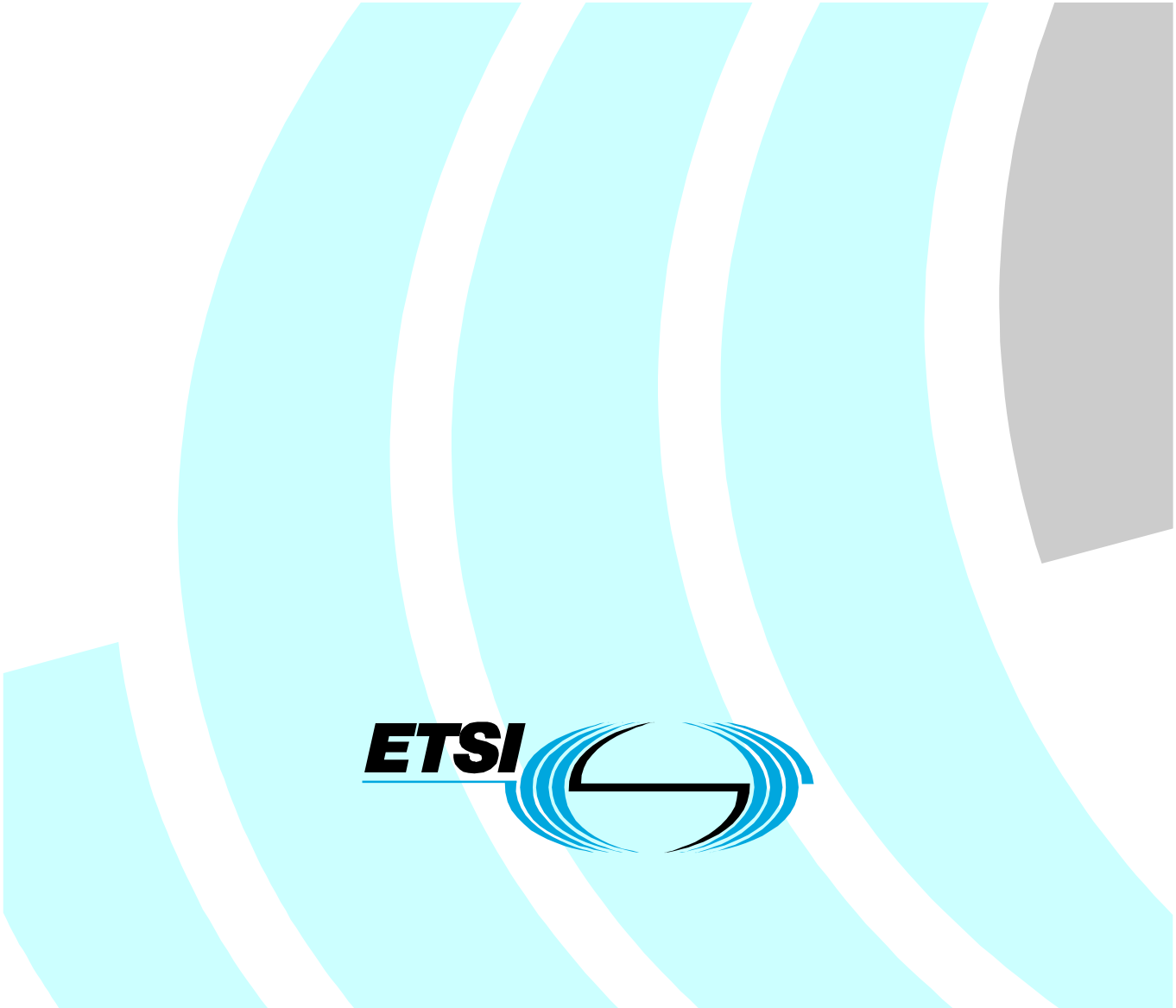
ETSI TR 102 129 V1.1.1 (2003-01)

Technical Report

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Interworking of TIPHON and IPCablecom; Architecture, Protocol, QoS and Security



Reference
DTR/TIPHON-02010

Keywords
architecture, IP, IPCable, protocol, QoS,
telephony, VoIP

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

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

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

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

© European Telecommunications Standards Institute 2003.
All rights reserved.

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

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 Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1 Scope

The objective of ETSI Project TIPHON is the specification of interoperability mechanisms and related parameters to enable multimedia communications (particularly voice) to take place, to a defined quality of service, between Switched Circuit Networks (SCN) and Internet Protocol (IP) based networks and their associated terminal equipment.

The present document presents an overview of the architecture, protocols, QoS and security concepts for the interworking between TIPHON and IPCablecom systems. It introduces a possible framework for convergence between TIPHON and IPCablecom.

Annexes A and B give a general overview of IPCablecom and TIPHON.

Annex C addresses architectural issues for interworking between TIPHON and IPCablecom systems.

Annex D provides information on the protocol aspects relating to TIPHON and IPCablecom system interworking.

Annex E examines TIPHON and IPCablecom QoS Policies, architectures and the control of network resources

Annex F reviews TIPHON and IPCablecom security policies and describes the results of a threat analysis.

2 References

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

[1] ITU-T Recommendation J.160: "Architectural framework for the delivery of time-critical services over cable television networks using cable modems".

[2] ETSI TS 101 882 (V1.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition; General (meta-protocol)".

[3] ETSI TR 101 963: "Access and Terminals (AT); Report on the Requirements of European Cable Industry for Implementation of IPCablecom Technologies; Identification of high level requirements and establishment of priorities".

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

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

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

[7] ITU-T Recommendation Q.767: "Application of the ISDN user part of CCITT signalling system No. 7 for international ISDN interconnections".

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

[9] ETSI EN 300 659-1: "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; Part 1: On-hook data transmission".

[10] ETSI ES 200 778-1: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Protocol over the local loop for display and related services; Terminal Equipment requirements; Part 1: On-hook data transmission".

[11] ETSI ETR 206: "Public Switched Telephone Network (PSTN); Multifrequency signalling system to be used for push-button telephones [CEPT Recommendation T/CS 46-02 E (1985)]".

[12] ETSI EN 300 659-2: "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; Part 2: Off-hook data transmission".

[13] ETSI ES 200 778-2: "Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Protocol over the local loop for display and related services; Terminal Equipment requirements; Part 2: Off-hook data transmission".

[14] ETSI ETS 300 128: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Service description".

[15] ETSI TS 101 909-19 (sub-parts 1 and 2): "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 19: IPCablecom Audio Server Protocol Specification".

[16] IETF RFC 2719: "Framework Architecture for Signalling Transport".

[17] IETF RFC 2960: "Stream Control Transmission Protocol".

[18] ITU-T Recommendation J.165: "IPCablecom signalling transport protocol".

[19] ETSI TS 101 909-12: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 12: Internet Signalling Transport Protocol (ISTP)".

[20] ETSI TR 102 088: "Public Switched Telephone Network (PSTN); Subscriber line protocol for Advice of Charge (AoC) display services".

[21] ETSI TS 101 909-2 (2001): "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".

[22] IETF RFC 1899: "Request for Comments Summary RFC Numbers 1800-1899".

[23] ETSI TS 101 312: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Scenario 1".

[24] ETSI TS 101 909-4: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call Signalling Protocol".

[25] IETF RFC 2705 (1999): "Media Gateway Control Protocol (MGCP) Version 1.0".

[26] IETF RFC 2234 (1997): "Augmented BNF for Syntax Specifications: ABNF".

[27] 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".

[28] IETF RFC 2205 (1997): "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification" (Updated by RFC 2750).

[29] IETF RFC 2748 (2000): "The COPS (Common Open Policy Service) Protocol".

[30] IETF RFC 2210 (1997): "The Use of RSVP with IETF Integrated Services".

[31] ETSI TS 101 329-3 (V1.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); End-to-End Quality of Service in TIPHON Systems; Part 3: Signalling and Control of end-to-end Quality of Service".

[32] ETSI TS 101 909-17: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 17: Inter-domain Quality of Service".

[33] IETF RFC 2543: "SIP: Session Initiation Protocol".

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

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

[36] ETSI TS 101 323: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable security profiles".

[37] ETSI TR 101 771: " Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent requirements definition; Threat Analysis".

[38] ITU-T Recommendation J.170: "IPCablecom security specification".

[39] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[40] ITU-T Recommendation J.162: "Network call signalling protocol for the delivery of time critical services over cable television networks using cable modems".

[41] ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[42] ITU-T Recommendation J.166: "IPCablecom management information base (MIB) framework".

[43] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[44] IETF RFC 1890: "Using the Flow Label Field in IPv6".

[45] ITU-T Recommendation H.248: "Gateway control protocol".

[46] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[47] ETSI TS 101 909-13: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 13: Trunking Gateway Control Protocol".

[48] IEEE 802.2001: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".

[49] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[50] ETSI TS 101 909-9: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 9: Network Call Signalling (NCS) MIB Requirements".

[51] ITU-T Recommendation X.800: "Security architecture for Open Systems Interconnection for CCITT applications".

[52] ITU-T Recommendation X.811: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework".

3 Definitions and abbreviations

3.1 Definitions

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

authentication header: IPSec security protocol that provides message integrity for complete IP packets, including the IP header

Application-Specific Data: application-specific field in the IPSec header that along with the destination IP address provides a unique number for each SA

Baseline Privacy Interface Plus (BPI+): security portion of the ITU-T Recommendation J.112 standard that runs on the MAC layer

Certification Authority (CA): trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates

Call Agent (CA): part of the CMS that maintains the communication state, and controls the line side of the communication

Call Management Server (CMS): controls the audio connections

NOTE: Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.

DiffServ Code Point (DSCP): field in every IP packet that identifies the DiffServ per hop behaviour

NOTE: In IP version 4, the Type Of Service (TOS) byte is redefined to be the DSCP. In IP version 6, the traffic class octet is used as the DSCP.

Hashed Message Authentication Code (HMAC): message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104

Internet Key Exchange (IKE): key management mechanism used to negotiate and derive keys for SAs in IPSec

IKE-: IKE with pre-shared keys for authentication

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

Message Authentication Code (MAC): fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC

Operational Support System (OSS): back-office software used for configuration, performance, fault, accounting, and security management

Public Key Infrastructure (PKI): process for issuing public key certificates, which includes standards, certification authorities, communication between authorities and protocols for managing certification processes

quintet: UMTS authentication vector

Record Keeping Server (RKS): device which collects and correlates the various event messages

Signalling Gateway (SG): signalling agent that receives/sends SCN native signalling at the edge of the IP network

NOTE: In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.

Session Initiation Protocol (SIP): application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants

Signalling System number 7 (SS7): architecture and set of protocols for performing out-of-band call signalling with a telephone network

triplet: GSM authentication vector

Transaction Capabilities Application Protocol (TCAP): protocol within the SS7 stack that is used for performing remote database transactions with a Signalling Control Point

Ticket Granting Server (TGS): sub-system of the KDC used to grant Kerberos tickets

3.2 Abbreviations

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

AN	Access Node
ANC	ANnouncement Controller
ANP	ANnouncement Player
ANS	ANnouncement Server
AOC	Advice Of Charge
API	Application Programming Interface

ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
BNF	Backus-Noun Form
BPI+	Baseline Privacy Interface Plus
BRI	Basic Rate ISDN
C7	Signalling System Number 7
CA	Call Agent
CA	Certification Authority
CC	Call Control
CDR	Call Detail Record
CLIR	COnnected Line Identity Restriction
CM	Cable Modem
CMS	Call Management Server
CMSS	Call Management Server Signalling (CMS to CMS) signalling
CMTS	Cable Modem Termination System
COLP	COnnected Line identity Presentation
COPS	Common Open Policy Service
CS	Circuit Switched
CUG	Closed User Group
DCS	Distributed Call Signalling
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DNS	Domain Name System/Server/Service
DOCSIS	Data Over Cable Service Interface Specification
DSCP	DiffServ Code Point
E-MTA	Embedded MTA
ER	Edge Router
FG	Functional Grouping
GC	Gate Controller
HFC	Hybrid Fibre/Coaxial [cable]
HLR	Home Location Register
HMAC	Hashed Message Authentication Code
HTTP	HyperText Transfer Protocol
ID	IDentifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IN	Intelligent Network
IN	Intelligent Network
IntServ	Integrated Services
IP	Internet Protocol
ISTP	Internet Signalling Transport Protocol
ISUP	Integrated Services digital network User Part
ITSP	IP-Telephony Service Provider
KDC	Key Distribution Centre
LNP	Local Number Portability
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message Digest 5
MF	Multi-Frequency
MG	Media Gateway
MGC	Media Gateway Controller
MGC	Media Gateway Controller
MGCI	Media Gateway Controller Interface
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MMH	Multilinear Modular Hash
MP	Media Player
MPC	Media Player Controller
MPLS	MultiProtocol Label Switching
MSC	Message Sequence Chart

MSC	Message Sequence Charts
MSC	Mobile Services switching Centre
MTA	Multimedia Terminal Adapter
NCS	Network Call Signalling
NTS	Number Translation Services
OSS	Operational Support System
PKI	Public Key Infrastructure
PKINIT	Public Key Cryptography Initial Authentication
PS	Packet Switched
PSTN	Public Switched Telephone Network
PSTN	Public Switched Telephony Network
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
QoS	Quality of Service
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAS	Request Admission Status
RFC	Request For Comments
RKS	Record Keeping Server
RSVP	Resource reSerVation Protocol
RTCP	Real-Time Control Protocol
RTP	Real-Time Transfer Protocol
SA	Source Address
SAP	Service Access Point
SCN	Switched Circuit Networks
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SDL	Specification and Description Language
SDP	Session Description Protocol
SG	Signalling Gateway
SHA-1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol
SIP	Session Initiation Protocol
SIP+	Session Initiation Protocol Plus
S-MTA	Standalone MTA
SNMP	Simple Network Management Protocol
SOCLIR	System Override of Calling Line Identity Restriction
SS7	Signalling System 7
SS7	Signalling System number 7
T	Triplet, GSM authentication vector
TCAP	Transaction Capabilities Application Protocol
TCP	Transmission Control Protocol
TCP	Transport Control Protocol
TD	Timeout for Disconnect
TFTP	Trivial File Transfer Protocol
TGCP	Trunking Gateway Control Protocol
TGS	Ticket Granting Server
TIPHON	Telecommunication and Internet Protocol Harmonization Over Networks
TLV	Type-Length-Value
TMSI	Temporary Mobile Subscriber Identity
TOS	Type of Service
TR	Technical Report
UDP	User Datagram Protocol
USIM	User Services Identity Module
VoIP	Voice over IP

4 Overview

The study was initially conducted to identify what was needed to be done for convergence between IPCablecom and TIPHON. However, it was recognized that this task was extremely ambitious, hence the present document describes an analysis of interworking between IPCablecom and TIPHON.

Three interworking scenarios have been defined, interworking through:

- Switched Circuit Network interfaces.
- Media Gateway Control interfaces.
- Session Initiation Protocol interfaces.

The main issues are addressed in the remainder of clause 4 of the present document.

Of interest are the limitations on end-end QoS and security introduced by interworking between TIPHON and IPCablecom systems.

The three interworking scenarios are summarized in the following clauses.

4.1 Interworking through SCN Interfaces

Both TIPHON and IPCablecom support an SCN interface for basic call. The signalling is done through ISUP whilst the media transfer is either PSTN or IP in the case of TIPHON and only PSTN for IPCablecom at this point in time. It is likely that IPCablecom will evolve to ISDN.

This interworking assumes that TIPHON completes the protocol mapping to ISUP. When the protocol mapping to ISUP is completed, then the TIPHON Release 3 basic call will be supported.

That interworking could be assured either through an actual network which would act as a transit network or without an intermediate network in a piggy back fashion (like a null modem). In the later case, one network plays the role of the PSTN and the other plays its normal role.

The advantage of this interworking through SCN Interfaces approach is that it could be readily available.

The drawbacks of this interworking through SCN Interfaces approach are the weaknesses in terms of loss of capabilities in the areas of security and QoS. ISUP does not offer QoS parameter negotiation and does not support security mechanisms for signalling.

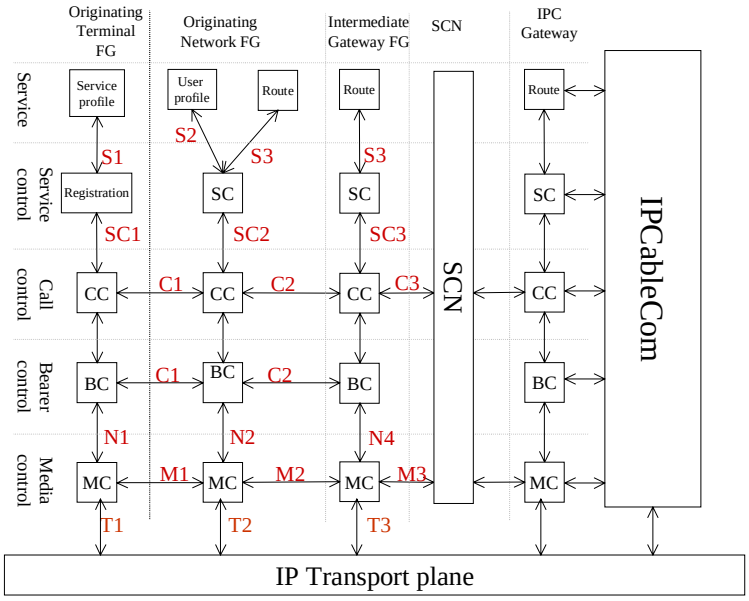


Figure 1: IPCablecom interworking with TIPHON through SCN

4.2 Interworking through MGC interfaces

Both TIPHON and IPCablecom provide Media Gateway Control. However, until recently, IPCablecom is based on MGCP variations and TIPHON is based on H.248. Three interworking scenarios are considered and a proposed way forward is given.

4.2.1 Interworking through MGCP

This is the most controversial scenario from a TIPHON point of view and may not get any support from the TIPHON membership. However, this is of course the most popular way forward within IPCablecom community. This scenario which is recalled at least for completeness and to highlight the opportunities for ETSI and TIPHON in the introduction of some formalism in the definition of MGCP and its variations NCS, TGCP etc. An informative annex gives what it would take to map MGCP into a TIPHON meta-protocol.

In the case where TIPHON undertakes a mapping to MGCP, the interworking would not need to operate through SCN, and would offer some extra capabilities of QoS and security above the case of interworking through ISUP. Whether this approach would ensure convergence as well as interworking is another issue which is addressed in the annexes of the present document.

It is understood that IPCablecom is addressing IP Multimedia in later releases and interworking with TIPHON would fit in with TIPHON Release 5 either through MGCP or H.248 described below.

The following functions are not presently supported in MGCP:

- multimedia;
- multi party (conferencing);
- improved security (IPSEC);
- TCP and SDP transport options;
- formalized extension process for enhanced functionality.

4.2.2 Interworking through H.248

While this is the preferred TIPHON solution, it is still under discussion within the IPCablecom community. IPCablecom has now accepted, with a lot of reluctance, the implementation of H.248 as an option for the case of the Audio Server Protocol. It is assumed that once this conversion specified, elements of code could be used to operate H.248 to interwork with TIPHON.

4.2.3 Interworking through MGCP to H.248 converter

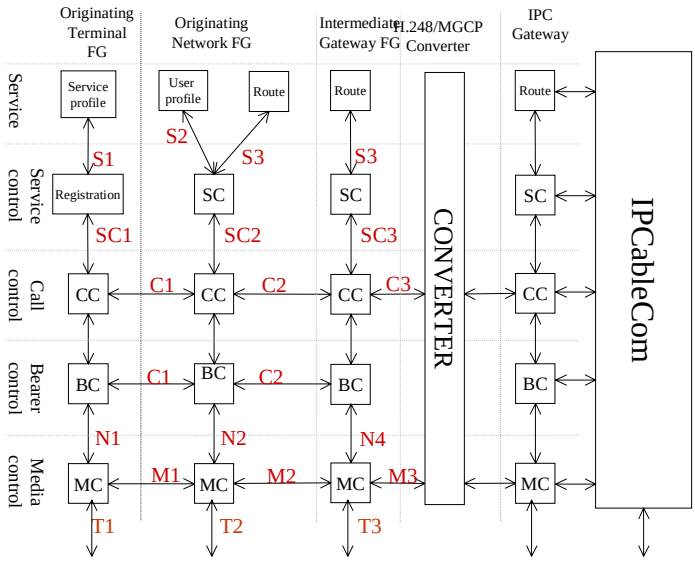
In this case, it is assumed that the IPCablecom network provides the MGCP part and that TIPHON provides the mapping to H.248 meta-protocol.

It is believed that the same implementation can do both protocols.

The converter can:

- either be provided by and within IPCablecom in which case we are back to the case of clause 4.2.2;
- be provided as a separate "box"(or entity); or
- be provided within TIPHON in which case we are back to the case of clause 4.2.1.

NOTE: The conversion is not totally transparent when going from H.248 to MGCP. As TIPHON migrates towards multi-media and/or multi-party calls, the present versions of MGCP will not allow conversion of those functions from Megaco to MGCP.



NOTE 1: The MGCP/H.248 converter could be located either within IPCablecom or within TIPHON.
NOTE 2: Whether MGCP is provided by TIPHON or H.248 does not change the figure.

Figure 2: Interworking between IPCablecom and TIPHON using MGCP/H.248 converter

4.3 Interworking through SIP

In TIPHON, SIP is supported for setting up end-to-end sessions in the IP environment. Though IPCablecom is based on MGCP and its variants for the inner part of the network, an extension based on SIP will likely be developed for network interconnection where two or more IPCablecom networks (not in each others vicinity) need be interconnected. In the version 1.x of the IPCablecom standards, interdomain QoS, where interconnection is over an IP network, is based on RSVP.

Obviously, interconnection of two or more IPCablecom networks can be done by connecting them both to the SCN.

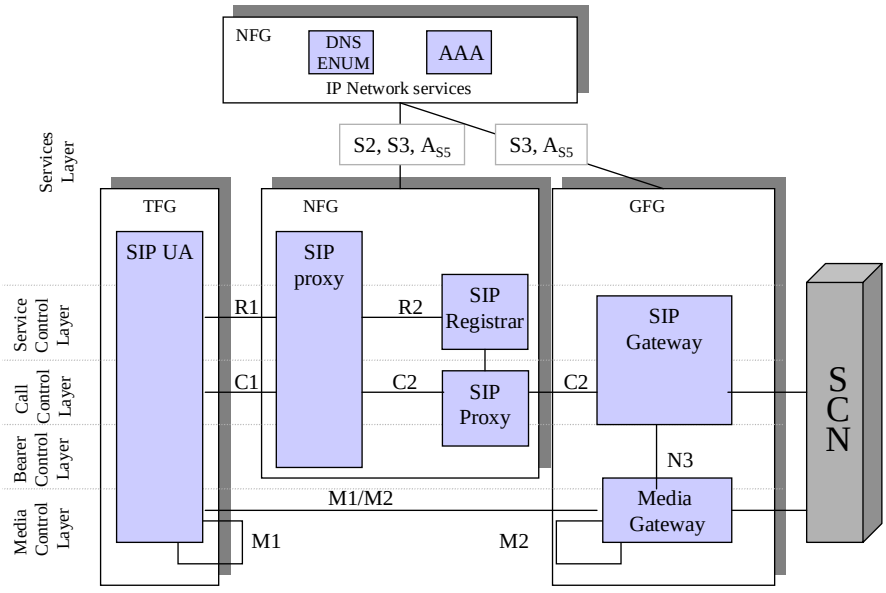


Figure 3: TIPHON model for SIP interface

However, it is possible to interconnect the two domains through a managed IP backbone network, bypassing the SCN completely. In order to support this functionality, IPCablecom is about to introduce an extension in version-2 that supports SIP in the outer part of the network.

As SIP is very well supported by TIPHON, an interconnection model can be derived in which end-to-end connections can be established from the IPCablecom MGCP Gateway to the TIPHON network, using SIP. This model does not require any invocation of the SCN, and implies an all-IP solution for the interconnection of the two networks.

The advantages of interconnecting through SIP are multiple. As the SCN forms an unbreakable barrier for parameter settings related to QoS and Security, a more robust, simpler, and all-IP based solution can be realized by means of interworking through SIP. The end-to-end network can be divided in two major parts, i.e. the IPCablecom part (deploying MGCP variants), and the TIPHON part (deploying SIP). The interface lies within the IPCablecom gateway, where the MGCP is terminated, and an Interface to SIP is provided. As such, IPCablecom has provided two parts f the gateway interface: the SCN interface and the SIP interface.

NOTE: The full functionality of the SIP interface on IPCablecom is not fully known at the time of writing the present document.

With a SIP interconnect, the end-to-end overall voice quality, QoS, and security can be better established and guaranteed than with the SCN as an interconnect means. Less media stream encoding and decoding has to take place. QoS and Security might eventually be established end-to-end, provided that the SIP interface on IPCablecom can.

To take account of and support lawful intercept, billing considerations, dynamic QoS, calling line identification or anonymity, the following extensions to SIP have been felt needed by IPCablecom and are not presently planned in the TIPHON mapping to SIP:

- PRACK (provisional acknowledge);
- COMET (Comit);
- REFER (one agent refers another agent to a third agent);
- SIP Header Extensions:
  - REMOTE-PARTY-ID;
  - DCS-TRACE-PARTY-ID;
  - ANONYMITY;
  - MEDIA AUTHORIZATION;
  - DCS-GATE (block for D-QoS);
  - STATE;
  - RSEQ AND RACK;
  - DCS-BILLING-ID AND DCS-BILLING-INFO;
  - DCS-LAES AND DCS-REDIRECT (LI in Europe);
  - CONTENT-DISPOSITION: PRECONDITION;
- SIP RESPONSE EXTENSIONS:
  - 580 PRECONDITION FAILURE.

(More details on the actual justification of those extensions are given in annex D.)

This proposal to interwork the control planes of both TIPHON and IPCablecom with SIP is also in harmony with ideas on TIPHON interworking with 3GPP.

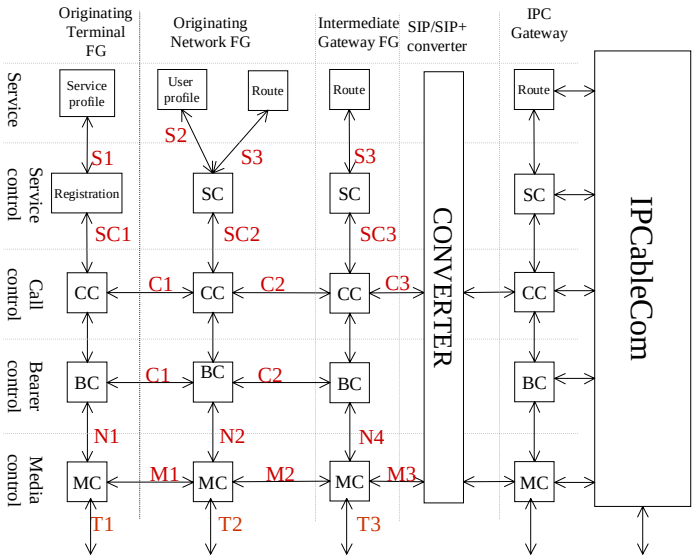


Figure 4: SIP TIPHON to SIP IPCablecom Interworking

5 Conclusions

The present document was initially addressing convergence between TIPHON and IPCablecom. It became apparent that convergence was a formidable task, hence its scope was changed to interworking scenarios between TIPHON and IPCablecom networks. Additionally, it was decided that the material produced during the initial phase of the convergence study should be kept as annexes to the present document.

The following summarizes several important technical areas for TIPHON/IPCablecom convergence.

Interworking of TIPHON release 5 and IPCablecom phase 3 should be the target.

Alignment of supplementary services provided by TIPHON Release 4 and IPCablecom phase 2 should be considered.

An architecture model needs to be developed to indicate the points of interworking if the SIP approach is adopted.

In terms of protocol interworking, SIP is the best candidate assuming that IPCablecom "SIP+" can be mapped into the TIPHON meta-protocol and harmonized with the TIPHON SIP profile.

IPCablecom can greatly benefit from TIPHON competence in the field of QoS. It is recommended that IPCablecom consider improvement of their QoS algorithms for inter domain operations. The principle of protecting the QoS signalling by security mechanisms needs to be addressed by TIPHON with some possible architecture implications.

In terms of security, terminology used in TIPHON and IPCablecom need to be aligned. It is suggested that TIPHON evaluate IPCablecom end to end security algorithm implementations.

Given the broad scope of this study, the identification of further service capabilities relating to IPCablecom may be required in future versions of TIPHON TS 101 878 [49]. These items are expected to cover technology mapping for Call Management Server (CMS) and Network Call Signalling (NCS) with TS 101 882 [2], QoS mapping with TIPHON TS 101 329-3 [31] and updates for IPCablecom Security in TIPHON security related documents.

Annex A: IPCablecom

IPCablecom is an end-to end system for delivery of time-critical communications services, including telephony, to the homes and businesses of cable TV customers and has found wide international support from standards organizations including ETSI, SCTE and the ITU. The system is based on specifications originated in the United States by CableLabs and uses Internet Protocol (IP) and advanced packet transmission to solve the current problems of internet based telephone calls.

IPCablecom is a set of protocols and associated 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.

A.1 IPCablecom phases

A.1.1 Achieved situation

Releases are called phases in IPCablecom jargon.

The first set of documents defines the fundamental requirements necessary to implement a single-zone IPCablecom solution for the residential IP voice services. A typical zone is expected to serve anything from a few tens of thousands to several hundred thousand subscribers. Eventually, the specifications will be developed to enable IPCablecom service providers to interconnect their networks to form a national or even international footprint.

ITU has approved the majority of the first set of IPCablecom documents for worldwide use. ETSI work has been developed in a series of base documents aligned with ITU. ETSI has co-operation agreements with SCTE and ITU and produces European Standards with global relevance.

A.1.2 Possible evolutions

A requirements capture is produced as TR 101 963 [3]. The main input to this TR was provided by ECCA, the European Cable Communications Association. The latest version of the input document can be found on the IPCablecom Website. TS 101 909 (a multi-part document, later to become ES 201 909), is the centrepiece of the ETSI work, to facilitate the implementation in Europe of IPCablecom and is the European contribution to the ITU work. A first set of deliverables has been published. A second set of documents will be published later in the year and will include significant enhancements for the European implementation of this technology. Further documents will be produced during the following year, to extend the capabilities of these systems.

A global team of experts representing all market sectors are working together to add any extensions necessary to support national and regional requirements that may differ slightly from each other, due to the existing infrastructures and standards.

IPCablecom builds upon digital cable modem architectures specified in ITU-T Recommendation J.112 [4] that was developed for global use. These alternative architectures are currently DOCSIS™ and EuroDOCSIS™ as annexed to ES 201 488 [5] and the return channel for cable of the DVB project as in ES 200 800 [6].

A.1.3 Project phases

Phase 1 work covers packetized voice for the single zone. In additions, this work includes European capabilities for V5.2, ISDN and analogue packages (these additions had been identified by the European members of DVB-Packet in parallel within AT-D). ITU-T SG9 Recommendations identified areas for further study.

A summary list is provided below and is extracted from TR 101 963 [3]:

- QoS (same as PSTN, changed from better than PSTN).
- Supporting trunking gateways to PSTN through MGCP; H.248/Megaco is phase 2.

Full support of SS7 signalling protocol including connectivity to STP and SCP for the provision of Number Translation Services (NTS) and other Intelligent Network (IN) facilities.

Within the SS7 ITU-T Recommendation Q.767 [7], i.e. ETSI ISUP V.2, (EN 300 347 [8]) support as required for the particular country.

- V5.2 Gateway connection to PSTN.

An alternative implementation of a PSTN gateway is to use a V5.2 access to the PSTN. In the case, the implementation may be based on the mapping of the NCS protocol to V5.2.

The following supplementary services are to be provided for phase 1; note that this list has to be compared with the TIPHON release 4 list of supplementary services to evaluate interworking with TIPHON.

Classical Services
Abbreviated Dialling / Speed Dialling
Call Wait / Call Hold*
Cancel Call Waiting*
Three-way (or more) Conference Calling*
Wake-up Call
Enhanced Services
Barring all outgoing calls (BAOC) (both operator or user controlled)
Barring outgoing national calls (BONC) (both operator or user controlled)
Barring outgoing international calls (BOIC) (both operator or user controlled)
Barring of premium rate numbers (BPRE) (both operator or user controlled)
Barring of information service numbers (BINF) (both operator or user controlled)
Barring of mobile numbers (BMOB) (both operator or user controlled)
Call forwarding services
Call forwarding unconditional (CFU)
Call forwarding unconditional to voice mail
Call forwarding conditional on busy signal (CFB)*
Call forwarding conditional no reply (CFNR)*
Call forwarding conditional to voice mail on busy signal or no reply
Call forwarding conditional to e-mail (Unified Messaging)
Call forwarding to a default number (CFD) NOTE 1: When the user de-activates CFU, the user line reverts back to CFNR and CFB.
Identification based services
Calling Line Identity Presentation (CLIP), on-hook data transmission* NOTE 2: CLIP functionality should be implemented according to EN 300 659-1 [9], including annex C, ES 200 778-1 [10], including annex A and ETR 206 [11].
Calling Line Identity Presentation (CLIP), off-hook data transmission* NOTE 3: CLIP functionality should be implemented according to EN 300 659-2 [12], ES 200 778-2 [13] and ETR 206 [11].
Calling Line Identity Restriction (CLIR) on a per call basis*
Permanent CLIR (via operator)
Malicious Call Identification (MCID) NOTE 4: This feature should be implemented according to ETS 300 128 [14].
Call completion services
Completion of calls to busy subscriber (CCBS)
Last Number redial

Common functionality
Message waiting indicator (MWI)*
NOTE 1: This facility should be implemented using a stuttered dial tone and/or a visual indication, according to specific operators' or other national requirements.
Other services
Pulse metering
NOTE 2: This feature will require implementation in accordance with country specific regulations.
Emergency call
Anonymous Call Rejection*
Tele/memory message
NOTE 3: Bold features marked with an asterisk (*) have already been specified within IPCablecom ITU-T Recommendation J.160 [1].

Phase 2 work covers additional parts in support of Primary Line services and Interdomain communication between two Cable Operator domains. These early drafts are based on contributions from CableLabs as well as European Cable Vendors and ECCA. These ETSI deliverables are not based on any ITU-T SG9 work. However, it is intended that those drafts be contributed to the work of this phase to ITU-T SG9. Present target for phase 2 implementation is end of 2003.

The following phase 2 content can be extracted from the same TR 101 963 [3].

Fulfilment of EN 300 659-1 [9] requirements to support ES 200 778-1 [10] terminals and enable the implementation of supplementary services (Phase 2).

Call forwarding services
Remotely enabled call forwarding
Call forwarding Indication
Identification based services
Call return with number announcement
Automatic number recall on busy
Call Screening Description: The user will be able to reject calls from a defined list of sources or those that do not present the Calling Line Identity.

NOTE: Phase 2 seems an empty shell.

Phase 3 work is under discussion, and may consider Interdomain communication between IPCablecom Domain and other IP Network Domains (such as TIPHON). Phase 3 implementation is not expected to take place prior to end of 2003.

The content of phase 3 as can be extracted from TR 101 963 [3] is as follow.

Where practicable within the framework of IPCablecom, support of the appropriate protocols defined for SIGTRAN [16] and [17] is seen as a Phase 3 requirement. Interfacing to support these requirements is already under study for annex B of ITU-T Recommendation J.165 [18], shortly to be published as TS 101 909-12 [19].

Identification based services
System Override of Calling Line Identity Restriction (SOCLIR) Description: This feature allows the calling line identity to be presented to emergency services even when restriction is applied to originating line.
COnnected Line identity Presentation (COLP)
COnnected Line Identity Restriction (CLIR)
Vanity numbers using number translation
Other services
Advice Of Charge (AOC) NOTE: This feature should be implemented according to TR 102 088 [20].
Network Announcements
Closed User Group (CUG)
OLI
Dialable number selection
Changeable number selection
Sniffer possibilities based on G10
CTI-functionality
Number Translation Services

Conformance testing specifications are an important part of work in the interest of Operators and Vendors. A consistent set of test specifications can be used to verify that a product conforms to a specification/standard and helps to improve interoperability. The conformance testing work will be performed in parallel to each individual phase.

Annex B:
TIPHON overview

B.1 Recall of scenarios

Scenario 0: IP terminal to IP terminal.

Scenario 1: IP terminal to Circuit Switched.

Scenario 2: Circuit Switched to IP terminal.

Scenario 3: Circuit Switched to Circuit Switched via IP terminal.

B.2 Releases

B.2.1 Content of Release 3

- Service capabilities to support simple call;
- Service independent requirements for service and network management;
- Service independent requirements for the transport plane;
- Amendments of architecture to include lawful interception, security and usage information;
- Extension for Inter Domain services;
- Profiling of key protocols (SIP, H.323, H.248);
- Protocol Independent Framework;
- Choice of identification/contact address;
- Address resolution service;
- QoS Classification;
- QoS Functions & Primitives;
- QoS Control;
- QoS Measurement;
- QoS Design Guidelines;
- Complete set of test specs for H.225.0;
- PICS for H.245 and H.248;
- Interoperability test spec;
- Lawful interception;
- Security profiles.

B.3 Possible evolutions

From recent TIPHON questionnaire survey results, while the content of releases is not frozen yet, the most likely candidates are.

B.3.1 Release 4

The following additional technologies are the most likely candidates to be supported by TIPHON in Release 4:

- Reference Point C2 implementation through BICC CS2.
- Mapping to specific QoS transport protocols (e.g. RSVP/IntServ, DiffServ).
- Extending of the meta-protocols to add QoS support (e.g. SDP).
- Further security support (confidentially, authenticity, non-repudiation).
- Supplementary services description and functional models.

B.3.2 Release 5

The following additional technologies are the most likely candidates to be supported by TIPHON in Release 5:

- Support of multiple media flows and types within a single session to provide Multimedia Service Capabilities.

NOTE 1: TIPHON Release 3 addresses only voice media for telephony applications. However the existing solutions are readily extended to address multi-media applications. This proposal provides this extension.

- Support of multiple endpoints within a single session to provide Multiparty capability.

NOTE 2: TIPHON release 3 is based upon a two party calling model. However the solution is readily extensible into a multi-party solution. This proposal provides this extension.

- Extend the support for confidentiality, authenticity, and non-repudiation within TIPHON systems.

NOTE 3: The existing TIPHON model addresses certain security concerns. This proposal aims to complete the solution set offered by TIPHON in this area.

- Define a framework for the classification of QoS for multimedia services in TIPHON systems.

NOTE 4: TIPHON's existing QoS classification model is based upon voice transmission. As TIPHON extends to consider multi-media services, consideration will have to be given to the QoS aspects of other media types.

- Further the development of a standard interface between service provider and transport network operator for QoS/Firewall/NAT control. In particular, develop transport domain models and procedures for interfacing this standard interface to existing QoS mechanisms such as IntServ/RSVP, DiffServ and MPLS.

NOTE 5: The current TIPHON QoS solution is based upon a push model for establishing end to end QoS. The interfacing of this to standardized QoS mechanisms in underlying networks needs further refinement. This study will also need to consider management issues.

NOTE 6: At this point in time it is understood that the eventual changes to TIPHON to support IPCablecom would be brought as part of the Release 5 definition.

B.4 Relation between TIPHON scenarios and IPCablecom plans

Recall of scenarios.

With reference to the TIPHON scenario and slight variation in the definition:

Scenario 0: IP Terminal to IP Terminal: calls that originate on the cable network and terminate on the cable network within a single IPCablecom zone are supported; calls that originate within one IPCablecom zone and terminate in another IPCablecom zone are for further study and are not presently supported.

Scenario 1: IP Terminal to Circuit Switched: calls that originate from the cable network and terminate on the PSTN are supported.

Scenario 2: Circuit Switched to IP Terminal: calls that originate from the PSTN and terminate on the cable network are supported.

Scenario 3: Circuit Switched to Circuit Switched via IP: calls that originate on the PSTN, transit the IPCablecom network, and terminate on the PSTN are not specifically considered in this architecture and are not presently supported.

The combination of scenarios 1 and 2 lead to the case of IPCablecom interworking with another IPCablecom domain through a SCN domain; this is supported to PSTN and is planned to be supported to ISDN, ATM and possibly others Switched Circuit Network.

Annex C: Architecture

This annex gives guidance on the work to be accomplished for convergence of IPCablecom towards TIPHON in the area of architecture. While architecture convergence is not required to insure interworking, it will improve efficiency of interworking in particular in areas of QoS and security.

C.1 IPCablecom

C.1.1 Base architecture

The essential architecture described in ITU-T Recommendation J.160 [1] appears to be:

a) A layer 2 structure, referred to as the HFC network, which supports layer 3 datagram transfer between edge nodes referred to as MTAs and various internal nodes. (This appears to be specified in ITU-T Recommendation J.112 [4].)

b) An internal telephony structure, misleadingly referred to as the "Managed IP Network", which supports internal provision of PSTN services to terminals connected to MTAs.

c) A gateway function to the rest of the PSTN.

d) An interconnection interface between the IPCablecom component and the rest of the PSTN.

This may be shown as in figure C.1 essential architecture.

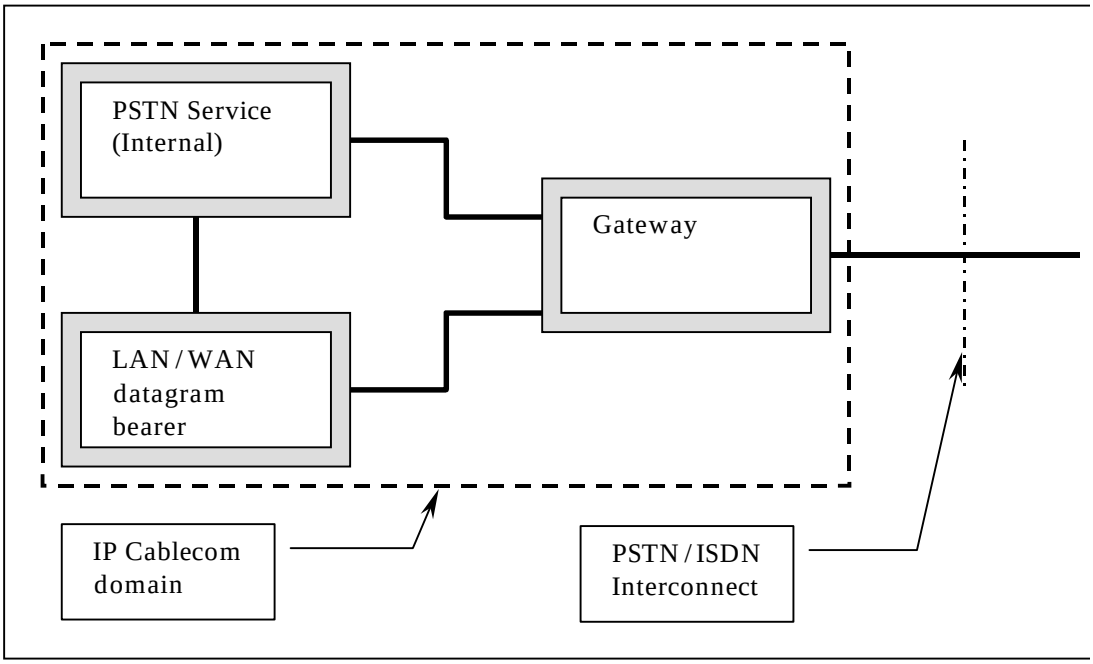


Figure C.1: Essential architecture

At a very high level, the IPCablecom architecture contains three networks: the "J.112 HFC Access Network", the "Managed IP Network" and the PSTN. The Access Node (AN) provides connectivity between the "J.112 HFC Access Network" and the "Managed IP Network". Both the Signalling Gateway (SG) and the Media Gateway (MG) provide connectivity between the "Managed IP Network" and the PSTN. The reference architecture for IPCablecom is shown in figure C.2.

Another way is to see IPCablecom as a combination of three networks:

- an access network;
- a wide area network for media transport;
- a signalling network.

Nowhere is stating that it is TIPHON conformant; or that IPCablecom architecture intends ultimately to evolve to be TIPHON conformant.

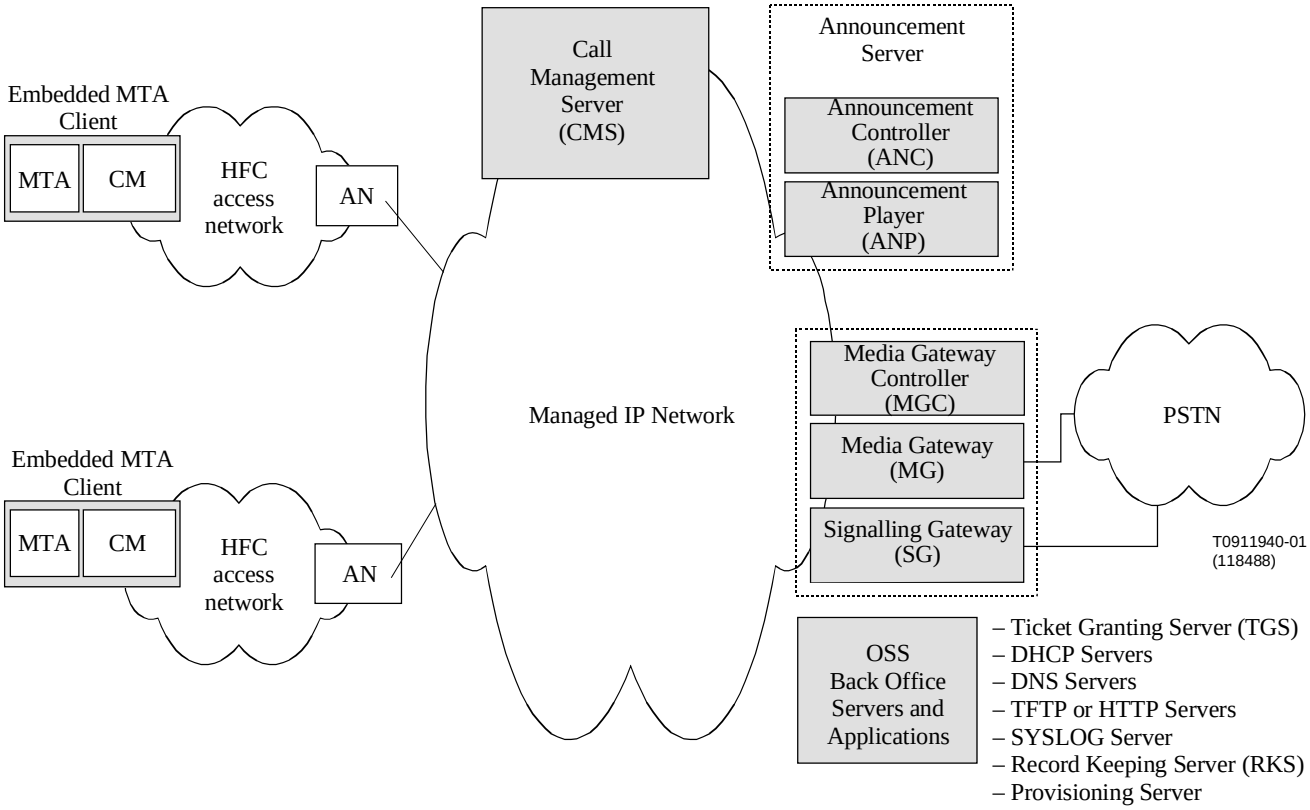


Figure C.2: IPCablecom reference architecture

The HFC access network corresponds to the transport plane of the TIPHON architecture model [2]. The Call Management Server, the Announcement Server and the OSS back office server correspond to the IP Telephony Application plane of the TIPHON Architecture model [2]. The PSTN corresponds to the SCN plane. The Management plane of TIPHON reference model does not seem to appear in the IPCablecom model. In fact, the management plane of IPCablecom is distributed among OSS (mostly for billing) and the other servers for provisioning and error reporting.

The following mapping can be proposed between TIPHON and IPCablecom architecture models in terms of FG (Functional Group):

Terminal Functional Group

- Terminal Functional Group: a Functional Group representing all the IP Telephony functionality within a user's terminal. Terminal Functional Groups may be classified as originating or terminating based upon their location within the topology of a specified call. It is composed in the case of IPCablecom of the MTA, the CM, the HFC and the Access Network.

- The Terminal Registration Functional Group: a Functional Group representing the registration within the User's terminal. The registration is called "provisioning" in the IPCablecom jargon; the function of provisioning is provided jointly by the MTA and the provisioning server.

IPCablecom introduces the concept of trusted and untrusted, untrusted applying to the Terminal FG at the subscriber site.

Network Functional Group

- Network Functional Group: a Functional Group containing the functionality required to establish a call between two terminals, a gateway and a terminal or two gateways. Network Functional Groups may be classified as originating or terminating based upon their location within the topology of a specified call. Is composed of the Call Management Server (CMS) and the Announcement Server, Controller (ANC) and Player (ANP) in the case of IPCablecom.

- Gateway Functional Group: a Functional Group containing the functionality of a Network Functional Group also the functionality necessary to connect calls to the SCN. Gateway Functional Groups may be classified as originating or terminating based upon their location within the topology of a specified call. Is composed of the Media Gateway Controller, the Media gateway and the Signalling Gateway in the case of the IPCablecom.

The Network Functional Group represents all of the functionality of an IP-based application in support of the call. In fixed network environments the originating end-user always has a contract with the service provider controlling the Service Domain containing the Originating Network Functional Group and the terminating user with the service provider controlling the Service Domain containing the Terminating Network Functional Group. For mobility considerations this may not be the case. Therefore Network Functional Groups are further divided into Serving Network Functional Group, Intermediate Network Functional Group and Home Network Functional Groups where these are defined:

- Serving Network Functional Group: a Functional Group that enables Terminal Functional Groups to connect to a service provider.

- The Intermediate (Transit) Functional Group: a Functional Group that connects the Serving Network Functional Group to the Home Network Functional Group. The Intermediate Network Functional Group is only present when the Serving Network Functional Group and the Home Network Functional Group are not directly connected.

- Home Network Functional Group: a Functional Group, which is aware of the service application, subscribed to by the end-user. Home Network Functional Groups may be classified as originating or terminating based upon their location within the topology of a specified call.

The Home Network Functional Group and the Serving Network Functional Group may reside in the same network or in different networks.

In the IPCablecom architecture very little attention is given to mobility excepted the provision of Line Number Portability. Moreover, an IPCablecom network is not presently intended to serve as a transit network between two other networks. In the IPCablecom architecture, the concepts of Serving Network FG, Intermediate FG and Home Network FG do not appear.

C.1.2 Architecture objectives

The following items are not yet handled by the existing documents:

- Mobility is only insured to the limit of LNP Local Number Portability; the subscriber keeps his own number.

- Migration to IPv6? Supports only IPv4?

- Support of SIP appears in CMS which has not yet been contributed into ETSI; IPCablecom uses its own version of SIP which may not be strictly compatible with the SIP version TIPHON is mapping to.

- Management plane is not described.

NOTE: This last item does not distinguish IPCablecom from TIPHON.

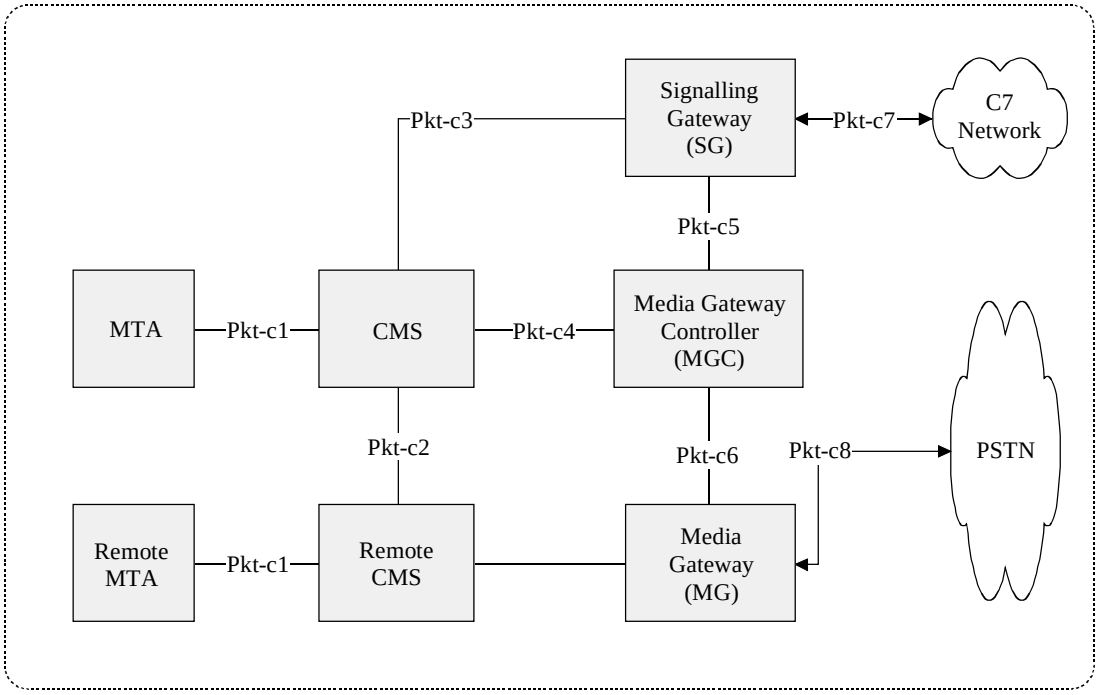
C.1.3 Architecture mapping

In IPCablecom documents, the models are presented in terms of a functional components reference model and not in a layered approach; this is similar to the 3GPP approach. It will take some effort to represent the IPCablecom model in terms of the TIPHON layered architecture. The following figures extracted from the IPCablecom documents show the difficulty of the task; several different interfaces may use the same lower layers and not the same higher layer levels.

NOTE: Those models will be picked up again in each of the documents relating to a specific topic such as protocol, QoS, security.

C.1.3.1 Call Signalling Interfaces

Call signalling requires multiple interfaces within the IPCablecom architecture. These interfaces are identified in figure C.3. Each interface in the diagram is labelled, and further described in the subsequent table C.1.



NOTE: C7 in the above figure means signalling system 7; pkt-c7 means packet cable interface call signalling 7.

Figure C.3: Call signalling interfaces

Table C.1: Call signalling interfaces

Interface	IPCablecom Functional Components	Description	TIPHON equivalent
Pkt-c1	MTA-CMS	Call signalling messages exchanged between the MTA and CMS using the NCS protocol, which is a profile of MGCP.	N/A
Pkt-c2	CMS-CMS	Call signalling messages exchanged between CMS's. The protocol for this interface is undefined.	C2
Pkt-c3	CMS-SG	Call signalling messages exchanged between CMS and SG using the ISTP/TCAP protocol.	C3
Pkt-c4	CMS-MGC	Call signalling messages exchanged between the CMS and MGC. The protocol for this interface is undefined.	CC/BC (Not defined in TIPHON)
Pkt-c5	SG-MGC	Call signalling messages exchanged between the MGC and SG using the ISTP/ISUP and ISTP/TCAP protocol.	C3
Pkt-c6	MGC-MG	Interface for media control of the media gateway and possibly in-band signalling using the TGCP protocol, which is a profile of MGCP, similar to NCS.	N3 (?)
Pkt-c7	SG-C7	The SG terminates physical C7 signalling links from the PSTN (A, F links). The following protocols are supported: • ISUP User Interface. Provides a C7 ISUP signalling interface to external PSTN carriers. • TCAP User Interface. Provides mechanism for certain trusted entities ("TCAP Users") within the IPCablecom network, such as Call Agents, to query external PSTN databases via TCAP messages sent over the C7 network.	M3, C3
Pkt-c8	MG-PSTN	This interface defines bearer channel connectivity from the Media Gateway to the PSTN and supports the following call signalling protocols: • In-Band MF Signalling. A future version of IPCablecom may support ISDN PRI (see note).	M3
NOTE: This function may be viewed as belonging in the Signalling Gateway function.			

C.1.3.2 Media streams

The IETF standard RTP (IETF RFC 1899 [22]) is used to transport all media streams in the IPCablecom network. IPCablecom utilizes the RTP profile for audio and video streams as defined in IETF RFC 1890 [44].

The primary media flow paths in the IPCablecom network architecture are shown in figure C.4 and are further described below.

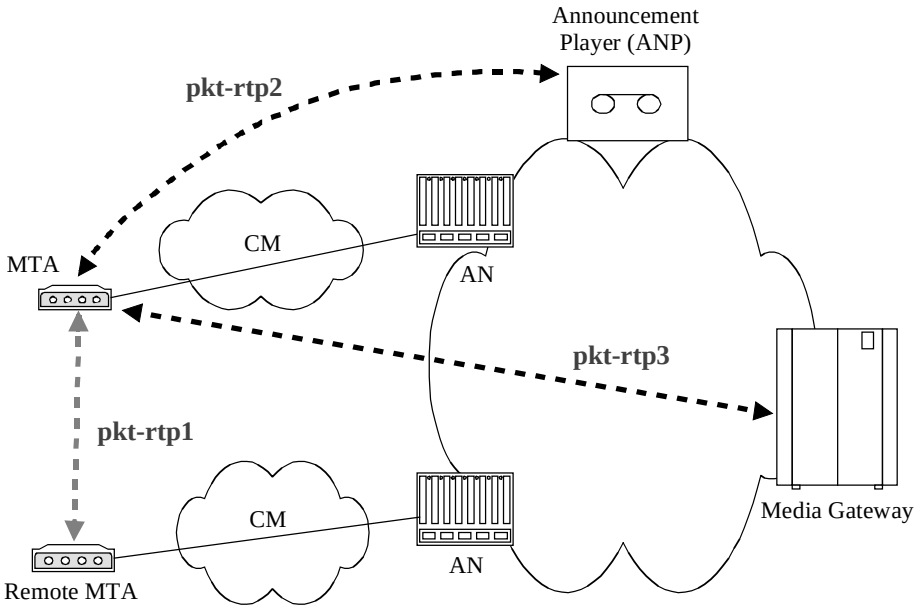


Figure C.4: RTP media stream flows in an IPCablecom Network

Table C.2 gives the main description of the media stream interfaces and their eventual TIPHON counterpart.

Table C.2: Media stream interfaces

Interface	EuroPacket Cable Functional Components	Description	TIPHON equivalent
Pkt-rtp1	local MTA-remote MTA	Media flow between MTAs. Includes, for example, encoded voice, video, and fax.	M1, M2
Pkt-rtp2	MTA-ANP	Media flow between the ANP and the MTA. Includes, for example, tones and announcements sent to the MTA by the Announcement Player.	M2
Pkt-rtp3	MTA-MG	Media flow between the MG and the MTA. Includes, for example, tones, announcements, and PSTN media flow sent to the MTA from the Media Gateway.	M2, M1

C.1.3.3 MTA device provisioning

The scope of MTA Device Provisioning is to enable a MTA to register and provide subscriber services over the HFC network. Provisioning covers initialization, authentication, and registration functions required for MTA device provisioning. The Provisioning Specification also includes attribute definitions required in the MTA configuration file. Figure C.5 shows the provisioning interfaces.

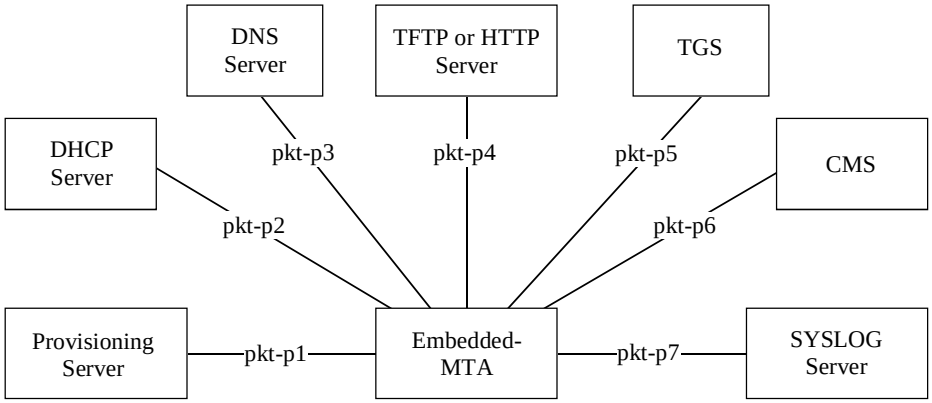


Figure C.5: IPCablecom provisioning interfaces

Table C.3 describes the provisioning interfaces shown in figure C.5.

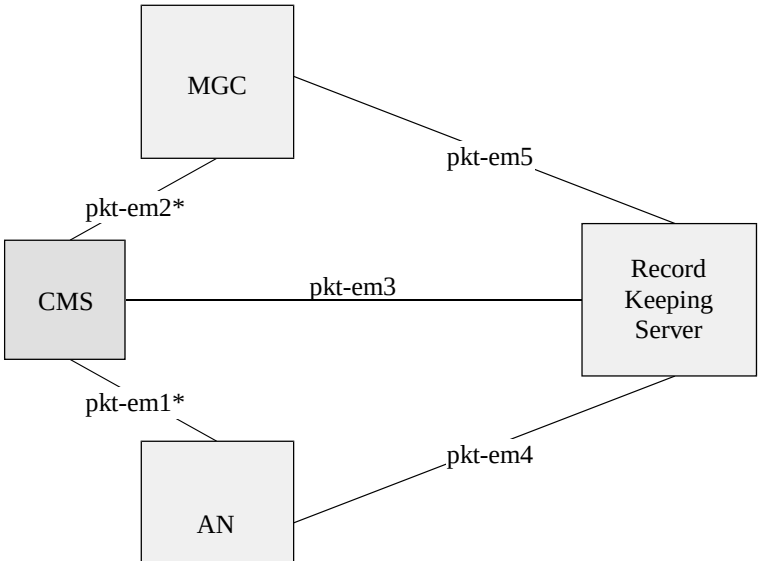
Table C.3: Device provisioning interfaces

Interface	IPCablecom functional components	Description	TIPHON equivalent
Pkt-p1	MTA-PROV Server	Interface to exchange device capability as well as MTA device and endpoint information between the MTA and Provisioning Server using the SNMP protocol. The MTA also sends notification that provisioning has completed along with a pass/fail status using the SNMP protocol.	S1, S2 or S3
Pkt-p2	MTA-DHCP Server	DHCP interface between the MTA and DHCP Server used to assign an IP address to the MTA. If a DNS server is required during provisioning, then the address of this server is also included.	SC1
Pkt-p3	MTA-DNS Server	DNS interface between the MTA and DNS Server used to obtain the IP address of an IPCablecom server given its fully qualified domain name.	?
Pkt-p4	MTA-HTTP or TFTP Server	MTA configuration file is downloaded to the MTA from the TFTP Server or HTTP Server.	S1
Pkt-p5	MTA-TGS	MTA obtains a Kerberos ticket from the Ticket Granting Server using the Kerberos protocol.	S2
Pkt-p6	MTA-CMS	MTA establishes an IPSec Security Association with the CMS using the Kerberos protocol.	SC1, SC2
Pkt-p7	MTA-SYSLOG	MTA sends notification that provisioning has completed along with a pass/fail status to the SYSLOG server via UDP.	?

C.1.3.4 Event Messages

An 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.

This IPCablecom Event Messages specification defines the structure of the Event Message data record and defines RADIUS as the transport protocol. Although the scope of the specification is limited to defining Event Messages for basic residential voice capabilities, it is expected that this specification will be expanded to support additional IPCablecom-based services.



NOTE: * Indicates that the billing correlation ID and other billing data is carried on an existing signalling interface.

Figure C.6: Event message interfaces

Table C.4 describes the Event Message interfaces shown in figure C.6.

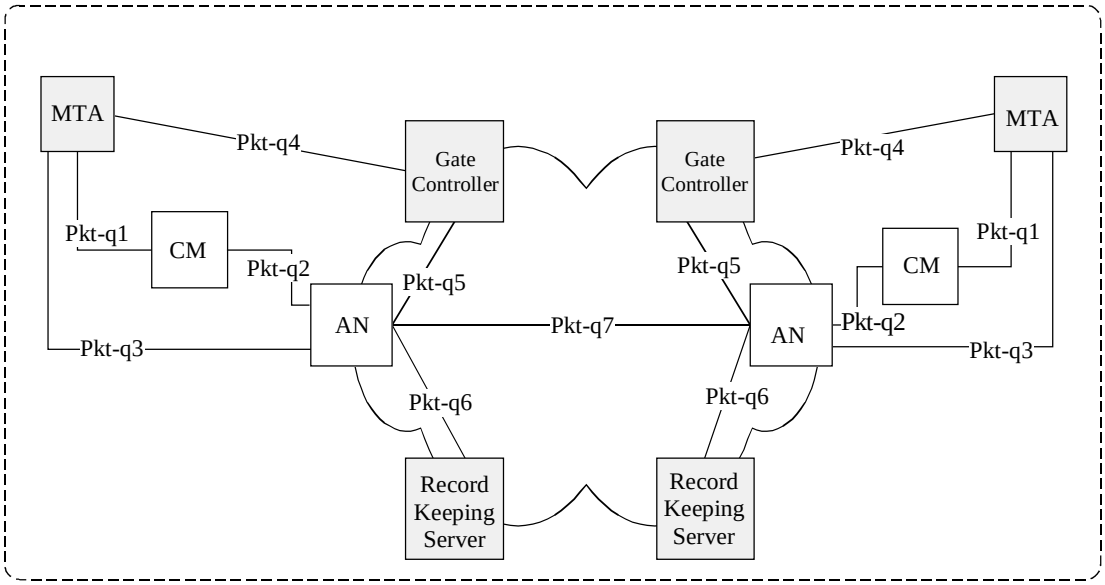
Table C.4: Event message interfaces

Interface	IPCablecom Functional Component	Description	TIPHON equivalent
pkt-em1	CMS-AN	DQoS Gate-Set message carrying Billing Correlation ID and other data required for AN to send Event Messages to an RKS.	AS5
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.	SC2'
Pkt-em3	CMS-RKS	RADIUS protocol carrying IPCablecom Event Messages.	AS5
Pkt-em4	AN-RKS	RADIUS protocol carrying IPCablecom Event Messages.	AS5
Pkt-em5	MGC-RKS	RADIUS protocol carrying IPCablecom Event Messages.	AS5

C.1.3.5 Quality of Service (QoS)

Quality of Service signalling interfaces are defined between many of the components of the IPCablecom network. Signalling may be handled at the application layer (e.g. SDP parameters), network layer (e.g. RSVP), or the data-link layer (e.g. J.112 QoS).

From the perspective of the MTA and its access network the IPCablecom QoS Framework is represented in figure C.7.



NOTE: Gate Controller is a function contained within a CMS node.

Figure C.7: IPCablecom QoS signalling interfaces

Table C.5 briefly identifies each interface and how each interface is used in the Dynamic QoS Specification (DQoS) [27]. Two alternatives are shown: first a general interface that is applicable to either embedded or standalone MTAs; second, an optional interface that is available only to embedded MTAs.

Table C.5: QoS Interfaces for standalone and embedded MTAs

Interface	IPCablecom Functional Components	DQoS Embedded/Standalone MTA	D-QoS Embedded MTA	TIPHON equivalent
Pkt-q1	MTA-CM	N/A	E-MTA, MAC Control Service Interface	N/A
Pkt-q2	CM-AN	J.112 [4], AN-initiated	J.112 [4], CM-initiated	M1
Pkt-q3	MTA-AN	Note RSVP+	N/A	M1
Pkt-q4	MTA-GC/CMS	NCS/DCS	NCS	S4
Pkt-q5	GC-AN	Gate Management	Gate Management	S4
Pkt-q6	AN-RKS	Billing	Billing	AS5
Pkt-q7	AN-AN	Gate Management	Gate Management	SC2'(?)
NOTE: For IPCablecom, only the embedded MTA interfaces as defined in clause 7 of the Dynamic Quality of Service specification [27] are required. The CMTS is not required to support RSVP across the MTA-CMTS interface as defined in DQoS [27], clause 6.				

The function of each QoS interface is further described in table C.6.

Table C.6: QoS interfaces

Interface	IPCablecom functional components	Description	TIPHON equivalent
Pkt-q1	MTA-CM	This interface is only defined for the embedded MTA. The interface decomposes into three sub-interfaces: *Control*: used to manage J.112 [4] service-flows and their associated QoS traffic parameters and classification rules. *Synchronization*: used to synchronize packet and scheduling for minimization of delay 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 ITU-T Recommendation J.112 [4]	N/A
Pkt-q2	CM-AN	This is the J.112 [4] QoS interface (control, scheduling, and transport). It should be noted that, architecturally, control functions can be initiated from either the CM or the AN. However the AN is the final policy arbiter and granter of admission into the J.112 [4] access network. The following capabilities of the J.112 [4] MAC are used within IPCablecom: • Multiple service flows, each with its own class of upstream traffic, both single and multiple voice connections per J.112 [4] service flow. • Prioritized classification of traffic streams to service flows. • Guaranteed minimum/constant bit rate scheduling service. • Constant bit rate scheduling with traffic activity detection service (slow down, speed up, stop, and restart scheduling). • J.112 [4] packet header suppression for increased call density. • J.112 [4] classification of voice flows to service flow. • J.112 [4] synchronization of CODEC to AN clock and Grant Interval. • Two-phase activation of QoS resources. • TOS packet marking at network layer. • Guarantees on delay and jitter. • Internal sub layer signalling between IPCablecom MTA and the CM (embedded MTA). • This interface is further defined in ITU-T Recommendation J.112 [4]	QM1
Pkt-q3	MTA-AN	The interface is used for request of bandwidth and QoS resources related to the bandwidth. The interface runs on top of layer 4 protocols that bypass the CM. As a result of message exchanges between the MTA and AN, service flows are activated using AN-originated signalling on interface PKT-Q2. An enhanced version of RSVP is utilized for this signalling.	QM1
Pkt-q4	MTA -CMS/GC	Signalling interface between the MTA and CMS/GC. Many parameters are signalled across this interface such as media stream, IP addresses, and Codec selection, but it is possible for certain protocols to either derive QoS semantics from the signalling, or to extend the application layer signalling protocol to contain explicit QoS signalling parameters.	QS4
Pkt-q5	CMS/GC-AN	This interface is used to manage the dynamic Gates for media stream bearer channels. This interface enables the IPCablecom network to request and authorize QoS changes without requiring any layer two J.112 [4] access network QoS control functions in MTA. When supporting standalone MTAs no new client-side QoS signalling protocol needs to be designed. The GC/CMS takes responsibility for requesting policy, and the AN takes responsibility for access control and quickly setting up QoS on the J.112 [4] access link.	QS4

Interface	IPCablecom functional components	Description	TIPHON equivalent
Pkt-q6	AN-RKS	This interface is used by the AN to signal to the RKS all changes in call authorization and usage. This interface is defined in the Event Messages specification.	QAS5
Pkt-q7	AN-AN	This interface is used for coordination of resources between the AN of the local MTA and the AN of the remote MTA. The AN is responsible for the allocation and policing of local QoS resources.	QSC2'(?)

C.1.3.6 Announcement services

Announcements are typically needed for calls that do not complete. Additionally, they may be used to provide enhanced information services to the caller. The signalling interfaces to support IPCablecom Announcement Services are shown in figure C.8 and are summarized in table C.7.

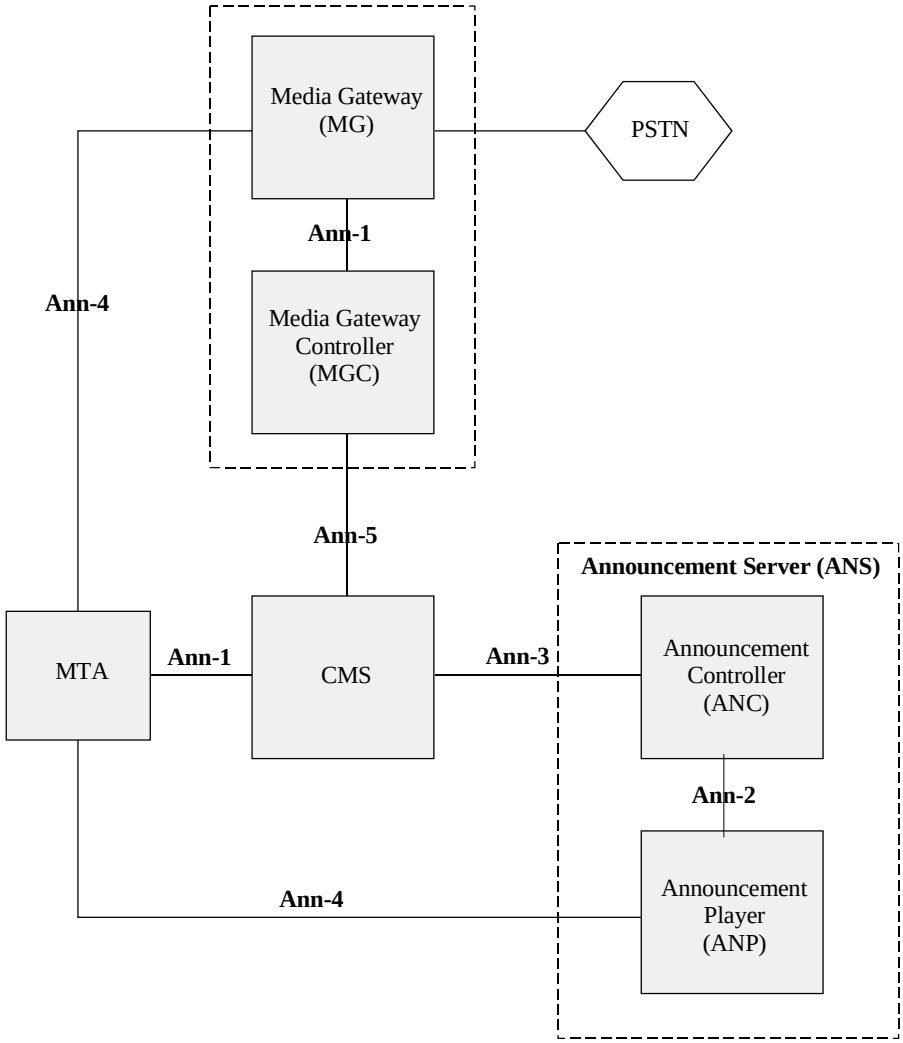


Figure C.8: Announcement services components and interfaces

Table C.7: Announcement interfaces

Interface	IPCablecom Functional Components	Protocol
Pkt-ann1	MTA-CMS MGC-MG	The CMS to MTA interface provides a mechanism for the CMS to signal the MTA to play locally stored announcements. Storing announcements in the MTA allows for providing informative progress tones to the end user independently of the network state (e.g. congestion). An NCS-based announcement package has been defined that can be used for both the CMS-MTA and MGC-MG interfaces. Simple, fixed-content announcements (e.g. all-lines-busy) may also be stored at the Media Gateway to provide announcements to PSTN users. The MGC to MG interface provides a mechanism for the MG to play fixed-content announcements to PSTN end-users involved in off-net to on-net calls.
Pkt-ann2	ANC-ANP	The signalling protocol for the ANC to ANP interface is NCS with an announcement package. When the CMS identifies a need for an ANS-based announcement, it sends a request to the ANC over interface Ann-3. Upon receiving a request from the CMS, the ANC opens a session with the Announcement Player using the NCS package.
Pkt-ann3	CMS-ANC	The protocol for the Ann-3 interface is undefined for IPCablecom.
Pkt-ann4	ANP-MTA	Defines the media stream format (RTP) for delivery of the announcement from the Announcement Player to the MTA using the RTP protocol.
Pkt-ann5	CMS-MGC	The Ann-5 protocol interface is undefined for IPCablecom.

C.1.3.7 Security

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).

Figure C.9 provides a summary of all the IPCablecom security interfaces.

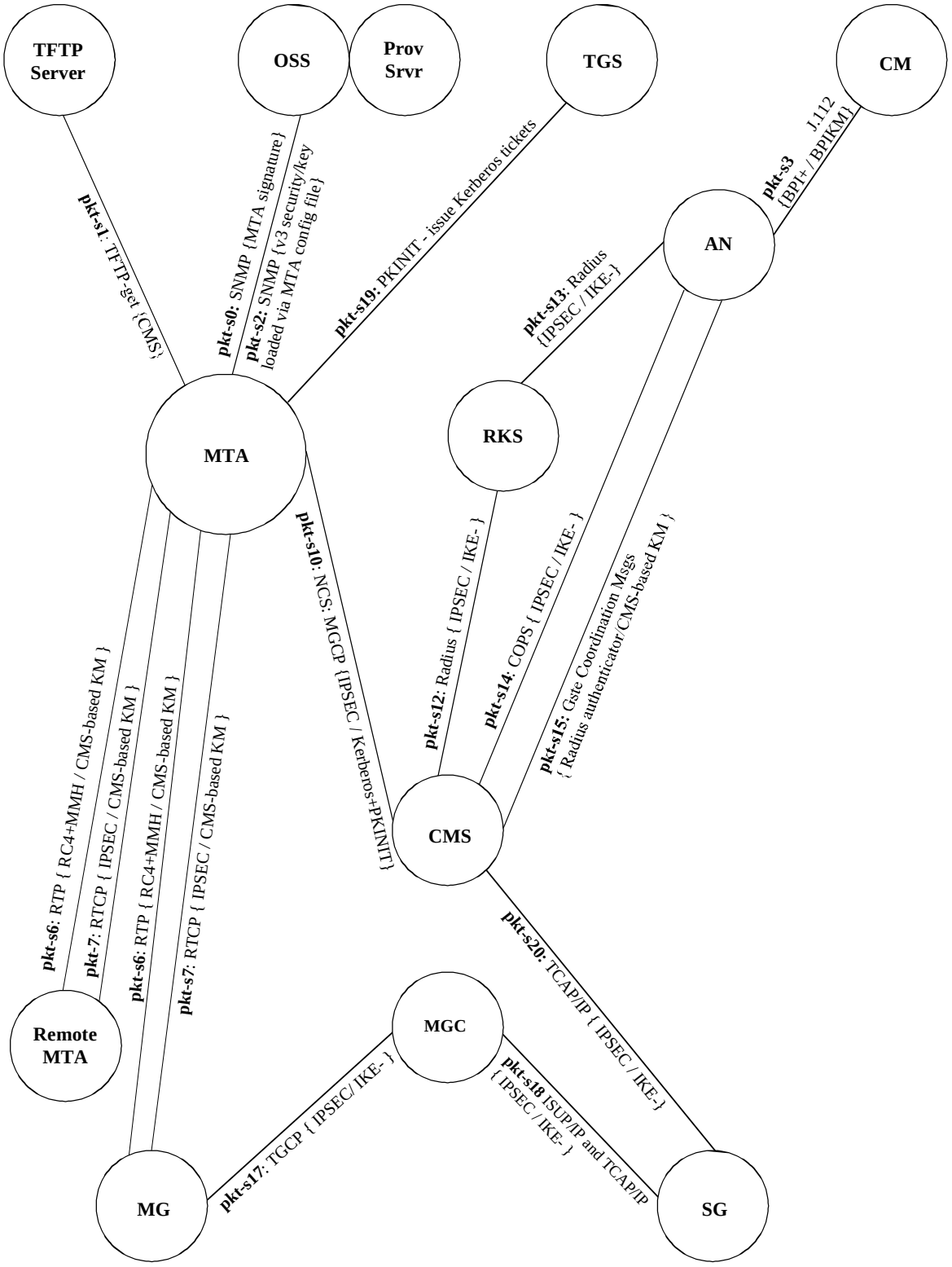


Figure C.9: IPCablecom security interfaces

In figure C.9, each interface is labelled as:

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

If the key management protocol is missing, it means that it is not needed for that interface. IPCablecom interfaces that do not require security are not shown on figure C.9.

The following abbreviations are used in figure C.9:

- **IKE-:** IKE with pre-shared keys.
- **IKE+:** IKE requires public key certificates.
- **CMS-based KM:** Keys randomly generated and distributed by CMS.

Table C.8 describes each of the interfaces shown in figure C.9.

Table C.8: Security interfaces

Interface	IPCablecom Functional Components	Description
pkt-s0	MTA-Provisioning App	SNMPv3 INFORM from the MTA to the SNMP Manager, followed by optional SNMP GET(s) by the SNMP Manager are 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 CMS (Cryptographic Message Syntax).
Pkt-s1	MTA-TFTP or HTTP Server	MTA Configuration file download. The MTA downloads a configuration file (with TFTP-get) that is signed by the TFTP server and sealed with the MTA public key, with a CMS (Cryptographic Message Syntax) wrapper. This flow occurs right after a SNMPv3 INFORM followed by an optional SNMP GET(s) - see flow pkt-s0.
pkt-s2	MTA-Provisioning App	Standard SNMPv3 security. The SNMPv3 keys are downloaded with the MTA configuration file, using interface pkt-s1.
Pkt-s3	CM-AN	BPI+ privacy layer on the HFC link. Both security and key management are defined by J.112 [4].
pkt-s6 (note)	MTA-MTA	End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with RC4, without any additional security layers. An MMH-based MAC (Message Authentication Code) optionally provides message integrity. Keys are distributed by the CMS to the two endpoints.
Pkt-s7	MTA-MTA	RTCP control protocol for RTP, defined above. Message integrity and encryption provided with IPSEC. Key management is same as for RTP - keys are distributed by CMS.
Pkt-s10 (note)	MTA-CMS	MTA-CMS signalling for NCS. Message integrity and privacy via IPSEC. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
Pkt-s12	CMS-RKS	Radius billing events sent by the CMS to the RKS. Radius authentication keys are hard coded to 0. Instead, IPSEC is used for message integrity as well as privacy. Key management is IKE-.
Pkt-s13	AN-RKS	Radius events sent by the AN to the RKS. Radius authentication keys are hard coded to 0. Instead, IPSEC is used for message integrity, as well as privacy. Key management is IKE-.

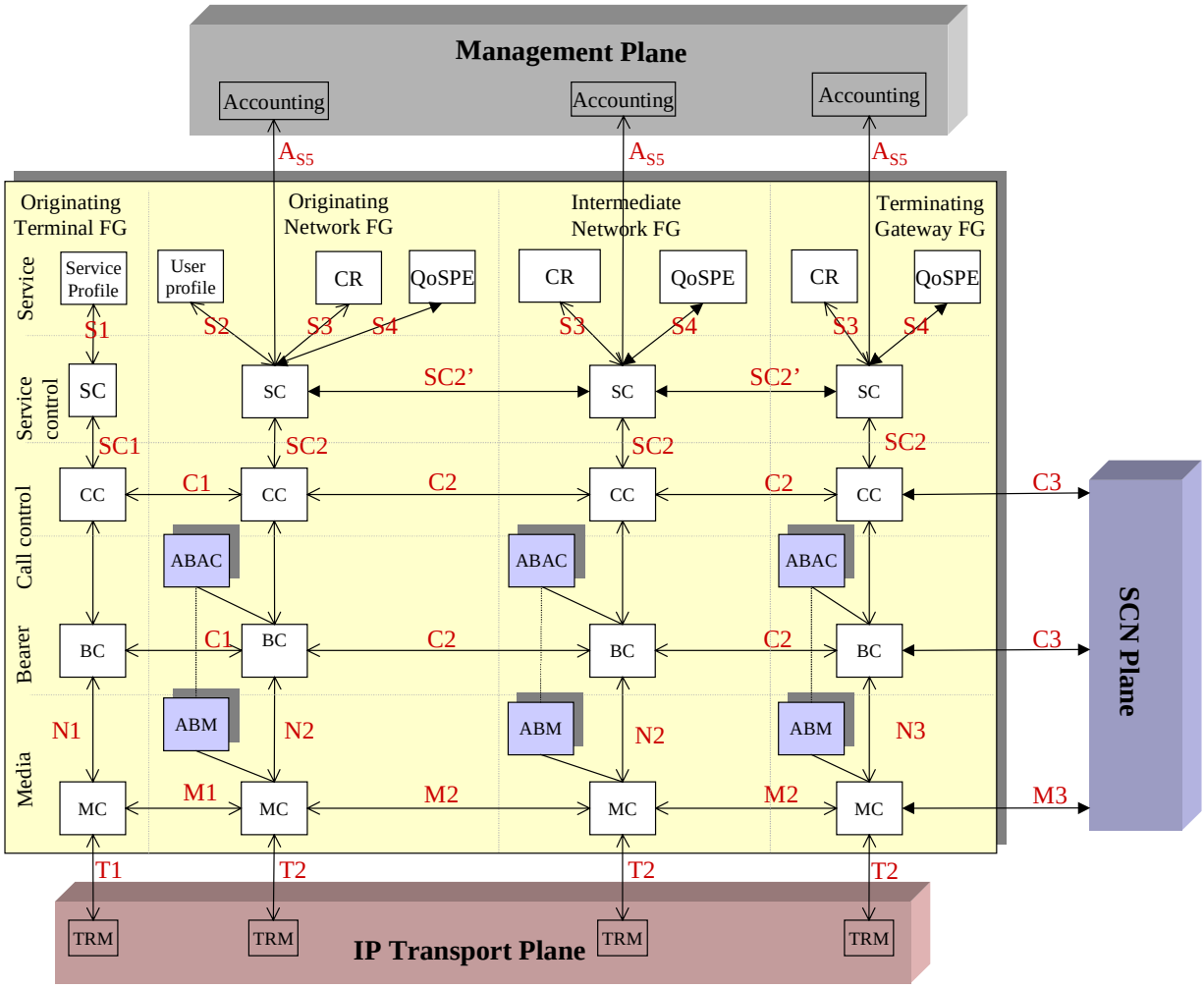
Interface	IPCablecom Functional Components	Description
Pkt-s14	CMS-AN	COPS protocol between the GC and the AN, used to download QoS authorization to the AN. Message integrity and privacy provided with IPSEC. Key management is IKE-.
Pkt-s15	CMS-AN	Gate Coordination messages for DQoS. Message integrity is provided with an application-layer (Radius) authenticator. Keys are distributed by local CMS over COPS.
Pkt-s16	N/A	N/A
pkt-s17	MGC-MG	IPCablecom interface to the PSTN Media Gateway. IPSEC is used for both message integrity and privacy. Key management is IKE-.
Pkt-s18	MGC-SG	IPCablecom interface to the PSTN Signalling Gateway. IPSEC is used for both message integrity and privacy. Key management is IKE-.
Pkt-s19	MTA-TGS	Kerberos/PKINIT key management protocol, where the TGS issues CMS tickets to the MTAs.
Pkt-s20	CMS-SG	CMS queries the PSTN Gateway for LNP (Local Number Portability) and other telephony services. IPSEC is used for both message integrity and privacy. Key management is IKE-.

The information flows defined in TIPHON document TS 101 312 [23] called s1 through 17 are not to be confused with the interfaces defined in IPCablecom TS 101 909-2 [21] alias J.160 [1]; those IPCablecom interfaces bear similar names s0 to s20. In fact [4] falls into the same trap as the IPCablecom security document which is to define information flows without defining security objectives.

C.2 TIPHON

C.2.1 TIPHON reference model recall scenario 1

The calling user is registered directly to its home network in the Originating Network Functional Group.



NOTE: Parts of the ABAC and the ABM function belongs to the Management Plane. Aggregate Bearer load control information flows between ABM and ABAC at N2 with the capability to provide admission control functionality based on aggregate bandwidth usage measurements and transport network QoS performance.

Figure C.10: Reference points for the Scenario 1; user at home

The Access Network in the IPCablecom model can be mapped to the three lower layers of the TIPHON scenario 1 reference model in the figure C.10.

The Managed IP Network of IPCablecom can be mapped to the Originating Network FG and the Intermediate FG of TIPHON.

The Call Management Server of IPCablecom can be mapped to the CC (Call Controller) of TIPHON.

The Media Gateway of the IPCablecom model can be mapped to the Media Control of the Terminating Gateway FG of TIPHON.

The Media Gateway Controller of IPCablecom can be mapped to the Bearer Control of the Terminating Gateway FG of TIPHON.

The Signalling Gateway of IPCablecom can be mapped to the Call Control of the Terminating Gateway FG.

Note should be taken that the Signalling Network Plane of TIPHON reference model is split into two sub planes for IPCablecom, one plane being the Media PSTN and one plane being the Signalling Gateway CCS7 level which is not necessarily bearer dependent.

The Managed IP Network in IPCablecom is the combination of The Originating Network FG, the Intermediate Network FG and the Terminating Gateway FG.

The Call Management Server (CMS), respectively remote CMS of IPCablecom can be mapped to the Call Control of the corresponding network FG (Originating, respectively Terminating).

IPCablecom depends upon SNMP to provide billing, accounting and some of the Quality of Service parameters "getting" and "setting".

IPCablecom introduces a multi layer QoS concept; some of the QoS parameters deal with the ITU-T Recommendation J.112 [4] lower layer 2 (MAC) while other QoS define layer 3 and even layer 4 parameters.

IPCablecom security reference model is intricate to say the least and needs some more care to be mapped into the security TIPHON model; the end result of end to end encryption is the same but seems to involve a large number of interfaces in the IPCablecom reference model.

The TIPHON accounting interface AS5 is equivalent to the pkt-em* interface.

Some of the protocols between components are not defined; for example protocol between CMSs is not specified.

C.3 Conclusions

The architecture of the IPCablecom is reasonably close to the TIPHON model.

There does not seem to be much definition of roaming except for number portability which is a very limited case of roaming.

IPv6 and SIP are not clearly supported.

The efforts to have IPCablecom converge towards TIPHON at the architecture level are:

- to establish the layered model according to TIPHON model;
- to evaluate the possibility of unifying the different interfaces for the different applications;
- to define the functional entities and their information flows for each of the process;
- to improve the description of when and why centralized network signalling and when distributed network signalling are to be used;
- to model inter-domain architecture when the two IPCablecom domains are tied by an intermediate network which is a SCN such as ISDN (this holds true for QoS, security as well as for architecture);
- to evaluate changes to the architecture so as to allow signalling Gateway operating on Megaco protocol instead of MGCP;
- to evaluate if there are major difficulties in the architecture to support IPv6, SIP and roaming.

Annex D: Protocols

The present annex gives guidance on the work to be accomplished for convergence between IPCablecom and TIPHON in the area of protocol(s). The convergence of one network towards the other in terms of protocols would insure interworking without intermediate converters.

D.1 TIPHON

The protocol definitions for TIPHON are provided in TS 101 882 [2].

D.2 IPCablecom

IPCablecom uses a number of different protocols to fulfil the different dialogs needed for its system operation.

The different protocols are:

- Network Call Signalling protocol (NCS, a profile of MGCP); defined in TS 101 909-4 [24].
- IPCablecom Signalling Transport Protocol (ISTP); defined in ITU-T Recommendation J.165 [18].
- Simple Network Management Protocol (SNMP); defined by IETF.
- Trunk Gateway Control Protocol (TGCP, another profile of MGCP); defined in TS 101 909-9 [50].
- Audio Server Protocol (another profile of NCS); defined in TS 101 909-19 [15].

Besides the actual choices of protocols and the high numbers of different protocols, we will concentrate on MGCP, ISTP, TGCP and Audio Server protocol.

Basically there are two protocols, MGCP and ISTP; in relation to convergence to TIPHON, the following questions are valid and we will try to answer for each of those two basic protocols MGCP and ISTP the following basic questions:

1) Is Protocol X a Meta-Protocol?
2) If no, how much effort is required to convert it to a Meta-protocol?
3) If protocol X is not a Meta-protocol, what is the protocol recommended by TIPHON and how close is that protocol to protocol X?

At least one less basic question but still valid:

4) How to define and how to establish conformance of IETF Protocols defined mostly by text and BNF notations in an ETSI way?

D.3 MGCP

The basic questions are:

1) Is the Media Gateway Control Protocol (MGCP) a Meta-Protocol?
2) If not, how much effort is required to convert it to a Meta-protocol?
3) What is the closest protocol recommended by TIPHON?

At least one less basic question but still valid:

4) How to define and how to establish conformance of MGCP defined mostly by text and BNF notations?

   - Is MGCP an agreed method of "communication" between 2 parties? Yes.
   - Does MGCP provide a set of rules for "communication"? Yes.
   - Does MGCP provide a means to determine progress? Yes.
   - Does MGCP provide a means to determine completion? Yes.
   - Does MGCP provide a means to recognize failure? Yes.
   - Is MGCP not restricted to "technology"? yes to some extent even though it is used to-day only in the context of a single technology.

D.3.1 Present methods to define MGCP

MGCP uses mostly text (as is the case for most of IETF defined protocols) and is based on IETF RFC 2705 [25]; it is derived from the merge of two IETF protocols:

1) Simple Gateway Control Protocol;

2) IP Device Control (IPDC) family of protocols.

The present design and definitions of MGCP do not use at all MSC, UML or ASN.1; it uses SDL for a very specific case of dynamic QoS description; it uses part of UNIX egrep and BNF notations (derived from ABNF IETF RFC 2234 [26] "Augmented BNF notation").

It will be a significant part of the effort to convert MGCP to TIPHON Meta-Protocol to convert the descriptive text to formal description tools such as SDL and ASN.1.

MGCP text is quite clear in terms of "must", "must not", optional, forbidden etc. so that it will not be difficult to get exact behaviour defined.

MGCP does use some definition language mentioned above that should be able to be converted manually to ASN.1 format.

MGCP does define a "complete" protocol by mandating behaviour and data existence. MGCP does allow for transport extensibility so as to carry proprietary and future feature extension without breaking mandates its own rules.

Would MGCP have to be developed as a Meta-protocol, the following stages would have to be followed.

Stage 1 To develop MGCP as a Meta-protocol using:

- Data-syntax described in ASN.1.
- Behaviour described in MSCs with SDL ***and*** normative text.

Stage 2 Determine protocol mapping:

- Syntax mapping using encoding rules.
- Behavioural mapping using text and SDL.

MGCP can qualify as a meta-protocol since it is:

- Closed (i.e. finite states, finite transitions).
- Failsafe (i.e. return to IDLE on error).
- Extensible (i.e. define rules for carriage of proprietary or new features).

In order to create the meta-protocol corresponding to MGCP, the following steps need to be performed:

1) Determine what it is meant to do.

2) Capabilities it has to support.

3) Determine its data requirement.

4) Formalize in ASN.1 (identify objects that can create, delete, modify the data).

5) Determine the states and state transitions at each architectural and protocol entity.

NOTE: States Protocols are described using Finite State Machines. For each state we define: Pre-conditions, Post-conditions, Transitions. Modelling tools: SDL, UML.

Once MGCP is described as a Meta-Protocol, it allows mapping between different Meta-Protocols. The scope of mapping contains a candidate protocol identification followed by data mapping, formalized syntax encoding, formalized element naming. The cable industry will benefit of a conversion of MGCP to a TIPHON conformant standard in particular to inter-work with networks with which it does not inter-operate today (such as BRI ISDN) and to provide the cable transit link that it cannot provide today.

The following mappings between the two meta-protocols will need:

- Behavioural mapping;
- State mapping;
- Transition mapping.

A detailed analysis of MGCP needs to be conducted to study if MGCP meet all the requirements of a TIPHON protocol as described in TS 101 878 [49] and of a meta-protocol.

There is the possibility of failure of the candidate MGCP on special features not met by meta-protocol; those need to be clearly identified and isolated from the whole process especially in the case of mapping between two meta-protocols.

The mapping of a candidate protocol such as MGCP may result into new capabilities for MGCP.

In the presently doubtful case where MGCP candidate to Meta-Protocol cannot support TS 101 878 [49] capabilities, where TS 101 882 [2] syntax/state/sequences cannot be supported and where no willingness on candidate owner to make changes is apparent, the effort should be aborted as soon as possible.

The primitives that are needed to exercise the MGCP protocol are expressed in the API called MGCI.

D.3.2 Meta-protocol check list

A clause by clause check list is conducted of MGCP against clauses of TS 101 882 [2].

D.3.2.1 Clause 4 of TS 101 882

4.1 performance requirements.

- In the event of any failure each entity in the current relationship shall return to a safe initial state (i.e. shall fail safe); fulfilled.
- Environment conditions shall be returned to a state equal to the condition prior to a call on clearance of a call; fulfilled.

4.2 security requirements.

- optionally fulfilled through RTP and RTCP features.

4.3 internal data stack management.

- apparently fulfilled.

D.3.2.2 Annex A of TS 101 882

There is no mention in MGCP of "visited", "home", "mobility"; the requirement "The registration service allows a user to receive service in both home and visited domains." is therefore not fulfilled since mobility is apparently not mentioned in the MGCP description.

The registration and authorization protocols are different from the Network Call Signalling MGCP. They are also described in a different document than the Network Call Signalling MGCP protocol. This document is the Media Terminal Adapter (MTA) provisioning [1] which states.

"This interface (MTA to Provisioning Application)" identifies specific requirements for the Provisioning Application to satisfy MTA initialization and registration. The Provisioning Application requirements are:

- The Provisioning Application MUST provide the MTA with its MTA configuration data file. The MTA configuration file is specific to the MTA-component of the embedded-MTA and separate from the CM-component's configuration data file.
- The configuration data file format is TLV binary data suitable for transport over the specified TFTP or HTTP access method.
- The Provisioning Application MUST have the capability to configure the MTA with different data and voice service providers.
- The Provisioning Application MUST provide secure SNMP access to the device.
- The Provisioning Application MUST support online incremental device/subscriber provisioning using SNMP with security enabled.

These requirements are in line with [2]. In IPCablecom there is no reference to a registration outside its own domain; however, registration can occur with several different service providers.

The concept of ticket is used in IPCablecom only in the context of security and attaching a particular MTA to a particular CMS; note that the concept of trusted and untrusted appears in IPCablecom; the MTA is an untrusted component because it is not integral part of the network and is provided by the subscriber. This concept does not appear in TIPHON.

The deregistration mechanism of clause 5.1.1 of TS 101 882 [2] is called "disabling" in IPCablecom provisioning clause 6.3.3 of [1].

According to clause A.1.2 of TS 101 882 [2], authentication of the following entities is provided:

- Terminals (MTA) with dynamically provisioned parameters;
- Functional elements within the network with dynamically provisioned parameters.

Following authentications are not provided because not applicable and/or not relevant:

- Terminals with variable point of network attachment;
- Terminals with variable point of service attachment;
- Functional elements within the network with variable point of network attachment; and
- Functional elements within the network with variable point of service attachment.

Registration service for IPCablecom is not defined in terms of primitives and primitive contents; this would need to be accomplished to align with TS 101 882 [2].

The process goes into loading configuration data into the MTA, then provisioning (registration) then authentication.

As part of the registration process, an IP address is assigned to the MTA (and a different address is assigned to the CableModem); this process uses the DHCP starting with a commonly option code "177".

From clause A.1.2: The registration meta-protocol is visible at pkt-p6 of figure 3 of [1].

The following requirements shall be met by the candidates that conform to this meta-protocol:

- The principle of "receive before transmit" shall be invoked (i.e. the terminal has to be registered and authorized before being able to make or receive calls). Fulfilled (the CMS shall not process a call request issued by an MTA not registered).
- Receive before transmit may be overridden for certain call types (e.g. emergency calls). Fulfilled.

Clause A.1.3 of TS 101 882 [2] is fulfilled.

Clause A.2 OK

Clause A.3 intent is to fulfil; need to investigate what is the corresponding parameter of TIPHON Registered Location in IPCablecom.

Clause A.4 table 3 of TS 101 882 [2] can be filled for IPCablecom as follows.

Table D.1: Registration functional elements

Identity	Name	Probable functional grouping
FE1	Registrant	MTA
FE2	Registrar (note)	Provisioning Application
FE3	SpoA (Service point of Attachment) Fixed	CMS
NOTE: Contains a register of currently registered terminals (keyed to Registration identity (regID)).		

Clause A.5 [2] most of the flows are present; needs cleaning up, formalizing and using ASN.1/SDL and formal naming of the entities. There is a different protocol between the initial registration flow and the following ones (i.e. modification) which uses SNMP as a protocol. The initial registration is not clearly indicated in terms of flow and uses DHCP.

Clause A.6 of TS 101 882 [2]; clause 5.3 of [1] gives state sketches in designer 7 format; will need formal tool and also improved definition of the functional entities exchanging those messages. Basically SDLs of clause A.6 of [2] should apply.

D.3.2.3 Clause 6 of TS 101 882

Clause 6 of July edition of 3016 seems to have disappeared in the November edition of TS 101 882 [2].

D.3.2.4 Clause annex B of TS 101 882

Mapping of TIPHON TCC-SAP to IPCablecom "commands".

Primitive	Corresponding IPCC command
TCC_CallSetup_req	CreateConnection
TCC_CallSetup_conf	CreateConnection
TCC_CallSetup_ind	CreateConnection
TCC_CallSetup_resp	CreateConnection
TCC_CallClear_req/conf	DeleteConnection (from the Call Agent)
TCC_CallClear_ind/resp	DeleteConnection (from the Embedded Client)
TCC_CallModify_req/conf	ModifyConnection
TCC_CallModify_ind/resp	ModifyConnection
TCC_SetLocalProfile_req/conf	Note
TCC_CallReport_ind	Auditing
NOTE: Not part of call related commands but part of management functions.	

IPCC supports also Restart in progress which does not seem to be a generic function in TIPHON meta-protocol.

At this point in time, first phases of IPCablecom supports only point-to-point on demand calls.

The interface where those commands alias primitives are presented is the interface between MTA and CMS names pkt c1 in the architecture document.

The call control elements from TS 101 882 [2] are mapped into the components of IPCablecom in table D.2.

Table D.2: call Control functional elements

Identity	TIPHON name	Corresponding IPCablecom name
FE5	Call control agent at originating terminal	Call Agent
FE6	Call control agent on serving network of originating terminal	Originating Call Management Server (CMS)
FE7	Call control agent in an intermediate network	Managed IP Network
FE8	Call control agent on serving network of terminating terminal	Terminating Call Management Server (CMS)
FE9	Call control agent at terminating terminal	Call Agent

The Call Control functional elements and supporting meta-protocol (candidate MGCP) shall do the following:

- Maintain the call state. Fulfilled; in fact the IPCablecom approach is to maintain half calls and their link.
- Set-up and release calls. Fulfilled.
- Allocate and release resources from the transport plane through the intrinsic Bearer Control functionality. Not quite the same allocations; assume to be what is called dynamic QoS.

Clause B.2.1 of TS 101 882 [2] fulfilled with other terminology; at least the capability is demonstrated in annex H of TS 101 909-4 [24] for Japan which could be extended to ETSI countries (regulatory European environment).

Table D.3: Call control MPMUs meta-protocol message unit

MPMU name	Capability	Parameters	M/O/C	IPCablecom supported
U_CallRequest (note 1)		CallID callingPartyID calledPartyID CallServiceId ticket priority	M M M M M M	Yes Yes Yes ? Yes ?
D_CallRequest (note 2)		CallID callingPartyID calledPartyID service priority	M M M M M M	yes Yes Yes ? ?
D_CallReport		CallId ReportReason ReportParameters	M M C	
U_CCAdditionalDigits		CallId AdditionalDigits	M M	Yes Yes
U_CallConnect				?
D_CallConnect				?
ConnectAcknowledge		CallID callingPartyID calledPartyID service.		?
U_CallClear				Yes
D_CallClear				Yes
U_CallAlert				Yes
CallModify				Yes
NOTE 1: MPMUs prefixed by "U_" indicate MPMUs generated by a terminal and have direction only towards the network (i.e. Up to the network). NOTE 2: MPMUs prefixed by "D_" indicate MPMUs generated by the network in the direction only of the terminal (i.e. Down from the network).				
Encoding of parameter: M = Mandatory; C = Conditional (i.e. dependent upon the value of a mandatory element is mandatory or not present); O = Optional				

Clause B.4 of [2] "Behaviour description".

states: MGCP original document IETF RFC 2705 [25] does not use states, state transitions, not very clear seems to use half connection states; MGCP actually sends commands to gateways from/to Call Agents which are not necessarily directly involved in the call they are setting up.

No MSCs, no SDLs a few coded examples and the details of the command format. How to check the syntax of a command expressed in what looks like pure text?

Functional entities are users 1 and 2, embedded clients 1 and 2 (EC-1 & EC-2), Call Agent (CA), Accounting data base (ACC), Configuration Data Base (CDB).

primitives: none described formally; layers not apparent; the different commands are:

- CreateConnection CA--- >Gateway
- ModifyConnection CA--- > Gateway
- DeleteConnection CA--- > Gateway / Gateway--- > CA
- NotificationRequest CA--- > Gateway
- Notify Gateway--- >CA
- AuditEndpoint CA--- > Gateway
- AuditConnection CA--- > Gateway
- RestartInProgress. Gateway--- > CA

The notation for description of those commands is not ASN.1. Naturally, MGCP protocol being now defined and deployed cannot be modified simply to migrate to ASN.1 notations; what could be achieved to make the formal process concrete would be to use ASN.1 notation to formally describe the data carried by the protocol leaving the actual exchanges of PDUs unchanged. The actual commands and responses of the present protocol would be "encapsulated" into ASN.1 declarations.

D.3.3 Use of BNF to specify a character-based syntax

The following are extracts of books by Dubuisson and Dartmouth on BNF and its relation to ASN.1:

- Where this character-based approach is employed, the precise set of lines of text permitted for each message has to be clearly specified. This specification is akin to the definition of an abstract syntax, but with more focus on the representation of the information on the line than would be present in an ASN.1 definition of an abstract syntax.
- The notation used to define this syntax is usually some variation of a notation frequently used to define the syntax of programming languages (and indeed used to define the syntax of ASN.1 itself), something called Bacchus-Naur Form (BNF), named after its original inventors.

For example, in ASN.1, the BNF statements:

```
EnumeratedType ::= ENUMERATED { Enumeration }
Enumeration ::= NamedNumber |
Enumeration , NamedNumber
NamedNumber ::= identifier(SignedNumber)
SignedNumber ::= number | - number
```

are used to specify that one of the constructs of the language consists of the word "ENUMERATED", followed, in curly brackets, by a comma-separated list with each item being an identifier followed by a number (possibly preceded by a minus sign) in round brackets.

Unfortunately, there are many variations of BNF in use today, and most applications employing it find it necessary to define their own particular BNF notation. This makes it more difficult than it should be to use common tools to support BNF-based specifications.

BNF is a relatively low-level notational support tool. It is very powerful for defining arbitrary syntactic structures, but it does not in itself determine how variable length items are to be delimited or iteration counts determined. Even where the same BNF notation is employed, the "look-and-feel" of two protocols defined in this way can still be very different, as the means of terminating strings (quotation marks, reserved characters, reserved characters with escapes) or of variable length repetitions of items, have to be written into the specific application using the BNF notation for this definition.

Of course, as with any tool, if the design is a good one, a good result can come out. Many of the Internet protocol designs take this approach, and the best designers ensure that the way in which length and iteration terminations are achieved follows as closely as possible the approach taken in other related specifications, and is consistent for different fields and commands within that application.

Software tools to support BNF-based specifications are usually restricted to lexical analysis of an incoming string, and generally result in the application-specific code and encoding matters being more closely intertwined than would normally be the case if an ASN.1 tool was used.

Identification fields for lines in the messages tend to be relatively long names, and "enumerations" also tend to use long lists of names, so the resulting protocol can be quite verbose. In these approaches, length fields are normally replaced by reserved-character delimiters, or by end-of-line, often with some form of escape or extension mechanism to allow continuation over several lines (again these mechanisms are not always the same for different fields or for different applications).

In recent years there has been an attempt to use exactly the same BNF notation to define the syntax for several Internet protocols, but variations still ensue.

At implementation-time, a sending implementation will typically hard-wire the encoding as a series of "PRINT" statements to print the character information directly onto the line or into a buffer. On reception, a general-purpose tool would normally be employed that could be presented with the BNF specification and that would parse the input string into the main lexical items. Such tools are available without charge for Unix systems, making it easy for implementations of protocols defined in this way to be set as tasks for Computer Science students (particularly as the protocol specifications tend also to be available without charge!).

In summary then, this approach can work well if the information to be transferred fits naturally into a two-level structure (lines of text, with an identifier and a list of comma-separated text parameters on each line), but can become complex when a greater depth of nesting of variable numbers of iterated items becomes necessary, and when escape characters are needed to permit commas as part of a parameter. The approach also tends to produce a much more verbose encoding than the binary approach of ASN.1 BER, and a very much more verbose encoding than the ASN.1 Packed Encoding Rules (PER)".

IPCablecom standards are proposed to be transposed into ETSI Technical Specifications; IPCablecom uses MGCP as NCS (Network Control Signalling) derived from (but not strictly identical to) IETF RFC 2705 [25]. As quite often in Internet protocol standards, BNF is used in lieu and place of ASN.1; apparently BNF text character oriented is not as easy to handle for large structure and leads to a less compact set of encoding.

D.4 Applications of MGCP to IPCablecom and closest Meta-protocol

D.4.1 NCS

D.4.2 TGCP

With respect to TS 101 909-13 [47] TGCP, TIPHON does address the broad requirements for gateway control protocols through reference point N of the TIPHON architecture. Therefore the TGCP proposals fall within the scope of existing TIPHON specifications. TIPHON notes that its current work programme does not include MGCP based gateway control protocols, but does include Megaco/H.248. TIPHON is working on a protocol mapping that embodies principles derived from the TIPHON architecture.

The closest meta-protocol to support TGCP extensions to MGCP is H.248; while TGCP is presently defined as a profile of MGCP with a few additions to MGCP, it is also possible to define TGCP as an H.248 profile and to support the same requirements as the MGCP version; this may result in some extensions of H.248 and by the same token of TS 101 882 [2].

The text below provides a list of additions of TGCP to MGCP and describes H.248 equivalent implementations in italic.

- Endpoint Naming Scheme.

A specific endpoint naming scheme has been introduced for DS-0 endpoints. The rules for wildcarding are more restrictive than in MGCP, and also introduces the "range" concept for DS-0 endpoints.

H.248: An equivalent naming scheme can be defined for physical terminations.

- Embedded ModifyConnection.

A new Embedded ModifyConnection action has been introduced.

H.248: The same result can be obtained by sending several Modify commands in a single transaction, as a response to the event notification.

- Security.

IPCablecom Security services are supported in TGCP. This affects the LocalConnectionOptions, Capabilities, and SDP.

H.248: There might be a need to define a specific package including the following properties: Secret, RTP Ciphering suite and RTCP ciphering suite.

- Endpoint Name Retrieval.

The AuditEndpoint command has been extended with a capability to return the number of endpoints that match a wildcard as well as mechanism for block-wise retrieval of these endpoint names. Besides extending the AuditEndpoint command, this implies the introduction of two new parameter names; MaxEndPointIds, and NumEndPoints

H.248: The list of termination ids matching a wildcard may be retrieved using an AuditValue command with an empty AuditDescriptor.

The specification of a maximum number of terminations is not supported. However, the amount of data sent in response to the audits may be controlled if the MGC understand the way terminations are named. The Naming Pattern package may be used by the MGC to retrieve the naming patterns and construct meaningful audits.

- Supported Versions.

The RestartInProgress response and the AuditEndpoint command have been extended with a VersionSupported parameter to enable MGCs and gateways to determine which protocol versions each support.

H.248 : The supported protocol version is available in the ServiceChange command.

- Error Codes.

Two new error codes have been introduced; 532 and 533.

H.248: Error code 532 (Unsupported value(s) in LocalConnectionOptions):Audited Property, Statistic, Event or Signal does not exist. Depending on the actual type of parameter, a more specific error code needs to be used: 441-446. Error code 533 (response too big): This error code is a valid code for H.248 (Response exceeds maximum transport PDU size).

- Usage of SDP.

A new SDP usage profile is included in TGCP. Most notably, the profile and all example use specifically require strict SDP compliance, regardless of the usefulness of the included fields. Also, IPCablecom specific extensions have been added to SDP.

*H.248: A valid SDP description is a valid text encoding for H.248. H.248 [*45*] clause 7.1.8 states "Implementations shall accept session descriptions that are fully conformant to RFC2327". IPCablecom specific extensions to SDP (i.e. new attributes) are discussed under other bullet points). If strict conformance to SDP is felt necessary, The H.248 profile for TGCP could specify that strict conformance to SDP is required.*

- Provisional Response.

Additional detail and Recommendation of the provisional response mechanism has been included in TGCP. A Response Acknowledgement response (000) has been introduced, an empty ResponseAck parameter has been permitted in final responses that follow provisional responses, and a procedure for the mechanism specified.

H.248: The TransactionPending message supported provisional responses. The final response (transactionReply) includes an immAckRequired field that triggers the sending of a transactionResponseAck message.

- Signal Parameters.

Signal parameter syntax has been extended to allow for the usage of balanced parenthesis within signal parameters. All Time-Out signals can have their time-out value altered by a signal parameter.

H.248: The duration parameter in a signal descriptor may be used to override provisioned time-out values.

- Event Packages.

D.4.2.1 TGCP introduces a set of new event packages

H.248: See below.

- Lawful Interception.

The Call Content Connection identifier and Call Content Destination parameters have been added to the LocalConnectionOptions.

H.248: There might be a need to define a specific package including the following properties: Call Content Connection and Call Content Destination.

The following table gives the correspondence between the TGCP packages to support IPCablecom and either existing H.248 packages or proposals for new packages.

Table D.4: TGCP packages vs. H.248 packages in support of IPCablecom

TGCP package	H.248 package	Description
SUP Trunk	Continuity (annex E), TDMF (annex F) dtfm event for fax tone TDMF (annex F) Generic (annex E) Signal Completion with Termination parameters set to Notify Completion Call Progress Generator (annex E) Call Type Detection (annex E)	Continuity tone 1, Continuity tone 2, fax tone, long duration connection (note 1), start media (note 2), modem tones, operation complete, operation failure, reorder tone, ring back tone, Telecommunication Devices for the Deaf TDD
MF FGD Operator Services Package	draft megaco cas	use in Europe?
MF Terminating Protocol Package	draft megaco cas	use in Europe?
NOTE 1: There is no equivalent event in H.248 packages. However, such an event is not required since the H.248 architecture assumes that the context lifetime is monitored by the MGC. NOTE 2: None of the H.248 packages support a similar event. The requirements for supporting it should be further studied with IPCablecom experts. Should this appear to be necessary, an appropriate package might be defined.		

A Trunking Gateway Control Profile draft has been produced by SPAN where H.248/Megaco is used.

D.4.3 Audio Server Protocol

The IPCablecom Audio Server Protocol Specification defines a suite of signalling protocols for providing announcement and media services in an IPCablecom network.

The significant part of work will be to work on the incorporation of TIPHON compliance into the Megaco/H.248 version of TS 101 909-19 [15].

The following text summarizes how H.248 fulfils the requirements of IPCablecom in relation to Advanced Audio Server protocol; as it will be seen, extensions to H.248 may be needed; note that the recent draft of annex M.1 of ITU-T Recommendation H.248 [45] is assumed to be adopted in the following discussions.

NOTE: There are changes brought forward by SPAN13 simply to europeanise the Audio Server such as content of actual messages etc. Those changes have not been taken into consideration and only the protocol changes have been considered.

This specification defines a set of signalling interfaces that are used to provide announcement services within a cable network. For one of these interfaces, this specification uses either of the following protocols:

- The IPCablecom Network Call Signalling (NCS) protocol, extended with two new event packages defined in this specification:
  - A Base Audio Package.
  - An Advanced Audio Package.
- The H.248 protocol with the packages defined in annex M.1 of ITU-T Recommendation H.248 [45]:
  - Advanced Audio Server package.
  - AAS digit collection package.
  - AAS recording package.

- AAS segment management package.

Naming conventions for endpoint identifiers belongs only to the MGCP protocol and have been removed from the H.248 [45] based document.

The IPCablecom Audio Server signalling Interface Descriptions to support Media Services are summarized in table D.5.

Table D.5*:* Announcement interfaces

Interface	Signalling components	Protocol
Ann-1	MTA/CMS, MGC/MG	NCS/TGCP with announcement packages
Ann-2	MPC/MP	NCS with announcement packages or H.248 [45] with annex M1 packages.
Ann-3	CMS/MPC, CMS/MGC	Undefined. (proprietary?)
Ann-4	MP/MTA	RTP

The Ann-2 interface - MPC/MP Announcement Package.

The MPC to MP protocol is based upon either two NCS announcement packages or H.248 [45] with the annex M1 packages. Less frequently used tones and fixed-content announcements, as well as all variable content and interactive announcements are provided by MPC and MP complex.

When the CMS identifies a need for an AS-based announcement, it sends a request to the MPC over interface Ann-3. Upon receiving a request from the CMS, the MPC opens a session with the Media Player using the NCS package. The MP then interacts with the specified endpoint over interface Ann-4.

The Ann-3 interface allows the CMS to request the MPC to establish announcement sessions between the MP and another endpoint. It also allows the CMS to request the MGC to have the MG play fixed-content announcements to a PSTN endpoint. This interface is currently undefined. It is expected that this signalling interface will be based upon the IPCablecom CMS/CMS signalling protocol being specified in draft Recommendation J.icms. This draft corresponds to TS 101 909-16; both documents are not yet available.

The addition of an annex A to H.248 [45]/MEGACO Protocol case is then needed.

D.5 ISTP IPCablecom signalling transport protocol

The transport plane protocol used in IPCablecom is ISTP (Internet Signalling Transport Protocol). The following text is based on the ITU-T Recommendation J.165 [18] which at this time contains only a US ANSI annex. It is the intent of SPAN to generate a European Annex which will include the European specific and the country specific of SS7 signalling system.

As a result of SPAN 6 meeting, one can quote the following possible choices of SPAN as represented in the SPAN 13 meeting report: "SPAN deemed part 12 as not really suitable for interconnecting between European SS7 networks. This was because it is based heavily on ANSI standards. SPAN13 has agreed a work item for this work, which is based on the IETF work. M3UA status is work group last call completed. However, there appear to be more open issues and the IETF discussions continue. The IETF draft is unlikely to be available for ISNG last call before the next IETF meeting in October. SPAN13 may have to do some of our own work - in any case the completed work may not be available until Autumn 2002 - which is outside IPCablecom standardization deadlines to meet market requirements. This standards track document may not reach maturity. SU3A should also be considered."

SPAN13 confirmed that the interconnect between different operators related to TS 101 909-12 [19] should be based on IETF draft protocols. There are, however, a list of open issues that do not appear to be completed before then end of 2002. Should SPAN use a previous draft of M3UA, e.g. version 6 which has been subject to interconnect test, but does not contain a dynamic routing procedure? The message tagging and procedures may be slightly out of date, but at least it has been subject to operability tests. It was noted that V9 may have similar problems to V6. A thin layer could be built on top of M3UA V5 or V6 to cover for remaining open issues and provide for interconnect.

The SPAN developed architecture should cover all the scenarios of an IP network talking to:

- IP network.
- Cable network.
- PSTN / ISDN network.

TS 101 909-2 [21] does not show all of these scenarios. M3UA provides a lowest common denominator to provide all of the above, provided an interworking layer is used.

The meeting further considered the use of M3UA v6 and IPCablecom. M3UA would not be able to replace all of the ISTP functionality. M3UA could be used in conjunction with some of the ISTP functionality, but this is not the ISTP of the IETF. Interworking between MTP3 and M3UA, i.e. between different network types, would cause a number of problems and need careful consideration and interworking.

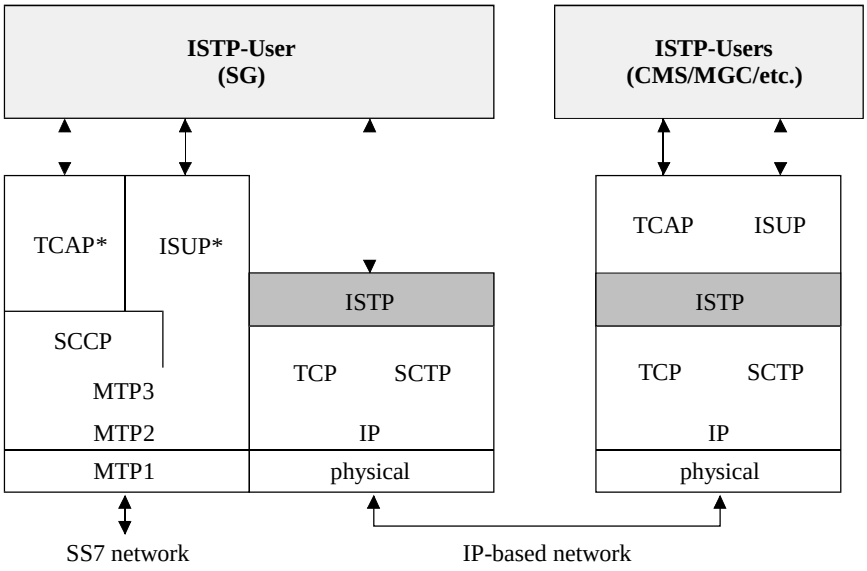
It was proposed to use M3UA v6 as the basis for SPAN13 work and this was agreed as the working assumption. SPAN13 needs to provide additional functionality (to be identified by STF) to M3UA v6 to make it IPCablecom compatible. The long term view for VoIP still needs careful consideration. It was agreed to create a new work item to specify a function to provide the additional items above M3UAv6 for the IPCablecom network and between other narrowband stacks. The changes to the technical architecture will need documenting, either in TC-AT or SPAN. Two of the additional items, dynamic route processing and n+k within M3UAv6 and ITU-T version of ISTP is not thought to be covered by any IPR.

The updating and management of Global titles will become an issue because these would need to be understood in the protocol stack. This implies global title translation would need to be covered in each protocol stack. The meeting deemed that SUA would therefore be required. The work of 3GPP should be taken into account to ensure compatibility and the need to avoid duplicating work. SPAN already has the following work items; TS 102 141 covering M2UA, TS 102 142 covering M3UA, TS 102 143 covering SUA, TS 102 144 covering SCTP to provide interworking. SPAN need to ask ECCA representatives of time scales. Phase 1 basic interworking will be completed by the end of this year. Country specific part is phase 2. SPAN13 wishes to know if, given the likely time frames (mid 2002) if there is a need to produce a version of TS 101 909-12 [19] for interconnect to the existing narrowband network.

1) The current part 12 [19] of the IPCablecom document (ISTP) does not provide for interconnection using an ETSI version. If this is required, then SPAN13 will need a rapporteur to translate the original comments assembled by ITU-T SG11 and SPAN into a Europeanised version of TS 101 909-12 [19], it should be noted that this is a network risk as even with these comments included then SPAN13 cannot guarantee that it would be acceptable to networks for interconnect using this amended part 12 [19].

2) Interworking with ETSI networks should be to the current ETSI standards (EN 300 356 [46] etc.).

SPAN is still hoping to see SIGTRAN converge to a reasonable text which then could be picked up to interface IPCablecom to SS7 networks.



NOTE: * May be a partial implementation to obtain required ISUP/TCAP parameters for ISTP.

Figure D.1: Protocol distribution in IPCablecom elements

Figure D.2 describes the situation of ISTP with respect to the different elements of the IPCablecom architecture.

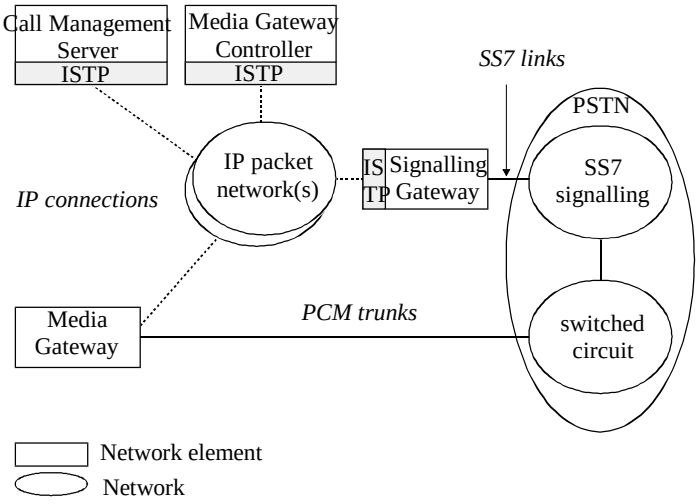


Figure D.2: ISTP in decomposed IPCablecom gateway

The ISTP contains functions for:

- Initialization.
- Registration of circuit IDs with the SS7 gateway.
- Address mapping between the SS7 and IP domains.
- ISUP maps based on point code and circuit identification code.
- TCAP maps based on point code and transaction ID.
- ISUP/TCAP message delivery using reliable transport.
- Maintenance operations.

- Activation/deactivation of circuit IDs within the SS7 gateway. (The actual physical circuits terminate on the Media Gateway.)
- Error recovery due to faults.
- SS7 signalling point inaccessible.
- SS7 signalling network inaccessible.
- MGC inaccessible.
- CMS inaccessible.
- Error recovery due to congestion.
- Signalling point congested.
- Signalling link congested.
- MGC congested.
- CMS congested.

In order to meet the performance and reliability requirements mandated by IPCablecom and SS7 interconnection, ISTP requires the services of an underlying reliable transport service. ISTP currently specifies TCP as the underlying transport mechanism, with the recognition that the network needs to be properly engineered. It is anticipated that the Stream Control Transport Protocol (SCTP) defined by the IETF SIGTRAN group (IETF RFC 2960 [17]) may provide a superior alternative to TCP in this regard. UDP is not considered an acceptable option, as it does not supply sufficient reliability to meet IPCablecom requirements.

The protocol uses an octet format (and not an ASCII 7 bit format) to cater for conversion to existing SS7 standards. It provides for two formats one raw format, one encoding format aligned with ISUP and TCAP.

ISTP supports today only IPv4; no word about IPv6 in the text of ITU-T Recommendation J.165 [18] or any word for a migration to different addressing scheme.

Because of its interworking with SS7, ISTP uses graphics close to SDL, uses PDU encoding easily translatable into ASN.1 and uses an octet data format instead of an ASCII format for MGCP. It is much closer to a meta-protocol than MGCP.

D.6 SIP

This clause is added to the initial protocol study since SIP seems to be the best candidate for interworking. Formally speaking at this point in time, TS 101 909-16 dealing with CMS to CMS is not available at ETSI. However the following differences between the TIPHON SIP and the IPCablecom "SIP+" extracted from the US CableLab documents which proposes extensions to SIP for multimedia [42].

D.6.1 PRACK

The PRACK method provides a simple extension to SIP for ensuring that provisional responses to all SIP requests are delivered reliably end to end, independent of the underlying transport mechanism. The extension works for provisional responses for any method. The extension is simple, requiring two new header fields, and one new method. The extension does not require support in proxies. The extension is indicated with the option tag "org.ietf.sip.100rel".

The reliability mechanism is based on the standard windowed acknowledgement technique. When a server generates a provisional response that is to be delivered reliably, it places a sequence number (via the RSeq header field) in the provisional response. These sequence numbers are chosen with a random initial value, for security reasons. The provisional response is then retransmitted with an exponential backoff, in a fashion that is identical to final responses to INVITE. Note that a CMS/Agent does not send a response reliably unless there was a Supported header in the request indicating support for this extension.

The reliability provided is end-to-end. Proxies do not retransmit the provisional responses; they are simply forwarded. This is similar to the way in which 200 responses for INVITE messages are handled in proxies.

NOTE: However, the PRACK message described here is sent reliably using the same hop-by-hop techniques for all non-INVITE requests. The provisional response is then received at the CMS/Agent. The CMS/Agent can determine that the response is to be transmitted reliably by the presence of the RSeq header. Responses that are not transmitted reliably do not contain the RSeq header.

D.6.2 COMET

This section discusses how network QoS establishment can be made a precondition to sessions initiated by SIP, and described by SDP. These preconditions require that the participant reserve network resources (or establish a secure media channel) before continuing with the session. We do not define new QoS reservation mechanisms; these preconditions simply require a participant to use existing resource reservation mechanisms before beginning the session. The option tag for this extension has not yet been defined at time of writing but is assumed to be "org.ietf.sip.precondition".

This results in a multi-phase session setup mechanism, with the resource management protocol interleaved between two phases of session signalling. The objective of such a mechanism is to enable deployment of robust IP multimedia services, by ensuring that resources are made available before the endpoint alerts and the participants of the session are "invited" to participate.

The general idea behind the extension is simple. A new SDP attribute, "qos" is defined. The "qos" attribute indicates whether end-to-end resource reservation is optional or mandatory, and in which direction (send, recv, or sendrecv). When the attribute indicates mandatory, this means that the participant who has received the SDP must not proceed with participation in the session until resource reservation has completed in the direction indicated. In this case, "not proceeding" means that the participant behaves as if they had not received the SDP at all. If the attribute indicates that QoS for the stream is optional, then the participant should proceed normally with the session, but should reserve network resources in the direction indicated, if they are capable. Absence of the "qos" attribute means the participant may reserve resources for this stream, and should proceed normally with the session. This behaviour is the normal behaviour for SDP.

The direction attribute indicates which direction reservations should be reserved in. If "send", it means reservations should be made in the direction of media flow from the session originator to participants. If "recv", it means reservations should be made in the direction of media flow from participants to the session originator. In the case of "sendrecv", it means reservations should be made in both directions. Either party may include a "confirm" attribute in the SDP. When the "Confirm" attribute is present, the recipient must send a COMET message to the sender, with SDP attached, telling the status of each precondition as "success" or "failure." If the "confirm" attribute is present in the SDP sent by the session originator to the participant (e.g. in the SIP INVITE message), then the participant must send the COMET message to the originator. If the "confirm" attribute is present in the SDP sent by the recipient to the originator (e.g. in a SIP response message), then the originator must send the COMET message to the participant.

The COMET method is used for communicating successful completion of preconditions from the originating to terminating CMS/Agent. The signalling path for the COMET method is the signalling path established as a result of the session setup. This can be either direct signalling between the originating and terminating CMS/Agents or a signalling path involving SIP proxy servers that were involved in the session setup and added themselves to the Record-Route header on the initial INVITE message.

The precondition information is communicated in the message body, which MUST contain an SDP. For every agreed precondition, the strength-tag must indicate "success" or "failure".

D.6.3 REFER

The REFER method extends SIP to allow one CMS/Agent to request another one to issue an INVITE to a specified CMS/Agent. The extension requires two new header fields and one new method. The extension will require support in proxies when DCS-URL modification is required. The option tag for this extension is not available at the time of writing but it is assumed to be "org.ietf.sip.refer". Further information about this extension is contained in [29]. The REFER transaction consists of the REFER request, a final response indicating the outcome, and possible 100-Trying interim responses. The REFER request must contain one Refer-To header and one Referred-By header. The intent of the REFER request is that the receiving CMS\Agent will initiate a session to the address given by the DCS-URL in the Refer-To header. The INVITE contains a copy of the Referred-By header sent in the REFER request. The final response to the REFER request is returned when the final response to the INVITE transaction has been received or the receiving CMS\Agent has rejected the REFER.

Once the REFER transaction has completed, the action of the initiator of the REFER transaction is unspecified and depends upon the specific application. Any session already set up between the issuer and receiver of the REFER request remains in place, unchanged by the REFER transaction and the INVITE transaction that it triggers. In typical usage, once the REFER has completed successfully the initiator of the REFER transaction takes down a session-leg made redundant by the new one resulting from processing of the REFER.

There is no indication that the receiver of the INVITE should alert the user before accepting the new session. Where NCS is used, it is important not to re-initiate ringing once the user has gone off-hook (although originator's name/number displays may be updated as a result of the transfer). This document therefore specifies alerting behaviour for the CMS/Agent receiving the INVITE, based on whether the session-leg indicated in the Referred-By header it receives is recognized as active at that CMS/Agent.

D.6.4 SIP header extensions

This clause describes extensions to SIP headers for support of multimedia services. This clause includes modifications to existing SIP headers as well as definitions of new SIP headers.

D.6.4.1 REMOTE-PARTY-ID

In the telephone network, calling identity information is needed to support the calling number delivery and calling name delivery services which provide the called party with identity information about the calling party prior to the called party answering the call; the calling party is here identified as the station originating the call. In order for this service to be dependable, the called party must be able to trust that the calling identity information being presented is valid. Consider for example a tele-marketer presenting himself with the identity of one of your co-workers, or, even worse, an automated credit-card activation system using calling identity information as an authentication check. In order for the calling identity information to be trustworthy, the information must come from a trusted source.

Calling identity information may also be needed to support regulatory requirements for a public telephony service. An example of this is the customer originated trace service, which enables a called party to have the identity of a calling party recorded by the telephony service provider. This enables, e.g. the receiver of harassing phone calls to make the identity of the originator of such calls available to the proper authority. Again, in order for this service to be useful, the calling identity information recorded must be trustworthy.

D.6.4.2 DCS-TRACE-PARTY-ID

In the telephone network, calling identity information is also used to support regulatory requirements such as the customer originated trace service, which provide the called party with the ability to report obscene or harassing phone calls to law enforcement. This service is provided independent of caller-id, and operates even if the caller requested anonymity. The calling party is here identified as the station originating the call. In order for this service to be dependable, the called party must be able to trust that the calling identity information being presented is valid.

To initiate a customer-originated-trace from a CMS/Agent, an additional header is defined for the INVITE request sent from the CMS/Agent. This header is called DCS-Trace-Party-ID, and does not appear in any other request or response. The CMS/Agent receiving a properly formed INVITE request with this header performs the service-provider-specific functions of recording and reporting the caller identity for law enforcement action. CMS/Agent then completes the call to either an announcement server or to the service-provider's business office to collect further information about the complaint. A CMS/Agent does not use this header, as it initiates this action locally. The option tag for this extension is not available at time of writing but is assumed to be "com.packetcable.sip.dcs".

D.6.4.3 ANONYMITY

When a call is placed, the calling identity delivery services reveal privacy information to the called party, and the calling party therefore has the option to block the delivery of this information to the called party. In the PSTN, this is typically achieved by subscribing to a calling identity delivery blocking service but can be done on an individual call basis as well. When the calling identity delivery blocking service is invoked, information about the calling party is still passed through the trusted intermediaries, however presentation restriction indicators are set in the signalling messages to signal the far-end side, that the calling identity information is not to be provided to the called party.

More generally, we may say that the service provided is that of preventing the called party from obtaining information about the calling party that may either be used to identify the party or reveal location information about the party. In an IP environment, IP addressing information may provide the other party with information to reach or identify the calling party. IP addressing information may reveal some level of location information, for instance if one has knowledge of which addresses are deployed where, or by revealing that a given caller is using a different IP-address or address block than usual.

When such a privacy service is to be provided in a SIP environment, it leads to two requirements. First, calling identity information present in SIP messages must not be delivered in an intelligible form to the called party, yet it must be possible to determine the identity of the call originator even in the case where the call is routed through one or more untrusted intermediaries. Secondly, when using SIP in an IP environment, IP addressing information must be able to be hidden from the other party. Furthermore, in an IP environment, these requirements apply equally well in the opposite direction, i.e. the calling party may wish to identify the called party and the called party may have privacy concerns as well.

The Anonymity extension allows an originating or terminating client to indicate the degree of privacy that should be provided by the service provider. The option tag for this extension is not available at time of writing but is assumed to be "org.ietf.sip.privacy".

D.6.4.4 MEDIA-AUTHORIZATION

Enhanced quality of service, as required for high-grade voice/video multimedia communication, needs special authorization for better than 'best-effort' service. Without such a capability, it is possible that a single berserk IP endpoint device can cause denial of service to a significant number of others.

The SIP Proxy authorizes the media data flow to/from an untrusted entity and supplies to the entity a media authorization token, which is to be used for authorization when bandwidth is requested for the data-stream. Currently, a trusted CMS/Agent does not use this header field. However, it is included here for future use.

When the entity is ready to send the media data-stream to the other end-point, it first requests bandwidth, using the authorization token it received from its SIP-Proxy.

The Media-Authorization extension conveys the token to a SIP UA needed in resource reservation messages to identify the connection and to associate the resources with an authorized connection. There is no option tag defined for this extension.

D.6.4.5 DCS-GATE

The DCS-Gate header extension is used only on requests and responses between CMS/Agents. The CMS/Agent-CMS/Agent signalling establishes a synchronization path that may be required by the Dynamic Quality of Service (D-QoS) specification [3] to coordinate the release of resources of the session. As per the D-QoS specification, the CMTS monitors the packet flow, and generates a Gate-Close message in response to either an explicit close request from the MTA/RGW, or when an equipment or facility failure causes the connection to be broken. This Gate-Close message is directed either to the local CMS, or to the remote CMS, or to the CMTS serving the remote MTA, depending on the capabilities of the entities. When a CMS receives such a Gate-Close message, it considers it identical to a session termination request.

The initiating proxy authenticates the UAI, and verifies the UAI is authorized to receive the requested level of QoS. In cooperation with an entity that authorizes QoS for the media streams, they generate a Media-Auth-Token that contains sufficient information for the originating client to get the authorized bandwidth for the media streams.

The initiating proxy must insert the media-authorization header in the first non-100 response message to the initial INVITE, or mid-session INVITE that require a QoS change, that it sends to UAI. remote gate, identity of the gate to be used in gate coordination messages. The option tag for this extension is not available at time of writing but is assumed to be "com.packetcable.sip.dcs".

D.6.4.6 STATE

The Distributed Session Signalling (DCS) architecture provides signalling support for creating a session using a signalling scheme so that session state is distributed to the clients.

There are three kinds of state associated with a session - transaction state, connection state, and session state. The goal with managing state is to store state about the session at places where it is needed.

Transaction state includes information about the current request and how it is being processed, how the response needs to be routed, and any partial processing done with the request that is needed in forming the response. SIP presently defines a mechanism by which transaction state associated with a request can be passed to the entity and returned in the response to the proxy - through the use of via header encryption. A proxy that encrypts the via headers can include other transaction state in the encrypted string, which can be decrypted and recovered in every provisional and final response generated to this request. DCS uses this mechanism to provide anonymity to the originator.

Connection state refers to the state associated with the media path. This includes the characteristics of the flow, admission control and policing parameters and is stored in devices in the network/media path where admission control and policing decisions are made. Connection state also includes billing information, and the unique call-identifying token (also known as the billing-correlation-id) used by the billing subsystem to correlate event records generated by the session. Connection state is distributed to the network elements during the session setup phase, and not stored by the proxy during the session.

Session state refers to entity identification, originating and terminating user preferences that affect active session characteristics, and network and transactions state hooks or identifiers in the active session that can be used by the proxy to modify the characteristics of the session. By using this mechanism, the proxies can offer the full range of required services, yet remain stateless during the session.

This state information is distributed to the UAs during session setup through the use of state headers. The state information may also be encrypted, signed, and contain an integrity check value, to guarantee detection of tampering by the untrusted client/server.

D.6.4.7 RSEQ and RACK

The RSeq and Rack headers, combined with the PRACK method described above, provide a simple extension to SIP for ensuring that provisional responses to all SIP requests are delivered reliably end to end, independent of the underlying transport mechanism. The extension works for provisional responses for any method. The extension is simple, requiring two new header fields, and one new method. The extension does not require support in proxies. The extension is indicated with the option tag org.ietf.sip.100rel.

D.6.4.8 DCS-BILLING-ID and DCS-BILLING-INFO

In order to deploy a residential multimedia service at very large scale across different domains, it is necessary for trusted elements owned by different service providers to exchange trusted information that conveys billing information and expectations about the parties involved in the session.

There are many billing models used in deriving revenue from telephony services today. Charging for telephony services is tightly coupled to the use of network resources. It is outside the scope of this document to discuss the details of these numerous and varying methods.

A key motivating principle of the DCS architecture is the need for network service providers to be able to control and monitor network resources; revenue may be derived from the usage of these resources as well as from the delivery of enhanced multimedia services such as telephony. Furthermore, the DCS architecture recognizes the need for coordination between session signalling and resource management. This coordination ensures that users are authenticated and authorized before receiving access to network resources and billable enhanced services.

Proxies have access to subscriber information and act as policy decision points and trusted intermediaries along the session signalling path. Edge routers provide the policy enforcement mechanism and also capture and report usage information. Edge routers need to be given billing information that can be logged with record keeping or billing servers.

For these reasons, it is appropriate to consider defining SIP header extensions to allow proxies to exchange information during session setup. It is the intent that the extensions would only appear on trusted network segments, should be inserted upon entering a trusted network region, and removed before leaving trusted network segments. Rules for inserting and removing headers exchanged only between proxies are for further study. Significant amounts of information is retrieved by an originating proxy in its handling of a connection setup request from a user agent. Such information includes location information about the subscriber (essential for emergency services sessions), billing information, and station information (e.g. coin operated phone). In addition, while translating the destination number, information such as the local-number-portability office code is obtained and will be needed by all other proxies handling this session.

For Usage Accounting records, it is necessary to have an identifier that can be associated with all the event records produced for the session. Call-ID cannot be used as such an identifier since it is selected by the originating user agent, and may not be unique among all past sessions as well as current sessions. Further, since this identifier is to be used by the service provider, it should be chosen in a manner and in a format that meets the service provider's needs.

Billing information may not necessarily be unique for each user (consider the case of sessions from an office all billed to the same account). Billing information may not necessarily be identical for all sessions made by a single user (consider prepaid calls, credit card calls, collect calls, etc). It is therefore necessary to carry billing information separate from the originating and terminating party identification. Furthermore, some billing models call for split-charging where multiple entities are billed for portions of the session.

It is the intent that the billing extensions would only appear on trusted network segments, and MAY be inserted by a proxy in INVITE requests entering a trusted network segment, and removed before leaving trusted network segments. The DCS-Billing-ID and DCS-Billing-Info header extensions are used only on requests and responses between proxies. They are never sent to, nor sent by, an untrusted CMS/Agent.

The option tag for this extension is not available at time of writing but is assumed to be "com.packetcable.sip.dcs".

D.6.4.9 DCS-LAES and DCS-REDIRECT

The DCS-LAES extension contains the information needed to support Lawfully Authorized Electronic Surveillance. This header contains the address and port of an electronic surveillance delivery function for delivery of a duplicate stream of event messages related to this session. The header may also contain an additional address and port for delivery of session content. This header is only used between proxies.

The DCS-Redirect extension contains session identifying information needed to support the requirements of Lawfully Authorized Electronic Surveillance of redirected sessions. This header is only used between proxies.

The option tag for this extension is not available at time of writing but is assumed to be "com.packetcable.sip.dcs".

D.6.4.10 Content-Disposition: Precondition

The Content-Disposition header indicates how the body or a part of a multi-part body in a SIP message is to be interpreted by the UAC or UAS. CMSS uses a new disposition type: "precondition", to indicate the presence of SDP preconditions for QoS within an initial INVITE and the 183-Session-Progress response. A general description of procedures for assuring that the required QoS is in place prior to alerting of the called party.

The "precondition" extension to the set of possible disposition types is documented is indicated with the same Option tag as the COMET method; i.e. it is assumed to be "org.ietf.sip.resource".

D.6.5 SIP response extensions

D.6.5.1 580-precondition failure

The 580-Precondition-Failure is a server failure error code. It is sent by the CMS/Agent as a final response to an INVITE request that specified mandatory QoS and/or security preconditions for the session. If those preconditions were unable to be satisfied, the CMS/Agent responds with the 580-Precondition-failure error code.

The option tag for this extension is assumed to be "org.ietf.sip.resource".

D.7 Conclusions

It is certain that IPCablecom is one of the best candidate to either interwork or to converge with TIPHON. It is felt that IPCablecom convergence to TIPHON should be reached by the time of Release 5 of TIPHON and phase 3 of IPCablecom.

D.7.1 TGCP

With respect to TS 101 909-13 [47] TGCP, TIPHON does address the broad requirements for gateway control protocols through reference point N of the TIPHON architecture. Therefore the TGCP proposals fall within the scope of existing TIPHON specifications. TIPHON notes that its current work programme does not include MGCP based gateway control protocols, but does include Megaco/H.248. TIPHON is working on a protocol mapping that embodies principles derived from the TIPHON architecture.

The significant part of work will be to work on the incorporation of TIPHON compliance into the Megaco version of TS 101 909-13 [47].

It is our understanding that there will now be an H.248 [45] version of TS 101 909-13 [47] and that this will align IPCablecom with TIPHON for that access protocol.

D.7.2 MGCP

In the case where IPCablecom would wish to continue with MGCP, to try to comply with TIPHON and to align with ETSI Standards, the MGCP will require the most work; this work includes:

- Definition of functional entities.
- Layer definitions.
- Definitions of primitives.
- Definitions of information flows.
- MSCs.
- SDLs.
- ASN.1 encoding or accept to stay with ABNF?

- Definition of conformance methods and testing not based on attaching an X mfr MGCP to an Y mfr and tuning both until they can talk.
- Provision of a priority mechanism (not necessarily provided in PSTN)?

NOTE: To avoid any possible misunderstanding, this list does not imply in any way that TIPHON is going to work on defining MGCP as a meta-protocol.

D.7.3 ISTP

At the occasion of the definition of ISTP for the annex II of ITU-T Recommendation J.165 [18], alignment with TIPHON could be contributed; ISTP is in a better shape than MGCP. Possibility of using SIGTRAN would allow easy convergence of TIPHON and IPCablecom. For the existing US Appendix, one can list the following items to have ISTP mapped into a meta-protocol:

- some MSCs are needed;
- SDLs;
- formal encoding through ASN.1 but definitions of the PDUs are already made.

D.7.4 Audio Server Protocol

After discussions, it has been decided that there will be two sub-parts to TS 101 909-19 [15] and that part 19-1 will encompass H.248 [45]/Megaco audio server specification; this will insure convergence of IPCablecom and TIPHON; this may necessitate extensions to H.248 [45] which are already underway and/or already accepted.

NOTE: It is our understanding that the provision of H.248 [45] for the Audio Server Protocol does not modify the basic structure of IPCablecom and does not imply that signals carrying MGCP are now using Megaco. So that each time an H.248 [45] interface to the outside world is provided, it will be through an internal converter.

D.7.4.1 Call Management Server Signalling

There seems to be another document in the series of protocols which deal with Call Management Server Signalling and which would be contained in TS 101 909-16. However, at the time the present document is being written, those documents are not available. A US counterpart of that document is now publicly available for CMS to CMS version 2 [42]. It is this version which is used in the SIP extension in clause D.6.

Annex E:
Quality of Service

There are several aspects to the quality of service; one aspect deals with the quality of speech transmission end to end (and with possible extensions to other media such as video, fax etc.); one aspect deals with the performance of signalling and call related parameters such as call set-up delay, call clearing delay, transmission delay, lost calls, stolen calls; another aspect is error rate end to end including lost packets.

The concept of dynamic Quality of Service which is not defined by IPCablecom could be picked up with different meanings.

In the context of IPCablecom, dynamic QoS is understood as the user may ask for different QoS as his/her call evolves; the call could start as a high quality audio, switch to fax then down to low quality audio.

E.1 TIPHON QoS architecture

In the context of TIPHON, dynamic QoS is understood to be allocation of overall resource in a dynamic way; however, once the resource are allocated for a call they do not change unless one of the resource on the link changes its characteristics; for example if its error rate suddenly increases.

E.1.1 TIPHON architectural planes

The Generalized TIPHON Architecture is shown in figure E.1.

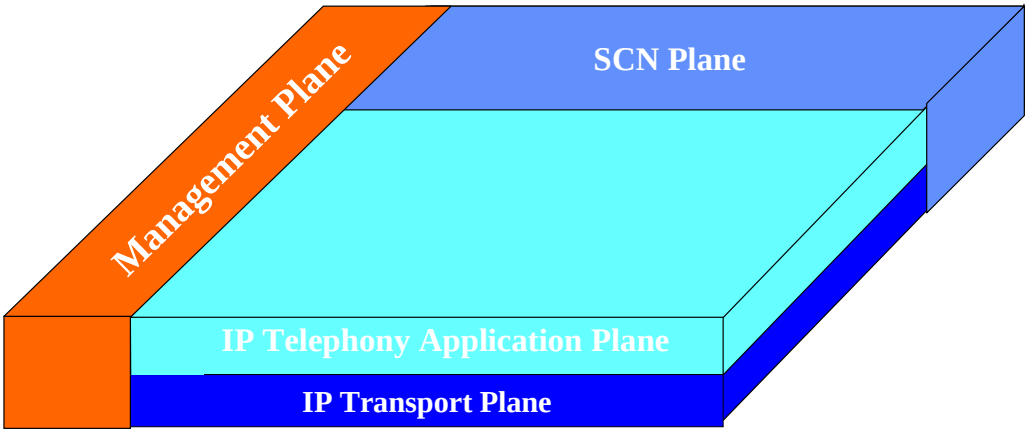


Figure E.1: Generalized TIPHON architecture

End to end QoS signalling and control will in general involve QoS information flows in each of the architectural planes.

The Required end-to-end QoS levels are established within the IP Telephony Application Plane between end users and service provider(s) and decisions determining QoS, specific to the application, will take place in the IP Telephony Application Plane (e.g. codec type, packetization etc).

The IP Transport Plane (IP network operators) provides a QoS service to the Application Plane (service providers). QoS control within the IP Transport Plane is the responsibility of the IP network operators.

E.1.1.1 IP telephony application plane

Within this plane, QoS parameters specific to the application are requested, authorized, signalled, controlled and accounted.

E.1.1.2 IP transport plane

Within this plane, general non-application specific parameters effecting QoS must be controlled and accounted to achieve the QoS requirements requested by the application.

E.1.1.3 Management plane

Within this plane QoS management entities applicable to both application and transport planes will reside and information flows applicable to QoS management will terminate.

E.1.2 Service and transport domains

A TIPHON-compliant deployment will in the general case be made up of a number of separate services and end-user domains, each representing the domain of control of an ITSP or end-user. These domains will generally be restricted to IP telephony application plane functionality. e.g. gatekeepers, softswitches, call agents etc.

Similarly, a TIPHON-compliant system will, in general, also be made up of a number of separate Transport Domains. transport domains consist solely of transport related functionality; this includes IP routers and switches, firewalls etc. Each transport domain may have its own QoS policies and/or differ from other domains in terms of administrative control (e.g. network operator), QoS mechanisms (RSVP /IntServ, DiffServ, MPLS), access, metering, addressing schemes (global, local) and transport protocol (IPv4, IPv6) etc.

Since these policies are local, functional entities are needed to interface to other domains. These entities are called InterConnect functions.

E.1.2.1 End to End QoS control

End-to-end QoS control across multiple domains may be achieved in one of two ways:

a) By having an IP telephony application service domain control each transport domain. The service domain would request the transport resources with QoS from each of the transport domains and establish the interconnect in a controlled fashion.

b) By means of end-to-end signalling within and between transport domains which share common policies.

These two mechanisms are explained below.

E.1.2.2 IP application plane control

In this first case, the routing of the call between transport domains is under the control of the ITSPs. In this general case, where the transport plane is made up of a number of heterogeneous transport domains, each domain may have its own QoS mechanisms and policies.

Figure E.2 illustrates the general case where a number of separate ITSPs and transport domains are involved in a call. Call-Control signalling takes place in the IP telephony application plane between ITSPs and between end users and ITSPs. Transport flows are between end users and transport domains and between transport domains. QoS signalling and SLAs are between end users and ITSPs and between ITSPs and follow call routing. Between each ITSP involved in the call and its associated transport domain(s) QoS SLAs then ensure that the required QoS parameters are met by each transport domain involved in the call.

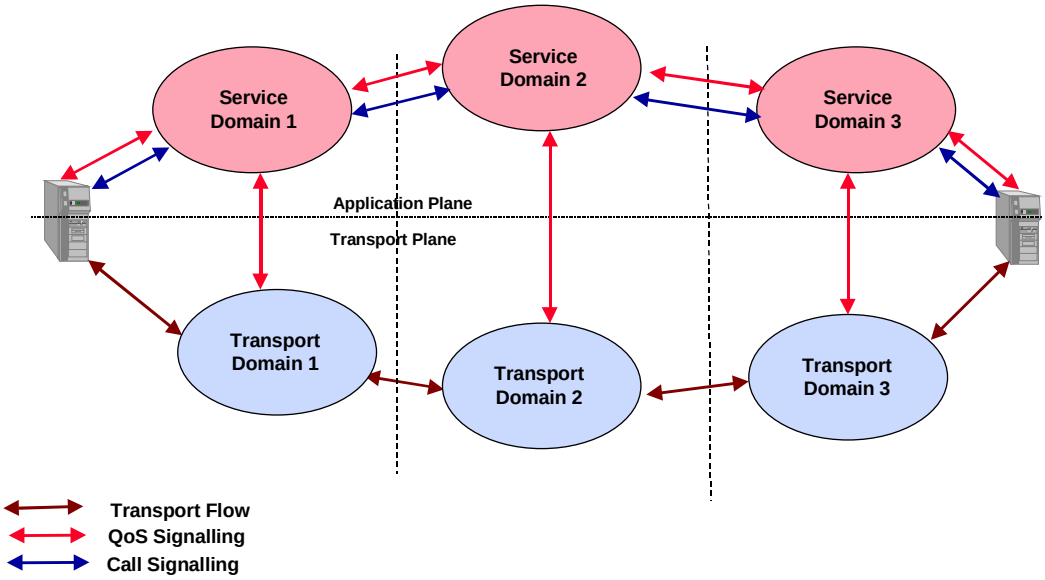


Figure E.2: Generalized TIPHON Architecture with Service Domain End-to-end QoS Control

E.1.2.3 Transport plane control

In this case, the QoS control of the call between transport domains is performed by the local transport domain and by agreement between transport network operators. QoS SLAs are required between End-Users and ITSPs and between transport network operators. The end-users may first register with their ITSP and receive authorization to make a call before establishing a media connection with the local transport network operator.

This approach is a viable option where the transport plane comprises a single homogeneous policy space. Addressing, Access and QoS mechanisms and policies all have to be uniform for this case to work.

Figure E.3 illustrates the case where end-to-end control of QoS is performed by signalling in the transport plane with QoS authorization by the access service provider.

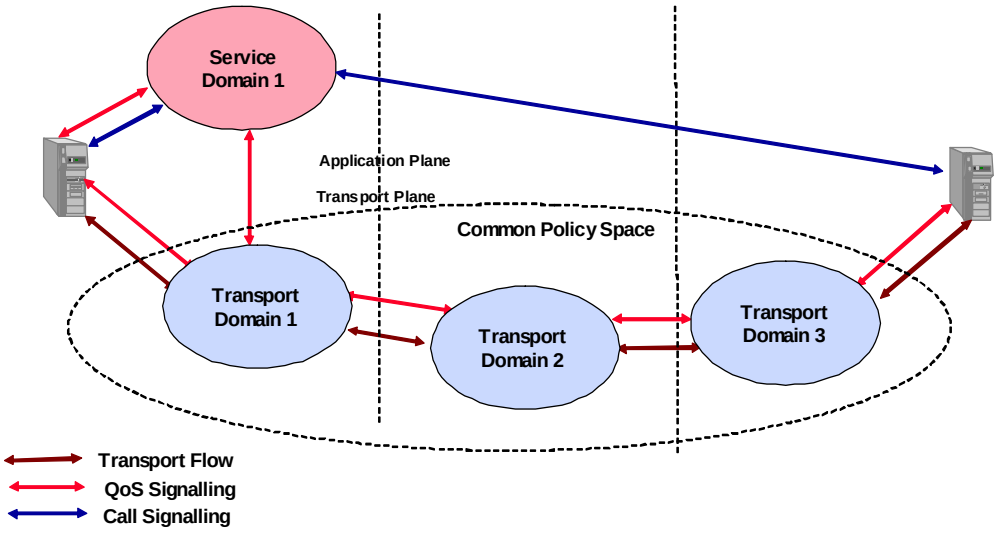


Figure E.3: Generalized TIPHON architecture with transport plane end-to-end QoS control

Hybrid situations are possible where a service domain may control several transport domains or one transport domain may control others.

E.1.3 QoS functional elements

The TIPHON QoS mechanisms have elements in both the transport and in the IP telephony application plane. They are described in this clause.

The following functional elements are involved in the QoS control framework.

E.1.3.1 QoS Service Manager (QoSM)

A functional entity that mediates requests for end-to-end QoS in accordance with policy determined by the QoSPE. It communicates with, other QoSMs and with TRMs to determine, establish and control the offered QoS.

E.1.3.2 QoS Policy Entity (QoSPE)

A functional entity that manages IP telephony QoS policies and provides authorization of permitted and default QoS levels. It receives requests from and issues responses to QoSMs to establish the authorized end-to-end QoS levels.

E.1.3.3 Transport Resource Manager (TRM)

A functional entity that applies a set of policies and mechanisms to a set of transport resources to ensure that those resources are allocated such that they are sufficient to enable QoS guarantees across the domain of control of the TRM.

E.1.3.4 Transport Policy Entity (TPE)

A functional entity that maintains the policies of a transport domain.

E.1.3.5 InterConnect Function (ICF)

A functional entity that interconnects transport domains. It provides a policy and/or administrative boundary and may police authorized transport flows between two transport domains to ensure they are consistent with the QoS policy specified by the relevant transport resource manager.

E.1.3.6 Transport Function (TF)

A functional entity representing the collection of transport resources within a transport domain which are capable of control by a Transport Resource Manager.

E.1.3.7 Relationship between Functional Entities

The relationship between these QoS Functional Entities is shown in figure E.4.

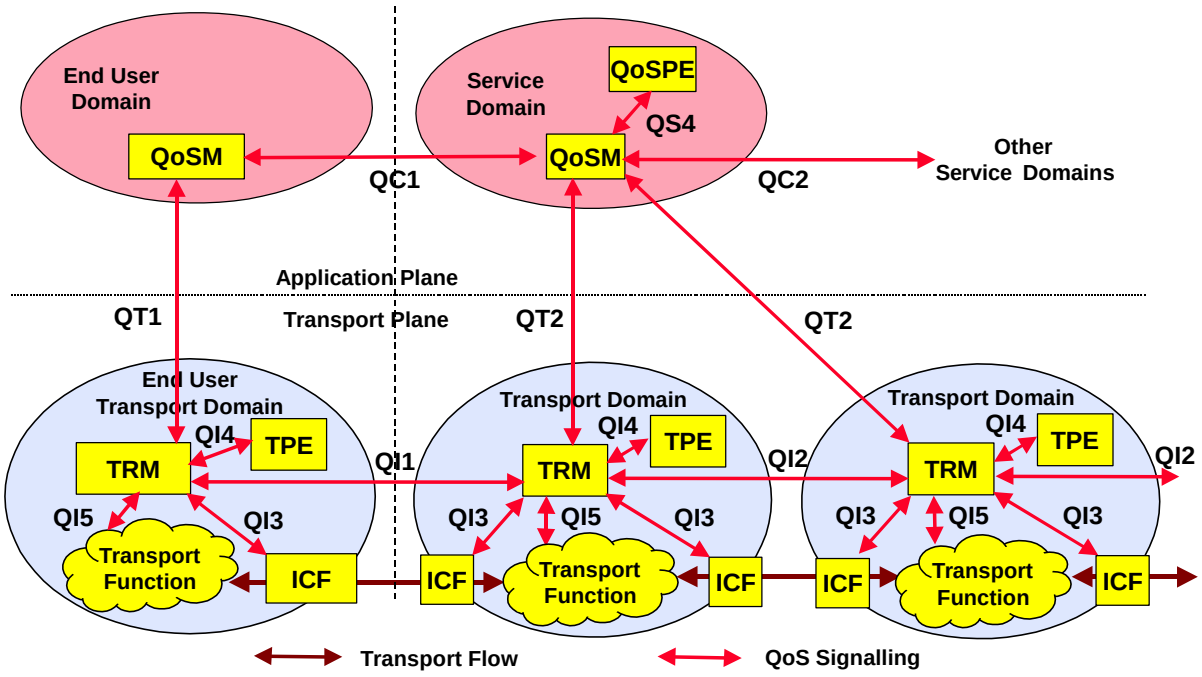


Figure E.4: TIPHON QoS Functional Entities

E.2 IPCablecom

E.2.1 General

The IPCablecom Quality of Service specifications address only the media QoS and do not address the signalling QoS, in particular they do not address the call set up times, the call clearing time.

The framework for IPCablecom QoS includes:

- low delay (not more than 300 ms round trip delay).
- low packet loss both for voice quality and data quality.
- short post-dial delay (of the order of one second).
- short post pick-up delay (less than a few hundred milliseconds, ideally less than 100 ms).

In order to fulfil those objectives, a coordination function is needed between signalling and resource management; this coordination function will ensure that:

- users are authenticated and authorized before receiving access to the enhanced QoS associated with the service;
- network resources are available end-to-end before alerting the destination MTA;
- the use of resources is properly accounted for, consistent with the conventions of traditional voice-grade telephone service (to which some IPCablecom services are similar from a customer perspective) in which charging occurs only after the party receiving a communication picks up.

It has been desired that the mechanisms used to implement the session be based on existing standards and practices, and also that the results of this work be usable to support alternative call models.

This lead to:

- the use of the IETF Real Time Protocol (RTP) to carry multimedia data, carried over the IETF User Datagram Protocol (UDP);
- the use of a superset of the IETF Resource reSerVation Protocol (RSVP+} for in-band signalling to set up Quality of Service.

The QoS architecture should provide support for new emerging applications that are dependent on multicast data delivery. Although this is not a strict requirement in the QoS architecture, providing support for multicast will enable the future development of a rich set of multimedia applications.

For purposes of managing Quality of Service, the bearer channel for a session is managed as three distinct segments: the access network for the originating side of the session, a backbone network, and the access network for the terminating side of the session. Network resources and flows are managed on the basis of ITU-T Recommendation J.112 [4]. Backbone resources may be managed either per-flow or, more likely, through an aggregated quality of service mechanism.

E.2.1.1 Intra-domain

The QoS specification addresses mostly the access network QoS; the access network is the part of the network between the MTA and the Access Node (AN). The protocols for backbone network resource management are outside the scope of the quality specification.

IPCablecom addresses requirements for a client device to obtain access to network resources. In particular, it specifies a comprehensive mechanism for a client device to request a specific Quality of Service from the network. IPCablecom defines only at this point in time the QoS Architecture for the "Access" portion of the IPCablecom network, provided to requesting applications on a per-flow basis; the access portion includes only the part between the MTA and the Access Node. The total QoS will therefore be the concatenation of the "up" link access QoS and the "down" link access QoS; up link is considered as the link from one MTA to the AN; down link is the link from the AN to the MTA at the other end of the session. Up link is equivalent to local and down link is equivalent to remote.

The general objective of IPCablecom QoS was initially to be of a better or equal speech transmission quality as the one perceived in normal PSTN operation; it has now been reduced to as good as normal PSTN speech transmission quality for economic reasons. Another general concept is that IPCablecom introduces the concept of dynamic quality of service which may vary along the call.

Resources are allocated on the ITU-T Recommendation J.112 [4] network for individual flows associated with each session of an application, per subscriber, on an authorized and authenticated basis. A DQoS session, or simply a session, is defined by this specification to be a single bi-directional data flow between two clients. When a multimedia application needs multiple bi-directional data flows (e.g. one for voice and a separate for video), separate DQoS sessions are established for each. Applications may use only half of the session's bi-directional data flow, thereby providing send-only or receive-only services.

Two IPCablecom call signalling protocols are being defined network-based call signalling (ITU-T Recommendation J.162 [40]) and distributed call signalling (IETF RFC 2543 [33]). This Dynamic QoS specification is the underlying QoS framework for both of these call signalling protocols. QoS is allocated for flows associated with a session in concert with the signalling protocol.

The concept of a segment-by-segment QoS framework is introduced; notably, a "local" provider and a "remote" provider may allocate and handle their QoS to insure a total QoS.

Different charging are provided and left to the discretion of the service provider, each charging corresponding to a possible different QoS.

It is important to ensure that resources are available before the two parties involved in the session are invited to communicate. Thus, resources are reserved before the recipient of the communication is notified that someone is trying to initiate a communication. If there are insufficient resources for a session, then the session is blocked.

The protocols developed for IPCablecom explicitly recognize the need to ensure that there is no potential for fraud or theft of service by endpoints that do not wish to cooperate with the call signalling and QoS signalling protocols with the intent of avoiding being charged for usage. This specification introduces the concept of a two-phase activation for resource reservation (reserve and commit).

While not clearly defined in the IPCablecom specifications, it is understood that dynamic QoS means that the resource with the proper quality of service is actually allocated only as the call is cut through. It is our understanding that dynamic has also the meaning that billing is associated to the actual allocation of QoS resource.

Another meaning of dynamic appearing at several occasions in IPCablecom QoS specifications is the dynamic adjustment of QoS parameters in the middle of sessions (going from speech to fax and then back to speech).

The following list presents the QoS requirements for supporting multimedia applications over IPCablecom Networks.

1) Provide IPCablecom accounting for the QoS resources on a per-session basis.
2) Support both two-phase (reserve-commit) and single-phase (commit) QoS activation models.
3) Provide IPCablecom defined policies to control QoS in both the J.112 network and the IP backbone.
4) Prevent (minimize) abusive QoS usage.
5) Provide admission control mechanisms for both upstream and downstream directions in the J.112 network.
6) Use QoS mechanism of the J.112 MAC layer.
7) Policy is enforced by the AN.
8) IPCablecom entities must be as unaware as possible of specific J.112 [4] QoS primitives and parameters.
9) Reclamation of QoS resources for dead/stale sessions.
10) Dynamic QoS policy changes.
11) Absolute minimum session set-up latency time and post pick-up delay.
12) Multiple concurrent sessions.
13) Dynamic adjustment of QoS parameters in the middle of IPCablecom sessions.
14) Support multiple QoS control models.
15) Support both embedded-MTA and standalone-MTA QoS signalling.

The IPCablecom QoS architecture seems centralized on the AN; this seems contradictory with the distributed architecture of network call signalling and of IP based networks; it also may create some problems when interworking or interfacing with non IPCablecom based networks.

The IPCablecom QoS architecture is based upon J.112 [4], IETF RSVP+, and IETF Integrated Services Guaranteed QoS.

NOTE: RSVP+ indicates extension to the present RSVP in particular to allow for dynamic QoS.

E.2.1.2 Inter-domain

The QoS is not described in the case of inter-working with ISDN since that inter-working is not offered at this point in time.

The requirements for inter-domain operation are:

- Provide acceptable call setup times, comparable to those in the PSTN.
- Provide acceptable voice quality by providing mechanisms to guarantee sufficiently small delay, jitter, and packet loss.

- Ensure high quality is maintained for the entire duration of the session (e.g. block new call attempts when their completion would compromise the quality of existing calls).

The solutions proposed by TS 101 909-17 [32] consist more in a shopping list than an actual set standard; all solutions reside in the use of RSVP IETF RFC 2205 [28] which is mandatory. If an MTA does not support RSVP, the AN to which it is attached will replace it. Different algorithms for reservation are proposed using RSVP, RSVP per hop, aggregate RSVP.

They all assume that between two IP Cable domains there is a managed IP network; those solutions are not described/defined when the inter-domain core network is composed of other elements than an IP managed network such as ISDN, PSTN, ATM, etc.

Table E.1 illustrates the possible approaches in the case of an inter-domain through a managed IP network.

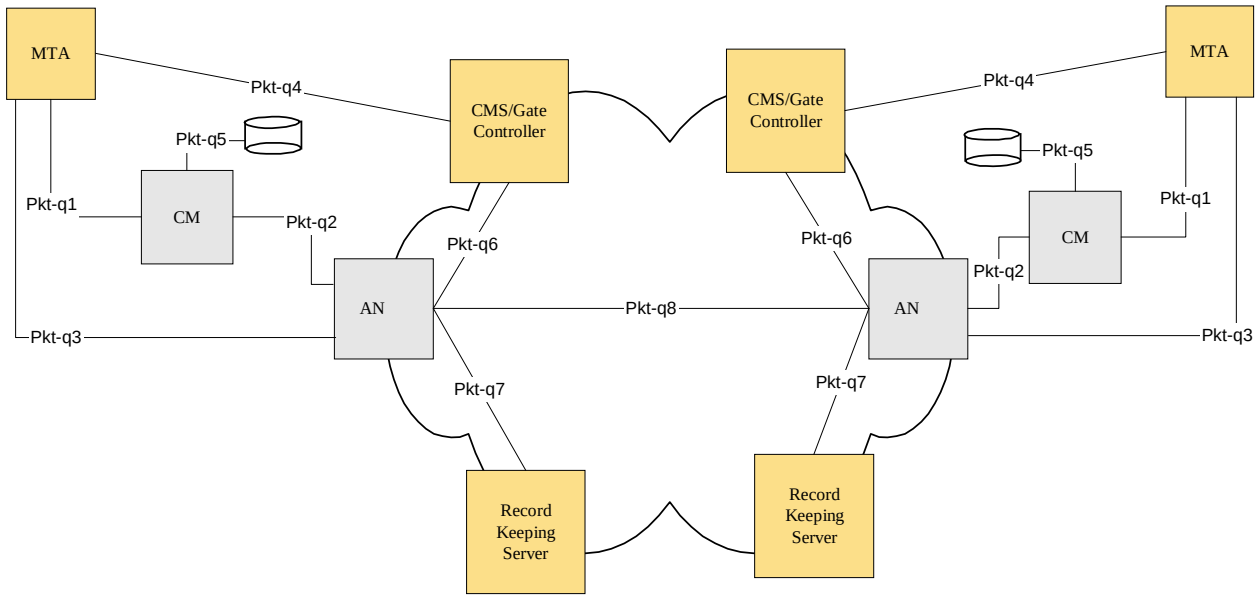
Table E.1

Approach	Required sections of TS 101 909-17 [32]			Comments
DiffServ	DiffServ			
Per flow RSVP	DiffServ	Per flow RSVP control plane		DiffServ is required for all IPCablecom backbone networks. IPCablecom devices must support DiffServ requirements contained in that section.
Aggregate RSVP	DiffServ	Per flow RSVP control plane	Aggregate RSVP	If per flow RSVP is supported 5and this is optional), then those section requirements re mandatory.
BW Broker	DiffServ	BW broker		

E.2.2 QoS Interfaces

E.2.2.1 Intra-domain

Quality of service signalling interfaces are defined between many of the components of the IPCablecom network as shown in figure C.7 already given in annex C. Signalling involves communication of QoS requirements at the application layer (e.g. SDP parameters), network layer (e.g. RSVP [3]), and at the data-link layer (e.g. J.112 QoS). Also, the requirement for policy enforcement and system linkages between the OSS subscriber provisioning, admission control within the managed IP backbone, and admission control within the network creates the need for additional interfaces between components in the IPCablecom network.



NOTE 1: This figure shows a number of interfaces without layer definitions.
NOTE 2: Some of those interfaces may share some lower layers.
NOTE 3: The relation between those interfaces and those shown for network signalling is not obvious.

Figure E.5: QoS signalling interfaces in IPCablecom network

The use/reuse of existing protocols has been encouraged; as a result, the IETF Real Time Protocol (RTP) is used to carry multimedia data over the IETF User Datagram Protocol (UDP) and in-band signalling to set up Quality of Service is carried out using a superset of the IETF Resource Reservation Protocol (RSVP).

For purposes of managing Quality of Service, the bearer channel for a session is managed as three distinct segments: the access network for the originating side of the session, a backbone network, and the access network for the terminating side of the session. Network resources are managed on the basis of ITU-T Recommendation J.112 [4]. Flows, using the mechanisms defined in ITU-T Recommendation J.112 [4]. Backbone resources may be managed either per-flow or, more likely, through an aggregated quality of service mechanism. Management of backbone resources is outside the scope of this specification. Figure E.6 shows the IPCablecom QoS framework.

IPCablecom assumes same QoS parameters in both directions of flows; could TIPHON handle different quality of services for different directions of flow? This could become of interest in particular in the case of conference or multi party calls and for audio server applications.

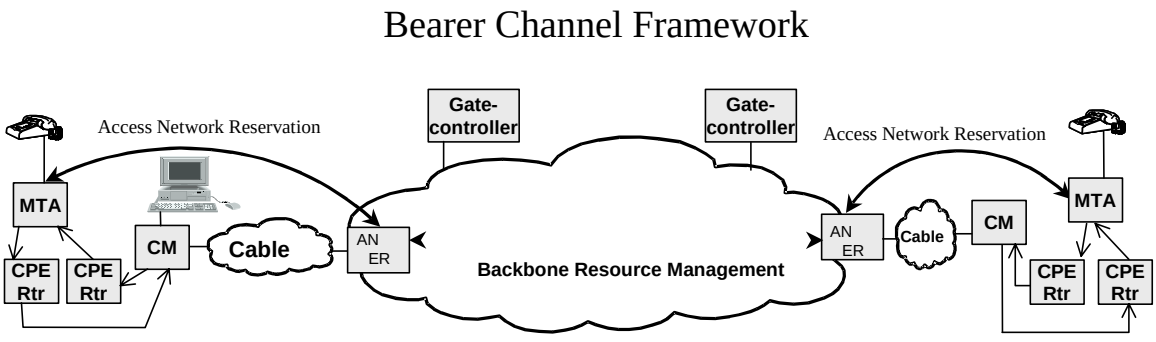


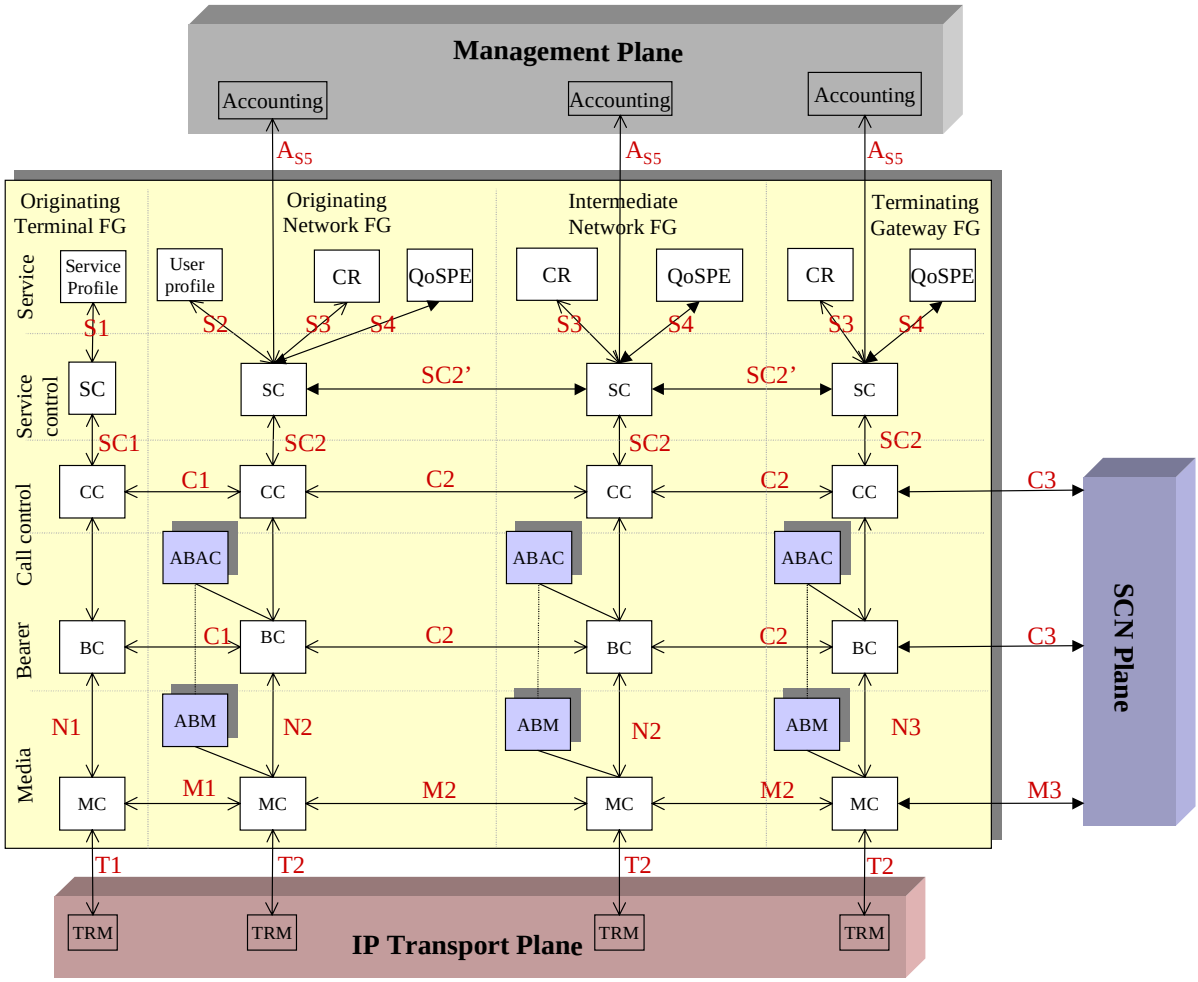
Figure E.6: Session framework

Table E.2 gives a mapping to the TIPHON interfaces to the IPCablecom interfaces.

Table E.2: DQoS interfaces of IPCablecom vs. TIPHON QoS interfaces

Interface	Description	DQoS embedded/ standalone MTA	TIPHON corresponding interfaces
pkt-q1	MTA - CM	N/A	NONE
pkt-q2	CM - AN	J.112 QoS, AN-initiated	NONE
pkt-q3	MTA - AN	RSVP+	QI1
pkt-q4	MTA - GC/CMS	NCS/DCS	QC1
pkt-q5	CM - Provisioning Server	N/A	QI4?
pkt-q6	GC - AN	Gate Management	QS4
pkt-q7	AN - RKS	Billing	QI6
pkt-q8	AN - AN	Gate Management	QI2

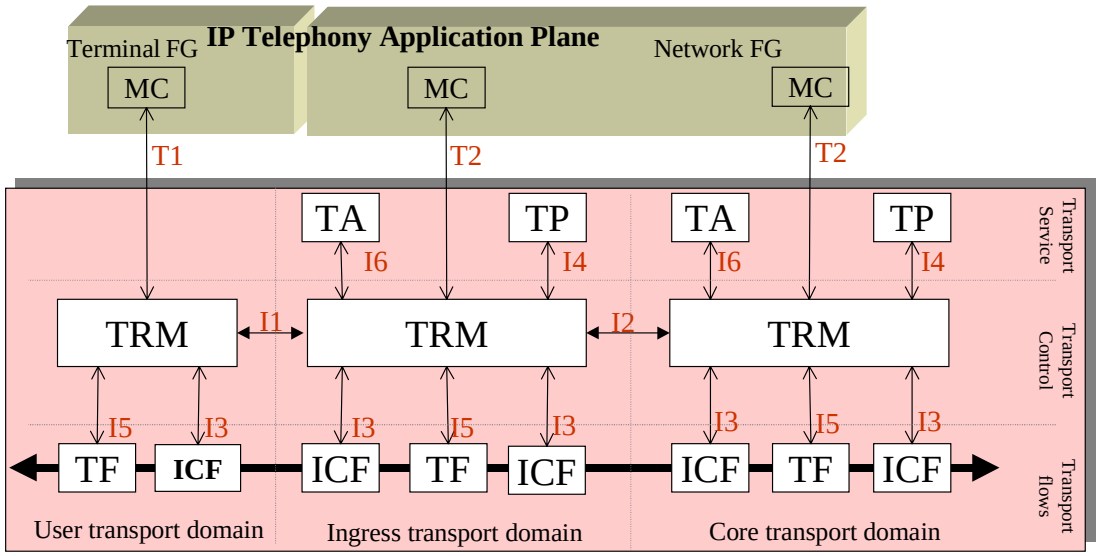
Figure E.7 recalls the architecture layered model of TIPHON.



NOTE: For the QoS interfaces, one should add a Q in front of the name of each interface in the figure above.

Figure E.7: Reference points for the TIPHON Scenario 1; user at home

Figure E.8 shows the reference points of the TIPHON transport layers in relation to the QoS algorithms.



NOTE: For the QoS interfaces, one should add a Q in front of the name of each interface in the figure above.

Figure E.8: Reference points in the IP transport plane

The mapping of interfaces has an interest in the case of IPCablecom convergence towards TIPHON; that mapping has little interest in the case of interworking. In the case of interworking, one has to detail the parameters available for QoS on both sides of the interworking interface and to convert those parameters using the proper protocol.

E.2.2.2 Inter-domain

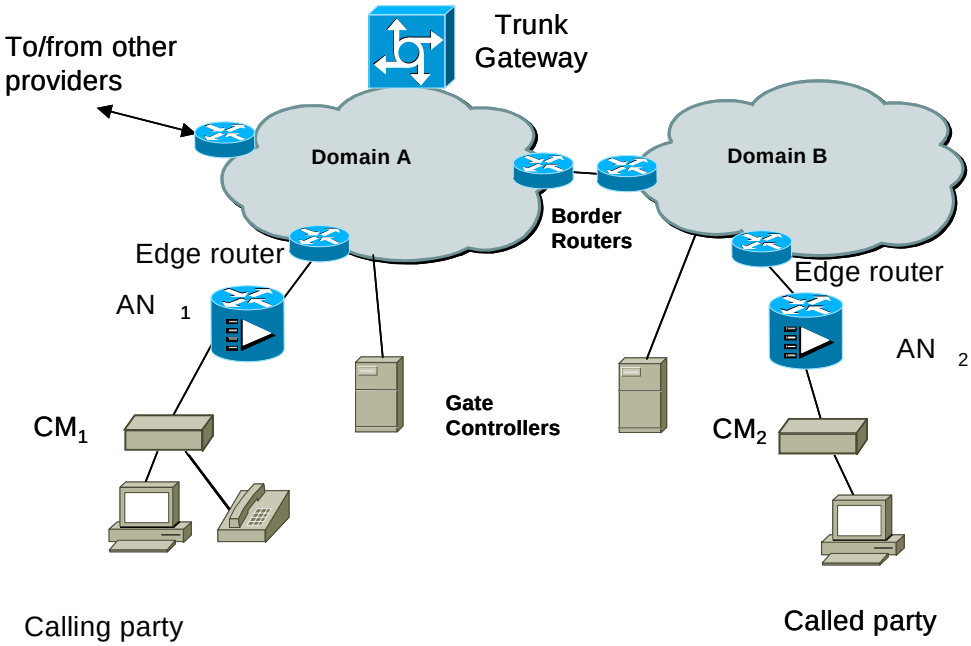


Figure E.9: Inter-domain QoS architecture

Before going into more details of some of the IPCablecom interfaces descriptions, a general theory of operation of IPCablecom for quality of service operation will now be given.

E.2.3 Theory of operation

E.2.3.1 Basic session set-up

Resource reservation is partitioned into separate reserve and commit phases. At the end of the first phase, resources are reserved but are not yet available to the MTA. At the end of the second phase, resources are made available to the MTA and usage recording is started so that the user can be billed for usage.

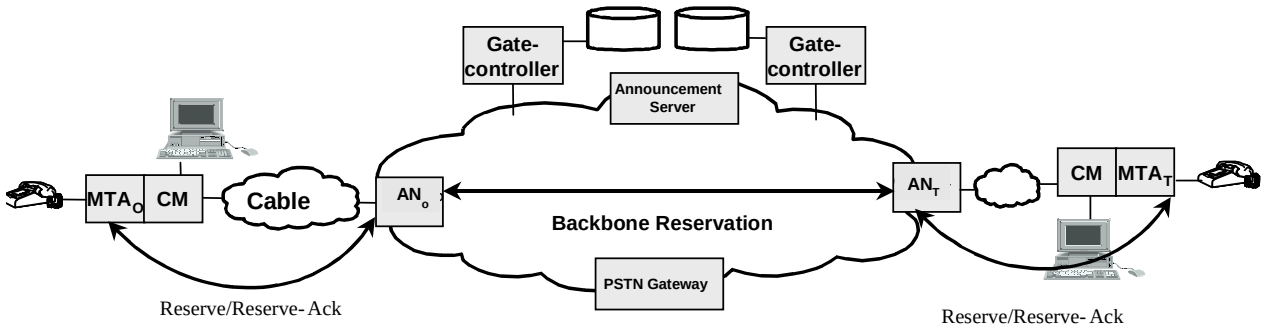


Figure E.10: Resource management Phase 1

Figure E.10 shows the first phase of the resource management protocol for a multimedia application. In this description, subscripts "O" and "T" designate the originating and terminating points of the call. The MTA can be either a standalone VoIP host or an embedded MTA; the latter is shown in figure E.9. MTA_O and MTA_T request resource reservation (PATH message in RSVP [3], or J.112 message in the optional interface for embedded clients) to AN_O and AN_T respectively. AN_O and AN_T perform an admission control check for resource availability (initiating signalling for resource reservation in the backbone if necessary) and send a reply to the respective MTAs. In the RSVP [3] framework, the RESV message from the AN (where the gate resides) is the acknowledgment to the MTA.

Figure E.11 shows the second phase. After determining that resources are available, MTA_O sends a RING message to MTA_T instructing it to start ringing the phone. MTA_T sends a RINGING indication to MTA_O indicating both that resources are available and that the RING message was received. When the called party picks up the phone, MTA_T sends an ANSWERED message to MTA_O and a COMMIT message to AN_T. When MTA_O receives the ANSWERED message, MTA_O sends a COMMIT message to AN_O. The COMMIT messages cause resources to be allocated for the call in the networks. The arrival of the COMMIT messages at AN_T and AN_O causes them to open their gates, and also starts accounting for resource usage. To prevent some theft of service scenarios, the ANs co-ordinate the opening of the gates by exchanging GATE-OPEN messages.

The RING, RINGING, and ANSWERED messages shown in this figure and in the above description are logical equivalents to the call signalling messages exchanged by TS 101 909-4 [24] and IETF RFC 2543 [33].

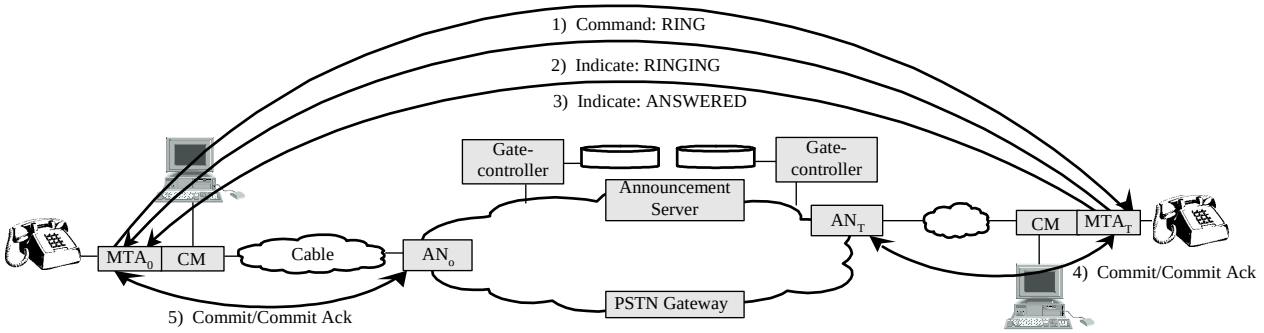


Figure E.11: Resource management Phase 2

E.2.3.2 Gate co-ordination

QoS signalling leads to the creation of a gate at each AN associated with a client involved in the session. Each gate maintains usage data for the session and controls whether the packets generated by the associated client receive access to enhanced QoS. Gate co-ordination is needed to prevent fraud and theft of service in situations where a malfunctioning or modified client does not issue the expected signalling messages. It is essential that protocol mechanisms are robust against abuse. A gate co-ordination protocol ensures that:

- A potential for one-way session establishment without billing is avoided. Because the clients may have adequate intelligence and are not trusted, one can envisage the clients establishing two one-way sessions to provide the users with an adequate interactive voice communication channel. Gate co-ordination prevents such sessions being established without the provider being able to charge for them.

- The resources reserved and committed by the two clients are consistent with the results of capability negotiation. If only one client pays for a session, it is important that the resources that are reserved and used are consistent with the expectations of the payer. Gate co-ordination prevents a malicious session recipient from defining session characteristics that will result in an unexpectedly high charge to the originator.

- The gates open and close virtually simultaneously (i.e. within a few hundred milliseconds of each other). Gate co-ordination assures that billing data at the two ends of the session is consistent so that the cost of the session does not depend on which end is paying for it.

E.2.3.3 Changing the packet classifiers associated with a gate

Once a pair of gates is set up, clients can communicate over the network with enhanced QoS. Several features needed for a commercial voice communications service involve changing the clients involved in a session, for example when a session is transferred or redirected, or during three-way calling. This requires the packet classifiers associated with a gate to be modified to reflect the address of the new client. In addition, changing the endpoints involved in a session may affect how the session is billed. As a result, gates include addressing information for origination and termination points.

E.2.3.4 Session resources

The relationship between different categories of resources, authorized, reserved, and committed, is shown in figure E.12. A set of resources is represented by an *n*-dimensional space (shown here as two-dimensional) where *n* is the number of parameters (e.g. bandwidth, burst size, jitter, classifiers) needed to describe the resources. The exact procedures for comparing *n*-dimensional resource vectors are given in ITU-T Recommendation J.112 [4].

When a session is first established, DQoS protocols authorize the use of some maximum amount of resources, indicated by the outer oval, specifying the authorized resources. When a client makes a reservation for a session, it reserves a certain amount of resources, which are not greater than those for which it has been authorized. When the session is ready to proceed, the client commits to some amount of resources, which are not more than the reserved resources. In many common cases, the committed and reserved resources will be equal. The committed resources represent resources that are currently in use by the active session, whereas reserved resources represent those that are tied up by the client and have been removed from the pool for admission control purposes, but which are not necessarily being used by the client.

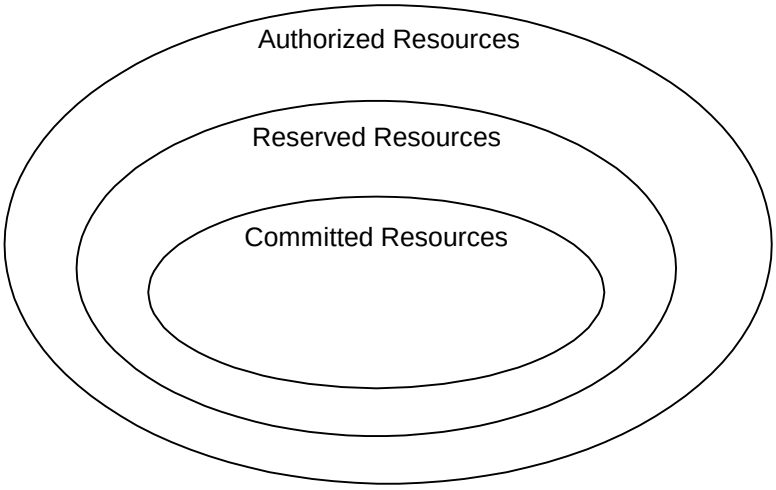


Figure E.12: Authorized, reserved and committed resources

Authorizations only affect future resource reservation requests. Resources that have been reserved prior to an authorization change are not affected.

Resources that have been reserved but not committed are available to the system for short-term uses only, such as handling of best-effort data. These resources are not available for other reservations (i.e. overbooking is not allowed). The maximum portion of the available resources that can be reserved at once is a policy decision by the AN, and outside the scope of DQoS.

Excess resources reserved above those committed are released unless the client explicitly requests they be kept through periodic reservation refresh operations. Maintaining such a condition for long periods of time is discouraged, as it reduces the overall capacity of the system. However, there are situations (e.g. call waiting service, where the call on hold requires resources beyond those needed for the active call) where excess reservations are necessary.

E.2.3.5 Admission control and session classes

It is envisaged that the gate at the AN may use one or more session classes for resources reserved from an MTA. Session classes define provisionable admission control policies, or their parameters. It is expected that the provider would provision the necessary parameters and/or the alternative admission control policies in the AN and in the Gate Controller. For instance, a session class for normal voice communications, and an overlapping session class for emergency calls could be defined to allow the allocation of up to, respectively, 50 % and 70 % of the total resources to these classes of calls, and leaving the remainder 30 % to 50 % of the total bandwidth available to other, possibly lower priority, services. Session classes may furthermore enable pre-emption of already reserved resources, in which case the policy for such pre-emption would be provisionable by the service provider. When the authorized envelope is communicated to the gate at the AN by the Gate Controller in the Gate-Set message, the Gate Controller includes adequate information to indicate which session class should apply when the corresponding RESERVE request is processed.

E.2.3.6 Resource renegotiations

Several of the supported session features require renegotiations of the QoS parameters associated with a session during the lifetime of the session. For example, clients might start communicating using a low-bit-rate audio codec. They can subsequently switch to a higher bit-rate codec or add a video stream, as long as the requested QoS is within the authorized envelope and there is available bandwidth on the network. The use of an authorized QoS envelope that is pre-authorized by the Gate Controller acting as the policy decision point gives clients the flexibility to renegotiate QoS with the network without requiring subsequent Gate Controller involvement. This essentially means that use of resources up to the limits of the envelope is pre-authorized but NOT pre-reserved. Successful allocation of resources within the authorized envelope requires an admission control decision, and is not guaranteed. Subsequent to admission control, the resources are reserved for the flow, although the actual usage of the resources is permitted only after the commit phase of the Resource Reservation protocol completes. However, no admission control decision is required at the time of commitment of resources. Each change in commitment of resources within the limits of the admission control decision does not require a further reservation. All reservation requests that pass admission control MUST fit within the authorization envelope.

E.2.3.7 Dynamic binding of resources (re-reserve)

The Dynamic QoS Architecture recognizes that there may be a need to share resources across multiple sessions, especially when resources are in short supply. In particular, when using the call-waiting feature in telephony-like applications, the client may be involved in two simultaneous sessions, but will be active in only one conversation at a time. It is feasible in this case to share the network-layer resources (in particular, on the access link) between the two conversations. Therefore, this architecture allows a set of network layer resources (such as a bandwidth reservation) to be explicitly identified, and allows one or more gates to be associated with those resources. Signalling primitives allow the resources associated with a gate to be *shared* with another gate at the same AN. This improves the efficiency with which resources in ITU-T Recommendation J.112 [4] network are utilized.

When switching back and forth between two sessions in a call-waiting scenario, a client needs to keep enough resources reserved to accommodate either of the sessions, which in general may not need the same amount of resources. Thus, the re-commit operation may change the committed resources. However, the reserved resources do not change in this case, as the client should not have to go through admission control when switching back to the other session.

Whereas the committed resources are always associated with the current active session (and its corresponding IP flow), the reserved resources may be bound to different flows and different gates at different times. A handle, called a resource ID, is used to identify a set of reserved resources for the purpose of binding a flow to those resources.

E.2.3.8 Support for billing

QoS signalling can be used to support a broad range of billing models, based on only a stream of event records from the AN. Since the gate is in the data path, and since it participates in resource management interactions with a client, resource usage accounting is done by the gate. The gate in the AN is the appropriate place to do resource accounting, since the AN is directly involved in managing resources provided to a client. It is also important to do usage accounting in the AN to cope with client failures. If a client that is involved in an active session crashes, the AN MUST detect this and stop usage accounting for the session. This can be accomplished using soft state through a resource management refresh message (by having RSVP [3]-PATH messages periodically transmitted for an active session), by monitoring the flow of packets along the data path for continuous-media applications, or by other mechanisms (such as station maintenance) performed by the AN. In addition, since the gate retains state for flows that have been authorized by a service-specific Gate Controller, it is used to hold service-specific information related to charging, such as the account number of the subscriber that will pay for the session. The policy function in the Gate Controller thus becomes stateless.

The support required in the AN is to generate and transmit an event message to a record keeping server on every change to the QoS, as authorized and specified by a gate. Opaque data provided by the Gate Controller that may be relevant to the record keeping server may also be included in the message. Requirements for handling of event records are contained in other Operations Support specifications.

E.2.3.9 Backbone resource management

When an AN receives a resource reservation message from an MTA, it first verifies that adequate upstream and downstream bandwidth is available over the access channel using locally available scheduling information. If this check is successful, the AN can either generate a new backbone resource reservation message, or forward towards the backbone a modified version of the resource reservation message received from the MTA. The AN performs any backbone-technology-specific mapping of the resource reservation that is needed. This enables the architecture to accommodate different backbone technologies, at the service provider's choosing. The specific mechanisms for reserving backbone QoS are outside the scope of the present document.

A bidirectional model is used for resource reservation in ITU-T Recommendation J.112 [4] network where the routing is symmetric. A unidirectional model is used for resource reservation in the backbone, which allows routing asymmetries. Thus, when MTA_O makes a reservation with the AN, it knows two things: that it has adequate bandwidth in both directions over the ITU-T Recommendation J.112 [4] network, and that it has adequate bandwidth over the backbone networks for the MTA_O to MTA_T flow. Thus, MTA_O knows that resources are available end-to-end in both directions once it gets a reply from MTA_T.

E.2.3.10 Setting the DiffServ code point

This architecture also 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. Access to the bandwidth and differentiated treatment is provided to packets with the appropriate encoding of bits in the field of the IP header specified for Differentiated Service. This is called the DiffServ Code Point (DSCP). The DS field maintains backward compatibility with the present use of the IP precedence bits of the IPv4 TOS byte (IETF RFC 2474 [34]). It is desirable to be able to set the DiffServ Code Point of packets that are about to enter the provider backbone from the Access Node (AN). Since resources consumed by these packets in the backbone may depend heavily on this marking, this architecture provides control of the marking to network entities. This allows the network and service provider the control on use of the enhanced QoS rather than trusting the MTA. The provider can configure policies in the AN that determine how to set the DSCP for flows that pass through it. Such policies are sent to the AN in the gate set-up protocol from the CMS/GC.

For implementation efficiency, we pass the information to the MTA about the appropriate DSCP for it to use on a given session. This is done with the IETF proposed DCLASS object in RSVP [3]. The AN 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.

E.2.3 A more detailed description of a few IPCablecom interfaces

pkt-q3 MTA to AN

To meet the requirements described previously, RSVP [3] and the IETF's Integrated Services architecture IETF RFC 2210 [30] is used as a basis for the signalling mechanism for providing local QoS. RSVP [3], as currently specified, needs some additional enhancements to meet the requirements of the Dynamic QoS architecture.

RSVP and the Integrated Services architecture specify QoS parameters in generic terms that are independent of the underlying layer 2 technology. It is necessary to specify a means of mapping those general traffic specifications into specific J.112 flow specifications. Such mappings exist for other layer 2 protocols (e.g. ATM, IEEE 802.2001 [48] LANs); this section describes mappings for J.112 networks.

The Dynamic QoS Architecture uses a superset of RSVP with the following differences:

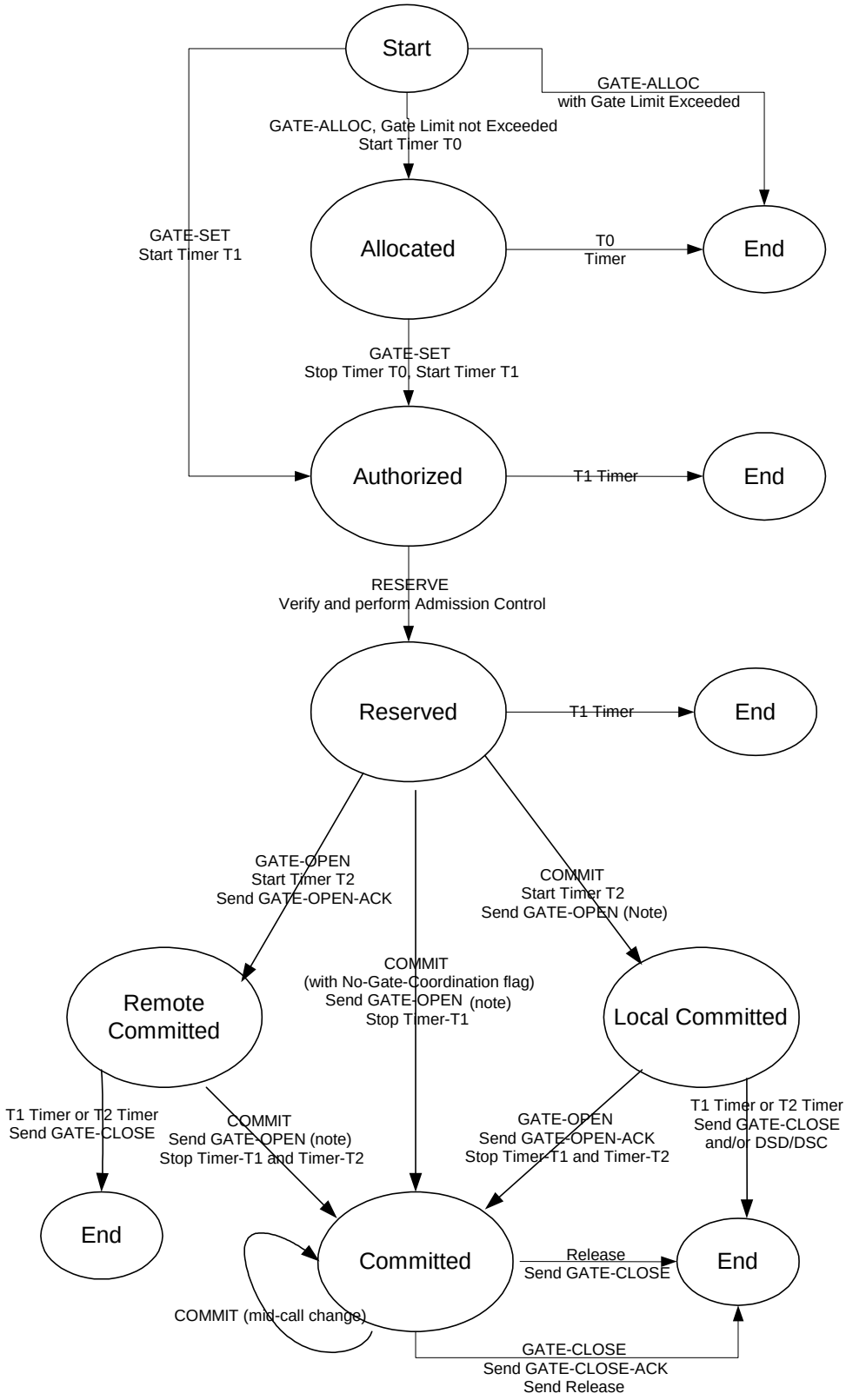
- Since resource reservations are independently initiated for each J.112 network (segmented resource allocation model), this specification does not depend on resource management messages propagating end-to-end.
- The resource management exchange between the MTA and AN reserves resources in *both* directions over the local area (i.e. customer-operated) and J.112 networks. This allows the AN to act as a proxy for the far endpoint, with the benefit of minimizing the number of messages required for resource management in bandwidth-constrained J.112 networks, and reduces the post-dial and post-pick-up delay.
- In the local area (i.e. customer-operated) portion of the network, existing RSVP-capable routers may be present. In this environment, unidirectional reservations are required. To enable these two functions (bi-directional reservations on the J.112 network and unidirectional reservations inside the customer-premises), an enhanced PATH message is issued by the MTA to the Gate.
- Ability to bind a single set of resources to a group of multiple reservations, based on information from the MTA that only one reservation in the group will be active at any given time.
- Support for the two-phase resource activation facility available in J.112, giving the ability to guarantee resources are available before ringing of the far-end phone. The RSVP exchange with the AN performs the first stage, the admission control, and the MTA sends a separate message to the AN to perform the activation.

The Dynamic Quality of Service operation does not address standard RSVP, which may or may not be supported. Regardless, standard RSVP messages will not trigger the DQoS operations specified in this document.

pkt-q6 Authorization interface

This is a particularity of the IPCablecom implementation and that is a two stage QoS process, one stage is to authorize the resource allocation and the other stage is to commit the resource; note that resource could be authorized but not available.

The following state diagram described in figure E.13 gives a good synopsis the two stages approach.



NOTE: Send GATE-OPEN unless the No-Gate-Open flag is set.

Figure E.13: Gate State Transition Diagram

The QoS admission control uses a client/server architecture and uses Common Open Policy Service (COPS) IETF RFC 2748 [29] as a database server policy.

pkt-q8 Gate-to-Gate Coordination Interface (AN-to-AN)

Messages are exchanged between the gates to synchronize their use. 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 (see figure E.13). 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.

Gate synchronization messages may be exchanged directly between the ANs, or may be exchanged through proxies (typically the IPCablecom Call Management System (CMS), who desires notification of various error cases that cause gates to be prematurely closed). Figure E.14 shows the direct gate-gate coordination, and figure E.15 shows the gate coordination through CMS-proxies at both ends. Also possible, but not shown, are configurations with a proxy at only one end.

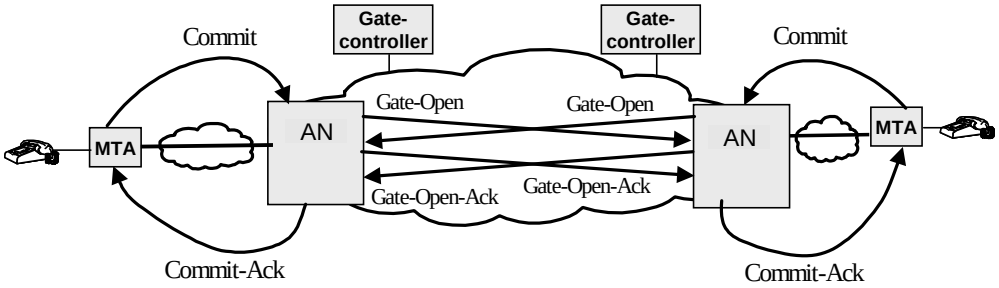


Figure E.14: End-to-end gate coordination

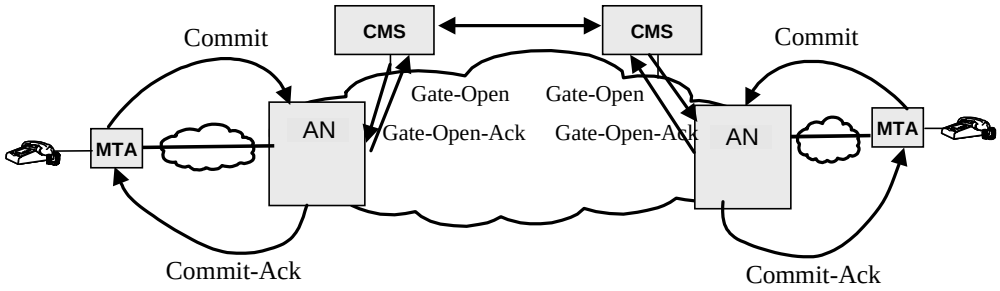


Figure E.15: CMS-Proxy gate coordination

A gate is initially created by a GATE-SET command from the Gate Controller. The GATE-SET command will contain such information as the prototype classifiers (i.e. 6-tuple) and Flowspecs for both the local and remote gates. It also contains the IP address and port number of the remote AN so they can implement Gate-to-Gate coordination.

E.3 Conclusions

With respect to TS 101 909-4 [24] and TS 101 909-17 [32], TIPHON does not preclude this form of implementation and TS 101 909-4 [24] and TS 101 909-17 [32] may be considered as minimally compliant with the TIPHON architecture and TIPHON draft protocols. TIPHON notes that TS 101 909-4 [24] and TS 101 909-17 [32] describe a statically provisioned QoS capability. As TIPHON is primarily focused on methods to achieve dynamic end-to-end QoS, in order to support the range of end-to-end QoS requirements for speech and multi-media systems it is felt that TS 101 909-4 [24] and TS 101 909-17 [32] cannot support the fundamental TIPHON capabilities. In the TIPHON approach networks with different packet transport and QoS technologies and protocols may be interconnected with guaranteed end-to-end QoS. The limitations of TS 101 909-4 [24] and TS 101 909-17 [32] imply that cablecom networks built according to TS 101 909-4 [24] and TS 101 909-17 [32] can only interconnect with like networks.

If IPCablecom wish to extend to the full feature set of PSTN / ISDN networks, future extensions to multi-media services and interworking to networks based on other technologies, these limitations will need to be addressed. TS 101 909-17 [32] does indicate that "In later sections we build on the foundation of DiffServ back bone by adding signalling capabilities to control access to resources in the backbone". TIPHON recommends that future IPCablecom studies adopt the methods of end-to-end QoS control outlined conceptually in TS 101 329-3 [31] and further developed in TS 101 882 [2] in protocol form.

IPCablecom intent is to push J.112 cable transmission as a media to the same title as ATM or LANs [48].

The introduction of dynamic QoS is certainly an interesting concept which needs a clear definition. Presently not covered by TIPHON is the change of QoS parameters during a call, for example a voice call becoming a fax call or vice-versa.

The segment by segment approach to QoS does not go into the direction of TIPHON.

In order to fully profit of interworking between a TIPHON network and an IPCablecom network in the area of QoS, some degrees of convergence needs to be reached. To reach convergence between IPCablecom and TIPHON in the field of QoS, the following main steps need to be implemented:

- improve the layer definition of the QoS interfaces for IPCablecom to come closer to the TIPHON layered approach;
- define the functional entities, the information flows, the primitives for QoS in line with the definitions of TIPHON primitives;
- define and align IPCablecom QoS classes with TIPHON classes;
- introduce the overall QoS budget approach of TIPHON into the IPCablecom segment by segment approach call parameters;
- define how DQoS IPCablecom algorithms would react to changes in QoS of one segment (degradation for example);
- define how to and establish conformance of an equipment to the DQoS algorithms;
- expand the QoS to non IP based networks such as ISDN, PSTN and more generally WANS inserted in between two IPCablecom networks (not presently covered even in part 17):
  - in particular investigate how IPCablecom could migrate to a decentralized architecture for QoS (similar to TIPHON) by opposition to the centralized AN based present architecture; this may imply distributing QoS knowledge and handling to elements such as MTA and gateways.
- elaborate if Dynamic QoS is ahead of TIPHON capability or if TIPHON can already provide DQoS and IPCablecom cannot;
- evaluate changes to IPCablecom for non speech related medias;
- elaborate the non speech related parameters in IPCablecom when using an IP managed core network (Call Set-Up time, Call Clearing time); no clear specifications exist for those parameters;

- investigate whether TIPHON QoS architecture prevents theft of service and protects from misuse:
  - the combination of QoS algorithm and security does not appear clearly in TIPHON;

NOTE: IPCablecom QoS has done a threat analysis to the protocols handling QoS and has provided solutions to protect against those threats, in particular combination of two half non charged connections result in a free call to the user misusing the network.

- investigate if TIPHON could benefit from the resource reservation mechanism defined in the inter domain QoS EN 300 659-1 [9];
- investigate why IPCablecom basically a new technology for an old POTS continuously ignores Erlang law and why TS 101 909-17 [32] is not a technical specification but a verbose description of what could be done in aggregation of aggregates of bandwidth;
- investigate why signalling of DQoS needs sometimes more signalling bandwidth than the actual media bandwidth.

Annex F: Security

At the time of preparation of this technical report, the ITU-T Recommendation J.170 [38] is picked up as the basis for the study while the TS 101 909-11 [35] is considered obsolete.

At the point of preparation of the present document, IPCablecom is the first instance of end-to-end network security implementation; TIPHON may therefore benefit from the IPCablecom experience and lead in the domain of security implementation. This annex may therefore lead to TIPHON future release definitions to converge with IPCablecom rather than IPCablecom converging towards TIPHON.

F.1 Definitions relating to security

Tentative mapping of TIPHON vs. IPCablecom terminologies first on the basic security objectives.

Table F.1: Terminology mapping

Term	TIPHON definition TS 101 323 [36]	IPCablecom definition J.170 [38]	ETR 232 [39]	ITU-T Recommendation H.235 [41]
Access control	Prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner (ITU-T Recommendation X.800 [51]).
Authentication	Property by which the correct identity of an entity or party is established with a required assurance	The process of verifying the claimed identity of an entity to another entity.	A property by which the correct identity of an entity or party is established with a required assurance.	The provision of assurance of the claimed identity of an entity (ITU-T Recommendation X.811 [52]).
Confidentiality	Avoidance of the disclosure of information without the permission of its owner	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.	The avoidance of the disclosure of information without the permission of its owner. Alternative definition: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.	The property that prevents disclosure of information to unauthorized individuals, entities, or processes.
Integrity	Avoidance of the unauthorized modification of information	A way to ensure that information is not modified except by those who are authorized to do so.	The avoidance of the unauthorized modification of information. Alternative definitions: The prevention of the unauthorized modification of information. A property by which the information contents of an object is prevented from being modified.	The property that data has not been altered in an unauthorized manner
Accountability			The principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation. Alternate definition: The property that ensures that the actions of an entity may be traced uniquely to the entity.	
Availability			Avoidance of unacceptable delay in obtaining authorized access to information or IT resources. Alternative definition: The property of being accessible and usable upon demand by an authorized entity.	

Term	TIPHON definition TS 101 323 [36]	IPCablecom definition J.170 [38]	ETR 232 [39]	ITU-T Recommendation H.235 [41]
Non-repudiation	Property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication	The ability to prevent a sender from denying later that he or she sent a message or performed an action.	Proof of the sending or delivery of data by communicating IT assemblies which prevent subsequent false denials by a user of transmission or receipt, respectively, of such data or its contents. Alternative definition: A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.	Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication.

F.2 Recall of TIPHON security

F.2.1 TIPHON security services

TIPHON defines five security services that are classified as follow:

- access control;
- authentication;
- confidentiality;
- integrity;
- non-repudiation;
- TIPHON defines also four or more protocol components (RAS, H.225.0, H.245, RTP);
- the security information flows identified in TS 101 312 [23] (S1-S18) which are recalled below.

The main security objectives for a TIPHON network are split into customers' security objectives, service and network providers security objectives and manufacturers' objectives:

- **Customers' Objectives.**

The objectives of customers are not uniform. An enterprise does not always require the same as a private person. The following list gives examples of objectives which may have implications on security:

- availability and correct functionality of service subscription (including reach ability, availability and correct functionality);
- correct and verifiable billing;
- data integrity;
- data confidentiality/privacy;
- capability to use a service anonymously;
- location confidentiality (is probably part of service anonymousity).

- **TIPHON Service and Network Providers Objectives.**

The following list gives examples of objectives that may have implications on security:

- availability and correct functionality of network procedures for TIPHON;
- availability and correct functionality of service, network and element management for TIPHON;
- correct and verifiable billing and accounting, above all no possibility of fraud;
- non-repudiation for all network procedures and for all management activities;
- preservation of reputation (above all preservation of customers' and investors' trust).

- **Manufacturers' Objectives.**

The following list gives examples of objectives that may have implications on security:

- fulfilling market objectives;
- preservation of reputation.

NOTE: An additional security related service is the lawful interception; lawful interception is not presently addressed in that report. All those aspects need to be provided at each interface to the network and must be supported by the proper protocols.

- **TIPHON threat analysis.**

TIPHON major categories of threats are defined in TR 101 771 [37] and are listed below:

- Denial of service.
- Eavesdropping.
- Masquerade.
- Unauthorized access.
- Loss of information.
- Corruption of information.
- Repudiation.

F.2.1.1 Recall of TIPHON security model

F.2.1.1.1 Call phases

The basic reference configuration is given as a reminder in figure F.1 extracted from TS 101 312 [23].

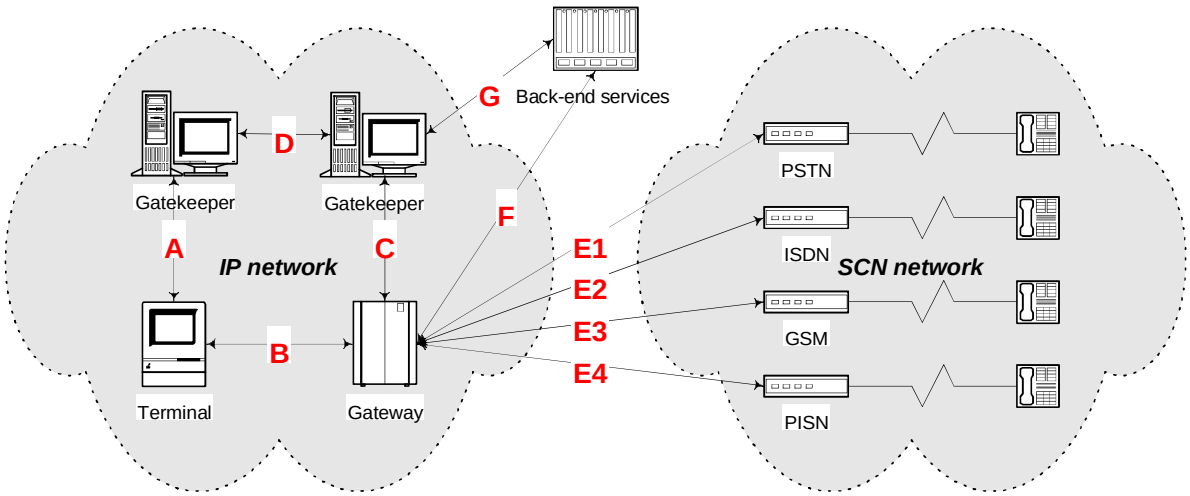


Figure F.1: Basic call reference configuration

F.2.1.1.1.1 Local (user) authentication and authorization

User authentication may be provided to allow a network element (such as a gatekeeper) and an end user to mutually establish some aspect of each other. In the case of an end user requesting service, that aspect may include the user's actual identity, or it may be simply that the user possesses coins, electronic cash, a valid Secure Exchange Transaction (SET) account, or other financial means to pay for the call. For network elements, an end user may wish to reliably establish the element's identity before revealing, for example, sensitive financial information. In many cases user authentication may support and lead to some form of authorization. Certain users, for example, may not be permitted to make toll calls.

NOTE: Figure F.2 shows an example of this authentication phase. In it, the gatekeeper must reliably and securely establish the identity of the terminal and/or its human user. The figure's scenario is that of a third party trust relationship because that is the most general case. Bilateral relationships and single domain environments are likely to rely on subsets of the architecture described in figure F.2.

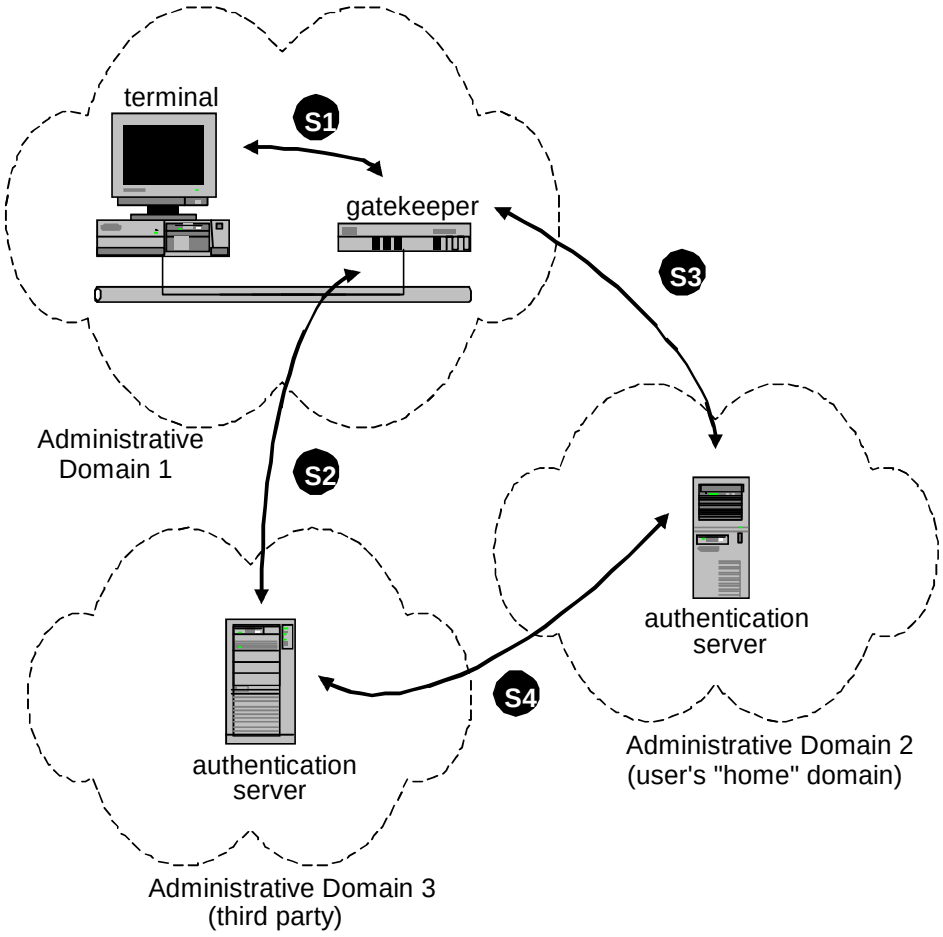


Figure F.2: Security information flows - user authentication and authorization

Figure F.2 identifies the following information flows:

S1: exchange of authentication and/or authorization information between terminal and gatekeeper (possibly supported by communication across the A reference point of figure F.1);

S2: exchange of authentication and/or authorization information between gatekeeper and third party server (possibly supported by communication across the D or G reference points of figure F.1);

S3: exchange of authentication and/or authorization information between gatekeeper and "home" domain (possibly supported by communication across the D or G reference points of figure F.1);

S4: exchange of authentication and/or authorization information between third party server and user's "home" domain (possibly supported by communication across the D or G reference points of figure F.1).

Information used to authenticate and authorize users (such as passwords) is almost certainly sensitive information and shall be protected by appropriate confidentiality measures. Such measures may include, for example, physical security of the network elements and encryption of the communication.

F.2.1.1.2 Remote (operator) authentication and authorization

Once the identity of the local user has been established, that user may be allowed to place one or more calls. With each call, the remote endpoint may authenticate and shall authorize the party attempting the call.

Figure F.3 shows how trust relationships can influence the security architecture. It illustrates operator authentication and authorization in the context of a third party trust relationship. That relationship is the most general case. In a single domain or in bilateral relationships, some of the information flows identified in figure F.3 may be unnecessary.

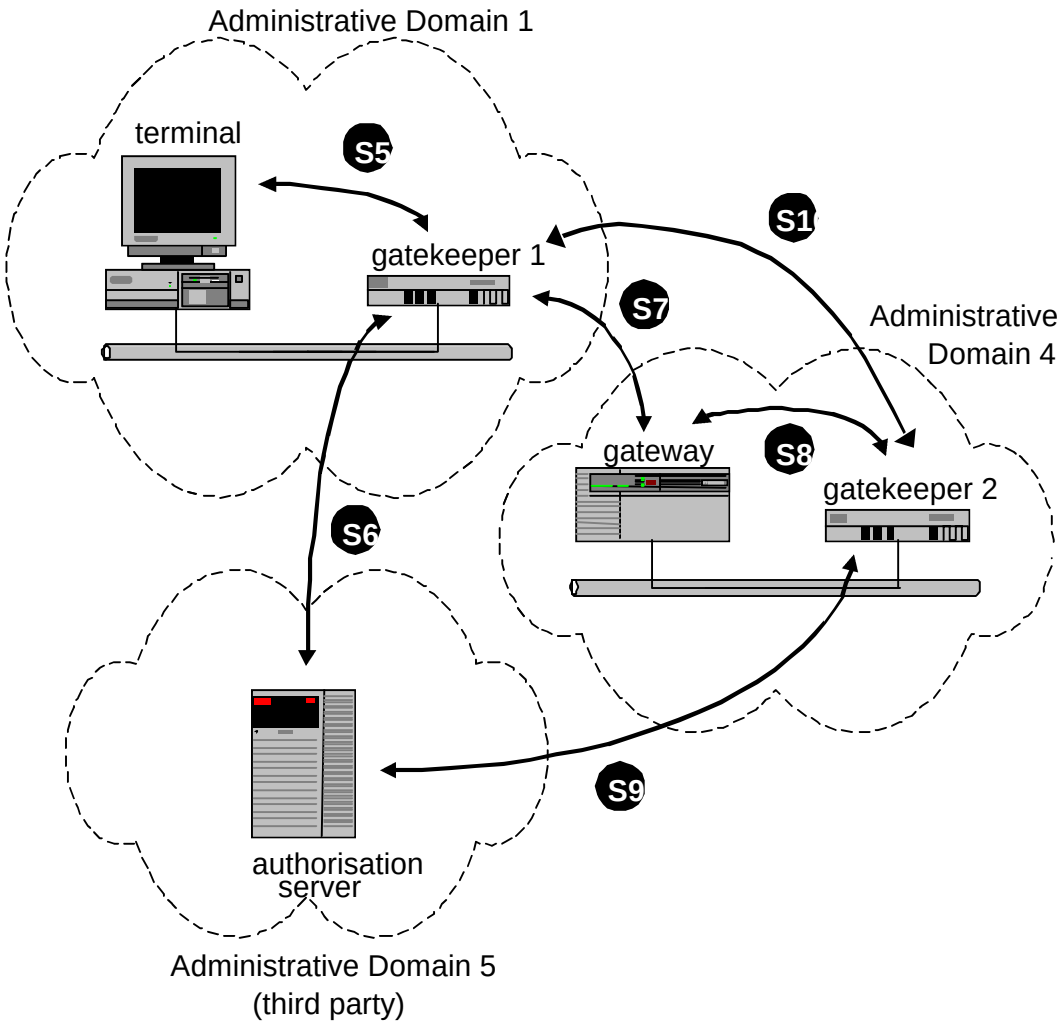


Figure F.3: Security information flows for Operator authentication and authorization

Figure 3 identifies the following information flows:

S5: exchange of call authorization information between the terminal and gatekeeper 1 (possibly supported by communication across the A reference point of figure F.1);

S6: exchange of call authorization information between gatekeeper 1 and third party server (possibly supported by communication across the D or G reference points of figure F.1);

S7: exchange of call authorization information between gatekeeper 1 and gateway (possibly supported by communication across the C reference point of figure F.1);

S8: exchange of call authorization information between gateway and its gatekeeper (possibly supported by communication across the C reference point of figure F.1);

S9: exchange of call authorization information between gatekeeper 2 and third party server (possibly supported by communication across the D or G reference points of figure F.1);

S10: exchange of call authorization information between gatekeepers (possibly supported by communication across the D reference points of figure F.1).

F.2.1.1.3 Call signalling

During call set-up, some environments may require that call set-up information be protected from eavesdropping. Users, for example, may wish that the called number be kept confidential. figure 4 identifies information flow S11 as the point through which call signalling messages are exchanged.

NOTE 1: for clarity the figure only shows the two endpoints of the call. S11 is intended to indicate any point through which call signalling passes. For gatekeeper-routed calls, for example, S11 would also apply to the interface between endpoints and gatekeepers.

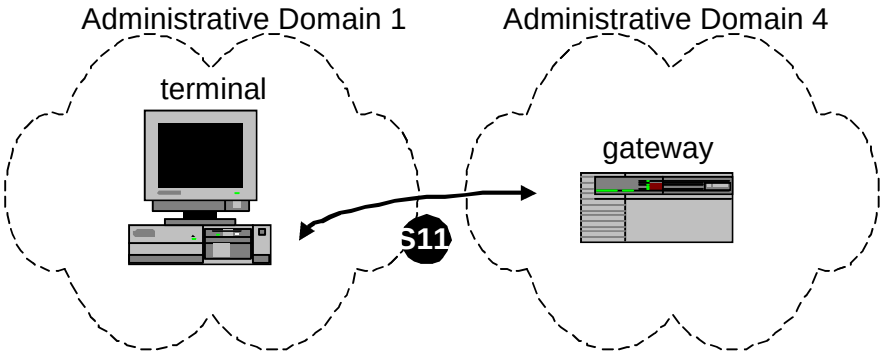


Figure F.4: Security information flows for call signalling

Figure F.4 identifies the following information flow:

S11: secure call signalling interface between endpoints and/or gatekeepers (possibly supported by communication across the A, B, C, or D reference points of figure F.1).

NOTE 2: As an example of the use of S11, it may represent the use of the Transport Layer Security (TLS) protocol as specified in H.235. [41]

F.2.1.1.4 Call activity

Once a call is established and active, it may require security services such as media stream privacy. Figure F.5 designates S12 as the information flow for media stream privacy. Gatekeepers are omitted for clarity.

Should any media streams be routed through a gatekeeper, S12 shall also apply.

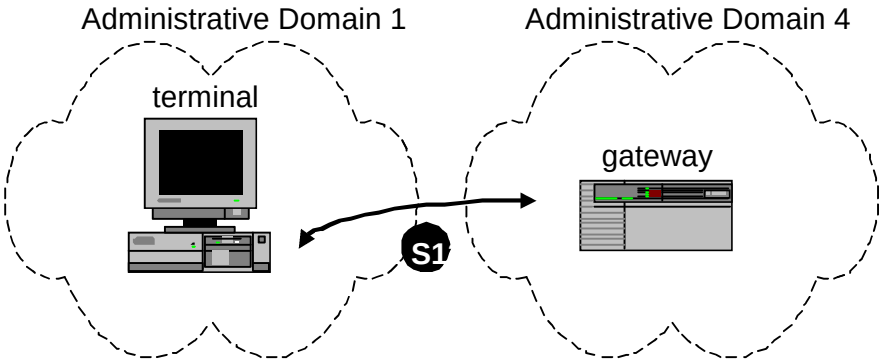


Figure F.5: Security information flows for call activity

Figure F.5 identifies the following information flow:

S12: secure media stream interface between endpoints and/or gatekeepers (possibly supported by communication across the A, B, C, or D reference points of figure F.1).

F.2.1.1.5 Call clearing

When a device other than the end users participating in a call (e.g. a gatekeeper) wishes to clear a call, that device shall establish its authority. A security architecture may also be important, however, in the simple case of end user call clearing. Security may be important in the third party trust relationship. In that relationship, the third party may not control either endpoint in a call, and may not know directly when the call is cleared. That third party, though, facilitated the call through its trust relationships, and as a result may have an economic stake in the call. The economic stake may require that the third party know securely and reliably when the call is cleared. Figure F.6 identifies the information flows.

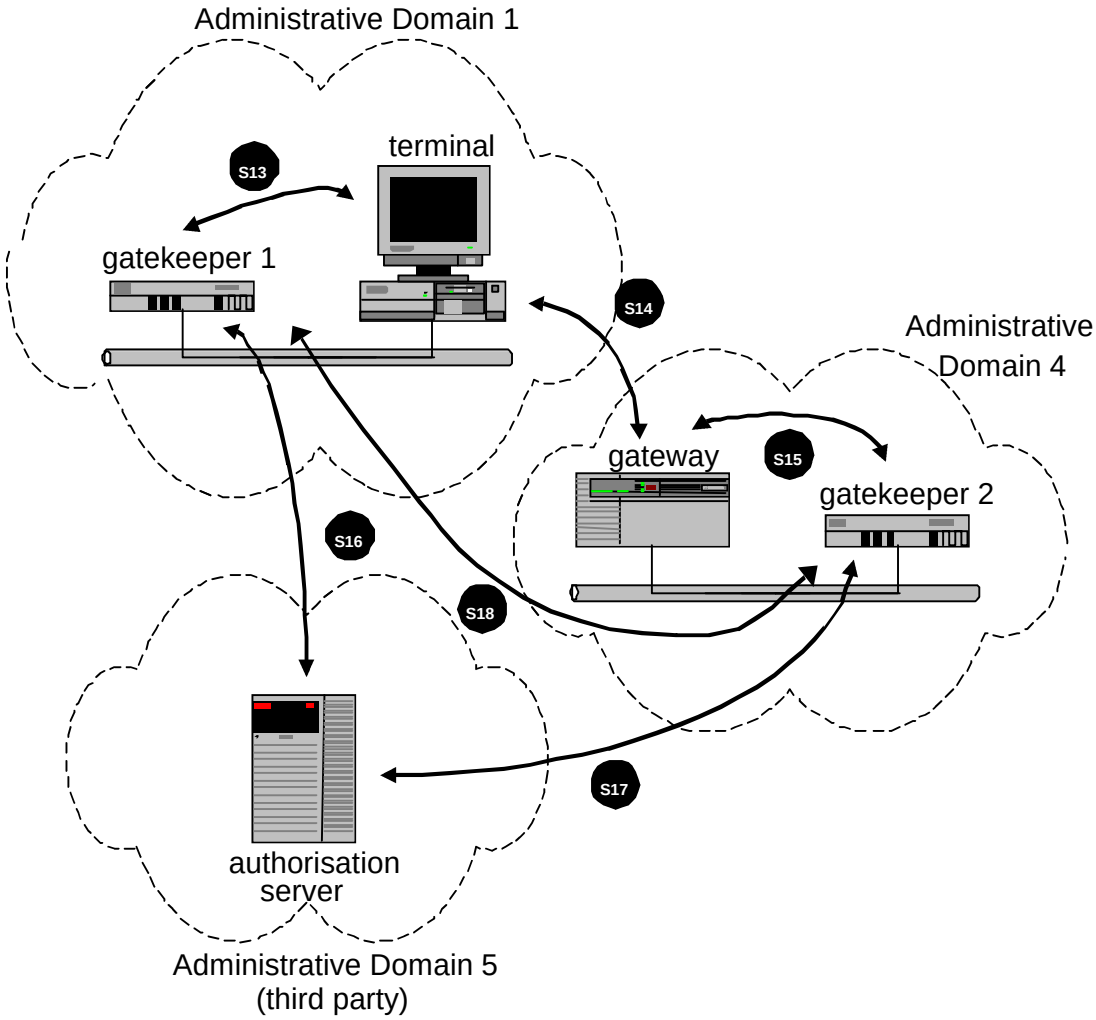


Figure F.6: Security information flows for call clearing

Figure F.6 identifies the following information flows:

S13: secure call clearing interface between the terminal and its gatekeeper (possibly supported by communication across the A reference point of figure F.1);

S14: secure call clearing interface between endpoints (possibly supported by communication across the A, B, C, or D reference points of figure F.1);

S15: secure call clearing interface between gateway and its gatekeeper (possibly supported by communication across the C reference point of figure F.1);

S16: secure call clearing interface between gatekeeper 1 and third party authorizer (possibly supported by communication across the D or G reference points of figure F.1);

S17: secure call clearing interface between gatekeeper 2 and third party authorizer (possibly supported by communication across the D or G reference points of figure F.1);

S18: secure call clearing interface between gatekeeper 1 and gatekeeper 2 (possibly supported communication across the D reference point of figure F.1).

F.2.2 Security matrix summary

As a convenient reference, profiles may include a summary matrix of the following form for each security information flow.

Table F.2: Security summary profile

Security Services	Call Functions				
	RAS	H.225.0 [5]	H.245 [6]	RTP	Other(s)
Authentication					
Access Control					
Integrity					
Confidentiality					
Non-Repudiation					
Security mechanism (added to the TIPHON table)					

Each element in the matrix identifies the security mechanism (Not applicable, None, IPSEC, TLS/SSL, Token, H.235 [41], or Other) and the cryptographic algorithm(s) and parameters supported.

In addition, each profile description includes the detailed information sufficient to ensure interoperability, and lists the attacks it counters, the provided security level, and the potential consequences of a breach in its security.

If a profile includes multiple tables (e.g. for multiple security information flows), then the security mechanisms specified for each service shall not contradict each other.

F.3 IPCablecom according to ITU-T Recommendation J.170

F.3.1 Description of IPCablecom security

Each of IPCablecom's protocol interfaces is subject to threats that could pose security risks to both the subscriber and service provider. The IPCablecom architecture 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 large number of 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 end-to-end encryption of RTP media streams, thus substantially reducing the threat to privacy.

The security services available through IPCablecom's core service layer are authentication, access control, integrity, confidentiality and non-repudiation. An IPCablecom protocol interface may employ zero, one or more of these services to address its particular security requirements.

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

- Identifying the threat model specific to each constituent protocol interface.
- Identifying the security services (authentication, authorization, confidentiality, integrity, and non-repudiation) required to address the identified threats.
- 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).

The Security interface model is recalled on figure F.7. In that figure F.7, each interface is labelled as:

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

If the key management protocol is missing, it means that it is not needed for that interface. IPCablecom interfaces that do not require security are not shown on figure F.7. Interfaces to DHCP and to DNS are not listed on that figure F.7. Those interfaces include the key management interfaces.

The following abbreviations are used in figure F.7:

- **IKE-:** IKE with pre-shared keys.
- **IKE+:** IKE requires public key certificates.
- **CMS-based KM:** Keys randomly generated and distributed by CMS.

IPCablecom Security Interfaces

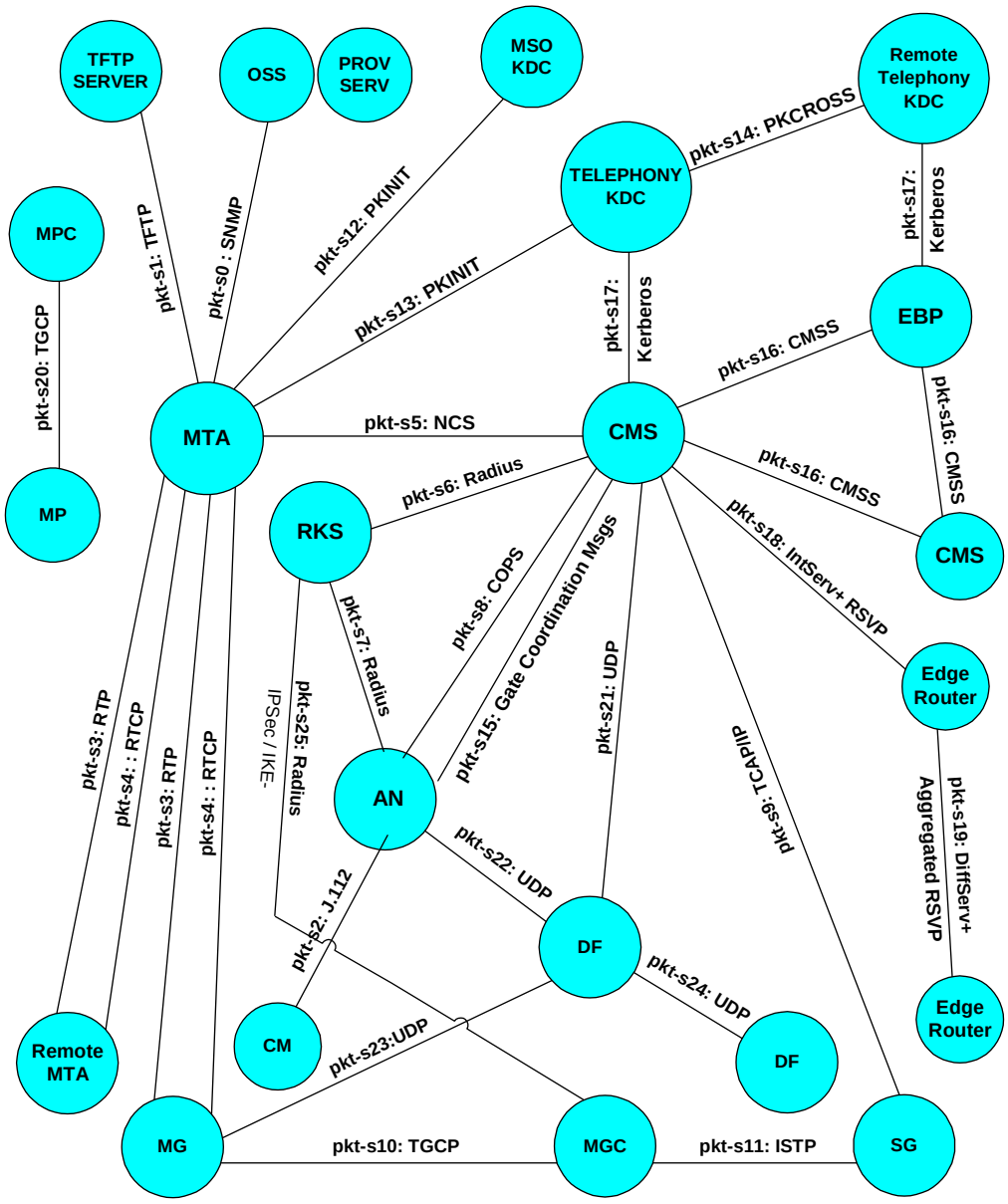


Figure F.7: Subset of IPCablecom interfaces

Table F.3 briefly describes each of the interfaces shown in figure F.7.

Table F.3: IPCablecom Security Interfaces

Interface	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 - AN	J.112 [4]: Secured with BPI+ using BPI Key-Management. BPI+ privacy layer on the HFC link.
pkt-s3	MTA - MTA MTA - MG	RTP: End-to-end media packets between two MTAs, or between MTA and MG. 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 CMS or other application server.
pkt-s4	MTA - MTA MTA - MG	RTCP: RTCP control protocol 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 - CMS	NCS: Message integrity and privacy via IPSec. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
pkt-s6	RKS - CMS	Radius: Radius billing events sent by the CMS to the RKS. Radius authentication keys are hard coded to 0. IPSec is used for message integrity, as well as privacy. Key management is IKE-.
pkt-s7	RKS - AN	Radius: Radius events sent by the AN to the RKS. Radius authentication keys are hard coded to 0. IPSec is used for message integrity, as well as privacy. Key management is IKE-.
pkt-s8	CMS - AN	COPS: COPS protocol between the GC and the AN, used to download QoS authorization to the AN. Security is provided with IPSec for message integrity, as well as privacy. Key management is IKE-.
pkt-s9	CMS - SG	TCAP/IP: CMS queries the PSTN Gateway for LNP (Local Number Portability) and other voice communications services. Security is provided with IPSec for message integrity as well as privacy. Key-Management is IKE-.
pkt-s10	MGC - MG	TGCP: IPCablecom interface to the PSTN Media Gateway. IPSec is used for both message integrity and privacy. Key management is IKE-.
pkt-s11	MGC - SG	ISTP: IPCablecom interface to the PSTN Signalling Gateway. IPSec is used for both message integrity and privacy. Key management is 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 - Telephony KDC	PKINIT: See pkt-s12 above.
pkt-s14	Telephony KDC - Remote Telephony KDC	PKCROSS utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signalling (CMSS).
pkt-s15	CMS - AN	Gate Coordination messages for DQoS. Message integrity is provided with an application-layer (Radius) authenticator. Keys are distributed by local CMS over COPS.
pkt-s16	CMS - CMS CMS - EBP	SIP: IPSec is used for both message integrity and privacy. Key management is Kerberos.
pkt-s17	CMS - Telephony KDC EBP - Remote Telephony KDC	Kerberos: PKINIT requests (AS Request - AS Reply) for a TGT between Kerberos realms, both Intradomain and Interdomain. The TGT request generates a cross-realm TGT request using the TGS Request - TGS Reply and the PKCROSS mechanisms. The cross-realm TGS Reply is used to generate the AS Request - AS Reply needed to establish Security Associations between two domains.

Interface	Components	Description
pkt-s18	CMS - ER	IntServ + RSVP: Secured using RSVP Integrity Objects.
pkt-s19	ER - ER	Aggregated RSVP: Secure using RSVP Integrity Objects.
pkt-s20	MPC - MP	TGCP: IPSec is used for both message integrity and privacy. Key management is IKE-.
pkt-s21	DF - CMS	UDP: IPSec is used for both message integrity and privacy. Key management is IKE-.
pkt-s22	DF - AN	UDP: IPSec is used for both message integrity and privacy. Key management is IKE-.
pkt-s23	DF - MG	UDP: IPSec is used for both message integrity and privacy. Key management is IKE-.
pkt-s24	DF - DF	UDP: IPSec is used for both message integrity and privacy. Key management is IKE+.
pkt-s25	RKS-MGC	Radius: Radius events sent by the MGC to the RKS. Radius authentication keys are hard coded to 0. IPSec is used for message integrity, as well as privacy. Key management is IKE-.

F.3.1.1 Analysis of threats

The threats are analysed in a different classification for TIPHON and for IPCablecom; as seen above, TIPHON analyses threats according to their external consequences while IPCablecom analyses threats according to component/element under threat. The threat analysis is given in that part of the document in the section of security according to ITU-T Recommendation J.170 [38] parts 1 and 2 because the threat analysis is much more detailed and much better than in TS 101 909-11 [35].

The following analysis of threats is provided by IPCablecom.

F.3.1.1.1 Theft of network services

In the context of voice communications, the main services that may be stolen are:

- Long distance service.
- Local (subscription) voice communications service.
- Video conferencing.
- Network-based three-way calling.
- Quality of Service.

F.3.1.1.2 Bearer channel information threats

This class of threats is concerned with the breaking of privacy of voice communications over the IP bearer channel. Threats against non-VoIP communications are not considered here and assumed to require additional security at the application layer.

F.3.1.1.3 Signalling channel information threats

Signalling information, such as the caller identity and the services to which each customer subscribes may be collected for marketing purposes. The caller identity may also be used illegally to locate a customer that wishes to keep his or her location private.

F.3.1.1.4 Service disruption threats

This class of threats is aimed at disrupting the normal operation of voice communications. The motives for denial-of-service attacks may be malicious intent against a particular individual or against the service provider. Or, perhaps a competitor wishes to degrade the performance of another service provider and use the resulting problems in an advertising campaign.

F.3.1.1.5 Repudiation

In a network where masquerading (using the above-mentioned cloning and protocol manipulation techniques) is common or easily achievable, a customer may repudiate a particular communication (and, thus deny responsibility for paying for it) on that basis.

In addition, unless public key-based digital signatures are employed on each message, the source of each message cannot be absolutely proven. If a signature over a message that originated at an MTA is based on a symmetric key that is shared between that MTA and a network server (e.g. the CMS), it is unclear if the owner of the MTA can claim that the Service Provider somehow falsified the message.

However, even if each message were to carry a public key-based digital signature and if each MTA were to employ stringent physical security, the customer can still claim in court that someone else initiated that communication without his or her knowledge, just as a customer of a telecommunications carrier on the PSTN can claim, e.g. that particular long distance calls made from the customer's telephone were not authorized by the customer. Such telecommunications carriers commonly address this situation by establishing contractual and/or tariff relationships with customers in which customers assume liability for unauthorized use of the customer's service. These same contractual principles are typically implemented in service contracts between information services providers such as ISPs and their subscribers. For these reasons, the benefits of non-repudiation seem dubious at best and do not appear to justify the performance penalty of carrying a public key-based digital signature on every message.

F.3.1.1.6 Threat summary

This clause provides a summary of the above of threats and attacks and a brief assessment of their relative importance.

F.3.1.1.6.1 Primary threats

- **Theft of Service**. Attacks are:
  - **Subscription Fraud**. This attack is prevalent in today's telephony systems (i.e. the PSTN) and requires little economic investment. It can only be addressed with a Fraud Management system.
  - **Non-payment for services**. Within the PSTN, telecommunications carriers usually do not prosecute the offenders, but simply shut down their accounts. Because prosecution is expensive and not always successful, it is a poor counter to this attack. Methods such as debit-based billing and device authorization (pay as you play), increasingly common in the wireless sector of the PSTN, might be a possible solution for this attack in the IPCablecom context. This threat can also be minimized with effective Fraud Management systems.
  - **MTA clones**. This threat requires more technical knowledge than the previous two threats. A technically-knowledgeable adversary or underground organization might offer cloning services for profit. This threat is most effective when combined with subscription fraud, where an MTA registered under a fraudulent account is cloned. This threat can be addressed with both Fraud Management and physical security inside the MTA, or a combination of both.
  - **Impersonate a network server.** With proper cryptographic mechanisms, authorization and procedural security in place, this attack is unlikely, but has the potential for great damage.
  - **Protocol manipulation.** Can occur only when security protocols are flawed or when not enough cryptographic strength is in place.
- **Bearer Channel Information Disclosure**. Attacks are:
  - **Simple Snooping**. This would happen if voice packets were sent in the clear over some segment of the network. Even if that segment appears to be protected, an insider may still compromise it. This is the only major attack on privacy. The bearer channel privacy attacks listed below are possible but are all of secondary importance.
  - **MTA clones**. Again, this threat requires more technical knowledge but can be offered as a service by an underground organization. A most likely variation of this attack is when a publicly accessible MTA (e.g. in an office or apartment building) is cloned.

- **Protocol manipulation**. A flawed protocol may somehow be exploited to discover bearer channel encryption keys.
- **Off-line cryptanalysis**. Even when media packets are protected with encryption, they can be stored and analysed for long periods of time, until the decryption key is finally discovered. Such an attack is not likely to be prevalent, since it is justified only for particularly valuable customer-provided information (IPCablecom security is not required to protect data). This attack is more difficult to perform on voice packets (as opposed to data). Still, customers are very sensitive to this threat and it can serve as the basis for a negative publicity campaign by competitors.
- **Signalling Information Disclosure.** This threat is listed as primary only due to potential for bad publicity and customer sensitivity to keeping their numbers and location private. All of the attacks listed below are similar to those for bearer channel privacy and are not described here:
  - Simple snooping.
  - MTA clones.
  - Protocol manipulation.
  - Off-line cryptanalysis.
  - Service disruption.

F.3.1.1.6.2 Secondary threats

- **Theft of MTA-based services.** Based on the voice communications services that are planned for the near future, this threat does not appear to have potential for significant economic damage. This could possibly change with the introduction of new value-added services in the future.
- **Illegally registering a leased MTA with a different Service Provider.** Leased MTAs can normally be tracked. Most likely, this threat is combined with the actual theft of a leased MTA. Thus, this threat does not appear to have potential for widespread damage.

In relation to TIPHON security profiles, there are two aspects: one is for IPCablecom to be TIPHON compliant and one is for IPCablecom to be interoperable with another TIPHON compliant system on a security level.

F.3.2 Preliminary conclusions

ITU-T Recommendation J.170 [38] gives much better threat analysis, much better definitions of the IPCablecom security objectives and a better interface model; moreover, it leads to an operation much closer to TIPHON recommended security recommendation which is ITU-T Recommendation H.235 [41], in particular annex D of that recommendation.

The following areas of definitions should be studied in the context of future TIPHON releases:

- TIPHON to align its security terminology with ITU-T.
- TIPHON is quite silent on the handling of keys and this may constitute an area where IPCablecom is ahead of TIPHON and where TIPHON could pick up some algorithm.
  - TIPHON to select key management algorithm(s) or to decide to be outside the scope of TIPHON.
- Key management in a distributed system like IPCablecom does not appear to be defined in TIPHON; this could be one of the input to TIPHON Release 4 security work.
  - TIPHON to define principles and algorithms for security of widely distributed systems.
- TIPHON does not presently define interfaces, flows and protocols for audio server and more generally for media server which occupy a particular position in the network.
  - TIPHON to define its model for media server: protocols and security mechanisms.

- TIPHON does not seem to define security algorithms to protect quality of service and dynamic quality of service flows.

  - TIPHON to define its security mechanisms and algorithms for QoS and DQoS.

- TIPHON does not seem to take into consideration security across domains and seems to take into account only the security within one domain.

On the other hand, IPCablecom seems to ignore mobility in its security algorithms; mobility is meant here to say on one hand number portability in fixed networks and on the other handling of mobiles, in particular home and visited infrastructures.

- IPCablecom to define its security mechanisms, threats and algorithms in case of terminal mobility and number portability.

- IPCablecom to define its security mechanisms, threats and algorithms in case of mobiles (GSM, etc.).

Annex G: Bibliography

- ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".
- ETSI TS 101 909-6: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 6: Media Terminal Adapter (MTA) device provisioning".
- ETSI TS 101 909-16: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 16: Signalling for Call Management Server".
- ETSI TS 102 141: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; M2UA [Endorsement of RFC 3331 (2002), modified]".
- ETSI TS 102 142: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; M3UA; [Endorsement of RFC 3332 (2002), modified]".
- ETSI TS 102 143: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; SUA, [Endorsement of SIGTRAN-SUA-14 (Dec. 2002), modified]".
- ETSI TS 102 144: "Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN; SCTP; [Endorsement of RFC 2960 and RFC 3309 , modified]".
- ITU-T Recommendation J.163: "Dynamic quality of service for the provision of real time services over cable television networks using cable modems".
- PKT-SP-CMSS-I01-001128: "PacketCableTM CMS to CMS Signalling Specification".
- ITU-T Recommendation J.164: "Event message requirements for the support of real-time services over cable television networks using cable modems".
- ITU-T Recommendation J.167: "Media Terminal Adapter (MTA) device provisioning requirements for the delivery of real time services over cable television networks using cable modems".
- ITU-T Recommendation J.168: "IPCablecom media terminal adapter (MTA) MIB requirements".
- ITU-T Recommendation J.169: "IPCablecom network call signalling (NCS) MIB requirements".
- ITU-T Recommendation J.171: "IPCablecom Trunking Gateway Control Protocol (TGCP)".
- ITU-T Recommendation J.172: "IPCablecom management event mechanism".
- ITU-T Recommendation J.173: "IPCablecom embedded MTA primary line support".
- ITU-T Recommendation J.174: "IPCablecom interdomain quality of service".

History

Document history		
V1.1.1	January 2003	Publication