still must implement the Gate Coordination interface as part of the full IPCablecom VoIP architecture. However, the CMTS will not be requested to initiate Gate Coordination message exchanges by an IPAT so this part of the DQoS state machine will not be exercised when used with the LCS application.

Should Gate Coordination be used:

The LCS IPAT uses the RADIUS-based Gate Coordination interface of the TS 101 909-5 [5]. A gate is initially created by a GATE-SET command from the IPAT/GC. The GATE-SET command will contain such information as the prototype classifiers and Flowspecs for both the local and remote gates. It also contains the IP address and UDP port number of the IPAT/CMTS Proxy so they can implement Gate-to-Gate co-ordination.

The No-Gate-Open flag in the GATE-SET (Remote-Gate-Info) command should be set, causes CMTS to skip sending of the Gate-Open message when a Commit is processed.

Gate Coordination messages:

- GATE-OPEN (IPAT to CMTS) GATE-OPEN-ACK (CMTS to IPAT)
    - GATE-OPEN-ERR (CMTS to IPAT)
    - GATE-CLOSE (IPAT to CMTS & CMTS to IPAT)
    - GATE-CLOSE-ACK (IPAT to CMTS & CMTS to IPAT)
- GATE-CLOSE-ERR (IPAT to CMTS & CMTS to IPAT)

Annex E (informative): Bibliography

ETSI ES 200 800: "Digital Video Broadcasting (DVB); DVB interaction channel for Cable TV distribution systems (CATV)".

IETF RFC 2212: "Specification of Guaranteed Quality of Service".

IETF RFC 2475 (1998): "An Architecture for Differentiated Service".

IETF RFC 2597 (1999): "Assured Forwarding PHB Group".

IETF RFC 2598 (1999): "An Expedited Forwarding PHB".

IETF RFC 2638 (1999): "A Two-bit Differentiated Services Architecture for the Internet".

IETF RFC 2702 (1999): "Requirements for Traffic Engineering Over MPLS".

IETF RFC 2998: "A Framework for Integrated Services Operation over Diffserv Networks".

IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)".

IETF RFC 3181 (2001): "Signalled Preemption Priority Policy Element".

History

Document history		
V1.1.1	December 2002	Publication