ECMA Technical Report TR/81
September 2000

ECMA

Standardizing Information and Communication Systems

Interoperation of PISNs with IP Networks

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

ECMA Technical Report TR/81
September 2000

ECMA

Standardizing Information and Communication Systems

Interoperation of PISNs with IP Networks

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

IW TR-081.DOC 04-09-00 16,36

Brief History

This Technical Report investigates the interoperability of Private Integrated Services Networks (PISNs) and Internet Protocol (IP) networks within the context of Corporate Telecommunication Networks. The purpose is to identify possible scenarios for interoperation, problems that will have to be solved if particular scenarios are to be pursued further, and possible future standardization activities in this area. It forms the foundation for further work in ECMA on this subject, including the production of Standards where found to be required.

This Technical Report is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

This ECMA Technical Report has been adopted by the General Assembly in September 2000.

Table of contents

1 Scope

The purpose of this Technical Report is to investigate the interoperability of Private Integrated Services Networks (PISNs) and Internet Protocol (IP) networks, with a view to identifying possible scenarios for interoperation, problems that will have to be solved if particular scenarios are to be pursued further, and possible future standardization activities in this area. In particular, the following aspects of interoperability are investigated:

- the interworking of PISNs and IP networks via a gateway;
- the connection of PISN components via IP networks.

For each of the above, aspects considered include architecture, addressing (including use of IP addressing), services, protocols, security, quality of service and mobility. This is conducted within the context of leading standards for voice and multimedia communication over IP networks, including ITU-T recommendation H.323, IETF Session Initiation Protocol (SIP) and ITU-T recommendation H.248.

Possible future standardization activities resulting from this Technical Report can include work items relating to IP networks and work items relating to PISNs, as well as work items concerned specifically with interoperability.

The dominant traffic in PISNs is voice, and therefore this Technical Report focuses on interoperability considerations for voice traffic. However, many of the standards that support voice in an IP network are also applicable to multi-media traffic (e.g., voice, video and data). Although in many respects similar to voice, fax traffic has slightly different requirements and is not explicitly considered in this Technical Report. It could be the subject of further study.

2 References

ECMA-133	Private Integrated Services Network (PISN) - Reference Configuration for PISN Exchanges (PINX) (International Standard ISO/IEC 11579-1)
ECMA-143	Private Integrated Services Network (PISN) - Circuit-mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol (International Standard ISO/IEC 11572)
ECMA-155	Private Integrated Services Networks - Addressing (International Standard ISO/IEC 11571)
ECMA-163	Private Integrated Services Network (PISN) - Specification, Functional Model and Information Flows - Name Identification Supplementary Services (International Standard ISO/IEC 13864)
ECMA-164	Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Name Identification Supplementary Services (International Standard ISO/IEC 13868)
ECMA-165	Private Integrated Services Network (PISN) - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol (International Standard ISO/IEC 11582)
ECMA-174	Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Call Diversion Supplementary Services (International Standard ISO/IEC 13873)
ECMA-178	Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Call Transfer Supplementary Service (International Standard ISO/IEC 13869)
ECMA-186	Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Call Completion Supplementary Services (International Standard ISO/IEC 13870)
ECMA-242	Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Message Waiting Indication Supplementary Service (International Standard ISO/IEC 15506)

ECMA-300	Private Integrated Services Network (PISN) - Inter–Exchange Signalling Protocol - Single Step Call Transfer Supplementary Service (International Standard ISO/IEC DIS 19460)
ECMA TR/57	Private Integrated Services Networks
ECMA TR/76	Private Integrated Services Network (PISN) - Architecture and Scenarios for Private Integrated Services Networking
ETSI TS 101 313	Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); Network architecture and reference configurations; Phase II: Scenario 1 + Scenario 2
ITU-T Rec. G.107	The E-Model, a computational model for use in transmission planning
ITU-T Rec. G.711	Pulse Code Modulation (PCM) of voice frequencies
ITU-T Rec. G.723.1	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s
ITU-T Rec. H.225.0	Call signalling protocols and media stream packetization for packet-based multimedia communication systems
ITU-T Rec. H.235	Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals
ITU-T Rec. H.245	Control protocol for multimedia communication
ITU-T Rec. H.248	Gateway control protocol
ITU-T Rec. H.261	Video codec for audiovisual services at p x 64 kbits
ITU-T Rec. H.320	Narrow-band visual telephone systems and terminal equipment
ITU-T Rec. H.323	Packet based multimedia communications systems
ITU-T Rec. H.450.1	Generic functional protocol for the support of supplementary services in H.323
ITU-T Rec. H.450.2	Call transfer supplementary service for H.323
ITU-T Rec. H.450.3	Call diversion supplementary service for H.323
ITU-T Rec. H.450.4	Call hold supplementary service for H.323
ITU-T Rec. H.450.5	Call park and call pickup supplementary services for H.323
ITU-T Rec. H.450.6	Call waiting supplementary service for H.323
ITU-T Rec. H.450.7	Message waiting indication supplementary service for H.323
ITU-T Rec. H.450.8	Name identification supplementary service for H.323
ITU-T Rec. H.450.9	(draft) Call completion supplementary services for H.323
ITU-T Rec. Q.921	ISDN user-network interface - Data link layer specification
ITU-T Rec. Q.931	Digital Subscriber Signalling system no. 1 (DSS1) - ISDN user-network interface layer 3 specification for basic call control
IETF RFC 791	Internet Protocol (IP), version 4.
IETF RFC 1034	Domain names - concepts and facilities
IETF RFC 1035	Domain names - implementation and specification
IETF RFC 1889	RTP: a transport protocol for real-time applications
IETF RFC 2205	Resource ReSerVation Protocol (RSVP) - Version 1 functional specification
IETF RFC 2246	The TLS Protocol Version 1.0
IETF RFC 2251	Lightweight Directory Access Protocol (version 3)

IETF RFC 2326	Real-time streaming protocol (RTSP) for controlling delivery of streaming media
IETF RFC 2327	SDP: Session Description Protocol
IETF RFC 2401	Security Architecture for the Internet Protocol (IPSec)
IETF RFC 2402	IP Authentication Header (AH)
IETF RFC 2406	IP Encapsulating Security Payload (ESP)
IETF RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
IETF RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
IETF RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
IETF RFC 2475	An architecture for differentiated services
IETF RFC 2543	SIP: Session Initiation Protocol
IETF RFC 2719	Framework architecture for signaling transport
TIA/EIA/IS-811	Telephone Terminal Equipment - Performance and Interoperability Requirements for Voice-over-IP (VoIP) Feature Telephones
TIA/EIA/TSB-116	Voice Quality Recommendations for IP Telephony

3 Definitions

For the purposes of this Technical Report the following definitions apply.

3.1 Corporate telecommunication Network (CN)

Sets of equipment (Customer Premises Equipment and/or Customer Premises Networks) that are located at geographically dispersed locations and are interconnected to provide telecommunication services to a defined group of users.

NOTE
A CN can comprise a PISN, a private IP network (intranet), or a combination of the two.

3.2 Internet

A public IP network.

3.3 Intranet

A private IP network.

3.4 Internet Protocol (IP)

The protocol specified in RFC 791 (IP version 4) or in RFC 2460 (IP version 6).

3.5 IP network

A public or private network offering connectionless packet-mode services based on the Internet Protocol (IP) as the network layer protocol.

NOTE
The Internet is the prime example of a public IP network.

3.6 Private Integrated Services Network (PISN)

A private SCN.

3.7 Private Integrated services Network eXchange (PINX)

See ECMA-133.

3.8 Switched Circuit Network (SCN)

A public or private network offering connection-oriented circuit-mode telecommunication services.

3.9 Tunnelling

A means of transporting protocol information between two entities that are interconnected by a network, without the need for that interconnecting network to comprehend the transported protocol information.

4 Acronyms

AC	Admission Control (functional entity)
AH	Authentication Header
BICC	Bearer-Independent Call Control
CC	Call Control (functional grouping)
CLIP	Calling Line Identification Presentation
CLIR	Calling/connected Line Identification Restriction
CN	Corporate telecommunication Network
COLP	COnnected Line identification Presentation
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESP	Encapsulating Security Payload
GK	Gatekeeper
GW	Gateway
HLS	Higher Layer Signalling (functional entity)
HTTP	Hyper-Text Transfer Protocol
ICC	Inter-PINX Connection Control (functional grouping)
ICN	InterConnecting Network
IP	Internet Protocol
IPC	Inter-PINX Connection
IPL	Inter-PINX Link
IR	Identity resolution (functional entity)
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part (of SS7)
IVN	InterVening Network
IW	InterWorking (functional entity)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLS	Lower Layer Signalling (functional entity)
MG	Media Gateway
MGC	Media Gateway Controller
MP	Mapping (functional grouping)
MPP	Media processing and packetization (functional entity)
MTP	Message Transfer Part (of SS7)

PINX	Private Integrated services Network eXchange
PISN	Private Integrated Services Network
PNP	Private Numbering Plan
QoS	Quality of Service
RAS	Registration, Admission and Status
RC	Resource Control (functional entity)
RC-P	RC-Proxy (functional entity)
RFC	Request For Comment
RGR	Registrar (functional entity)
RGT	Registrant (functional entity)
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SC	Session Control (functional entity)
SCN	Switched Circuit Network
SC-P	SC-Proxy (functional entity)
SC-R	SC-Redirect (functional entity)
SCTP	Simple Control Transport Protocol
SG	Signalling Gateway
SIP	Session Initiation Protocol
SSL	Session Security Layer
SM	Scenario Management (functional grouping)
SS7	Signalling System number 7
SW	Switching (functional grouping)
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TRIP	Telephony Routing Information Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network

5 Introduction

5.1 Background

Private Integrated Services Networks (PISNs), based on 64kbit/s-based Time Division Multiplexing (TDM) techniques, have for many years been the basis of corporate voice communications, and additionally have supported other services such as facsimile, video and data (circuit-switched and packet-switched). The technology is similar to that of public Integrated Services Digital Networks (ISDNs). More recently, the connection of virtually every desktop to a Local Area Network (LAN), the growth of the Internet and the

building of “intranets” and “extranets” have led to the desire to use these data networks also for voice communications. There are a number of motives behind this, including cost savings (by the use of common wiring and equipment) and the potential for applications that exploit the integration of voice, data and other media to the benefit of the business.

The network layer protocol is of great importance in data networks, since it has to support a wide range of applications and the higher layer protocols that they employ, whilst at the same time being able to operate over a wide variety of infrastructures. Because of the growth of the Internet, the Internet Protocol (IP) has become the dominant network layer protocol. Although at present version 4 of IP (IPv4, RFC 791) is almost universal, lack of address space and other considerations are creating a lot of interest in version 6 (IPv6, RFC 2460). Except where otherwise stated, the term IP in this Technical Report refers to either IPv4 or IPv6.

To carry voice over data networks, it has to be carried over IP, and hence the term “Voice over IP” (VoIP) has come into being. Voice over IP can be used in a number of ways, including:

- end-to-end between terminal equipments attached to IP networks;
- between a terminal equipment attached to an IP network and a point of interworking with a PISN or other network;
- between two networks, in particular between two PISNs or between a PISN and another network;
- between two parts of the same network, in particular between two Private Integrated Service Network eXchanges (PINXs) belonging to the same PISN; or
- between a terminal equipment and its point of attachment to its serving network, in particular between a terminal equipment and its serving PINX.

From this list it can be seen that PISNs can interoperate with IP networks in a number of different ways, and this is the subject of this Technical Report. The Technical Report focuses chiefly on voice, this being the service most often provided by a PISN. In particular, this means that packet mode aspects of PISNs are not considered.

Figure 1 shows an example illustrating these different means of voice communication through an IP network. The IP terminal equipments have direct access to the IP network, telephones 1 and 2 have access to the IP network through a gateway (labelled as gateway type 1) and PINXs A and B have access to the IP network through a gateway (labelled as gateway type 2). All these entities can communicate with each other through the IP network using the respective gateways.

In addition, PINX A and PINX B may be able to communicate with each other via the IP network using gateways that provide special support for inter-PINX communication. For this purpose PINX A and PINX B are shown as being attached to the IP network also through gateways labelled as gateway type 3.

Finally, telephones 3 and 4 are shown as being served by PINX B, access being achieved via the IP network using gateways (labelled as gateway type 4 on the telephone side of the IP network and gateway type 5 on the PINX side of the IP network). These telephones cannot make and receive calls directly through the IP network to other destinations (e.g., IP terminal equipments) but make and receive all calls via PINX B.

NOTE
Although these different gateway types have functional differences, there may also be substantial similarities in practice between some of these types. Also a physical realisation of a gateway might incorporate more than one of these gateway types.

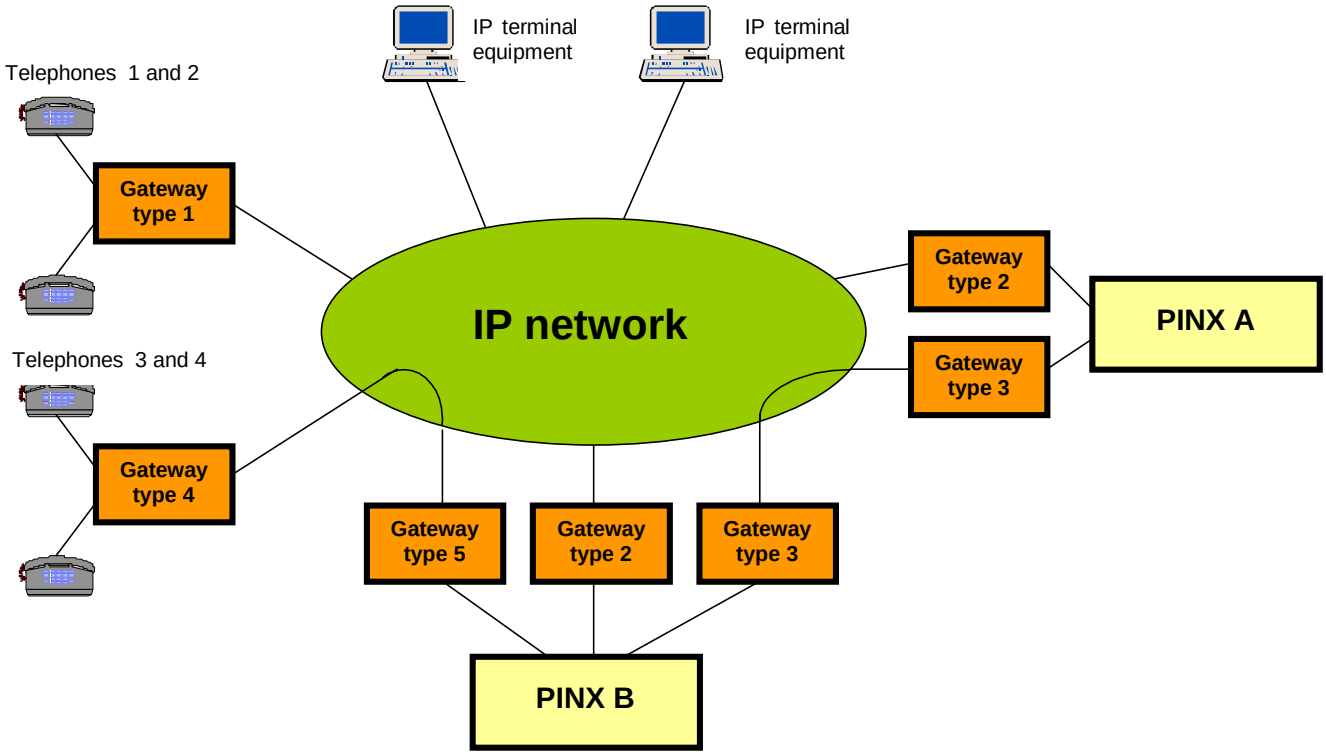


Figure 1 – Example of voice communication through an IP network

Gateway type 2 can be used for interworking between PISNs and IP networks, which is considered in clause 8. Gateway type 3 can be used for interconnecting PISNs or PISN components via IP networks, which is considered in clause 9. Gateway types 1, 2, 4 and 5 can be used for connection of (remote) telephones to a PINX via an IP network, which is considered in clause 10.

5.2 Types of network

An IP network operates in packet mode, since information is sent in packets, when information is available, rather than as a continuous stream. Each packet is routed individually, rather than being switched in accordance with a pre-established connection. This makes an IP network a connectionless packet network.

This contrasts with a PISN, where information is transmitted along the path of a pre-established connection (connection-oriented). A PISN can operate in circuit mode, where information is transmitted as a continuous stream of bits, or in packet mode, where information is sent in packets. In the case of voice, circuit mode is used, and therefore this Technical Report regards a PISN as a private connection-oriented circuit mode network.

Similar considerations apply to public ISDNs, which can be regarded as public connection-oriented circuit mode networks. Although the focus of this Technical Report is on PISNs interoperating with IP networks, public ISDNs have to be considered in the overall picture.

An IP network can provide services to a limited set of users (in a corporation), and therefore can be considered to be a private IP network (or intranet). Alternatively an IP network can provide services to the general public (as is the case with the existing Internet), in which case it can be considered to be a public IP network (or Internet). The term “extranet” is often used to describe an intranet that is spread over multiple administrative domains. “Extranets” are not considered further in this Technical Report.

A Corporate telecommunication Network (CN) can comprise a PISN, an intranet, or a combination of the two.

Based on these considerations, this Technical Report uses the following terminology:

- switched circuit network (SCN): a PISN or public ISDN offering connection-oriented circuit-mode services;

- IP network: a public or private network offering connectionless packet-mode services based on IP as the network layer protocol.

Therefore in examining the interoperability of PISNs and IP networks, this Technical Report focuses on the interoperation of SCNs and IP networks, with particular emphasis on Corporate telecommunication Networks.

5.3 Arrangements for interworking of SCNs and IP networks

Figure 2 illustrates possible interworking between the following types of network:

- private switched circuit network (PISN);
- public switched circuit network (public ISDN);
- private IP network (intranet);
- public IP network (Internet).

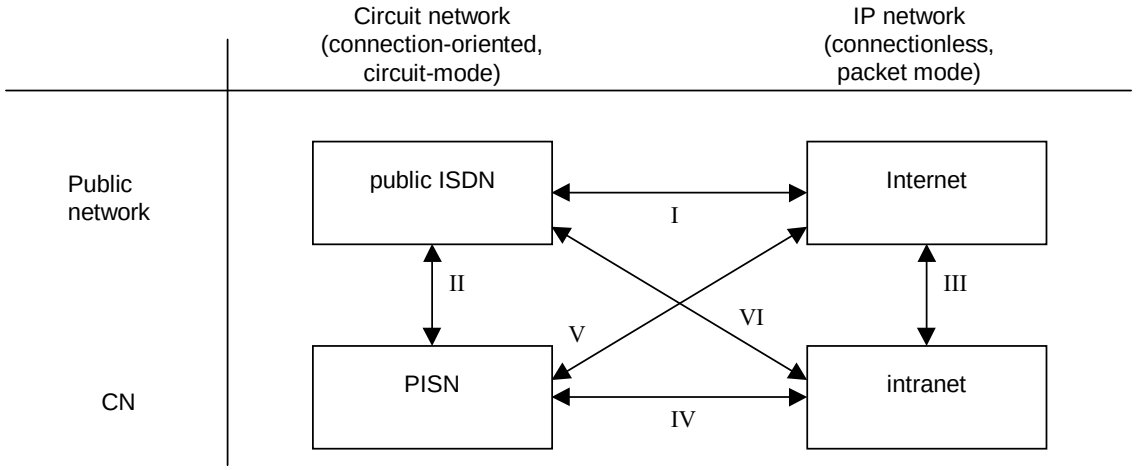


Figure 2 – Interworking arrangements

Arrangements I to VI are listed in table 1, along with their coverage in standards bodies and their security implications.

Table 1 – Interworking arrangements

No.	Description	Coverage in standards bodies	Security implications
I	public ISDN / Internet	No CN impact, outside the scope of this Technical Report and covered by ETSI project TIPHON (see 7.5).	No CN impact, outside the scope of this Technical Report.
II	public ISDN / PISN	SCNs only, outside the scope of this Technical Report.	SCNs only, outside the scope of this Technical Report.
III	Internet / intranet	IP networks only, outside the scope of this Technical Report and covered by IETF.	IP networks only, typically covered by firewalls. Outside the scope of this Technical Report and covered by IETF.
IV	PISN / intranet	Covered by this Technical Report, see clause 8.	Possible security impact leading to the employment of some firewall functions in addition to gateway capability – the two functions may be combined or separate.

V	PISN / Internet	Covered by this Technical Report, see clause 8.	Requires firewall capability in addition to gateway capability – the two functions may be combined or separate.
VI	public ISDN / intranet	No PISN impact, and therefore outside the scope of this Technical Report.	As for V.

5.4 Arrangements for interconnection of SCN components over IP networks

Two SCNs (or two parts of the same SCN) can be interconnected via an IP network. Each of the networks involved can be public or private, leading to the particular arrangements shown in table 2.

Table 2 – Arrangements for interconnection of SCN components over IP networks

Arrangement	Outer networks	Inner network	Remarks
1	Public (ISDN)	Public (Internet)	Outside ECMA's field of responsibility – covered by ETSI project TIPHON.
2	Public (ISDN)	Private (intranet)	Probably of no practical value, but could be considered as arrangement 4 with public-private SCN interworking at each end.
3	Private (PISN)	Public (Internet)	Covered by this Technical Report, see clause 9.
4	Private (PISN)	Private (intranet)	Covered by this Technical Report, see clause 9.
5	1 public (ISDN), 1 private (PISN)	Public (Internet)	Should not be considered as a separate arrangement, since it is effectively a combination of arrangement 1 and public-private SCN interworking at one end.
6	1 public (ISDN), 1 private (PISN)	Private (intranet)	Should not be considered as a separate arrangement, since it is effectively a combination of arrangement 4 and public-private SCN interworking at one end.

The focus for ECMA is therefore on arrangements 3 and 4, both of which involve PISNs as the SCNs. The network signalling protocol used in the SCNs is therefore assumed to be QSIG, as specified in ECMA-143, ECMA-165 and other ECMA Standards.

6 General principles of multimedia communication over an IP network

In classical telephony, the whole functionality of Signalling System number 7 (SS7) and other signalling protocols encompasses routing, resource reservation, call admission, address translation, call establishment, call management and billing. In IP telephony those functions will generally be handled by a series of separate and largely independent packet switched protocols. In particular, in IP telephony, the orthogonality between signalling, resource reservation (or any other kind of QoS provision mechanism) and media transport functions is aimed at affording greater architectural flexibility.

In addition to QoS provision and media transport mechanisms, IP telephony requires a means for call participants to find each other, signal their desire to communicate and agree on the means of communication. This is what is generally referred to as "signalling" in IP telephony. Sessions (i.e. associations between parties) will thus have to be created and managed by IP telephony signalling.

IP telephony signalling itself can be further divided into several functions:

- *Name translation and user location*. It should be possible to map between names of different levels of abstraction (e.g. a common name at a domain and a user name at a particular host). Location of the user may be relevant in this process.
- *Media negotiation* (also known as *capabilities exchange*). Parties should agree on what media to use for communication. Parameters of those media (e.g. encodings) can be negotiated too.
- *Call participants management*. Number, type and role of participants during a call may vary. For example, it should be possible to invite others into an existing call, or terminate associations with some users, or transfer and hold other users.
- *Media changes*. It should be possible to modify the media used during the course of a session, for example because the participants require additional or reduced functionality.

6.1 Architecture

In this clause the functional entities that in general are required to achieve multimedia communication over an IP network are derived and the way in which they relate to each other is represented diagrammatically. The resulting generic functional architecture can then be used as the basis for evaluating relevant existing and evolving standards and identifying areas where further standardization is required. This clause limits itself to the case where communicating users have direct connection to the IP network. Interworking with a switched circuit network is discussed in clause 8.

For the purposes of this Technical Report the IP network is assumed to use the Internet Protocol (IP) at the network layer, on top of which any suitable transport protocol is used, e.g., UDP, TCP. The services of an appropriate transport layer are used to communicate packets of information between functional entities identified in this document when geographically dispersed.

For the purposes of this Technical Report a user can be a human user or a software application.

6.1.1 Media processing and packetization (MPP) functional entity

In order to transport a medium across an IP network between two users the medium has to be processed into a suitable form and packetized. At the receiving end it has to be de-packetized and processed back into its original form (or some other form suitable for onward transmission). For data these functions can be null if the data is already in a suitable packetized form. For real-time media these functions are unlikely to be null. Audio, for example, comprises a continuous stream of information that has to be packetized for transmission and de-packetized on reception. It can also require some or all of the following processing functions:

- coding / decoding or transcoding, including compression / decompression;
- silence suppression;
- echo cancellation;
- timing management.

Collectively these functions form a media processing and packetization (MPP) functional entity. A simple functional architecture involving only users and MPP functional entities, without any control functions, is shown in figure 3.

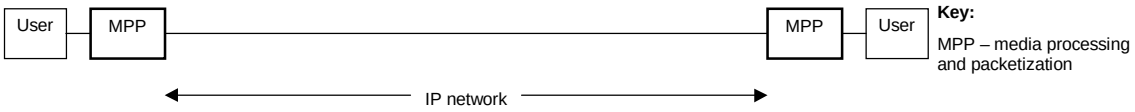


Figure 3 – Functional architecture for transport of media across an IP network

The services of an appropriate transport layer are used to communicate packets of information between the MPP functional entities. In the case of real-time media, recovery from packet error or loss is not normally feasible, and therefore UDP is normally the transport protocol used.

6.1.2 Resource control (RC) functional entity

The functional architecture above does not include control functionality for establishing, maintaining and clearing down the transport of media. At any given time there can exist one or more unidirectional medium streams between two communicating users. Bidirectional transport of a given medium will involve two unidirectional streams. Streams can be added and removed as required by the users. At either end, transmission or reception of a medium stream utilizes resources (e.g., processing resources, memory resources, port numbers, etc.). In order to control the deployment of resources in achieving the desired transmission and reception of medium streams, an RC functional entity is needed at each end.

Before media can be transported, there has to be agreement between the two ends on the media to be transported and the form in which they will be transported, e.g., coding standard. This has to take account of media requirements from the two users as well as the available resources at each end. Furthermore, the transmitting end has to know the transport address to which to send media packets. This means that signalling is required between the two RC functional entities.

The functional architecture shown above therefore needs to be extended as shown in figure 4.

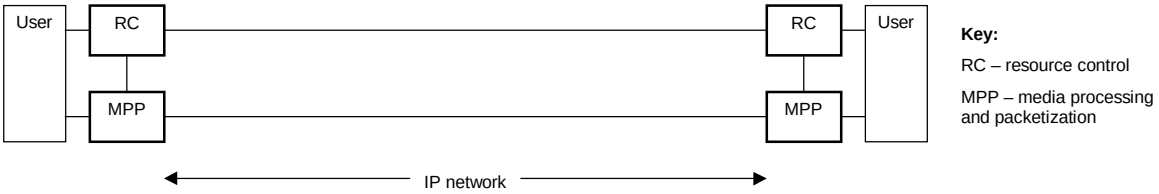


Figure 4 – Functional architecture for media transport with resource control

6.1.3 Session control (SC) functional entity

Media transport between two users occurs within the context of a communication session between the two users. The normal method of session establishment is that one of the users requests a session with the other user, that other user being identified by some means, e.g., name, address. Establishment is supported by SC functional entities acting on behalf of the two users. The calling user's SC functional entity interprets the user-supplied identity of the other user in order to be able to signal a session establishment request to the other user's SC functional entity. The latter functional entity determines whether to accept the session. The two functional entities supervise the completion of session establishment and the eventual clear down of the session, signalling to each other as appropriate. They also supervise any changes during the session (e.g., substitution of users, addition of further users to form a conference). RC functional entities act only within the context of a session established by SC functional entities.

The functional architecture shown above therefore needs to be extended as shown in figure 5.

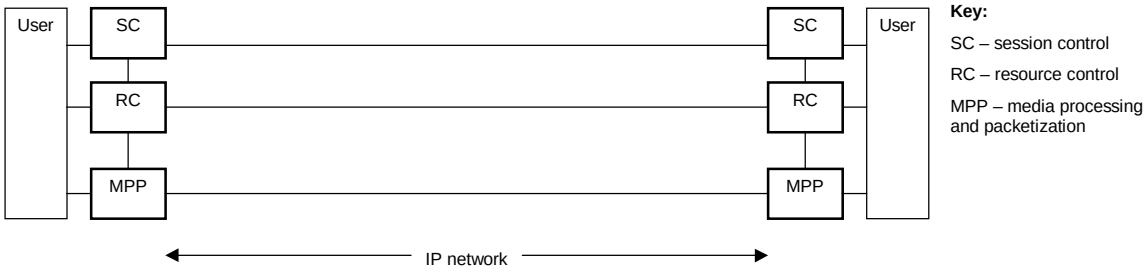


Figure 5 – Functional architecture for media transport with resource and session control

6.1.4 SC-redirect (SC-R), SC-proxy (SC-P) and RC-proxy (RC-P) functional entities

The capabilities of the SC functional entities that act on behalf of the two users may be insufficient to achieve establishment and maintenance of the session unaided. Additional SC functional entities may exist along the path of the session. For example, the SC functional entity acting on behalf of the calling

user may be unable to resolve the called user's identity sufficiently to route the session directly to the SC functional entity acting on behalf of the called user. Instead it might be able to establish the session as far as an intermediate SC functional entity, which in turn will either:

- redirect the session by clearing back the session to the preceding SC functional entity with an instruction where to route to; or
- extend the session towards the destination.

To distinguish the three types of SC functional entity identified, the following terminology is used:

- an SC functional entity associated with a user is an SC-user (SC-U) functional entity;
- an SC functional entity that redirects the session is an SC-redirect (SC-R) functional entity; and
- an SC functional entity that extends the session is an SC-proxy (SC-P) functional entity.

Any number of SC-R and/or SC-P functional entities can in theory be involved. In practice the number is likely to be influenced by the number of administrative domains that have to be transited in order to reach the destination.

SC-P functional entities may or may not remain involved throughout the lifetime of the session, whereas SC-R functional entities have only a transient involvement. SC-P functional entities that remain involved throughout the lifetime of a session can participate in changes during the session, e.g., involvement in certain supplementary services such as call transfer. This may require the use of a local RC functional entity, i.e., an RC-proxy (RC-P) functional entity, to manage the impact of session changes on resources.

To take account of SC-R, SC-P and RC-P functional entities the functional architecture is extended as shown in figure 6.

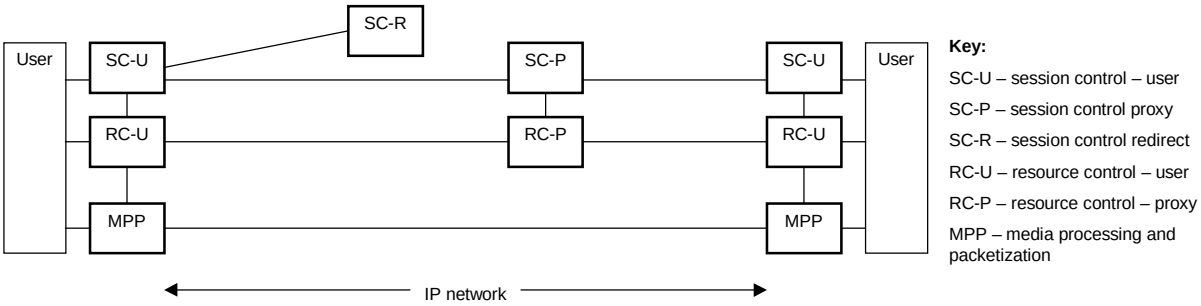


Figure 6 – Functional architecture showing SC-R, SC-P and RC-P functional entities

6.1.5 Admission control (AC) functional entities

An AC functional entity grants admission to the IP network for the purpose of establishing a session and grants permission to use IP network bandwidth during that session. A SC-U functional entity consults an AC functional entity for this purpose.

6.1.6 Identity resolution (IR) functional entity

IR functional entities convert user identities to addresses that the IP network can use for routing, i.e. IP addresses. IR functional entities are called upon by SC functional entities for this purpose. An IR functional entity may be able to resolve a given identity fully (to the address of the destination user), partially (to an address of another SC functional entity, i.e., an SC-R or SC-P) or not at all. IR functional entities can signal to each other for the purpose of sharing identity resolution information.

In principle all types of SC functional entity can make use of IR functional entities, although SC-U functional entities may instead route all sessions to an SC-R or SC-P functional entity for resolution.

6.1.7 Registrar (RGR) and registrant (RGT) functional entities

The relationship between a user identity and an IP address can be fixed. However, this means that the user must always use the same IP address and prevents the following:

- user mobility between different terminals with different IP addresses;
- terminal mobility between different sub-networks that use different IP address ranges;
- dynamic assignment of IP addresses using DHCP.

To allow these features to operate and allow the user to be located when an incoming call arrives, a means of registering a temporary relationship between a user identity and an IP address is required. For this purpose the registrar and registrant functional entities are required. The RGT functional entity acts on behalf of a user and submits registration requests to the RGR functional entity. The RGR functional entity accepts registration requests, stores the mapping of user identity to IP address, and makes this information available to IR functional entities.

6.1.8 Generic functional architecture (non-interworking)

With all of the functional entities identified above, the functional architecture is as shown in figure 7.

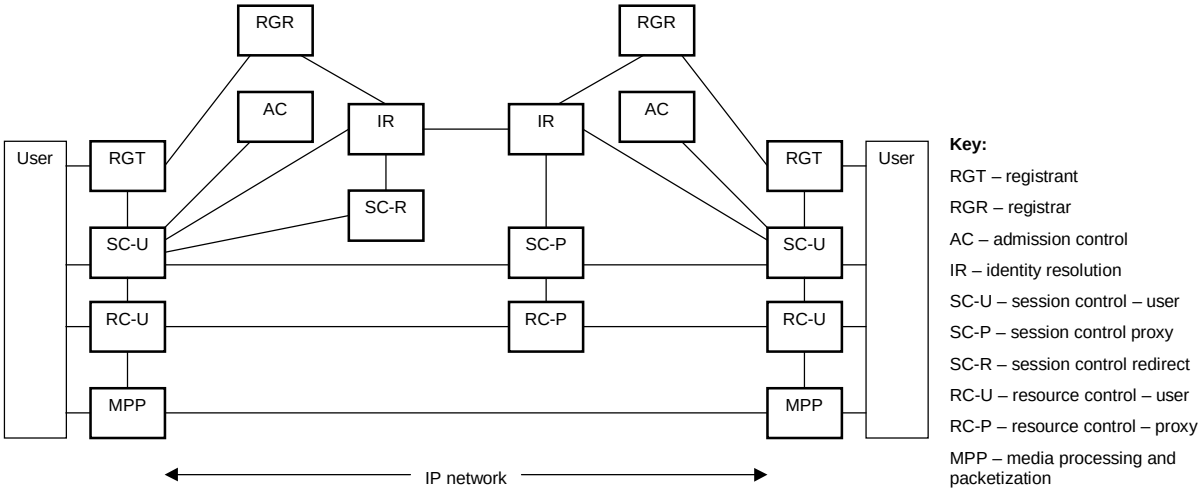


Figure 7 – Generic functional architecture

6.1.9 Physical realizations of generic functional architecture for multimedia communication over an IP network (non-interworking)

A typical physical realization of the generic functional architecture is shown in figure 8, where functional entities are implemented either in terminals (e.g., PCs) or in network servers.

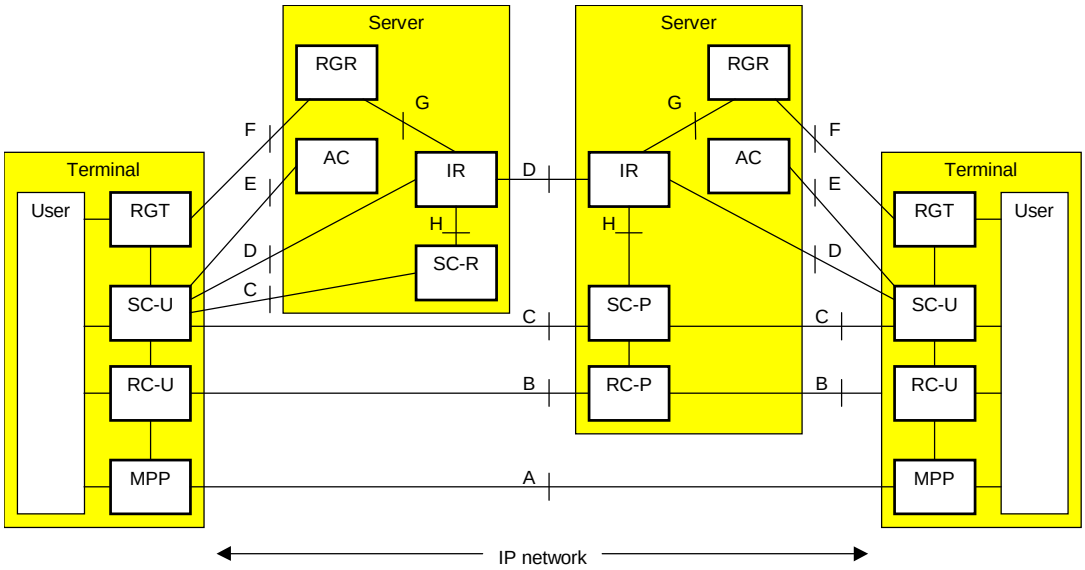


Figure 8 – Example of a physical realization of the generic functional architecture

This particular realization results in exposed interfaces at the following points:

- A (between MPPs) – transport of media streams;
- B (between RCs) – resource control signalling;
- C (between SCs) – session control signalling;
- D (between SC-U and IR and between IRs) – identity resolution signalling;
- E (between SC-U and AC) – admission control signalling;
- F (between RGT and RGR) – registration signalling.

Although not exposed in this particular example, other feasible physical realizations can result in exposed interfaces at the following points:

- G (between RGR and IR) – identity resolution management signalling;
- H (between IR and SC-R and between IR and SC-P) – identity resolution signalling.

Interface C applies also between two SC-P functional entities or between two SC-U functional entities. Likewise interface B applies also between two RC-P functional entities or between two RC-U functional entities.

Signalling between physical entities occurs over the IP network using an appropriate transport layer, e.g., TCP.

6.1.10 Generic functional architecture for interworking with an SCN

The generic functional architecture at either side of the IP network is modified as shown in figure 9 when interworking with an SCN. In the figure the SCN is represented by two functional entities: SCN switching (representing the collective switching capabilities of the SCN) and SCN control (representing the collective control capabilities of the SCN).

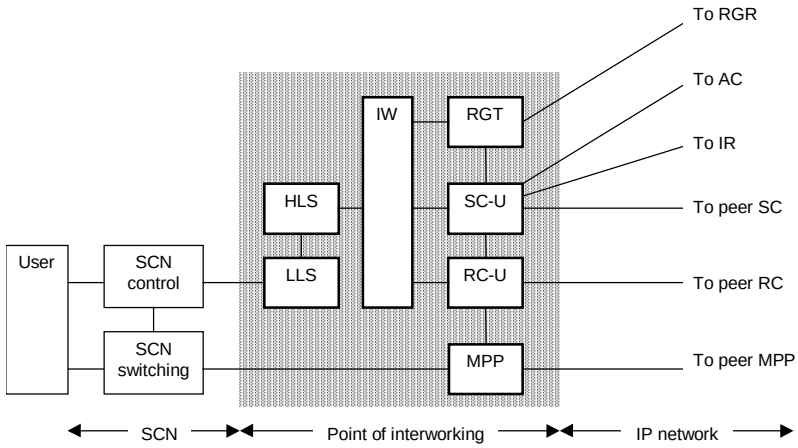


Figure 9 – Generic functional architecture for interworking with an SCN

The SCN side of the MPP functional entity terminates a switched circuit (e.g., an ISDN B-channel). SCN control plane lower layer signalling (e.g., up to layer 2) is terminated by a lower layer signalling (LLS) functional entity and SCN control plane higher layer signalling (e.g., layer 3 upwards) is terminated by a higher layer signalling (HLS) functional entity. These two functional entities are separated because some physical realizations being considered by standards bodies separate the termination of SCN signalling transport protocols (e.g., SS7 MTP, ISDN layer 2 signalling) from the termination of higher layer protocols. An InterWorking (IW) functional entity performs control plane interworking between SCN control plane signalling (for call control purposes) and IP network control plane functionality (primarily session control, but with impact on other aspects such as resource control).

Within the SCN, session and resource control normally exist only in the context of calls involving multimedia communications in accordance with a standard such as H.320. In this case, any session or resource control signalling is carried within the switched circuit, and therefore is delivered to the SC-U functional entity or RC-U functional entity respectively via the MPP functional entity, which handles multiplexing of the signalling and media streams. This is not explicitly shown in the figure.

Although an RGT functional entity exists on the IP network side of the IW functional entity, its purpose is to allow the interworking equipment (gateway) to register with an RGR and make known the SCN addresses that it is able to reach. The SCN user does not need to register in order to make calls to and receive calls from the IP network.

6.1.11 Physical realizations of generic functional architecture for interworking with an SCN

The functional entities involved at the point of interworking can be realized as an integrated gateway unit (figure 10).

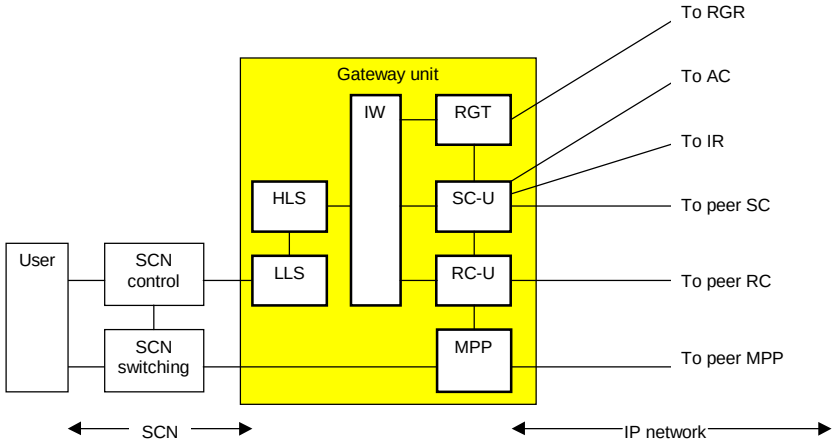


Figure 10 – Example physical realization of interworking with an SCN using an integrated gateway unit

Alternatively a number of separate units can be employed. Normally this involves physical separation of the MPP functional entity from the various control plane functional entities. The unit containing the MPP is commonly known as the media gateway (MG) unit and the unit containing the IW and other control plane functional entities is commonly known as the media gateway controller (MGC) unit. This results in the exposure of an interface at point J between the MPP and RC-U functional entities. Because MGC units tend to be more scaleable than MG units, a single MGC unit will typically control a multiplicity of MG units.

The MGC unit normally comprises at least the following functional entities: IW, RGT, SC-U, RC-U and HLS. The LLS functional entity can be included in the MGC unit, as shown in figure 11, included in the MG unit, as shown in figure 12, or provided as a separate Signalling Gateway (SG) unit, as shown in figure 13.

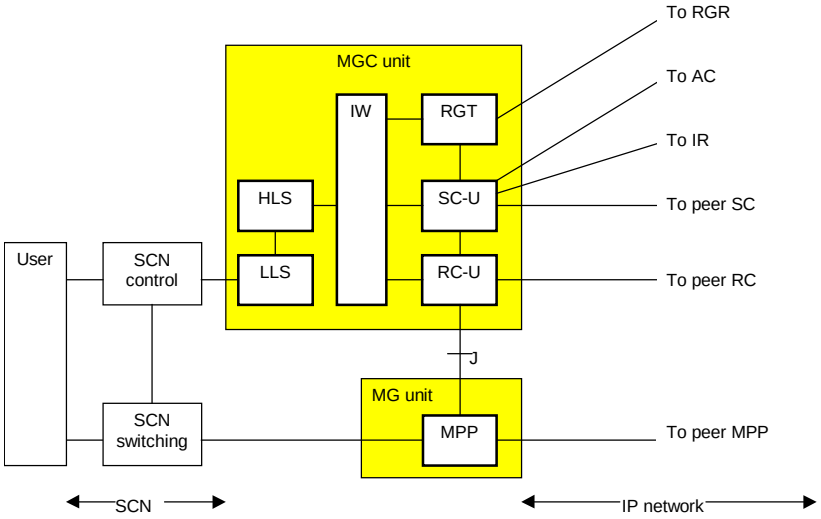


Figure 11 – Example physical realization of interworking with an SCN using separate MG and MGC units, with the LLS functional entity within the MGC unit

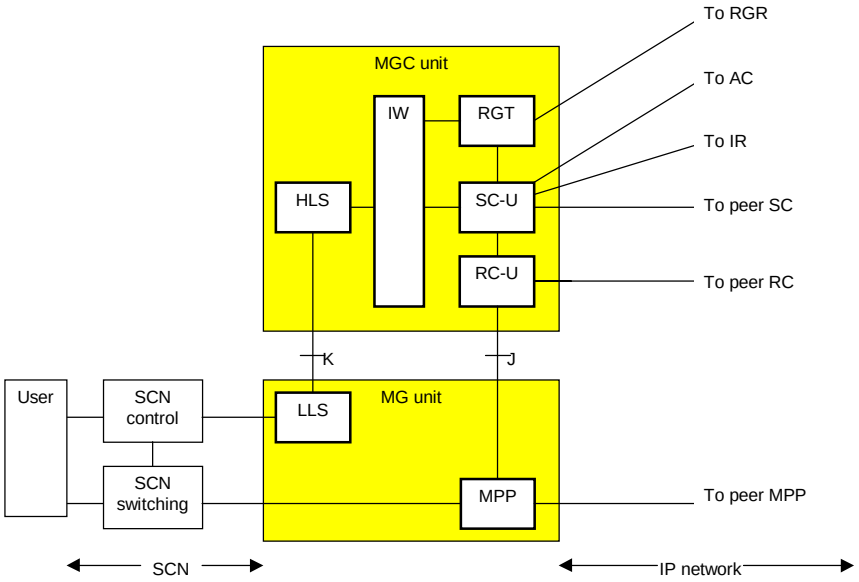


Figure 12 – Example physical realization of interworking with an SCN using separate MG and MGC units, with the LLS functional entity within the MG unit

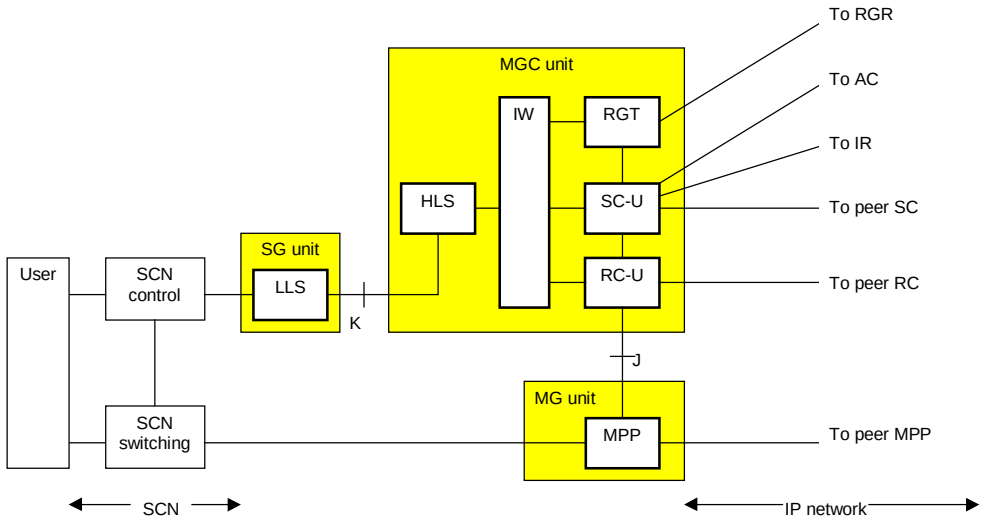


Figure 13 – Example physical realization of interworking with an SCN using separate MG, MGC and SG units

In the last two cases, interface K is exposed between the HLS functional entity and the LLS functional entity.

6.1.12 Simple terminals

As has already been shown (6.1.9), user endpoints comprise a number of functional entities (i.e., MPP, RGT, SC-U, RC-U), reflecting the fact that a user endpoint acts as the interface between the user and the packet environment. An alternative view of a user endpoint is that it performs interworking between a non-packet environment and a packet environment. In this case it would comprise some of the same functional entities as the gateway units described above (6.1.11).

Physical realization of a simple terminal can place the MPP functional entity in the terminal and the control plane functional entities in other equipment attached to the IP network, i.e., in a server or MGC unit. This is shown on the left hand side of figure 14. Typically a single MGC unit would control a multiplicity of terminals.

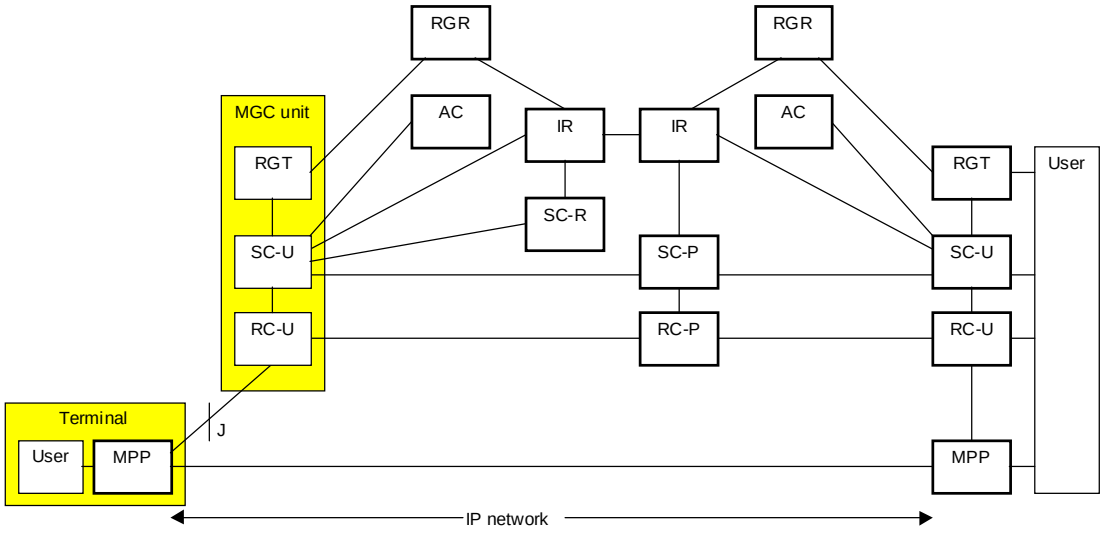


Figure 14 – Example physical realization of a simple terminal relying on network-based MGC unit

This arrangement exposes interface J between the MPP functional entity and the RC-U functional entity. No separate control interface is shown between the user and MGC unit and no LLS, HLS or IW functional entities are shown. This is because interface J can be extended to convey simple control

information between the user and the control plane functional entities in the MGC unit, via the MPP functional entity in the terminal. The control information concerned is stimulus in nature, comprising simple events (e.g., on-hook, off-hook, dialled digits, key presses, etc.) to the MGC unit and instructions (e.g., for display, lamp control, sound control, etc.) to the terminal.

6.2 Naming and addressing

For an IP network, the basic form of addressing is by means of IP addresses. At present this is almost predominantly IPv4 addresses comprising 4 octets. Longer IPv6 addresses are expected to be introduced eventually.

In many cases, for convenience of the user, names are used as aliases for IP addresses, because names can be remembered more easily than IP addresses. In addition, such aliases form a basis for user mobility, since a user may change IP address while keeping the same name. The use of names (aliases) requires mechanisms for assigning names to IP addresses and for translating names into IP addresses. These mechanisms can be enabled by the Domain Name System (RFC 1034 and RFC 1035), which provides a hierarchical administration of names facilitating a distributed database for mapping names to IP addresses.

6.3 Security

Present day IP packet-based networks do not in general provide end-to-end security services. Therefore, when interconnecting a secure private switched circuit network (SCN) to an IP network, there is an increased potential for risk of attack by an intruder. Simply by attaching a network monitor that is SCN protocol capable to an appropriate point on the IP network, an intruder can monitor and record on-going conversations that occur. For example, if the SCN interconnects through an Ethernet or other shared media sub-network, anyone on the network segment is a potential intruder. Besides the increased risk of privacy loss, other more disruptive forms of attack are also possible by inserting forged IP datagrams, which convey carefully crafted higher level protocol commands, into a communications stream. For example, an intruder could continually issue connection resets to shut down an on-going conversation relying on a TCP connection. More sophisticated attacks could also be directed against the various signalling and media stream transport interfaces described earlier.

A common solution for shielding a private network from a less restricted IP network is a firewall. A firewall is a functional entity stationed at the interface to the less restricted IP network for monitoring the communications, ensuring that only legitimate pre-authorised protocols flow across the interface and that prescribed access control policies are followed (e.g., from what IP address ranges can a call be initiated). While a firewall can shield the SCN to some extent, it does not prevent eavesdropping on a conversation or tampering with IP datagrams by an intruder. Something more is needed.

Under the banner of Internet Protocol Security (IPSec, IETF standardisation efforts have recently produced a framework (RFC 2401) and family of security protocols and mechanisms, e.g., Authentication Header (AH, RFC 2402), Encapsulating Security Payload (ESP, RFC 2406) and Internet Security Association and Key Management Protocol (ISAKMP, RFC 2408) for implementing IP security services. IPSec security protocols are able to encapsulate IP datagrams at the network level for authentication, confidentiality and integrity purposes. IPSec is designed to work with both versions 4 and 6 of IP. Similar security mechanisms to those employed by IPSec can also be applied one level higher, at the transport layer. IETF standardisation for TCP has resulted in the Transport Layer Security (TLS) protocol. TLS was drawn from a Netscape-developed security protocol called the Session Security Layer (SSL) protocol, which is in wide use today and is backward compatible with SSL.

6.4 Quality of service (QoS)

Quality of service is the collective effect of service performance factors, which determines the degree of satisfaction obtained by a user of the service. Traditional SCNs offer good quality speech transmission, which is based upon the fact that SCNs had a relatively slow evolution and have always been optimised for services with high quality and reliability demands. Quality impairments were decreased with each new generation of technology.

The Internet, on the contrary, intrinsically offers only a very basic level of quality of service. Usually only a best-effort point-to-point data delivery is offered. For real-time applications over IP (e.g. telephony over IP), when compared to SCNs, the QoS impairment by individual factors is increased.

The main factors affecting the QoS in an IP telephony network are:

- Delay. This is the elapsed time for a packet to traverse from the source to the destination. Delay results in problems like echo and talker overlap. Causes of delays in an IP telephony network are network delays and delays resulting from accumulation of data (for the purpose of packetization) and processing by (low bit-rate) voice coders.
- Jitter (delay-variation). This is the variation in end-to-end delay. Reasons for variations in end-to-end delay are that individual packets need not follow the same path between sender and receiver and that packets may be buffered in intermediate systems (i.e. routers) owing to temporary traffic peaks. In order to minimise the consequences of jitter, sequences of packets can be buffered so that they can be played in the correct order and without having to substitute for packets that arrive late. The drawback, however, is that this causes additional delay.
- Packet loss. Packet loss can occur due to congestion and/or unreliability of the network. In addition, jitter and delay can also result in packet loss, since packets arriving too late at the destination are deleted.
- Imposed bandwidth (i.e. the maximum available transfer rate between source and destination).

Before IP telephony can be used extensively, it is essential that the infrastructure of the IP network provides support of real-time QoS, giving control over end-to-end packet delays. Therewith it should be noted that provision and maintenance of end-to-end speech transmission performance can best be provided by “managed” or “engineered” Intranets.

Various standardization bodies are active in the area of QoS for Voice over IP, including:

- IETF. The work in the IETF focuses on two (complementary) types of QoS control:
  - Reservation of resources (integrated services). The mechanisms for reservation of network resources according to an endpoint’s QoS request are provided by the RSVP (RFC 2205).
  - Service differentiation. Here the different types of network traffic are classified, enabling preferential treatment to specific applications, and network resources are allocated in accordance with bandwidth management policy criteria. The framework for differentiated services is specified in RFC 2475.
- ITU-T Study Group 12 (“end-to-end transmission performance of networks and terminals”). The work in Study Group 12 focuses on:
  - identification of transmission parameters (e.g. packet loss, packet delay variation, echo) relevant to IP-based networks for which transmission planning guidance must be provided in order to implement voiceband and multimedia services;
  - quantification of the impact on end-to-end transmission quality of these transmission parameters;
  - identification of necessary planning rules for networks that use IP technology.
- ETSI TC STQ (“Speech processing, Transmission and Quality aspects”).
- ETSI project TIPHON. The general aspects of QoS for TIPHON networks can be found in TR 101 329. The TIPHON model distinguishes four classes for QoS (best, high, medium and best efforts). These classes take account of overall speech transmission quality rating R (according to the E-model described in ITU-T Recommendation G.107), one-way non-interactive speech quality and end-to-end delay.
- TIA TR 41 (“User Premises Telecommunication Requirements”). End-to-end voice quality guidelines for North American IP telephony are documented in PN-4689.

6.5 Mobility

Three types of mobility in networks are recognized:

- User mobility is the ability for a user to maintain the same user identity on different terminals or terminal types.

- Terminal mobility is the ability for a terminal to change location and network point of attachment and still be able to communicate.
- Service mobility is the ability for a user to obtain a particular service independently of user and terminal mobility.

The registration capabilities provided by the RGR and RGT functional entities provide a basic mobility capability, by removing the need for a fixed relationship between user identity and IP address. For example, a user can register with a registrar using different terminals with different network points of attachment and still be able to make and receive calls (user mobility) and receive the same service (service mobility). A terminal, on behalf of a user, can register with a registrar from different network points of attachment (terminal mobility). Terminal mobility is particularly associated with wireless access to the IP network and may or may not extend to maintaining calls in progress during re-registration (hand-over).

More complex mechanisms are required if there is a need for a roaming user or terminal to register with different registrars. This is typically the case when roaming over longer distances and registrars act only on local geographic zones, and is particularly so when roaming between administrative domains.

7 Standards for multimedia communication over an IP network

7.1 Overview

Important sources for existing and emerging standards for multimedia communication over a packet network are the ITU-T and the IETF. Figure 15 gives the generic functional architecture for multimedia communication over IP networks, including interworking with an SCN, showing most relevant interfaces.

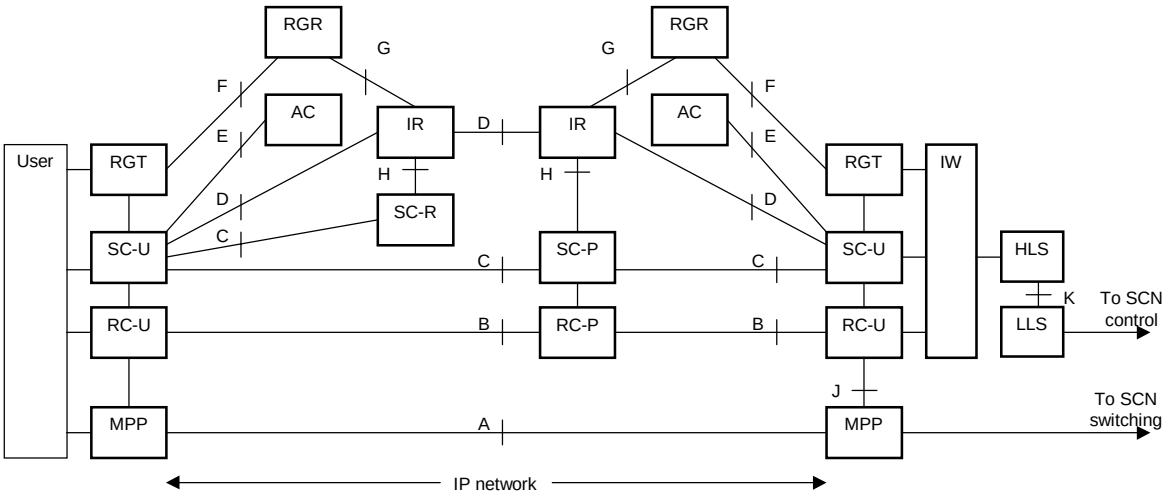


Figure 15 – Generic functional architecture showing relevant physical interfaces

NOTE
Interface designations above do not necessarily correspond to those in use in other bodies, e.g., ITU-T Study Group 16, ETSI project TIPHON.

Table 3 gives an overview of the main existing and emerging ITU-T and IETF standards applicable to the various interfaces:

Table 3 – Overview of standards applicable to the various interfaces

Inter -face	ITU-T specification	IETF specification
A	H.323 - H.225.0, RTP/RTCP part	RFC 1889 (RTP/RTCP)
B	H.323 – H.245 (resource control)	RFC 2327 (SDP)
C	H.323 - H.225.0, call control part BICC (Bearer-Independent Call Control in SS7/ISUP)	RFC 2543 (SIP)
D	H.323 – H.225.0, RAS part H.323 – H.225.0 annex G (when spanning administrative domains)	e.g. RFC 2251 (LDAP), RFC 1035 (DNS) TRIP (when spanning administrative domains)
E	H.323 – H.225.0, RAS part	-
F	H.323 – H.225.0, RAS part	RFC 2543 (SIP)
G	-	e.g., RFC 2251 (LDAP)
H	-	e.g., RFC 2251 (LDAP)
J	H.248 (=MEGACOP), optionally using SCTP for transport, as being defined in H.248 annex H	MEGACOP (=H.248), optionally using SCTP for transport
K	See NOTE	SCN adaptation specifications, SCTP for SCN-signalling transport

NOTE
ITU-T has not specified anything for interface K, although there is no reason why SCTP cannot be used for transport of SCN signalling (e.g., Q.931).

Except the ITU-T and IETF also other bodies, like ETSI (project TIPHON) and TIA are producing specifications for multimedia communication over a packet network. In most cases, these specifications are complementary to related ITU-T and/or IETF specifications.

7.2 The ITU-T H.323 family of recommendations

ITU-T recommendation H.323 (Packet-based Multimedia Communications Systems) is an umbrella recommendation that specifies protocols and procedures for multimedia communications over packet networks, including IP networks. H.323 itself refers to other ITU-T recommendations, e.g., H.225.0 for call signalling and media stream packetization and H.245 for control of multimedia communication.

NOTE
The Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP) defined in H.225.0 are compatible with the corresponding IETF protocols defined in RFC 1889.

Annex A contains an overview of H.323.

7.2.1 Functional architecture

The main H.323 entities are endpoints (endstations, gateways or MCUs) and gatekeepers. For the case where one endpoint is an endstation (terminal) and the other is a gateway to an SCN, the allocation of functional entities to H.323 entities is as shown in figure 16.

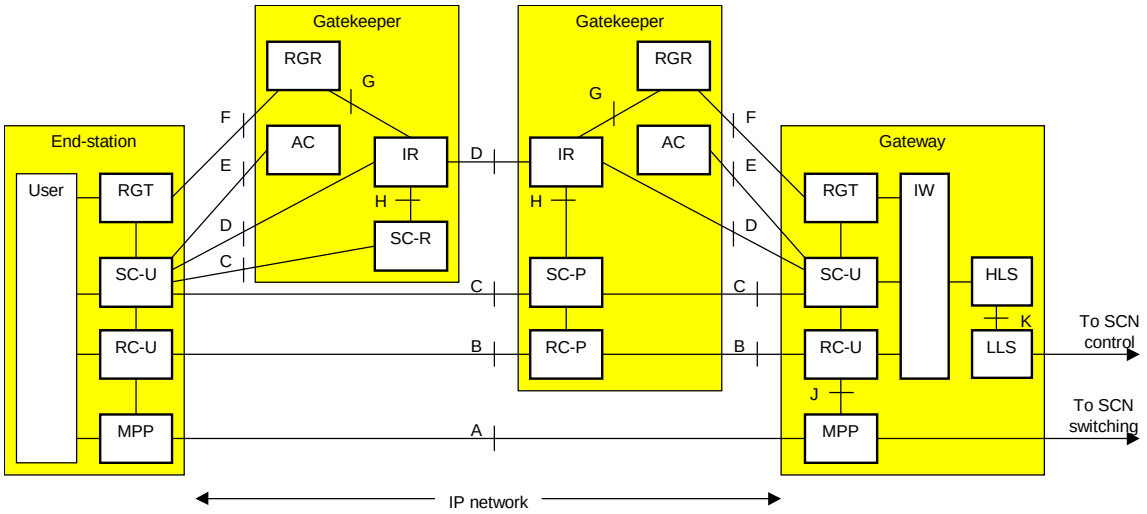


Figure 16 – Mapping of H.323 entities onto generic functional architecture

An H.323 endstation comprises MPP, RC-U, SC-U and RGT functionality. An H.323 gateway comprises MPP, IW, RC-U, SC-U, RGT, HLS and LLS functionality. An H.323 gatekeeper comprises RGR, AC and IR functionality. In addition a gatekeeper includes SC-R functionality (direct call model) and/or SC-P functionality (gatekeeper-routed call model). A gatekeeper that includes an SC-P functional entity may also include an RC-P functional entity, depending on whether actions of the SC-P functional entity have impact on resource control.

Assuming each H.323 entity is realized as a separate physical unit, interfaces are exposed at A, B, C, D, E and F.

H.323 makes use of the following protocols in support of physical separation of H.323 entities:

- H.225.0 media stream packetization for real-time media transport between MPP functional entities (interface A);
- H.245 resource control protocol between RC functional entities (interface B);
- H.225.0 "call control" protocol as session control protocol between SC functional entities (interface C);
- H.225.0 registration, admission and status (RAS) protocol for registration, admission and endpoint location purposes (interfaces D, E and F);
- H.225.0 annex G for interface D when spanning administrative domains.

7.2.2 Naming and addressing

In accordance with H.323 when applied to IP networks, addressing is by means of IP addresses. However, in H.323 the concept of aliases exists, whereby an addressable entity can have one or more other forms of identification in addition to an IP address. An alias can act as an address, but more often acts as a name. Examples of aliases are telephone numbers and email "addresses". A telephone number alias can be an E.164 number or a PNP number. Any entity outside the IP network (e.g., an entity in an SCN) has to be identified by an alias rather than an IP address.

The IP network, when required to establish a call to a given alias, will look up the corresponding IP address. In the case of an alias representing an entity in an SCN, the IP address will be that of a suitable gateway, and the gateway will use the alias as the means of identifying the final destination.

7.2.3 Supplementary services

Supplementary services for use with H.323 in an IP network are specified in the H.450.x series of recommendations. H.450.1 specifies the generic functional protocol that is used by other recommendations in the series. The following supplementary service recommendations are already specified:

- H.450.2 – Call Transfer;

- H.450.3 – Call Diversion;
- H.450.4 – Call Hold;
- H.450.5 – Call Park and Call Pickup;
- H.450.6 – Call Waiting;
- H.450.7 – Message Waiting Indication;
- H.450.8 – Name Identification;
- H.450.9 – Call Completion.

7.2.4 Security

H.323 VoIP security procedures are outlined in Recommendation H.235. The recommendation identifies a number of security services, including authentication, integrity, and confidentiality, which are intended to counter the primary threats of eavesdropping and media stream diversion. Confidentiality is also referred to as privacy or data encryption within the specification, which tends to blur these related but distinct notions.

H.235 covers three phases of an H.323 call and their associated protocols:

- Registration and call admission (H.225.0 RAS - interfaces D, E and F),
- Call establishment and control (H.225.0 call control - interface C), and
- Resource control and media transport (H.245 and RTP - interfaces A and B).

The underlying principle is that during each phase the H.235 security services can be independently negotiated and applied. The same principle applies to individual media streams as well. Communications are protected using the protocols and algorithms common to both entities. H.235 recommends the IPSec and TLS protocol standards to provide the associated security services whenever possible. Since TLS is not a viable candidate for those H.323 protocols that rely on a UDP connectionless transport service (e.g., RAS) instead of a TCP connection-oriented service, IPSec is in general the more versatile of the two. Proprietary algorithms and protocols may also be used in lieu of or in conjunction with the IPSec and TLS protocol standards. The H.235 recommendation defines a number of generic messages and procedures, which help in this regard.

NOTE
Because the H.235 recommendation comprises a wide range of alternatives for provisioning security services for communications systems compliant with the H.323 recommendation, which in itself is an umbrella recommendation, H.235 can be best viewed as a framework document. Implementers, therefore, are expected to interpret the specification for the particular application environment in which they are involved.

The various options and alternatives given in H.235 for provisioning security are varied and complex. Various profiles are being specified by ITU-T Study Group 16 (H.235 version 2 and H.323 annex J) and by ETSI project TIPHON to help in this respect. The following discussion gives some examples of the types of trade-offs one must consider for each of the H.323 call phases.

Call Admission: RAS signalling between an endstation and a gatekeeper relies on UDP and, therefore, appropriate for application of IPSec. Alternatively, RAS messages may directly convey H.235 defined extensions (e.g., ClearToken, CryptoToken) in order to perform authentication. While integrity protection of RAS messages is also possible at this layer, no confidentiality service exists.

Call Establishment and Control: Since the H.225.0 protocol relies on TCP, either TLS or IPSec can be applied during this phase. The transport connection must be made to a well-known port defined in H.235. Both the TLS and IPSec protocols can provide the required authentication, confidentiality, and integrity services and, therefore, no specific H.235 signalling is needed. However, as an alternative to performing authentication between the endstation and gatekeeper again during this phase through the TLS or IPSec protocols, it is possible instead to rely on the authentication performed during the earlier call admission phase. That is, by retaining any cryptographic associations produced in the earlier phase and applying them to the integrity and confidentiality services needed during this phase, the original authentication can be carried over.

Resource Control and Media Transport: H.245 operates over TCP and, therefore, may use either TLS or IPSec protocols to provide its security services. Security services are negotiated as any other capability in H.245. RTP was designed to be independent of the underlying transport and network layers, but for media transport typically operates over UDP. While IPSec could be used to secure individual media streams, RTP also provides a confidentiality service by applying encryption directly to the RTP payload, which may benefit performance and flexibility in multi-stream situations. Since key distribution is not within the scope of the RTP specification, H.245 signalling could be used to set up a cryptographic association by distributing the cryptographic keys needed to encrypt the RTP media streams. Some validity checks are specified in the RTP specification, but there is no overall integrity service provided as with IPSec.

Security-conscious organisations will likely deploy H.235 in conjunction with other security measures such as firewalls. A firewall can be considered to be a special type of gateway within the H.323 scheme, in that it accepts H.323 calls from one side (i.e., a trusted or secure side) and passes those calls to H.323 entities on the other (i.e., an untrusted side). On the trusted or secure side, appropriate protection is applied between the communicating endpoint and the firewall. Typically, an H.323 proxy on the firewall monitors all calls to and from the untrusted side, ensuring that only valid H.323 traffic goes through. The proxy can also enforce access control policies set by the administrator, such as whether an endpoint can initiate or receive calls, what facilities an endpoint is permitted to use, whether access is restricted to or from specific endpoints, and whether access can occur only during certain periods of time. Because of the multiple protocols involved under H.323, implementing a proxy is not as straightforward as with some other protocols. A firewall may also incorporate Virtual Private Network (VPN) technology to secure the untrusted side and extend the CN to a co-operating peer. VPN technology may also appear independently in special purpose standalone gateways as a distinct, but similar alternative to firewalls.

7.2.5 Quality of service

H.323 is concerned with multimedia communications services over packet based networks that do not necessarily provide a guaranteed Quality of Service (QoS). In order to fulfill the QoS requirements of real-time video and audio streams, H.323 recommends the use of transport level resource reservation mechanisms. Such transport level resource reservation mechanisms themselves, however, are beyond the scope of H.323. Appendix II of H.323 describes as an example the use of RSVP (Resource reSerVation Protocol) as a possible mechanism. Other protocols may be used.

RSVP is the transport level signalling protocol for reserving resources in unreliable IP-based networks. RSVP has been specified by the IETF in RFC 2205. Using RSVP, H.323 endpoints can reserve resources for a given real-time traffic stream based on its QoS requirements. If the network fails to reserve the required resources, or in the absence of RSVP, only best-effort delivery of the packets is possible.

ITU-T Study Group 16 is covering QoS aspects in H.323 annex N.

7.2.6 Mobility

H.323 inherently supports user mobility through the use of gatekeepers and the mapping of user identity (e.g., in the form of a telephone number) to IP address representing the user's current location. By registering with its gatekeeper, a user can make and receive calls in principle from any terminal at any location. Likewise, a terminal, on behalf of a user, can register with its gatekeeper from different locations (terminal mobility). In either case the user can receive a consistent service (service mobility).

However, gatekeepers generally control only a specific geographic zone within an administrative domain, and hence user or terminal roaming outside the zone or outside the administrative domain involves registering with a different gatekeeper. Work is in progress on H.323 annex H, which will describe extensions to H.323 to support mobility beyond a single gatekeeper zone. Hand-over is also being considered.

7.3 Other ITU-T standards

7.3.1 H.248

ITU-T Recommendation H.248 (Gateway Control Protocol) is complementary to H.323. It defines the protocols used between elements of a physically decomposed multimedia gateway, used in accordance with the architecture as specified in Recommendation H.323. H.248 is the result of co-operative work between ITU-T Study Group 16 and the IETF MEGACO working group. The protocol definition in H.248 is common text with a corresponding IETF RFC (not yet available), which is sometimes known as

MEGACO Protocol (MEGACOP). Consequently, the protocol is independent of the peer-to-peer signalling protocol used within the packet network (i.e., H.323 or SIP).

The H.248/MEGACO protocol operates between a media gateway unit (MG unit) and a media gateway controller unit (MGC unit), these being two component parts of a gateway to a switched circuit network (SCN). The MG and MGC units can be mapped onto the generic functional architecture of figure 15 in different ways. In any case, the MG unit comprises MPP functionality and the MGC unit is assumed to comprise at least HLS, IW, RC-U, SC-U and RGT functionality. The LLS functionality can be allocated to the MGC unit, the MG unit or a separate SG unit, as shown in figure 11, figure 12 and figure 13 respectively.

In support of physical separation of functional entities, H.248/MEGACOP complements the H.323 protocols by providing a protocol at interface J between the MG and MGC units (see figure 15). This also includes application at an interface J for simple terminals, as shown in figure 14.

H.248/MEGACOP specifies the use of IPSec [RFC 2401 to RFC 2411] as a security mechanism to prevent unauthorized entities from using the MEGACO/H.248 protocol for setting up unauthorized calls or interfering with authorized calls. The IPSec mechanisms can be used to provide data origin authentication, connectionless integrity, optional anti-replay protection of messages and confidentiality of messages passed between the MG unit and the MGC unit.

Annex C contains an overview of H.248/MEGACOP.

7.3.2 BICC

Bearer-Independent Call Control (BICC) is a protocol being developed by ITU-T Study Group 11 as an adaptation of SS7 ISUP. Initially developed for controlling bearers provided by ATM networks, work is now being extended to control bearers provided by IP networks. BICC itself runs in an existing signalling network. As for ISUP, it is applicable only to public networks.

For controlling bearers provided by IP networks, it is anticipated that BICC will fulfil the role of a session control protocol at interface C and will be used to establish a bearer for a resource control protocol, e.g., H.245.

7.4 IETF specifications for IP telephony

Different protocols related to IP telephony are emerging from the IETF. Logically, these individual protocols can be used to create a complete framework for multimedia communication over IP networks. The difference from ITU-T H.323 is that there is no umbrella specification that formally glues together the individual components.

Important IETF specifications in the area are the Session Initiation Protocol (SIP) and Session Description Protocol (SDP). These specifications complement earlier IETF protocols such as the Real time Transport Protocol (RTP) for media stream packetization.

7.4.1 Functional architecture

The main entities defined in relevant IETF protocols are SIP proxy servers, SIP redirect servers, location servers, SIP registrars and endpoints (endstations, gateways) containing SIP user agents. The mapping of SIP entities onto functional entities of the generic functional architecture is as shown in figure 17.

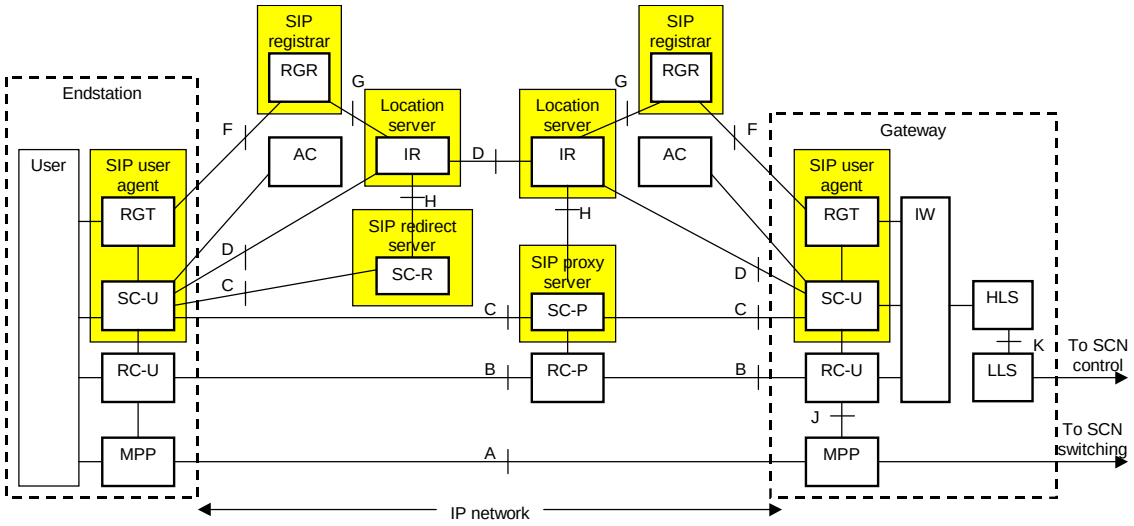


Figure 17 – Mapping of SIP entities onto generic functional architecture

A SIP registrar will typically be implemented in the same equipment as a SIP redirect server or SIP proxy server. A location server can be implemented in the same equipment as a SIP registrar or a SIP proxy or SIP redirect server.

Examples of protocols in support of physical separation of functional entities (see also table 3 in 7.1) are:

- RTP (RFC 1889) for real-time media transport between MPP functional entities (interface A);
- SDP (RFC 2327) session description protocol between RC functional entities (interface B);
- SIP (RFC 2543) as session control protocol between SC functional entities (interface C) and registration protocol between RGT and RGR functional entities (Interface F);
- LDAP (RFC 2251) and/or DNS (RFC 1035) and (when spanning multiple domains) TRIP (interface D);
- MEGACOP for media gateway control in the case of a decomposed gateway (interface J);
- SCTP (SIGTRAN) as transport mechanism for MEGACOP and SCN-signalling (interfaces J and K).

7.4.2 Main protocols

7.4.2.1 Real-time Transport Protocol (RTP)

The Real time Transport Protocol (RFC 1889) provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, time-stamping and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing, port addressing and checksum services; both protocols contribute parts of the transport protocol functionality. RFC 1889 also specifies the Real-time Transport Control Protocol (RTCP), which provides feedback on quality of transmission. RTP and RTCP serve as the basis for the corresponding ITU-T H.225.0 protocols and the two pairs of protocols are compatible.

7.4.2.2 Session Initiation Protocol (SIP)

The Session Initiation Protocol is a session control signalling protocol for IP telephony and multimedia conferencing. SIP can establish, modify and terminate phone calls or multimedia sessions. It has been developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, and is now a Proposed Standard RFC, RFC 2543.

Annex B contains an overview of SIP.

7.4.2.3 Session Description Protocol (SDP)

SDP (RFC 2327) is used to describe multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. Although not mandated, SDP is

the assumed candidate for use with SIP. Contrary to ITU-T's H.245, SDP is not intended for negotiation of media encodings, but merely for capability exchange.

NOTE
Endpoints recognize received media types from the RTP payload type information in the RTP header.

7.4.2.4 Domain Name System (DNS) and Lightweight Directory Access Protocol (LDAP)

The Domain Name System (DNS), specified in RFC 1034 and RFC 1035, can be used between SC-U and IR functional entities (interface D) to locate an appropriate SIP server. DNS is a distributed database, used for mapping between hostnames and IP addresses. DNS is less suited for locating individual endpoints.

LDAP (Lightweight Directory Access Protocol), specified in RFC 2251, provides a directory service that offers a means to locate individual endpoints without knowing their location. LDAP can be applied between SC-U and IR functional entities (interface D), between RGR and IR functional entities (interface G) and between SC-R/SC-P and IR functional entities (interface H).

NOTE
LDAP and DNS can also be used in H.323 systems.

7.4.2.5 Telephony Routing Information Protocol (TRIP)

The Telephony Routing Information Protocol (TRIP) is being specified by the IETF IPTEL group. TRIP is a policy driven inter-administrative domain protocol for advertising the reachability of telephony destinations between location servers, and for advertising attributes of the routes to those destinations. TRIP's operation is independent of any signalling protocol. Hence TRIP can serve as the telephony routing protocol for any signalling protocol.

Architecturally TRIP is applicable at interface D between two IR functional entities in different administrative domains. It can also be used for flooding inter-domain routing information within an administrative domain. It fulfils a similar function to H.225.0 annex G, which is part of H.323. Because H.323 implementations are likely to use H.225.0 annex G for inter-domain routing, use of TRIP is more likely to be with SIP.

7.4.2.6 Media Gateway Control Protocol (MEGACOP)

MEGACOP defines protocols used between elements of a physically decomposed multimedia gateway and is the result of co-operative work between ITU-T Study Group 16 and the IETF MEGACO working group. See 7.3.1.

7.4.2.7 Simple Control Transport Protocol (SCTP)

Work in the IETF SIGTRAN group is aimed at producing a transport protocol suitable for carrying signalling, in particular taking into account the high demands of SS7. Currently work is in progress on a Simple Control Transport Protocol (SCTP). Although it has a number of possible applications, the initial aim is to fulfil requirements of interface K between an LLS functional entity and an HLS functional entity, as shown in figure 12 and figure 13.

Annex D contains an overview of SIGTRAN work.

7.4.3 Naming and addressing

In SIP, users are identified and addressed by SIP URLs (such as sip:jack@company.com). Calls to this address must traverse SIP servers on the network, much like email traverses message transfer agents (MTA's), eventually arriving at the current location for this user. More precisely, SIP uses an email-like identifier of the form *"user@domain"*, *"user@host"*, *"user@IP address"* or *"phone-number@gateway"*. The identifier can refer to the name of the host that a user is logged into at the time, an email address or the name of a domain-specific name translation service. Addresses of the form *"phone-number@gateway"* designate SCN phone numbers reachable via the named gateway (in accordance with the numbering plan of the SCN concerned). SIP thus uses these addresses as part of SIP URLs, such as sip:jack@company.com or sip:+1-255-238-1234@gateway_provider.com.

7.4.4 Supplementary services

Assuming a high degree of decentralization, many supplementary services are enabled by basic SIP (RFC 2543). Without the need for further standardisation, many supplementary services can be

implemented in SIP endstations. A certain set of services however, need to be implemented in a network component, such as a SIP proxy server, a SIP redirect server or a registrar device. For example, services that are independent of a particular endsystem or services that need to be available even when a targeted endsystem is not operational.

A number of SIP Telephony Call Flow Examples have been documented in IETF drafts. Included in these examples are call flows for the following supplementary services:

- Call Hold;
- Consultation Hold;
- Unattended Transfer;
- Attended Transfer;
- Call Forwarding Unconditional;
- Call Forwarding – Busy;
- Call Forwarding - No Answer;
- 3-way Conference;
- Single Line Extension;
- Find-Me;
- Call Management (Incoming Call Screening);
- Call Management (Outgoing Call Screening).

For services where the capabilities provided by basic SIP are insufficient, extensions to basic SIP (in the form of additional messages and headers) are currently being defined by the IETF MMUSIC and SIP working groups.

Because IETF practice is to standardize building blocks rather than complete architectures or services, it is unlikely that supplementary services will be specified in standards track RFCs. However, if consensus is reached as to how certain supplementary services are best implemented, this might be documented in informational “best current practice” RFCs. There may be opportunity for ECMA members to influence this process and/or to produce their own SIP supplementary service standards, in order to achieve close alignment with the specifications, functional models and information flows on which QSIG supplementary services are based.

Personalization of services is enabled by running scripts on SIP proxy and SIP redirect servers using mechanisms like SIP-CGI (Common Gateway Interface) and CPL (Call Processing Language), currently being specified by the IETF IPTEL working group.

7.4.5 Security

The SIP specification includes capabilities for encryption and authentication of SIP messages. These mechanisms can protect against unauthorised use of the signalling information contained in SIP and SDP messages. Different, complementary forms of security are supported. End-to-end encryption of SIP message body and certain header fields provides confidentiality of information between endpoints. Additionally, hop-by-hop encryption of specific header fields can be used for securing routeing and address information over links between SIP endstations and SIP servers. Encryption of the media can be achieved using mechanisms provided by SDP. Authentication mechanisms are provided, e.g. to ascertain the identity of the caller, to prevent injection of unauthorised responses or to prevent unauthorised redirection of the call.

The security mechanisms of SIP and SDP are assumed to make use of common security tools such as IPSec [RFC 2401 to RFC 2411]. IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

Recently, the IETF SIP Working Group has launched a SIP Security Task Force with the special aim of evaluating the SIP security model, so that it can be clarified and strengthened in the next version.

7.4.6 Quality of service

Different mechanisms for Quality of Service control and measurement are available, including:

- RTP control Protocol (RTCP) defined in RFC 1889. RTCP provides feedback on quality of transmission.
- End-to-end QoS reservations based on for example the Resource reSerVation Protocol (RFC 2205).
- Differentiated services (DiffServ) described in RFC 2474 and RFC 2475. With DiffServ it is possible to implement scalable service differentiation in IP-based networks.
- Multiprotocol Label Switching (MPLS), introducing the use of labels for identification of particular traffic requiring special services, e.g., QoS. The requirements for traffic engineering over MPLS are described in RFC 2702. Further work on this subject is in progress in the IETF MPLS working group.

7.4.7 Mobility

SIP transparently supports user mobility by name mapping and by proxying and redirecting requests to the user's current location. Based on the use of a unique personal identity and the ability of SIP-users to register their current location, end users can originate and receive calls and access subscribed telecommunication services on any terminal in any location.

7.5 ETSI TIPHON specifications

ETSI project TIPHON is producing technical specifications for interworking between IP networks and SCNs. The following scenarios are being considered:

- a call between two users in IP networks (global IP-telephony service);
- a call from user in an IP network to a user in an SCN;
- a call from a user in an SCN to a user in an IP network;
- a call between two SCNs via an IP network;
- a call between two IP networks via an SCN.

Work to date has focused on H.323 as the signalling protocol, but SIP is now also being investigated. The following topics are covered:

- requirements;
- architecture;
- protocols;
- naming and addressing;
- QoS;
- security;
- mobility;
- testing and validation;
- management.

7.6 Terminal specifications from TIA TR-41.3.4

TIA TR-41.3.4 is producing a profile specification for terminals attached to IP networks, TIA/EIA/IS-811. As far as control is concerned, the profile specification allows for H.323, SIP or H.248. In each case the document specifies use of the protocols.

8 Interworking of PISNs and IP networks via a gateway

With an interworking scenario the circuit and IP networks operate as peers. The basic interworking scenario is a call between a user connected to a SCN and a user connected to a IP network. Instances of interworking between circuit and IP networks can be concatenated, e.g.:

- circuit-IP-circuit;
- IP-circuit-IP.

In either of these two cases, the network in the middle plays a full part in the provision of the communication service, and the originating network need not know, when establishing a call to the second network, that the call will terminate at a network of the same type as the originating network.

Any specifications for interworking between circuit and IP networks should be applicable at each concatenated instance of interworking, and there should not be a need to produce specifications for concatenation in general or for specific examples of concatenation.

In this Technical Report, attention is confined to the case where the circuit network is a PISN using QSIG (as specified in ECMA-143, ECMA-165 and other ECMA Standards) as the inter-exchange signalling system.

8.1 Architecture

An equipment that performs interworking between a PISN and an IP network can be regarded as a PINX. Figure 18 shows part of the PINX reference configuration from ECMA-133 superimposed onto the generic functional architecture for interworking from figure 9. The relationship between functional entities from the generic functional architecture for interworking and functional groupings from the PINX reference configuration is as follows:

- the RGT, SC-U, RC-U, IW and HLS functional entities together correspond to the Call Control (CC) functional grouping;
- part of the MPP functional entity corresponds to the Switching (SW) functional grouping;
- the LLS functional entity and the remainder of the MPP functional entity correspond to the Mapping (MP) functional grouping;
- the Scenario Management (SM) and Inter-PINX Connection Control functional groupings have no equivalents in the generic functional architecture for interworking.

The MP functional grouping is responsible for mapping logical signalling and user information channels at the Q reference point onto physical channels at the C reference point and terminating signalling transport protocols. The functionality relating to the signalling channel corresponds to the LLS functional entity. The functionality relating to user information channels can be regarded as being part of the MPP functional entity.

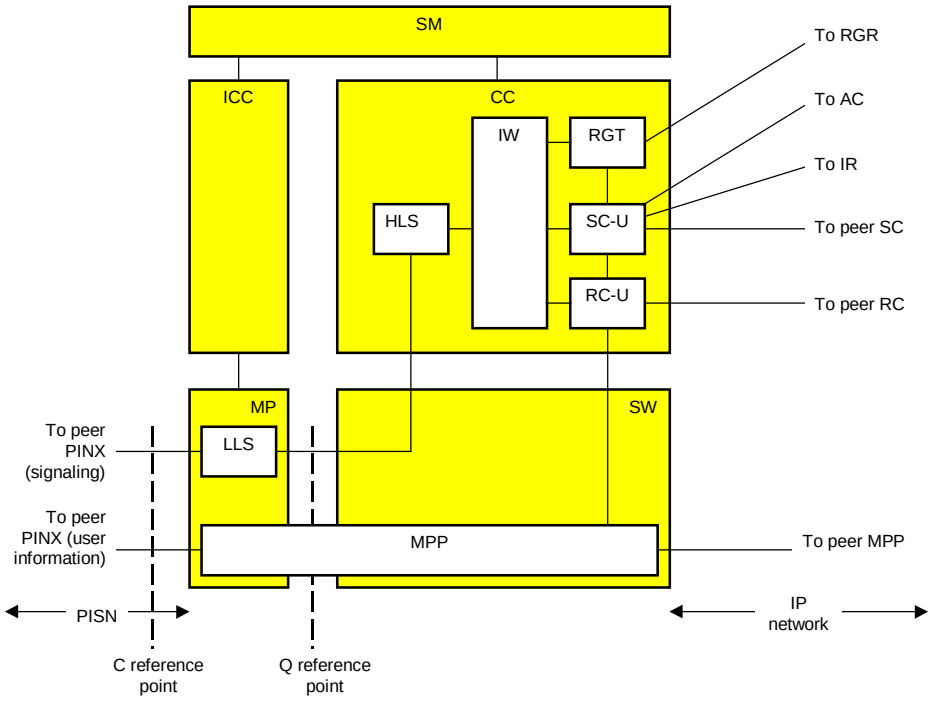


Figure 18 – Functional architecture for interworking with a PISN

8.2 Signalling

From 8.1 it can be seen that the IW functional entity is required to perform signalling interworking between signalling at the Q reference point (e.g., QSIG) and IP network session control signalling. If H.323 is used in the IP network, the IW functional entity needs to perform signalling interworking between QSIG and H.225.0 (basic call) and H.450.x (supplementary services). If SIP is used in the IP network, the IW functional entity needs to perform signalling interworking between QSIG and SIP. The IW functional entity needs to interact with the SC-U functional entity, and also with the RC-U functional entity to ensure that resources made available in the IP network are suitable for mapping onto the bearer capability used in the PISN and vice versa.

8.3 Naming and addressing

8.3.1 Naming and addressing in PISNs

In accordance with ECMA-155 / ISO/IEC 11571, addressing in a PISN is by means of numbers conforming to either E.164 or a Private Numbering Plan (PNP). Numbers can also be represented in an implicit format, where prefix digits or other means within the actual number identify the numbering plan, but the numbering plan is still either E.164 or a PNP.

NOTE
Sometimes numbers in a PISN are used as names (identifying users) rather than addresses (identifying points of attachment), and therefore the terms "address" and "addressing" are not always used in line with current ITU-T Study Group 2 use.

In addition, PISNs can use textual names in accordance with ECMA-163 / ISO/IEC 13864 for name identification of a user in a call. This is not considered further in this Technical Report.

8.3.2 Naming and addressing in IP networks

See 7.2.2 (H.323) and 7.4.3 (SIP).

8.3.3 Naming and addressing interworking when H.323 used in the IP network

H.323 supports the use of E.164, PNP and implicit numbers as alias addresses.

8.3.3.1 Interworking and PNP numbers

A characteristic of a PNP is that it belongs to a CN administration and numbers from that PNP have significance only within that administrative domain. An administrative domain may cover an entire CN or only part of a CN.

When an IP network is a public network, it is necessarily a different administrative domain from that of a PISN. The PISN may employ a PNP, but the public IP network will not. Therefore PNP numbers cannot be passed through a gateway between the two networks. Numbering considerations are similar to those in ECMA-155 between a PISN and a public ISDN.

When an IP network is a private network belonging to the same CN as a PISN, the use of a PNP in the IP network can be in accordance with any of the following:

1. No PNP in the IP network.
2. Use of separate PNPs in the IP network and the PISN (different administrative domains).
3. Use of a single PNP in the IP network and the PISN (same administrative domain).

In cases 1 and 2, a PNP number from the PISN cannot be passed on to the IP network and the gateway is required to translate such a number into an alias that is meaningful in the IP network.

In case 2, a PNP number from the IP network cannot be passed on to the PISN and the gateway is required to translate such a number into a number that is meaningful in the PISN.

In case 3, PNP numbers can be passed between the two networks, provided they are of a sufficiently high level to have meaning on either side of any regional boundary that might occur at the gateway.

8.3.3.2 Interworking and E.164 numbers

E.164 numbers can be passed between a PISN and a IP network, provided they are of a sufficiently high level to have meaning in both networks. An international number is necessary if the gateway is at a national boundary, but in other situations a national number is normally sufficient. In some cases a subscriber number may be sufficient.

8.3.3.3 Other forms of alias in the IP network

Any other form of alias in the IP network cannot be passed to a PISN and is required to be translated into a telephone number having meaning in the PISN.

8.3.3.4 Implicit forms of number

Implicit forms of telephone number can be passed between a PISN and an IP network subject to having meaning in the two networks and subject to the considerations above for PNP and E.164 numbers.

8.3.4 Naming and addressing interworking when SIP used in the IP network

Some of the considerations of 8.3.3 for H.323 apply also to SIP, but support of different types of number in SIP requires further study.

8.4 Supplementary services

8.4.1 H.323 supplementary services

For each of the H.450 supplementary services listed in 7.2.3, table 4 shows where there is potential for interworking with corresponding QSIG supplementary services.

Table 4 – Potential for interworking between H.450 supplementary services and QSIG supplementary services

H.450 supplementary service	QSIG supplementary service
H.450.2 (call transfer)	Call transfer (by consultation) as specified in ECMA-178 and single step call transfer as specified in ECMA-300
H.450.3 (call diversion)	Call diversion supplementary services as specified in ECMA-174.
H.450.4 (call hold)	There is no corresponding QSIG supplementary service. However, the Notification indicator information element specified in ECMA-165 can contain notification descriptors that are able to map to and from signals used in H.450.4 that indicate hold and retrieval from hold.
H.450.5 (call park and call pick-up)	There are no corresponding QSIG supplementary services.
H.450.6 (call waiting)	There is no corresponding QSIG supplementary service. However, the Notification indicator information element specified in ECMA-165 can contain a notification descriptor that is able to map to and from the signal used in H.450.6 that indicates that the call is waiting.
H.450.7 (message waiting indication)	Message waiting indication, as specified in ECMA-242.
H.450.8 (name identification)	Name identification supplementary services, as specified in ECMA-164.
H.450.9 (call completion)	Call completion supplementary services, as specified in ECMA-186.

Where there is potential for interworking of supplementary services, the method of interworking could be a subject for standardization by ECMA. In addition, interworking between the H.323 generic functional protocol (as specified in H.450.1) and the QSIG generic functional protocol (as specified in ECMA-165) could be a subject for standardization by ECMA.

8.4.2 SIP supplementary services

Where consensus has been achieved in IETF and there is potential for interworking of SIP supplementary services with equivalent QSIG supplementary services, the method of interworking could be a subject for standardization by ECMA.

8.5 Security

Security aspects of interworking require further study.

8.6 Quality of service

QoS aspects of interworking require further study.

8.7 Mobility

Mobility aspects of interworking require further study.

8.8 Network management

Network management aspects of interworking require further study.

8.9 Aspects requiring further study or standardization work

Further work on interworking between PISNs and IP networks could focus in more detail on the following aspects, taking into account both ITU-T standards (H.323 family) and IETF standards (SIP etc.) in the IP network:

- Protocol interworking between QSIG and H.323/SIP. For basic call protocol interworking considerations are similar to those for interworking between DSS1 and IP networks, which are being covered by work in ETSI project TIPHON, and it needs to be verified whether the same specification can apply to QSIG. However, for supplementary service interworking QSIG considerations are different from those of DSS1. At the time of writing this Technical Report, ECMA had already produced QSIG-H.323 interworking Standards for the generic functional protocol (ECMA-165 and H.450.1), call transfer (ECMA-178/ECMA-300 and H.450.2) and call diversion (ECMA-174 and H.450.3). There may be requirements for standardizing interworking for other supplementary services or for interworking between QSIG and SIP. In addition, ECMA may wish to standardize SIP supplementary services (using building blocks specified by IETF) and/or influence consensus in IETF on best current practice.
- ECMA-155 may need to be updated to reflect IP addressing.
- Derivation, screening and presentation of identification numbers in support of CLIP, COLP and CLIR.
- Routing considerations. Issues include selection of a suitable gateway, SCN end-to-end versus PISN-IP-PISN, avoiding networks with poor performance.
- Numbering considerations when interworking with SIP.
- Security aspects.
- QoS aspects.
- Mobility aspects.
- Network management aspects.

Work on these aspects may involve changes to standards for IP networks and/or changes to standards for PISNs in order to achieve satisfactory interworking.

9 Interconnection of remote PISNs via an IP network

This clause explores different methods of interconnecting remote PISNs (or two parts of the same PISN) via an IP network.

As described in clause 8, concatenated instances of interworking at a gateway can be used to achieve the interconnection of remote SCNs via an IP network. In particular, this approach can be applied to the interconnection of two PISNs (or two PINXs that are part of the same PISN) via an IP network.

However, concatenation has the limitation that information from one PISN that cannot be mapped onto corresponding information in the protocols used in the IP network will not be available to the peer PISN. This is a particular problem when the two PISNs employ the same network signalling protocol (e.g., QSIG), since any information from one PISN is likely to be of relevance to the other PISN. Loss of this information through interworking with IP network protocols will reduce the level of service to users compared with the level of service that would have existed if the two PISNs were joined directly. To avoid this a means of overlaying PISN services on top of services provided by the IP network needs to be found.

The remainder of this clause assumes that the signalling system used in the two PISNs is QSIG.

9.1 Classification of scenarios for the interconnection of PISNs

Concatenated instances of interworking at a gateway is equivalent to the concatenation concept described in TR/57 (known as the concatenation scenario in ECMA-133).

In TR/57 the alternative to the concatenation concept is the overlay concept (known as the overlay scenario in ECMA-133). With the overlay concept, PISN services are overlaid on top of the services of the network that interconnects the two PISNs. TR/57 identifies two approaches within the overlay concept:

- co-operative approach; and

- transparent approach.

With the co-operative approach (often known as “integrated scenarios”) the network that interconnects the two PISNs is known as an InterConnecting Network (ICN) and has enhanced capabilities (often known as “virtual private network” or VPN capabilities) that enable it to participate in PISN services in an integral manner. The ICN acts as a transit PINX.

With the transparent approach (often known as “overlay scenarios”) the network that interconnects the two PISNs is known as an InterVening Network (IVN). An IVN does not participate in and has no knowledge of PISN services. Instead the IVN provides a means for PISN services to operate between the two PISNs by conveying information transparently, i.e., through a tunnel.

Distinction between the two approaches is not always clear, since with the co-operative approach some aspects of PISN signalling can still be tunnelled. However, the fact that the network that interconnects the two PISNs provides at least some enhanced capabilities for the interconnection of PISNs signifies the co-operative approach. Typically with the co-operative approach the ICN routes based on PISN addresses, whereas with the transparent approach the IVN routes on native addresses rather than PISN addresses.

Both approaches can in principle be applied to the case where the two PISNs are interconnected by an IP network. The co-operative approach requires enhancements to the IP network to allow it to participate in PISN services (e.g., by routing on PISN addresses, participation in PISN supplementary services). Without such enhancements, the concatenation concept applies and certain PISN functionality will be lost.

With the transparent approach, the IP network is simply required to provide appropriate tunnelling mechanisms for PISN information, but does not need to be aware of the content of such information.

Figure 19 shows the generic architecture for scenarios in accordance with the overlay concept, transparent approach (overlay scenarios), as derived from ECMA-133.

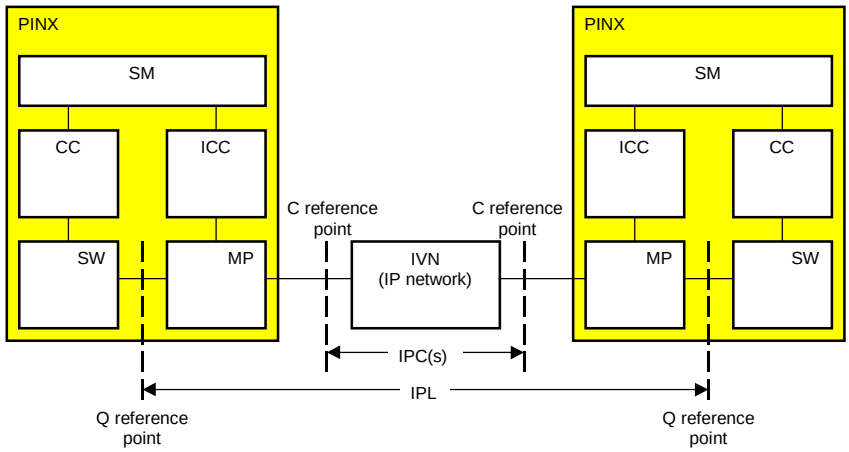


Figure 19 – Generic architecture for overlay scenarios

Conceptually the two PINXs are linked by an Inter-PINX Link (IPL) between the two Q reference points. The IPL comprises a packet mode D_Q-channel for signalling and a number continuous bit rate (normally 64 Kbit/s) U_Q-channels.

The function of the MP functional grouping is to map the D_Q- and U_Q-channels at the Q reference point onto bearer capabilities provided by the IVN as Inter-PINX Connections (IPCs). The ICC functional grouping can become involved if dynamic establishment and clear down of IPCs is involved. The SM functional grouping provides management.

For the D_Q-channel, transport across the IVN needs to be reliable, in terms of low loss and error rate. This is true also for the U_Q-channels when carrying data, but when carrying real-time information the emphasis is more on minimizing delay and delay variation. For real-time information transport over an IP network acting as the IVN, RTP (over UDP) is a suitable transport protocol. For other information, including PISN signalling information, more reliable transport is required. Therefore any overlay scenario has to provide separate transport means for the D_Q-channel and the U_Q-channels (at least for real-time PISN services).

9.2 Solutions for the interconnection of remote PISNs via an IP network

The following solutions have been proposed for the interconnection of remote PISNs via an IP network other than by simple concatenation:

- Solution 1 – QSIG tunnelling over IP network transport layer protocol;
- Solution 2 – QSIG tunnelling over IP network session control protocol;
- Solution 3 – enhanced QSIG ("QSIG+") in the IP network.

9.3 Solution 1 – QSIG tunnelling over IP network transport layer protocol

Solution 1 is in accordance with the overlay concept, transparent approach (i.e., overlay scenario). Both the D_Q-channel and the U_Q-channels are carried directly over an IP network transport layer protocol, but for reasons explained in 9.1 different transport layer protocols need to be employed.

9.3.1 Architecture

With this type of scenario, PISN signalling information (QSIG) is carried over a reliable transport protocol such as TCP or, if added functionality is required, a common signalling transport protocol, as introduced in RFC 2719 ("Framework architecture for signalling transport") from the SIGTRAN group in IETF. A brief introduction to the signalling transport concepts of RFC 2719 is given in annex D.

One possible scenario that could be a candidate for a PISN mapping Standard is as follows:

- D_Q-channel (QSIG signalling) transported over IP using a standard IP transport protocol with functions designed to meet transport requirements for SCN signalling (RFC 2719), such a protocol being referred to below as the SIGTRAN protocol;
- U_Q-channels transported using RTP over UDP (e.g. using G.711 encoding);
- UDP ports for RTP assigned either in a static manner, with semi-permanent mapping to U_Q-channel numbers or using scenario management procedures for more dynamic assignment.

A simple solution based on the principles above would mean that the only bearer capabilities supported are speech and 3,1 kHz audio at 64 Kbit/s. Figure 20 shows the architecture for the SIGTRAN approach.

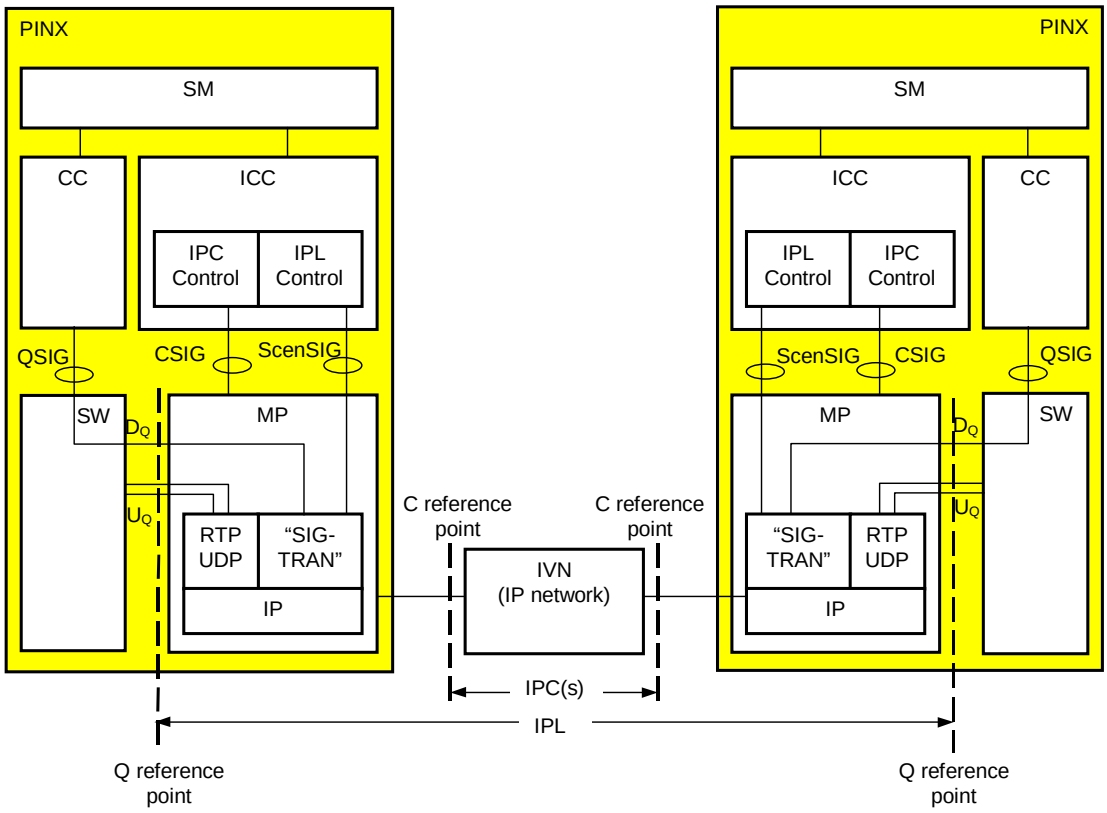


Figure 20 - Architecture for solution 1

The conceptual interconnection scenario shown in the figure is derived from ECMA TR/76. The IPC Control function is used for the control of the packet mode associations at the C-reference point (IP, UDP, TCP, RTP, "SIGTRAN"). The function shown as IPL control in the figure is required for the dynamic assignment of U_Q-channels. In this case a signalling protocol, known here as ScenSIG (scenario signalling), operates between the two peer IPL control functions. As for QSIG, ScenSIG requires the SIGTRAN protocol for transport.

9.3.2 Aspects requiring further study or standardization work

Solution 1 for QSIG tunnelling is particularly suited to static scenarios where an IPL with a fixed number of U_Q-channels exists on a semi-permanent basis. The setting of static pre-conditions then is mandatory. However, since the parameters and their values have local significance only, there is no need for standardization of their structure or format.

Nevertheless, there are some aspects that may be candidates for standardization (see also TR/76), particularly for implementation of dynamic scenarios, but also for semi-permanent scenarios, e.g.:

- Mapping matrix and bearer conditioning. Standards are needed for the mapping of IPL-service channels, D_Q-channels and U_Q-channels onto TCP/UDP/IP ports and for the provision and modification of Bearer Conditioning.
- ScenSIG information flows and the means for their transfer.
- The application of SIGTRAN's Simple Control Transmission Protocol (SCTP) for transport of QSIG and ScenSIG information over the IP-network.
- IPC establishment.
- Quality of Service aspects.
- Security aspects.
- Network management aspects.

9.4 Solution 2 – QSIG tunnelling over IP network session control protocol

9.4.1 Architecture

With this type of scenario an H.323 or SIP session is established between two PINXs to provide an IPL. Within the context of this session, resource control can be used to establish media streams to transport U_Q-channels. QSIG is tunnelled within the session control protocol, i.e., within the application layer. For H.323, a generic tunnelling capability is already being prepared for H.323/H.225.0 version 4. An object identifier identifies the tunnelled protocol, and therefore this mechanism can be used to tunnel QSIG. A similar capability could be introduced to SIP.

The architecture of solution 2 is shown in figure 21. The MP functional entity contains RGT, SC-U, RC-U and MPP functional entities. Signalling information across the Q reference point from CC (via SW) to MP is routed to the SC-U functional entity, which inserts it into the tunnel within the session control protocol. Likewise, tunnelled signalling information received within the session control protocol is extracted by the SC-U functional entity and sent to the CC (via SW).

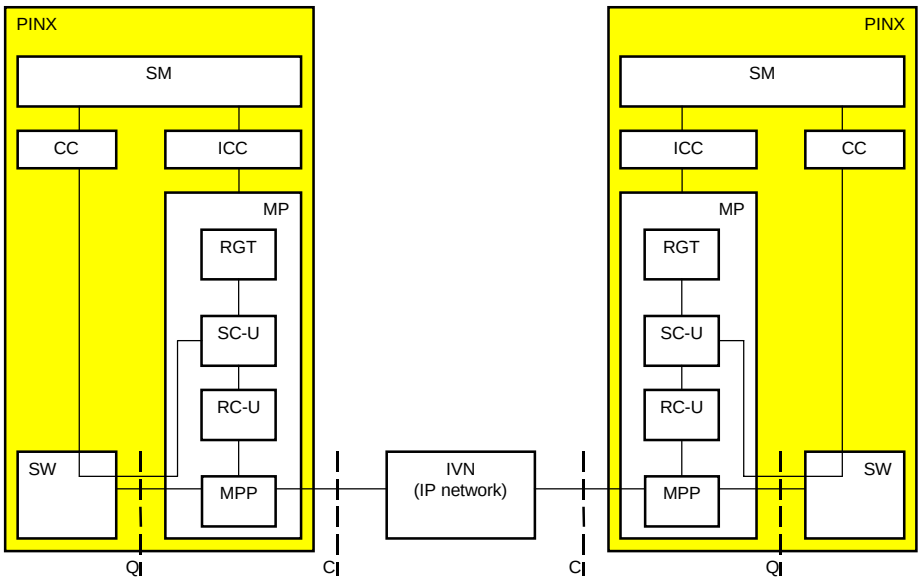


Figure 21 – Architecture for solution 2

The transport of U_Q-channels is the same as for solution 1, i.e., for real-time PISN services transport over RTP over UDP. However, the way of establishing RTP streams is different. With solution 2 the standard resource control protocol (H.245 for H.323, SDP for SIP) is used. With solution 1 there is no such means readily available, and either the U_Q-channels have to be provisioned on a semi-permanent basis (through management procedures at the two PINX, perhaps co-ordinated through network management) or a scenario signalling protocol (ScenSIG) has to be defined. This means that solution 1 is particularly suited to static scenarios where an IPL with a fixed number of U_Q-channels exists on a semi-permanent basis. Solution 2, on the other hand, is particularly suited to dynamic scenarios.

One possibility with solution 2 is to have a 1:1 mapping between PISN calls and IP network sessions, by establishing an IPL (session) each time a PISN call requires to be routed across the IP network to another PINX. Where there is more regular traffic between a given pair of PINXs, an alternative would be to keep the IPL (session) established on a semi-permanent basis and to open and close media streams on a dynamic basis as PISN calls are established and released.

When solution 2 is used with H.323, normally H.323 gatekeepers will be available in the IP network and can be exploited in various ways, e.g.:

- resolution of telephone number to IP address;
- determining that a QSIG gateway will be encountered at the IP network egress (included in H.225.0 version 4 as part of the generic tunnelling enhancement);
- bandwidth management and QoS services.

Similarly when using solution 2 with SIP, corresponding entities might be available for exploitation. Because solution 1 is independent of H.323 or SIP, solution 1 cannot depend on gatekeepers or equivalent for such functions, although solution 1 may be able to use gatekeepers or equivalent if available.

9.4.2 Aspects requiring further study or standardization work

Using the generic tunnelling mechanism in H.323/H.225.0 version 4, particular scenarios identified as being useful could be standardized. Standards should focus on the following aspects:

- Mapping matrix and bearer conditioning.
- ScenSIG information flows (if applicable) and the means for their transfer.
- Use of the H.323/H.225.0 tunnelling mechanism for transporting QSIG messages over the IP network.
- IPC establishment.
- Use of both public and private intervening networks.
- QoS considerations.
- Security considerations.
- Network management aspects.

Similar scenarios could be specified for tunnelling over SIP using a generic tunnelling mechanism in SIP (e.g., QSIG MIME type, currently being specified by IETF).

9.5 Solution 3 – enhanced QSIG in the IP network

9.5.1 Architecture

Solution 3 uses an enhanced QSIG ("QSIG+") as the session control protocol in the IP network in place of existing session control protocols (H.225.0 or SIP). Whereas QSIG includes negotiation of a circuit mode bearer (e.g., a B-channel), QSIG+ needs to negotiate resources (e.g., port numbers) for running a resource control protocol (e.g., H.245, SDP). In other respects QSIG+ is identical to QSIG, and therefore there is no requirement for tunnelling QSIG information.

This solution can be regarded as an integrated scenario (overlay concept, co-operative approach), since any IP network entities that are involved in session control (e.g., gatekeepers, SIP proxies and redirects) are required to support PISN functionality by supporting QSIG+ rather than H.225.0 or SIP.

In the special case where no such IP network entities are involved, this can be regarded as an overlay scenario, with QSIG+ simply tunnelled over an IP network transport layer protocol. It differs from solution 1 in that QSIG+ is tunnelled rather than QSIG.

Solution 3 is analogous to the BICC in public networks.

9.5.2 Aspects requiring further study or standardization work

This scenario requires the specification of the QSIG+ protocol in the form of deviations from QSIG. Other aspects that would require study include security, QoS and network management. Naming and addressing is unlikely to be a problem.

10 Connection of telephones to a PINX via an IP network

Figure 1 in 5.1 shows two ways in which (non-IP) telephones can be connected to a PINX via an IP network:

- via gateway type 1 (on the telephone side) and gateway type 2 (on the PINX side); or
- via gateway type 4 (on the telephone side) and gateway type 5 (on the PINX side).

NOTE
If certain security requirements are met, a public IP network (Internet) can be used for the connection of IP and non-IP telephones to a PINX, which can be regarded as another example of VPN capability. The requirements for such VPNs are not explicitly considered in this Technical Report, but could be the subject of further study.

10.1 Architecture

In the case of gateway type 2, an "end-to-end" signalling protocol (H.323 or SIP) is used in the IP network, and either the telephone (in the case of an IP telephone) or the telephone in combination with a gateway type 1 has to terminate this signalling protocol. Gateway type 2 is discussed in clause 8.

NOTE
Although calls between terminals connected to the same IP network can be routed directly over the IP network, there may be reasons to route at least the signalling part of such calls via a gateway, a PISN and a second gateway. This will be the case in configurations where the users of these terminals are to be regarded as users of the PISN and thus should have access to services of the PISN.

Figure 22 shows the architecture for the case where gateways type 1 and type 2 are employed and the telephone uses stimulus signalling. The stimulus signalling passes through the MPP functional entity to the relevant control plane functional entity in the gateway type 1. Hence no IW, HLS and LLS functional entities are shown in gateway type 1.

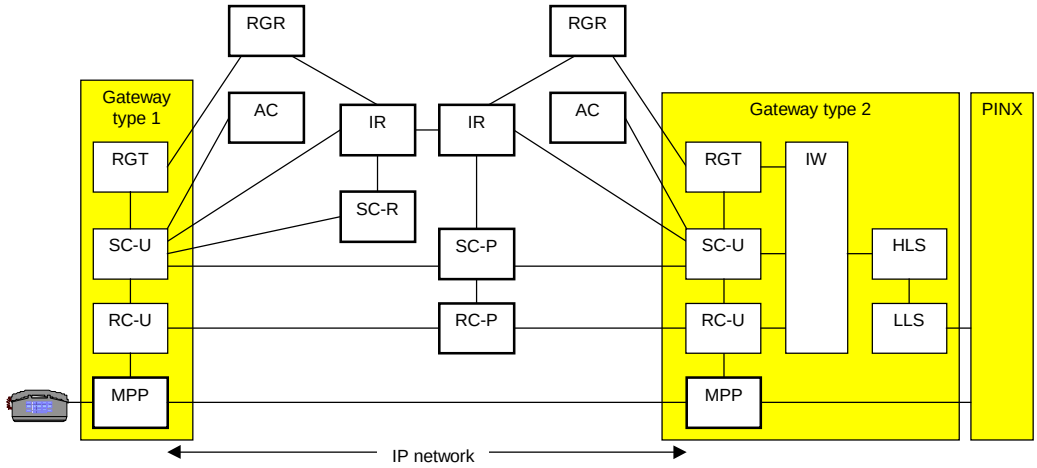


Figure 22 – Connection of telephone to PINX using gateways type 1 and 2

Alternatively the control plane part of the gateway type 1 can be collocated with the gateway type 2, leaving just the MPP functional entity on the telephone side of an IP network, as shown in figure 23 (RGR, AC and IR functional entities not shown). Interface J is exposed. The gateway type 1 becomes a gateway type 4 and the gateway type 2 becomes a gateway type 5. Within the gateway type 5, internal communication takes place between the SC-U functional entity on the user side and the SC-U functional entity on the PINX side. Similarly internal communication takes place between the two RC-U functional entities.

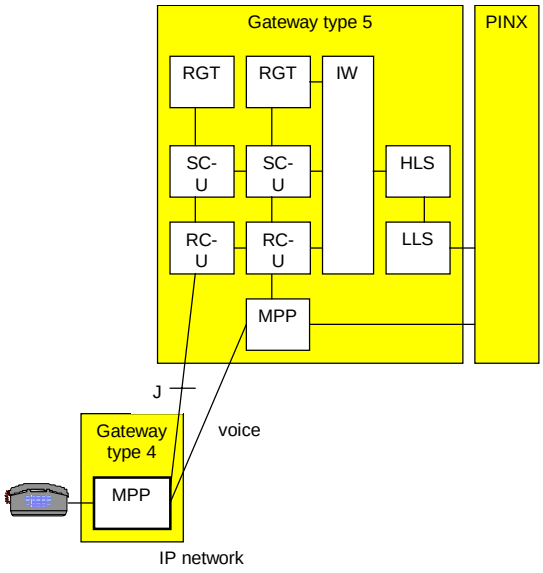


Figure 23 – Connection of telephone to PINX - using gateways type 4 and 5

Gateway type 4 can be omitted if the MPP functional entity is inside the telephone.

NOTE
In contrast to the situation where gateways type 1 and type 2 are employed, if gateways type 4 and type 5 are employed, signalling must always be routed via the PISN, even for calls between two terminals connected to the same IP network.

Different signalling protocols can be applied at interface J, e.g., H.248, MGCP (a predecessor of H.248).

For a call between two telephones attached via gateways type 4, routing of both signalling and voice is via gateways type 5, as shown in figure 24.

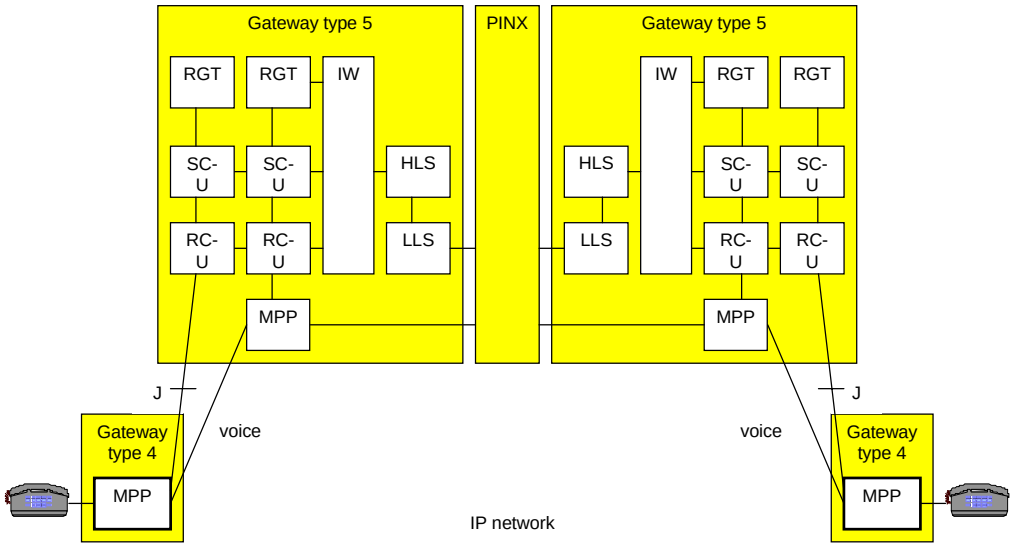


Figure 24 – Connection of two telephones via PINX using gateways type 4 and 5

Advantages might be gained in terms of QoS and use of gateway resources if voice were to be routed directly through the IP network between the gateways type 4, by-passing the PINX, as shown in figure 25.

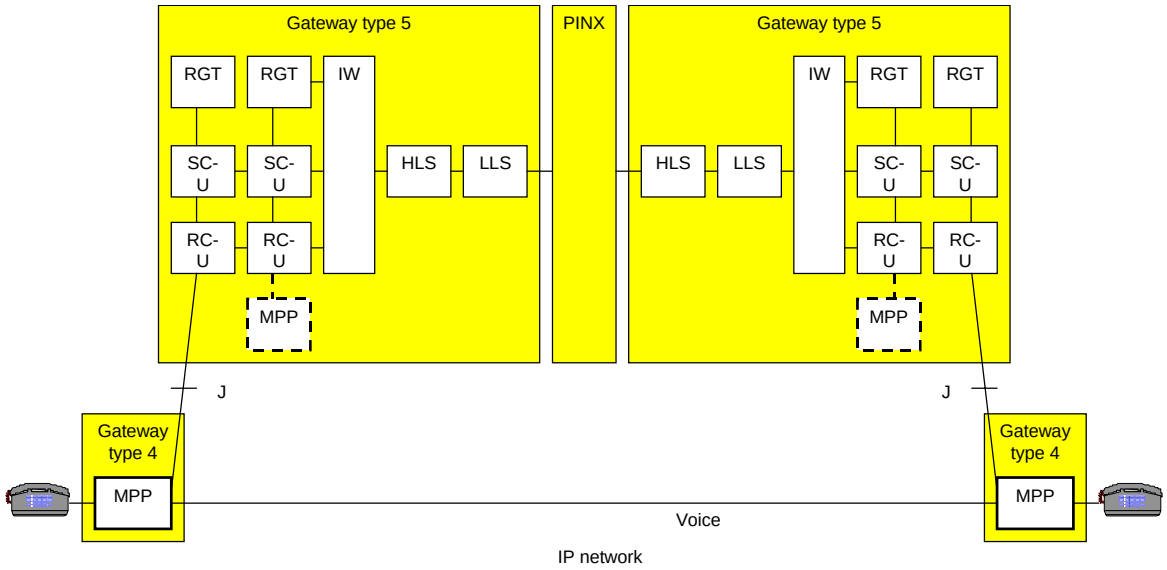


Figure 25 – Connection of two telephones via PINX using gateways type 4 and 5 – voice routed directly through IP network

Here the combination of the PINX and the two gateways type 5 acts as a signalling proxy. The MPP functional entities within the two gateways type 5 become redundant. This arrangement has to be determined dynamically on a call-by-call basis, since it applies only if the source and destination gateways type 4 are able to communicate directly via the IP network, taking into account issues such as QoS, addressing and security.

10.2 Aspect requiring standardization work

Further work on connecting telephones to a PINX via an IP network could focus on the following aspects:

- Requirements for VPNs for connecting telephones to PINXs via public IP networks, including aspects such as tunnelling and security.
- Are the candidate protocols for the J interface (H.248, MGCP) sufficient to provide a PBX-like service to remote users behind an IP network, or are additional protocol capabilities needed?

11 Summary

This Technical Report has examined the following:

- general principles of multimedia communication over an IP network;
- standards in support of multimedia communication over an IP network;
- interworking between PISNs and IP networks via a gateway;
- the interconnection of remote PISNs via an IP network (three possible solutions); and
- the connection of telephones to a PINX via an IP network.

For interworking between PISNs and IP networks via a gateway, for each of the three solutions for the interconnection of remote PISNs via an IP network, and for the connection of telephones to a PINX via an IP network, topics for further study or standardization are listed in the clauses concerned. The following is a summary of the topics identified:

- protocol interworking between QSIG and H.323 (basic call, additional supplementary services);
- SIP supplementary services (see 8.4.2);
- protocol interworking between QSIG and SIP (basic call and supplementary services);
- naming, addressing and routing aspects (particularly relating to PISN-SIP interworking, screening of numbers and restriction of numbers);

- mobility aspects of interworking;
- solution 1 for PISN interconnection;
- standardization of scenarios for solution 2 for PISN interconnection using the tunnelling mechanism in H.323/H.225.0 version 4;
- solution 2 for PISN interconnection using QSIG tunnelling in SIP;
- solution 3 for PISN interconnection;
- QoS aspects of interworking, tunnelling, etc.;
- security aspects of interworking, tunnelling, etc.;
- network management aspects of interworking, tunnelling, etc.;
- VPN aspects, e.g., for connection of telephones to PINXs via public IP networks.

In addition, the following candidates for further work emerged during work on this Technical Report:

- fax support;
- accounting and billing aspects;
- inter-domain working;
- profiling of standards for IP networks for CN use;
- use of unlicensed spectrum for terminal mobility in CNs;
- testing (e.g., production of interoperability test specifications, promotion of interoperability testing events);
- interconnection of remote IP networks via a PISN.

Annex A

Overview and status of H.323

A.1 Operation

ITU-T recommendation H.323 (Packet-based Multimedia Communications Systems) is an umbrella recommendation that specifies protocols and procedures for multimedia communications over packet networks, including IP networks. H.323 itself refers to other ITU-T recommendations, e.g., H.225.0 for call signalling and media stream packetization and H.245 for control of multimedia communication.

NOTE
The Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP) defined in H.225.0 are compatible with the corresponding IETF protocols defined in RFC 1889.

Communications in H.323 involve *endpoints* and possibly *gatekeeper(s)*. An *endpoint* can be a *terminal*, a *gateway* or a *multipoint control unit (MCU).*

Gateways allow interworking between SCNs and IP networks by performing protocol translations, in particular packetization/de-packetization and codec translation (the two networks will generally not use the same encoding schemes), but also signalling translation, since gateways will have to perform call set up/release and call control on both the IP side and the SCN side.

The *gatekeeper* acts as a "manager" for the terminals and gateway(s) within its "zone". The gatekeeper services are discussed below.

Basically, "signalling" in the context of H.323 comprises 3 functions : *RAS signalling function*, *call signalling function*, and *call control function*.

- the *RAS signalling function*, based on the *RAS signalling channel*, uses H.225.0 messages to perform registration, admission, bandwidth change, status, and disengagement procedures between endpoints (i.e. terminals or gateways) and gatekeepers. The RAS signalling channel runs on top of UDP.
- the *call signalling function*, based on the *call signalling channel*, uses H.225.0 messages and procedures to establish the call. The call signalling channel is independent of the RAS channel and the H.245 call control channel (see below). The call signalling channel usually runs on top of TCP, but new versions of H.323 also allow UDP as an optional transport protocol for call signalling. In certain cases the call signalling channel has to stay open during all the H.323 communication, e.g. if the H.245 protocol is tunnelled (see below), if interworking with an SCN occurs, or if supplementary services may be invoked. Otherwise call signalling may be terminated (without clearing the call) as soon as the call control channel is established.
- the *call control function*, based on the *call contro*l *channel,* uses H.245 messages to carry end-to-end control messages governing operation of the H.323 entity, including capabilities exchange, opening and closing of logical channels (for media), mode preference requests and flow control messages. The call control channel also runs on top of TCP, if established separately, and has to stay open for the entire H.323 communication. New versions of H.323 allow the call control protocol (H.245) to be tunnelled via H.225.0 call signalling messages as an alternative to opening a separate call control channel. If this option is used the call signalling channel has to stay open until the call is released (which is not necessary if the original method of separate channels is used). As a further alternative, the optional *fast start* procedure allows encapsulation within H.225.0 call establishment messages of call control information that is essential for the immediate opening of logical channels, thus reducing the time needed to start communication ("one shot signalling").

In most cases, the gatekeeper will be much involved in the H.323 signalling. In particular, the gatekeeper will (or may) perform the following actions:

- *address translation* : from LAN aliases to IP addresses, e.g., by using a table updated by registration messages from terminals and gateways;
- *call control signalling*: the gatekeeper may choose to complete the call signalling with the endpoints and may process the call signalling itself (*gatekeeper-routed call signalling*). In that case, the gatekeeper will have to handle all the H.225.0 call control signals between the communicating terminals. Alternatively, the gatekeeper may direct the endpoints to establish the call signalling channel directly between each other (*direct endpoint call signalling*), thus avoiding the handling of H.225.0 call control signals;
- *call authorization:* through the use of H.225.0 messages, the gatekeeper may reject calls from a terminal due to authorization failure. The reasons for rejection are outside the scope of H.323, but one can imagine: restricted access to/from particular terminals, restricted access during certain periods of time, etc.;
- *bandwidth management:* the idea is to control the number of H.323 terminals with permission for simultaneous access to the network. Through the use of H.225.0 messages, the gatekeeper may reject calls from a terminal due to bandwidth limitations, but the criteria for determining if bandwidth is available are outside the scope of H.323;
- *call management:* the gatekeeper may maintain a list of ongoing H.323 calls, in order for example to indicate that a called terminal is busy, and to provide information for the bandwidth management function.

The *RAS signalling function* in H.323 essentially covers 4 processes:

- *gatekeeper discovery:* this is the process an endpoint uses to determine which gatekeeper to register with. This may be done *manually* or *automatically*;
- *endpoint registration:* this is the process by which an endpoint joins a zone, and informs the gatekeeper of its transport address and alias address. If gatekeepers are installed, all endpoints have to register with an appropriate gatekeeper (as manually configured or identified through a discovery process) before any calls are attempted.
- *endpoint location:* an endpoint or gatekeeper which has an alias for a called endpoint also needs its "contact information", i.e., at least, a call signalling channel address (IP address plus port number), in order to reach that called endpoint. To achieve this the calling endpoint (or gatekeeper) sends a "location request" message to a specific gatekeeper RAS channel transport address, or "multicasts" it to a well-known DMA (Discovery Multicast Address). The gatekeeper that has the necessary contact information should then respond with a "location message" containing the contact information of the endpoint or the endpoint's gatekeeper.
- *admission, bandwidth change, status, disengage:* these are call related procedures; an endpoint sends an admission request to the gatekeeper it has registered with whenever it wants to initiate an outgoing or accept an incoming call; bandwidth change requests allow a gatekeeper to modify the bandwidth allocated to a call dynamically during the call; status messages keep endpoints and gatekeepers synchronised on call status; and disengage messages may be exchanged when a call ends.

The *call signalling function* in H.323 is based on H.225.0 procedures. Recommendation H.225.0 specifies the Q.931-derived messages that have to be used for call signalling in H.323. Basically, an initial *admission message* exchange takes place between the calling endpoint and the gatekeeper using the gatekeeper's RAS channel transport address. Within this message exchange, the gatekeeper instructs the calling endpoint whether to send the call signalling directly to the other endpoint, or to route it through the gatekeeper. The call signalling messages are then sent to either the endpoint's call signalling transport address *("direct endpoint call signalling")* or the gatekeeper's call signalling transport address *("gatekeeper routed call signalling").* Both methods use the same kinds of connections for the same purpose, and the same messages. On the called side, a similar admission message exchange takes place when a call arrives at the called endpoint, and may lead to the call signalling channel being redirected to pass through the called endpoint's gatekeeper if gatekeeper routed call signalling applies also on the called side and the gatekeeper is not already on the call signalling path.

Thus, admission messages are first exchanged on RAS channels with the gatekeeper, followed by an exchange of call signalling messages on a call signalling channel. This is then followed by the establishment of the H.245 control channel, unless fast start and/or H.245 tunnelling is used. The actions of the gatekeeper in response to the admission messages determine which *call model* is used; this is not under the control of the endpoint, although the endpoint can specify a preference.

The main procedures that H.323 endpoints have to support in the context of the H.245 call control are:

- *capabilities exchange:* this procedure provides for separate *receive* and *transmit capabilities* of the terminal, as well as a method by which the terminal may describe its ability to operate in various combinations of modes simultaneously. *Receive capabilities* describe the terminal's ability to receive and process incoming information streams (e.g., G.723.1 audio, H.261 video, etc.), while transmit capabilities describe the terminal's ability to transmit audio and/or information streams. Transmit capabilities serve to offer receivers a choice of possible modes of operation, so that the receiver may request the mode which it prefers to receive. Furthermore, a terminal may add capabilities during a conference, remove capabilities, or re-issue its capability set at any time, according to specific H.245 procedures;
- *logical channel signalling:* each *logical channel* carries user plane information relating to a particular medium from a transmitter to one or more receivers, and is identified by a logical channel number that is unique for each direction of transmission. Logical channels may be unidirectional or bidirectional. They have to be opened and closed with specific H.245 messages and procedures. In particular, when opening a logical channel, a message fully describes the *content* of the logical channel, including medium type, algorithm in use, any options, and other information needed for the receiver to interpret the content of the logical channel. Logical channels may be opened and closed during the lifetime of a call as needed, thus allowing endpoints to modify their communication streams dynamically. The optional fast start procedure is also based on logical channel signalling embedded in H.225.0 call establishment messages.

In contrast to call signalling and call control, which may be routed via gatekeepers, the logical channels used for media or data are always routed directly between the endpoints. Real time media (audio, video) are transported using RTP over UDP.

H.323 version 2 (1998) adds further capabilities to those described above, in particular:

- *security* : H.323 now refers to H.235 for security;
- *use of ATM for media*: ATM virtual channels may be used for the transport of media instead of UDP and IP;
- *supplementary services* : H.323 refers to the H.450 series of recommendations for additional services, in particular H.450.1 defines the signalling protocol between H.323 endpoints for the control of those services, H.450.2 defines Call Transfer, and H.450.3 defines Call Diversion, etc..

A.2 Standardization status

A.2.1 ITU

H.323 Version 1 was released in 1996. Version 2 was issued in February 1998, and Version 3 in 1999. Version 4 is currently under development within ITU-T Study Group 16.

Basically, the core of H.323 remains unchanged in the successive versions, but a lot of features or new procedures are added. Due to these successive versions, backward compatibility becomes an issue, since H.323 compliance mandates that each endpoint support all aspects of the signalling protocols that were mandatory in version 1, even when improved procedures exist (e.g. "Fast Start").

Below are descriptions of some complementary standardization efforts in other bodies or fora, aimed at completing or broadening the specification of H.323.

A.2.2 ETSI TIPHON

In May 1997, ETSI established Project TIPHON – "Telecommunications and Internet Protocol Harmonisation Over Networks". TIPHON addresses architectures, protocols and test specifications for systems that support voice communication over IP based networks and switched circuit networks (SCN) in an interoperable way. Starting points for the development of global standards are the models and protocols as they are defined in the H.323 framework. The different interoperability scenarios were tackled

sequentially: specifications for calls from SCN to IP network and from IP network to SCN have been produced; work on the SCN – IP – SCN scenario is progressing well. Scenarios are no longer considered in isolation, i.e. the current and future work applies to all scenarios. Instead the concept of "releases" with incremental sets of capabilities has been introduced. More than 50 companies support the TIPHON Project. The project's web site is at http://www.etsi.org/TIPHON/

A.2.3 IMTC

The International Multimedia Teleconferencing Consortium, Inc. (IMTC) has a mission is to promote, encourage, and facilitate the development and implementation of interoperable multimedia teleconferencing solutions based on open international standards. It has done much to promote H.323 as a standard, including the hosting of interoperability events. Its web site is at http://www.imtc.org/.

Annex B

Overview and status of SIP

The purpose of this annex is to give some background information on the Session Initiation Protocol (SIP), which can be regarded as the key protocol in the IETF approach to IP telephony.

B.1 Introduction

The Session Initiation Protocol (SIP) is an application-layer control (signalling) protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, IP telephony calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these.

B.2 Architecture

The main components in the SIP architecture are *user agents* and *network servers*. The user agent represents the user and is composed of a user agent client (UAC) for initiating SIP requests and a user agent server (UAS) for receiving and responding to SIP requests on behalf of the user.

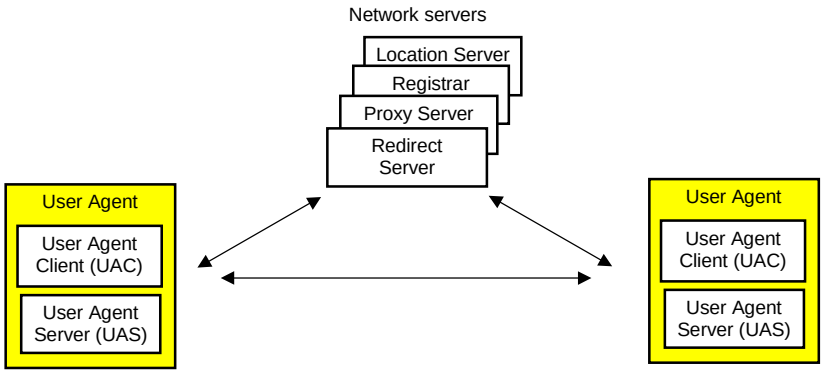


Figure 26 – SIP user agents and network servers

In addition to user agents, in the SIP model there are various types of network servers, including redirect servers, proxy servers, registrars and location servers. Different network server types may be implemented within the same physical component. A *registrar* enables user agents to register their location in the network. A registrar may offer location services, i.e. it may at the same time act as a location server. A *location server* provides information to SIP redirect or proxy servers about the possible location(s) of a called user. Setting up a session (a call) between user agents normally involves one or more redirect and/or proxy servers before the final destination is found. A *redirect server* is a network server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client. A *proxy server*, just like a redirect server, accepts SIP requests. The difference is that a proxy can forward the request, possibly after translation, to other servers. This implies that the proxy server acts as both a server and a client (on behalf of another client, e.g. UAC). Proxy servers have the possibility to forward SIP requests to multiple other servers in parallel. In addition to routing, proxy and redirect servers may also play a role in the provision of enhanced services (e.g. call diversion) to end-users.

B.3 Operation

Endpoints are identified by SIP addresses, of format *user@home*, in which the "user" is a user name or a telephone number and the "host" is either a domain name or a numeric network address. When establishing a call, the calling endpoint first determines an appropriate server, e.g. by local configuration or by consulting a

DNS server. Then a SIP request (invitation) is sent to that server. Such a SIP request may be redirected or proxied before it reaches a server that knows the actual location of the destination endpoint.

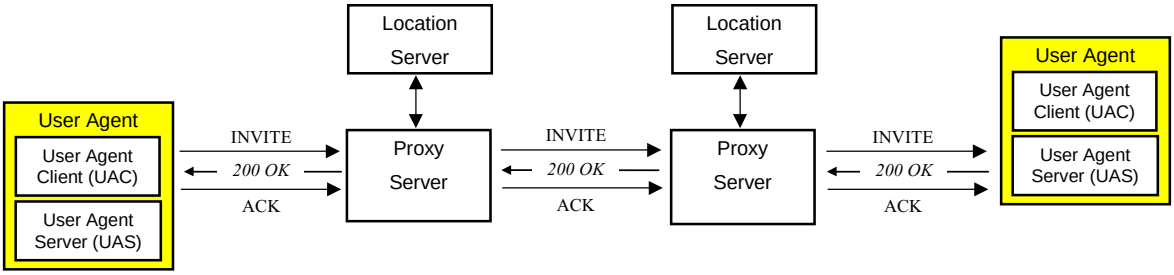


Figure 27 – Example of SIP session establishment via proxy servers

SIP invitations for establishing sessions carry session descriptions, e.g. in SDP-format (RFC 2327), which allow participants to agree on a set of compatible media types.

SIP is a text-based protocol and much of the message syntax and header fields are identical to the Hypertext Transport Protocol (HTTP 1.1). A SIP message is either a request from a client to a server, or a response from a server to a client. Each message contains a start-line, one or more header fields and an optional message-body. The start-line of a SIP message enables a client to invoke a *method* on the server. RFC 2543 defines the following methods:

- REGISTER conveys user location information to a SIP server
- INVITE invites a user to a conference (or a simple phone call)
- BYE terminates a connection between two users
- OPTIONS solicits information about user capabilities (but does not set up a call)
- CANCEL terminates a search for a user
- ACK confirms that the client has received a final response (200 OK) to an INVITE request

SIP supports user mobility by enabling users to register their current location and by proxying and redirecting requests via SIP network servers to a mobile user's current location. The grade of mobility that can be provided depends on the location and routing information available to the network servers and is outside the scope of the basic SIP specification.

SIP is not tied to any particular conference control protocol.

SIP is designed to be independent of the lower-layer transport protocol (e.g. it can run both on TCP and UDP) and can be extended with additional capabilities.

The basic SIP concept of methods and headers enables a number of enhanced call services, including call forwarding services, calling and called number delivery, call hold, call waiting and personal mobility (i.e. the ability to reach a called party under a single, location-independent address even when the user changes terminals).

B.4 Extensions to SIP and related work

A number of extensions and enhancements to basic SIP are being defined, including:

- Definition of a new method, the INFO method, to provide a generic mechanism for transporting mid-call session control information.
- Extensions to SIP to allow users to describe their communications capabilities and characteristics and to allow a caller to express preferences about request handling in servers.
- Extensions (i.e. new methods and/or headers) that will enable call transfer services and multi-party calls.
- The use of DHCP (Dynamic Host Configuration Protocol) as one of the many possibilities for a SIP client to obtain the address of a SIP server.

- Application of SIP to inter-MGC communication. This work will detail and/or reference the methods, standards and tools necessary to enable MGCs to interoperate via the SIP protocol in a standard way. A major new function here will be the encapsulation of SCN signalling (e.g. ISUP or QSIG), based on the use of MIME multi-part payloads in the body of the message (e.g., SIP INVITE or SIP INFO).
- Enhanced security mechanisms.

In addition, within the IETF, there is work in progress, not specifically for SIP, but that can complement the approach chosen by SIP in the provision of enhanced call services. This includes:

- Common Gateway Interface for SIP (SIP CGI). This work intends to provide a means by which new (call) services can rapidly be created and deployed. The concept is based on the Common Gateway Interface (CGI) as used in the World Wide Web for programming web services. The proposed SIP CGI interface can be used for providing SIP services on a SIP server.
- Call Processing Language (CPL). Whereas SIP CGI is regarded to be a tool for service creation by trusted users, the Call Processing Language is meant for use by e.g. the customer (end-user). CPL should provide the means in which network servers respond to call signalling events by triggering user-created programs written in a simple, static, non-expressively-complete language.

B.5 Standardization status

SIP has been developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, and is now a Proposed Standard RFC, RFC 2543. The MMUSIC working group has also produced related protocols like the Session Description Protocol (SDP, RFC 2327) and the Real-Time Streaming Protocol (RTSP, RFC 2326), which enables an endpoint to have VCR-like controls over a media server, e.g. for playing and recording voice-band messages.

During 1999 the responsibility for SIP and extensions to SIP was taken over by the new IETF SIP working group. The SIP working group is chartered to continue the development of SIP including the development of a number of the proposed extensions to basic SIP (see B.4).

Work on the Call Processing Language (CPL) is being performed by the IETF IPTEL (IP telephony) working group. A framework for CPL is near to completion, work on the CPL language itself is still in progress.

Clause 2 contains references to relevant and officially published RFCs. At the moment of publication of this Technical Report, all other SIP-related work mentioned in this annex is available only in draft form.

Annex C

Overview of H.248 / MEGACO protocol

H.248 (also known as the MEGACO protocol) operates between a MG unit (comprising the MPP functional entity of the generic architecture of this document) and an MGC unit (comprising various control plane functional entities).

The MG is viewed by the MGC as containing a number of terminations, consisting of:

- fixed terminations (e.g., physical circuits, timeslots, etc.); and
- ephemeral terminations (e.g., RTP ports).

Commands from the MGC can create and delete terminations and set properties of terminations, e.g., encoding algorithm, packet size, remote transport address, etc..

Commands from the MGC can establish and remove “contexts” or connections between terminations. For example, if a two-way context is established between an SCN channel and an RTP port, the MG is required to code and packetize data from the SCN termination and transmit the packets onto the IP network with the port number as source. Similarly data is to be extracted from packets received from the IP network with the port number concerned, decoded and transmitted to the SCN channel.

Commands from the MGC can request the MG to send signals (e.g., tones) to terminations.

Events detected by the MG at terminations (e.g., digits) can be reported to the MGC. Properties of the termination, as set by command from the MG, determine the events to be reported. Digits can be accumulated and reported only when a sequence matching a pre-defined digit map has been received.

Commands are provided for the MGC to audit the capabilities of the MG, properties of terminations, statistics, etc.. The MG can report changes of status of terminations (e.g., in-service, out-of-service) to the MGC.

Extensions to the protocol are achieved by packages. A package extends either the basic protocol or existing packages by defining additional properties, signals, events or statistics. Packages can be registered with IANA and can be published as RFCs, new annexes to H.248, etc.. Some basic packages are already included as annexes to H.248 to cover capabilities such as tone generation, tone detection, analogue line supervision (on-hook, off-hook and flash), continuity testing and basic network types.

Two encoding methods are specified for the protocol: text and binary. An implementation need support only one encoding method, although it is recommended that an MGC support both. This could lead to lack of interoperability. Market forces may eliminate one of the options in due course.

A number of proprietary-based protocols fulfilling functions similar to some of those of H.248 have appeared on the market, including MGCP (Media Gateway Control Protocol). The expectation of those involved in standardizing H.248 is that eventually it will replace proprietary solutions.

Annex D

Architecture for Signalling Transport over IP-networks (SIGTRAN)

An architecture for the transport of SCN-signalling over IP-networks has been defined by the SIGTRAN Working Group of the Transport Area in the IETF. This architecture takes into account the functional and performance requirements of the SCN signalling. A framework for this architecture is defined in RFC 2719 ("framework architecture for signalling transport"). This framework introduces a common transport mechanism for SCN signalling and identifies interfaces where this signalling transport may apply (see figure 28).

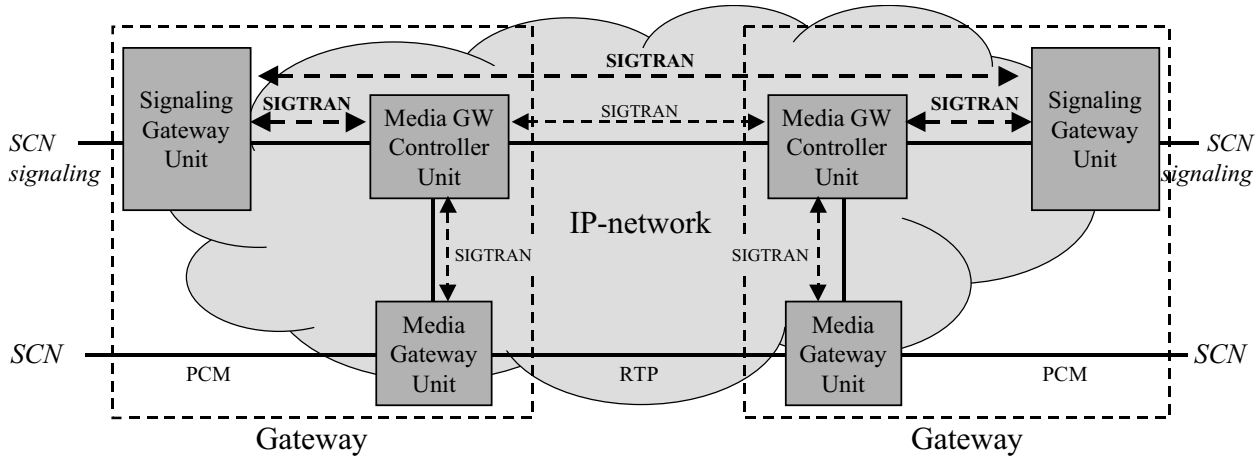


Figure 28 – Interfaces where SIGTRAN can be applied

The signalling transport (SIGTRAN) provides for **transparent** transport of message-based signalling protocols over IP-networks, and can be used between a Signalling Gateway unit and a Media Gateway Controller unit and between two peer Signalling Gateway units (i.e. a tunnel for SCN-signalling over the IP-network). Optionally, SIGTRAN can also be used between two Media Gateway Controller units and between a Media Gateway Controller unit and a Media Gateway unit.

NOTE
SIGTRAN can be used for tunnelling of SCN signalling over an IP-network, but its primary use is assumed to be for inter-working scenarios where the SCN signalling is to be transported from the point of the interface between SCN and IP-network (i.e. the Signalling Gateway unit) and the point of call processing in the IP-network (i.e. the Media Gateway Controller unit). This type of signalling transport is referred to as "backhaul". Here, the lower layers of the SCN protocol are terminated in the Signalling Gateway unit and only the higher layer is transported to the Media Gateway Controller unit for call processing.

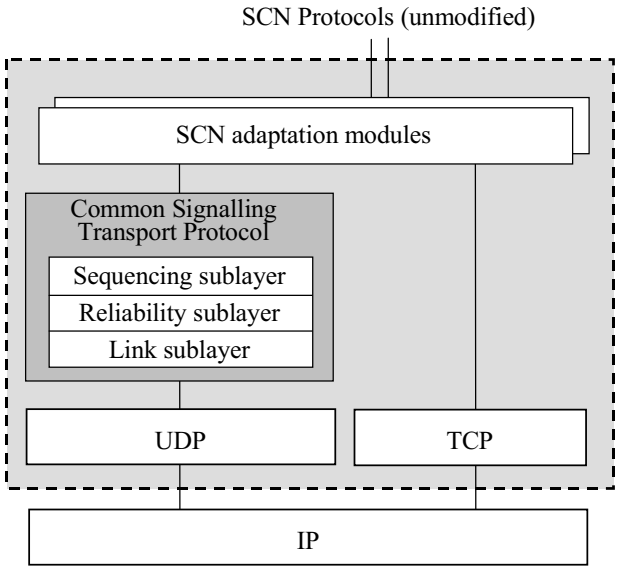
The common signalling transport mechanism is independent of any SCN protocol and includes the definition of encapsulation methods, end-to-end protocol mechanisms and the use of IP capabilities to support the functional and performance requirements for signalling. Translation functions take place only at the endpoints of the signalling transport.

The requirements for the transport of SCN signalling over IP-networks include:

- Must support transport of a variety of SCN protocol types, including ISUP, MTP3, SCCP, MAP, INAP, DSS1, PSS1 (QSIG).
- Provide means to identify the type of protocol being transported.
- Provide SCN-relevant functionality (e.g. flow control, error detection, …), e.g. for transport of Q.931, relevant functionality provided by Q.921 shall be provided.
- Multiplexing of several higher layer SCN sessions on one underlying signaling transport session.

- Support of suitable security schemes, e.g. signalling transport through firewalls should be possible.
- Congestion avoidance on the Internet.
- Performance requirements, e.g. Q.931 message delay.
- Security requirements (authentication, integrity, confidentiality, ..).

The protocol architecture for the signalling transport over IP-networks according to SIGTRAN is shown in figure 29:



The SIGTRAN protocol architecture is composed of the standard TCP/UDP layer, a Common Signalling Transport Protocol and a collection of SCN adaptation modules.

The Common Signalling Transport Protocol supports a set of reliable transport functions for signalling transport. In some scenarios, these functions could alternatively be provided by TCP, in which case the Common Signalling Transport Protocol layer would be null.

The SCN adaptation modules provide functions that are expected by a particular SCN signalling protocol, e.g. the mapping of SCN primitives to the primitives of the Common Signalling Transport Protocol.

Figure 29 – SIGTRAN protocol architecture

The SIGTRAN Common Signalling Transport Protocol is a common and reliable protocol, which is used to transport SCN signalling protocols over IP-networks. The protocol must support functions comparable to TCP (e.g. persistent associations, reliable transport and sequence preservation). Additionally, it should also provide functions that go beyond TCP, like a tighter timer control and a greater fan-out for example. The SIGTRAN Common Signalling Transport Protocol is to be designed for integration with H.323 as well as SIP, enabling SCN signalling transport in such systems. Within the IETF a protocol is being prepared to fulfil the role of SIGTRAN's generic concept of the Common Signalling Transport Protocol. This protocol under development is known as the "Simple Control Transport Protocol (SCTP).

Security aspects in the SIGTRAN model

Especially when SCN signalling is to be transported over insecure IP-networks (like the public Internet), security measures are required to ensure that the information is transported in a confidential way between trusted entities, and without the chance of modification by illegal parties. The SIGTRAN architecture itself does not include the definition of new security mechanisms, as the use of currently available mechanisms is assumed to be sufficient to provide the necessary security. It is recommended that IPSec or some equivalent method be used. IPSec (specified in RFC 2401) provides security services at the IP layer for data integrity and data confidentiality.

Free printed copies can be ordered from:
ECMA
114 Rue du Rhône
CH-1204 Geneva
Switzerland

Fax: +41 22 849.60.01
Email: documents@ecma.ch

Files of this Technical Report can be freely downloaded from the ECMA web site (www.ecma.ch). This site gives full information on ECMA, ECMA activities, ECMA Standards and Technical Reports.

ECMA
114 Rue du Rhône
CH-1204 Geneva
Switzerland

See inside cover page for obtaining further soft or hard copies.