ETSI TR 101 308 V1.1.1 (2001-12)

Technical Report

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; SIP and H.323 Interworking

Reference

DTR/TIPHON-01005

Keywords

H.323, Internet, interworking, network, protocol, SIP

ETSI

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

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

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

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

Introduction

The ETSI Project TIPHON is concerned with the interaction between IP based communication devices and circuit switched networks. The project focuses on voice communication and related multimedia aspects as required for interoperability between IP based networks and other types of networks.

The project has predicated much of its early work on the use of the ITU-T Recommendation H.323 [1] specification since this was the most mature and relevant base specification at the time. The IETF's Internet Multimedia Conferencing Architecture has continued to develop and has started to spawn technologies based upon its signalling and control component - the Session Initiation Protocol (SIP). A SIP Working Group has since been formed within IETF and SIP has been adopted by a number of derivative works, including the IPTEL working group in the IETF. It is therefore appropriate for TIPHON to consider the impact that the introduction of SIP based equipment may have on large-scale public networks.

1 Scope

The present document identifies and defines required service mechanisms to ensure service interoperability for TIPHON which are applicable to release 3. It includes, but is not limited to identifying requirements to interwork between SIP and H.323 administrative domain. The approved delivery from this work item should be used as a common base line for TIPHON and should be used during the whole project life cycle.

2 References

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

[1] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

[2] RFC 2543 (1999): "SIP: Session Initiation Protocol".

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

3 Definitions and abbreviations

3.1 Definitions

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

administrative domain: bounded entity within which all encompassed elements are under common ownership, operation and management

endpoint: Entity that can originate and terminate both signalling and media streams. An endpoint can both call and be called. Examples of endpoints include H.323 terminals, SIP User Agents, Gateways, or Multi-party Conference Units.

GateKeeper (GK): H.323 entity on the network which provides address translation and controls access to the network for H.323 terminals, gateways and MCUs. A Gatekeeper may also provide other services such as bandwidth management and gateway location to terminals, gateways and MCUs.

InterWorking Function (IWF): function connecting two networks of differing signalling technology or administrative policies

proxy server: Anetwork element that acts as both a client and server for the purpose of making SIP requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and if necessary rewrites a request message before forwarding it.

redirect server: Server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client. Unlike a proxy server, it does not initiate its own SIP request. Unlike a UAS, it does not accept calls.

registrar: SIP server that accepts REGISTER requests. A registrar is typically co-located with a proxy or re-direct server and MAY offer location services.

Switched Circuit Network (SCN): Telecommunications network, e.g. Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), and General System for Mobile communications (GSM), that uses circuit-switched technologies for the support of voice calls. The SCN may be a public network or a private network.

telephone call: two-way speech communication between two users by means of terminals connected via network infrastructure

terminal: endpoint other than a gateway or a multipoint control unit

User Agent (UA): application which contains both a UAC and UAS

User Agent Client (UAC): client application that initiates the SIP request

User Agent Server (UAS): Server application that contacts the user when a SIP request is received and that returns a response on behalf of the user. The response accepts, rejects or redirects the request.

3.2 Abbreviations

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

CMS	Call Management Server
CMTS	Call Modem Termination System
CSCF	Call Serve Control Function
DNS	Domain Name Server
GK	H.323 GateKeeper
HFC	Hybrid Fiber Coax
IP	Internet Protocol
ISUP	SS7 ISDN User Part
IWF	InterWorking Function
MT	Mobile Termination
MTA	Multimedia Terminal Adapter
SCN	Switched Circuit Networks
SIP	Session Initiation Protocol
UA	SIP User Agent
UAC	SIP User Client
UAS	SIP User Server
VoIP	Voice over IP

4 Operating modes

H.323 and SIP have a number of declared modes of operation that relate the various functions they identify and define how calls are routed and controlled within their environment. The following clauses identify each mode of operation that is relevant to a potential network context requiring interworking from one protocol technology to another.

4.1 Native H.323 operating modes

H.323 is an architecture for implementing multimedia conferencing over a packet network. It comprises application-layer control protocols that can establish, modify and terminate multimedia sessions or calls. These multimedia sessions may include multimedia conferences, distance learning, Internet telephony and similar applications. It has essentially three possible modes of operation relevant to possible interworking requirements in the context of TIPHON networks.

4.1.1 H.323 peer-to-peer mode

H.323 supports a peer-to-peer mode of operation. In a peer-to-peer architecture, endpoints contact each other directly, without any control or co-ordination from any gatekeeper or intermediate server.

4.1.2 H.323 gatekeeper routed call signalling mode

A gatekeeper may play an active role in mediating call signalling between the calling and called end-points in H.323 networks with gatekeepers. In this environment, a gatekeeper may not only assume responsibility for call routing and authorization on behalf of served endpoints but may also act as the signalling endpoint for calls entering an administrative domain.

4.1.3 H.323 direct call signalling mode

The strict peer-to-peer and gatekeeper routed models may be combined into a hybrid approach referred to as Direct Call Signalling. In this case, gatekeepers provide call routing and authorization while individual endpoints are responsible for establishing and disconnecting calls and media streams directly between each other.

4.1.4 H.323 registration

An H.323 zone is the collection of all terminals, gateways, and Multipoint Control Units managed by a single gatekeeper. Registration is the process by which an endpoint joins an H.323 zone and informs the gatekeeper of its transport and alias addresses. Once established, the registration of an end-point with a specific gatekeeper may need to be refreshed on a periodic basis. An end-point must register with a gatekeeper before it can accept any call attempts.

4.2 Native SIP operating modes

As defined in RFC 2543 [2], the Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. These multimedia sessions may include multimedia conferences, distance learning, Internet telephony and similar applications. The most common SIP operation is the invitation. Instead of directly reaching the intended destination, a SIP request may be redirected by Redirect Server or proxied through Proxy Server. Users can also register their location(s) with SIP Registrar.

4.2.1 SIP peer-to-peer

In a peer-to-peer architecture, User Agents (UA) contact each other by sending invitation directly, without any control or co-ordination from any proxy.

4.2.2 SIP proxy routed

SIP messages may be routed via an intermediary known as a proxy server. In such an environment, proxies not only assume responsibility for call routing and authorization on behalf of their endpoints, they may also act as the signalling endpoint for calls into their administrative domain. A proxy server can either be stateful or stateless.

A stateful proxy retains state information concerning both an incoming request and any associated outgoing requests. In contrast, a stateless proxy does not retain any information concerning a received message or its response once an outgoing request has been generated.

4.2.3 SIP with redirect server

SIP redirect servers represent an example of a loosely coupled distributed architecture. In this environment, the redirect server provides the call routing information such that the originating UA first establishes a signalling connection with the redirect server, before being re-directed to the terminating UA.

4.2.4 SIP registration

The SIP REGISTER method allows a client to let a SIP Registrar know at which address or addresses it can be reached. A client may also use it to install call handling features at the server. A SIP Registrar may be collocated with either a proxy or redirect server.

4.3 Recommended modes of operation

4.3.1 H.323 administrative domain

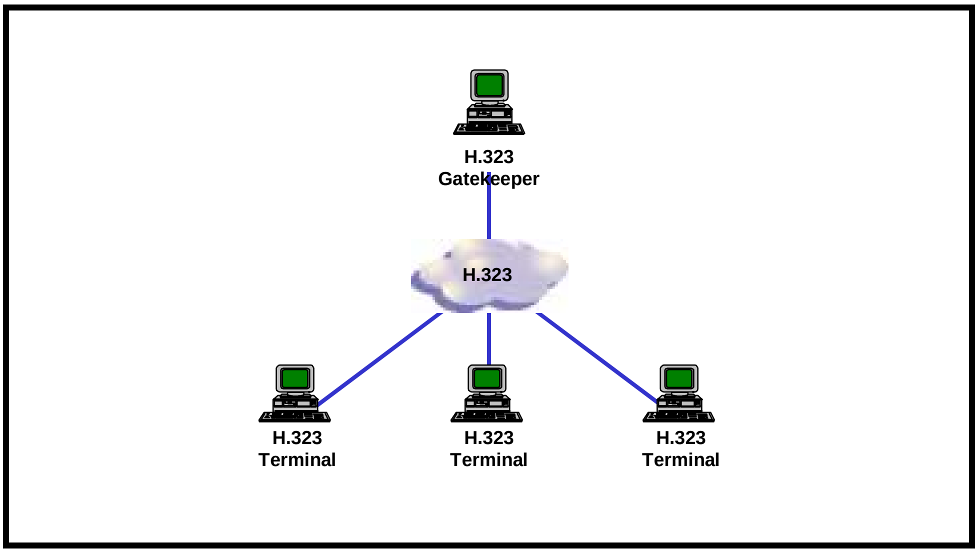

Figure 1: An H.323 administrative domain

While a gatekeeper is an optional element for an H.323 network, it is recommended that TIPHON based H.323 centric networks are deployed with an H.323 Gatekeeper. This should be configured to require registration with all the end points within its administrative domain. It is further recommended that Gatekeeper Routed Call Signalling is used in preference to Direct Call Signalling in order to support enhanced calling features such as availability look-ahead for the called terminal.

4.3.2 SIP administrative domain

As defined in RFC 2543 [2], SIP has no concept of an Administrative Domain. However for practical network engineering and operational reasons consistent with the TIPHON approach to QoS [3], the cocept of a SIP Administrative Domain is introduced. This enables the trust boundaries within which all SIP devices are controlled by a single operator to be delineated. Each SIP Administrative Domain is assumed to contain at least one Registrar. All SIP UAs within that domain must register with the Registrar in order to allow the user's or terminal's address(es) to be advertised within the domain.

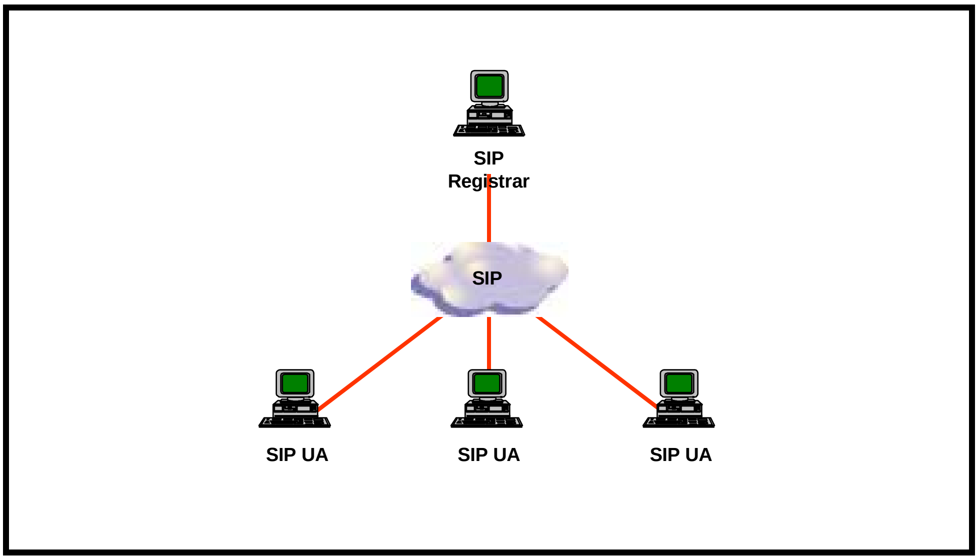

Figure 2: A SIP administrative domain

5 Interworking scenarios

Since the information elements and elements of procedure offered by both SIP and H.323 are capable of supporting a wide range of services and applications, connecting a SIP network and H.323 network together will be more or less complex to achieve depending upon the services being supported in a given scenario. To enable interworking between two such networks to occur reliably, it is necessary to identify the core the conditions and events that will typically be involved. The scenarios below are examples defined to facilitate the identification of such conditions and events.

5.1 Simple scenarios

5.1.1 Dual Stacking in endpoints

The simplest approach to achieving interworking between SIP and H.323 is to provide access to both protocol stacks within the same endpoint. However, while this will provide the means where calls can be originated and terminated from both types of network, it leaves any additional interworking issues to the responsibility of terminal equipment manufacturer and will be inherently non-standard. It is therefore not seen as a long term solution.

5.1.2 Interworking between a SIP domain and an H.323 domain

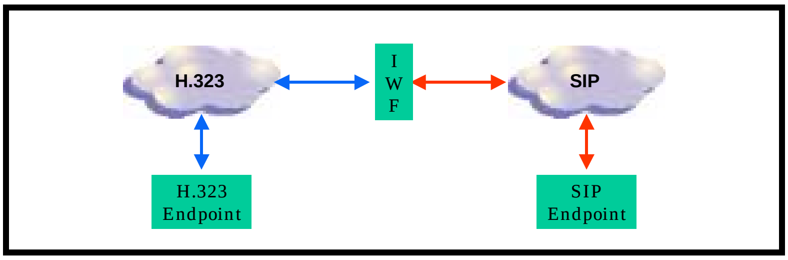

Figure 3: Interworking scenario - between a SIP domain and an H.323 domain

The alternative to providing access to both H.323 and SIP protocols within the same end-point requires the provision of a suitable Interworking Function (IWF) that allows a call originated using one protocol to be terminated using the other. This will necessitate the messages provided by SIP and H.323 to be related through a mapping process within the IWF. Message mapping between protocols may be achieved on either a state-full or state-less basis and will require careful attention depending upon the overall information flows required. However, before any such call flows can be provided, it will be necessary for the end-points to be able to addressable outside of their native protocol domain. This will have to be achieved in association with some form of registration process or procedure. Registration may be made from one domain to the other depending on the arrangement of the Administration Domains concerned as discussed further in clause 5.4.

5.2 Practical interworking scenarios

5.2.1 Interconnection between 3GPP SIP based network and TIPHON H.323 Network

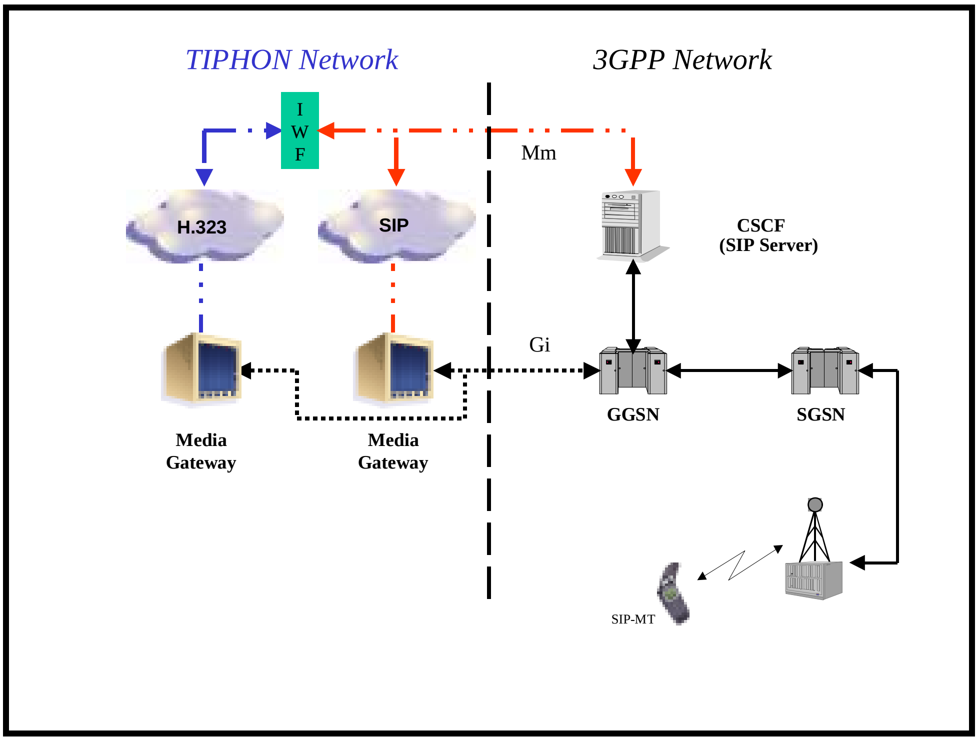

Figure 4: Interconnection between TIPHON and 3GPP Network

TIPHON envisages a future network environment where all types of network - whether fixed, mobile, or satellite - are combined in a manner permitting users to access services regardless of their terminal type, network connection or geographical location. 3GPP have developed a SIP based mobile network architecture for third generation mobile networks as part of the 3GPP Release 5 activities. This identifies a multimedia network interface (Mm in figure 4) that could be realized by a TIPHON compliant fixed network. The TIPHON vision of a fully IP based network interworking with existing fixed and mobile networks therefore complements the 3GPP Release 5 all-IP network vision. Where the TIPHON network connecting with the 3GPP network is based upon H.323, there would be the need to establish interworking between SIP and H.323 across the interface between the two networks, as indicated in figure 4.

5.2.2 Interconnecting PacketCable and TIPHON H.323 Networks

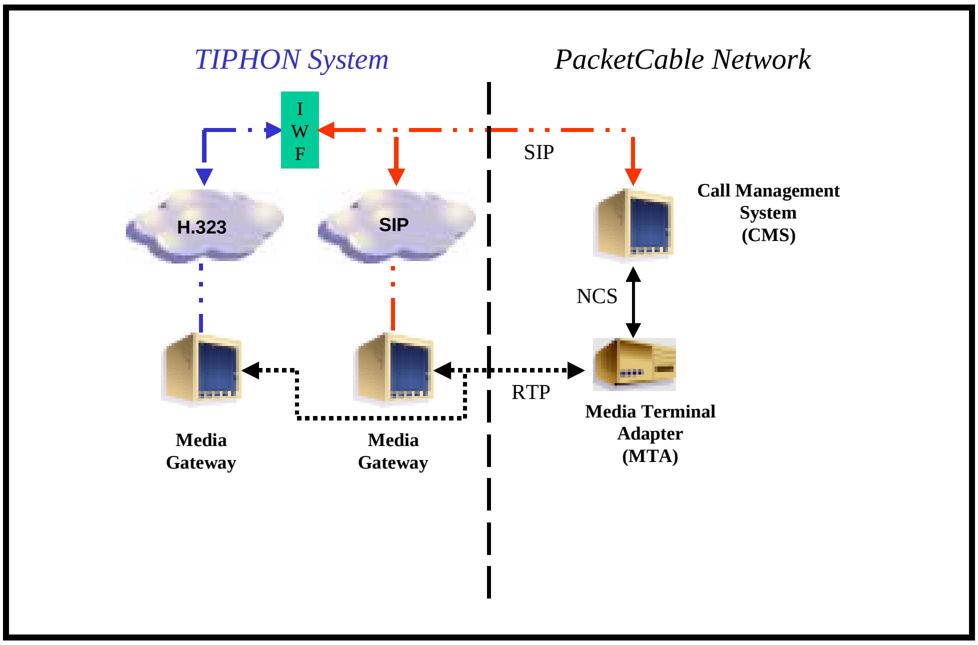

Figure 5: Interconnection between TIPHON and PacketCable Network

PacketCable™ is a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies. The PacketCable project is aimed at defining interface specifications that can be used to develop interoperable equipment capable of providing packet-based voice, video and other high-speed multimedia services over Hybrid Fibre Coax (HFC) cable systems based upon the DOCSIS protocol.

PacketCable consists of a variety of functional components, to create a mechanism for packet-based services. These include the:

- Multimedia Terminal Adapter (MTA) which is a PacketCable client device that contains a subscriber-side interface to the subscriber's CPE (e.g. telephone) and a network-side signalling interface to call control elements in the network. An MTA provides codecs and all signalling and encapsulation functions required for media transport and call signalling;
- Call Management Server (CMS) which provides call control and signalling related services for the MTA, Cable Modem Termination System (CMTS), and PSTN gateways in the PacketCable network. The CMS is a trusted network element that resides on the managed IP portion of the PacketCable network. The CMTS provides connectivity between the DOCSIS HFC Access Network and a Managed IP Network;
- Cable Modem Termination System (CMTS) which provides data connectivity and complimentary functionality to cable modems over the HFC access network. It also provides connectivity to wide area networks. The CMTS is located at the cable television system head-end or distribution hub.

As shown in figure 5, PacketCable are currently developing a SIP based interface for use between CMS functions. As this solution is deployed, there will be the opportunity to connect with networks of different types that may include H.323 based networks, or networks based upon other network protocols. As an illustration of possible future options, figure 5 depicts a scenario demonstrating a PacketCable network being connected with an H.323 based TIPHON network.

5.3 Tandem scenarios

5.3.1 Tandem connection of H.323 domains via a SIP intermediary

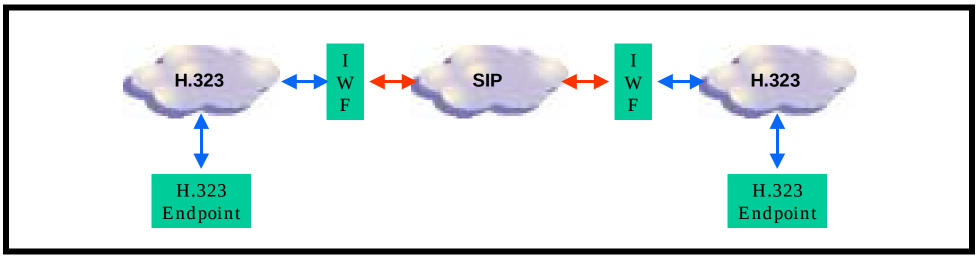

Figure 6: Interworking Scenario - H.323 domains Tandem through a SIP domain

As H.323 and SIP networks become increasingly deployed, it is likely that a call could originate from an H.323 network, be subsequently transported via an intermediate network based upon SIP and then terminate on a H.323 device via a second point of interworking. Ideally in such a case, H.323 messages would be terminated by the Interworking Function (IWF) at the originating H.323-to-SIP boundary with the message semantics being conveyed across the SIP domain using native SIP messages. The reverse operation would ideally be performed by the IWF at the SIP-to-H.323 boundary. However it is currently unlikely that the messages supported by H.323 and SIP can be exactly mapped. In addition, as both protocols increasingly support mechanisms to transport protocols such as DSS.1 by encapsulation, there is the added complication that the IWF may be presented with embedded information elements relating to neither H.323 nor SIP. Furthermore, tunnelling may be necessary to support end-to-end H.323 services that are not supported by the SIP domain. Other aspects of protocol tunnelling are discussed further in clause 6.2.

5.3.2 Tandem connection of SIP domains via an H.323 intermediary

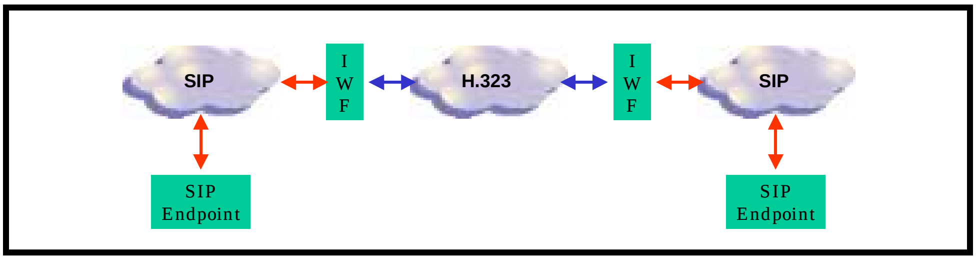

Figure 7: Interworking Scenario - SIP domains Tandem through an H.323 domain

An analogous situation to that described in clause 5.3.1 applies in the case where two SIP devices are interconnected through an intermediate H.323 based network. In this case, the SIP messages would usually be terminated by the IWF at the SIP-to-H.323 boundary and their semantics conveyed across the H.323 domain using native H.323 messages where it is possible to do so. The reverse operation needs to be performed by the IWF at the H.323-to-SIP boundary to produce the terminating call segment. As with the case described in clause 5.3.1, there is the potential scenario where protocols other than SIP may be transported in an encapsulated form. This scenario is discussed further in clause 6.2.

5.4 Support of administrative domains

The registration of end-points with intermediary server elements forms an essential feature of any large scale VoIP technology since without these elements, only a simple strictly peer-to-peer solution can be supported. There are three options for arranging such administrative control as discussed in the following clauses.

5.4.1 Administrative control from a SIP domain

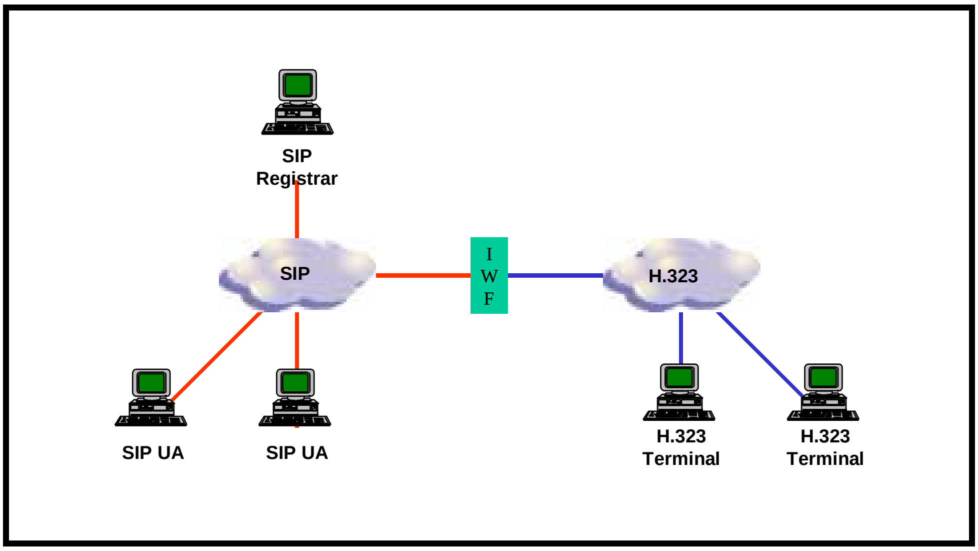

Figure 8: An IWF between SIP and H.323 within a SIP Administrative Domain

In this case, it is assumed that the SIP and H.323 networks fall under the control of the same administration and that the H.323 network is effectively considered to be sub-servant to the SIP network. The SIP Registrar within the administrative domain therefore provides the registration function for all end points within domain irrespective of the protocol type employed. The IWF and all H.323 terminals are therefore under the control of this SIP Registrar. To make this realisable from a practical point of view, the IWF will have to support a method of registering an H.323 end-point with a SIP registrar. This will need to support procedures that allow device discovery, end-point registration and de-registration in an appropriately secured manner.

5.4.2 Administrative control from an H.323 domain

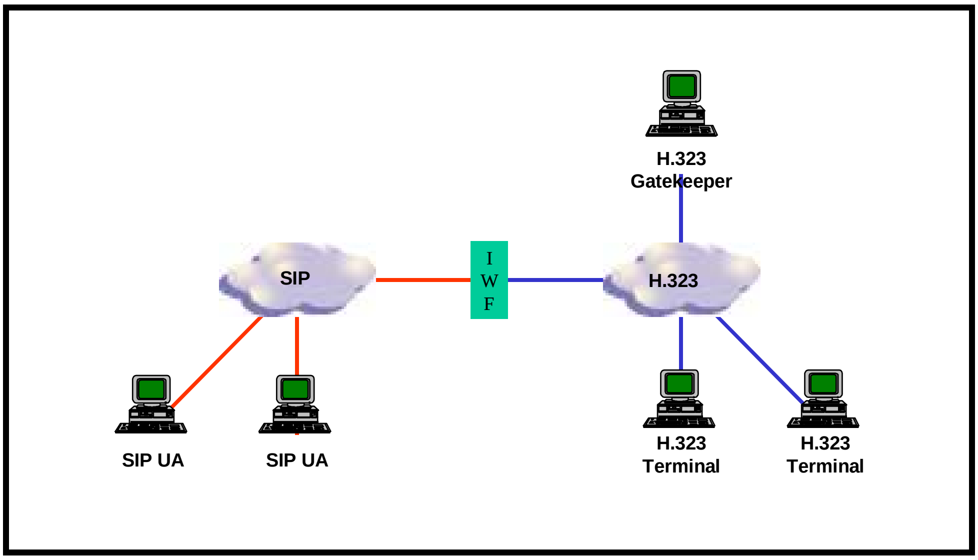

Figure 9: An IWF between SIP and H.323 within an H.323 Administrative Domain

In this case, the administrative control is provided by an H.323 based network with a Gatekeeper. Within the administrative domain all end-points must be registered with the Gatekeeper and the IWF and all SIP UA are therefore under its administrative control. This requires that the IWF needs to support methods of device discovery and registering and de-registering a SIP UA with an H.323 gatekeeper.

5.4.3 Interworking between administrative domains

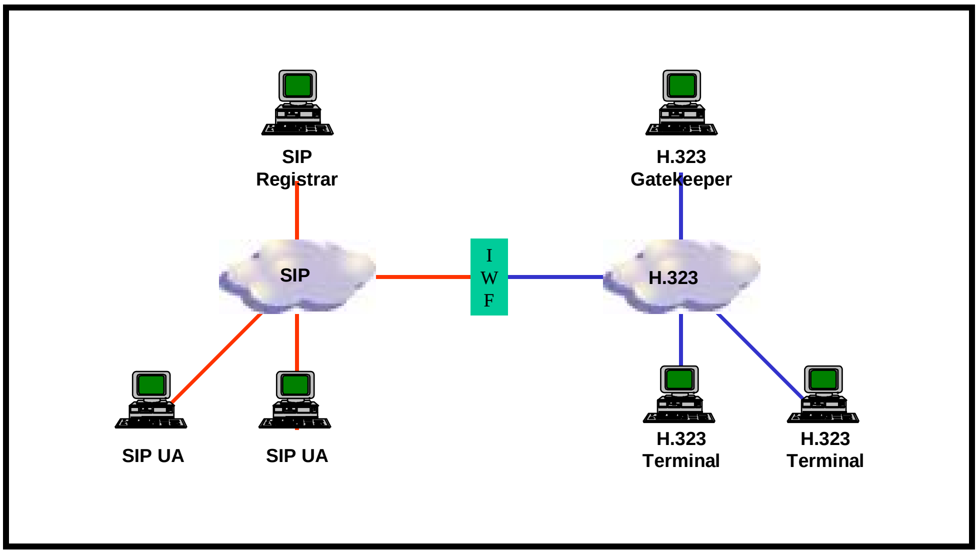

Figure 10: An IWF between SIP and H.323 among separate administrative domains

In this case, the SIP domain and the H.323 domain are controlled by separate and independent administrative domains with equal administrative status. The IWF may be administered within the SIP domain, the H.323 domain or an entirely separate domain administered by a third party. The explicit registration of individual end points across the boundary between the two domains may or may not be necessary depending on the arrangements between the domains concerned and the trust relationship between them. The identification and location of a user across the domain boundary needs to be supported by inter-domain protocols, procedures or processes as appropriate. This gives rise to two possible relationships concerning the actual interconnection between the two domains; a direct peering relationship and an in-direct peering relationship.

5.4.3.1 Direct peering

A direct peering relationship occurs where two administrative domains interwork without reliance on any intermediate third party. The signalling route and the required protocol are therefore known and agreed a-priori by the two administrative domains concerned. The SIP side of the IWF therefore belongs to the SIP administrative domain and the H.323 side of the IWF belongs to the H.323 administrative domain. The IWF registers its SIP interface to the SIP Registrar, and its H.323 interface to the H.323 Gatekeeper. Depending on the construction of the IWF, there may be a separate interworking interface exposed between the SIP side and H.323 side of the IWF. This may use either protocol configured in an inter-domain form or an entirely separate third protocol.

5.4.3.2 In-direct peering

With the in-direct peering scenario, neither domain has a-priori knowledge of the arrangement concerning the origination and termination route for any given call. The IWF is under the administrative control of a single domain that may be a SIP, H.323 or a protocol domain based on an alternative technology. A third party, such as a Clearinghouse server, is required to identify the destination of each call and possibly invoke an IWF if required. The administrative domain that controls the IWF may be the origination of the call, the termination of a call, or an independent third party. In-direct peering is not limited to calls that require charging facilities so information about the destination may be obtained by simple mean such as DNS where more complex features are not required.

6 Encapsulation of other signalling protocols

H.323 and SIP both have the capability to support the encapsulation and transport of signalling information elements associated with other signalling protocols. This is also known as tunnelling. Where an H.323 network interfaces with a SIP based network and either one implements tunnelling of other protocols, the handling of the tunnelled protocol at the interface between the two networks needs to be determined. This clause identifies a number of scenarios where this may occur and indicates the areas that need to be considered further.

6.1 Control of tunnels through IWF

The existence of a tunnel within a signalling stream and its handling at an IWF is an essential aspect of inter-domain interworking. Depending upon the specific context, it may be necessary to be able to identify a specific tunnel, determine the nature of the encapsulated information and be able to control whether the tunnel is allowed and active or prevented, depending upon some external policy applied at the IWF. Whether a tunnel will be allowed or not may be determined on a per call basis depending on the administrative policy within the terminating domain.

6.2 Encapsulation of native signalling

There are two cases of particular interest when considering the interconnection of SIP and H.323 networks from the point of view of the transport of encapsulated signalling that extend the scenarios described in clauses 5.3.1 and 5.3.2. In the first scenario which is shown in figure 11, a SIP network acts as the intermediary between an originating H.323 network and a terminating H.323 network and. To allow a fuller feature set to be supported between the H.32 end-points, there is the need to establish an H.323 protocol tunnel across the SIP network that allows the full H.323 protocol to be exposed between the end-points without exposing the overall routing across the intermediate SIP domain.

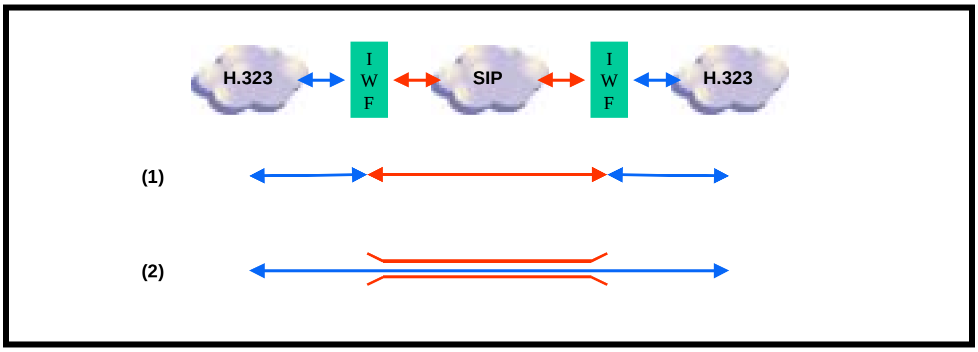

Figure 11: H.323 Tunnel Through SIP

The second scenario, shown in figure 12, an H.323 based network acts as the intermediary between two SIP networks. In this case, the simple mapping of protocol information elements described in clause 5.3.2 will prevent a richer set of SIP functionality to be exposed at the originating and terminating end-points. A protocol tunnel is therefore required that, under the control of the intermediate H.323 domain, can transport SIP information elements.

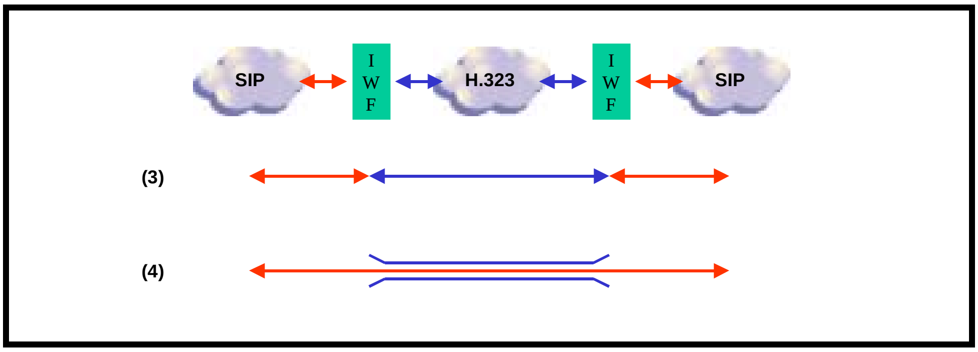

Figure 12: SIP Tunnels Through H.323

In either of the cases considered in this clause, there is the need to provide management and control of the protocol tunnels to ensure that external administrative policies are not being circumvented.

6.3 Encapsulation of other signalling

This clause considers the case where either SIP or H.323 are transporting foreign signalling system such a Q.SIG or ISUP. There are essentially two core scenarios to be considered depending on whether a SIP or H.323 based network constitutes the intermediate domain.

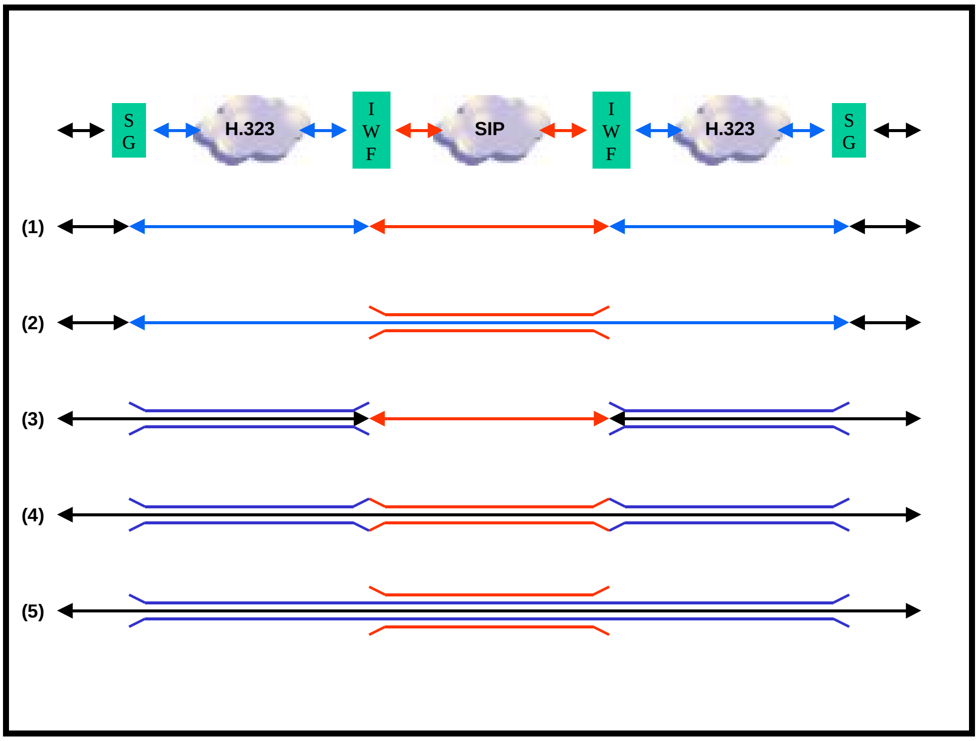

Figure 13: Tunnelling Scenarios - "H.323 Tandem Through SIP"

Figure 13 depicts the set of scenarios where a SIP network acts as the intermediary between an originating H.323 network and a terminating H.323 network. This exposes a number of sub-cases depending upon the arrangements of non-native signalling and the ability of H.323 and SIP to handle tunnels.

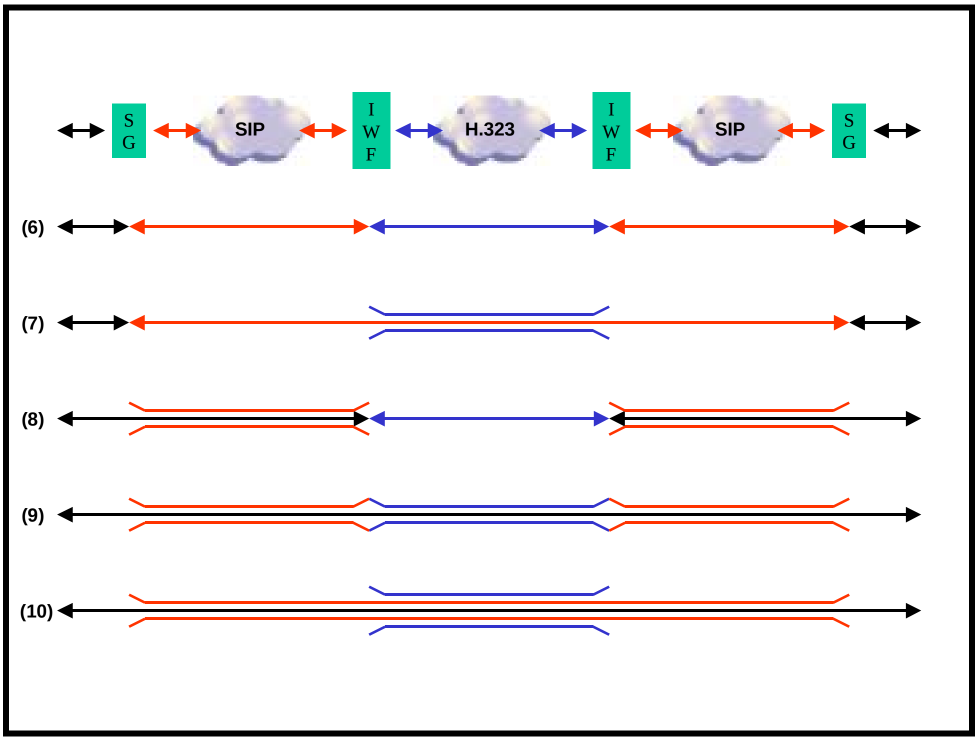

Figure 14: Tunnelling Scenarios - "SIP Tandem Through H.323"

An alternative arrangement is possible where an H.323 network forms the intermediary. This scenario is shown in figure 14. From both of these examples, the following generic are identified depending upon the behaviour required from either H.323 or SIP with respect to the management of protocol tunnels:

- Cases 1 and 6 - both SIP and H.323 support the semantics of the end-to-end signalling message and require no tunnelling.

- Cases 2 and 8 - H.323 supports the semantics of the end-to-end signalling message but SIP does not. A tunnel is therefore required through the SIP domain only.

- Cases 3 and 7 - SIP supports the semantics of the end-to-end signalling message but H.323 does not. A tunnel is therefore required through the H.323 domain only.

- Cases 4 and 9 - neither SIP nor H.323 support the semantics of the end-to-end signalling message. However, an IWF has a method to convert the tunnelled information between SIP and H.323. The tunnelled message is extracted at the IWF and re-encapsulated with the tunnelling method of the other protocol.

- Cases 5 and 10 - neither SIP nor H.323 support the semantics of the end-to-end signalling message. The IWF does not have a method to convert the tunnelling method between SIP and H.323. Therefore, the tunnel message has to be double encapsulated to pass through the concatenation of networks.

7 Other considerations

7.1 Security considerations

There are two distinct roles for IWFs depending on whether they are used to interconnect networks within a single administrative domain or form an interconnection between networks under the control of separate administrative policies. In particular;

- An intra-domain IWF need not be concerned with security to any degree other than that required for normal end-to-end operation.
- An inter-domain IWF, is positioned between administrative domains. It must by nature act as the final arbitrator between administrative domains. This implies that the IWF must be a trusted entity. In order to properly establish and maintain this trust, the IWF must have appropriate credentials.

An inter-domain IWF must therefore address:

- **Authenticated Administrative Access** - at least requiring a password, permitting password changes, and preventing the use of "bad" passwords. Mechanisms stronger than passwords (one-time tokens, etc) are recommended and should be supported.
- **Multi-level Administrative Access** - at least an operator view without the ability to change IWF configuration and an administrator view which does have the ability to change configuration. Each view should have its own authentication tokens (passwords, etc).
- **Access Control Rules** - to permit or disallow call setup requests from individual IP addresses as well as ranges of them.
- **Detailed Logging to Persistent Storage** - support for logging to one or more remote storage locations should be provided. This log should include administrator accesses, detailed descriptions of configuration changes by administrators, as well as some call-by-call detail logging. Settable logging levels should be provided, to allow either more or less detail than the default to be logged.

7.1.1 Signalling security

In inter-domain IWF should provide support for all standard authentication, privacy and other security methods relating to H.323 and SIP, as these are defined.

An IWF intended for intra-domain use need not support security mechanisms.

For cases involving tunnelling, the IWF should provide the ability to use both security mechanisms. For example, when tunnelling H.235-secure messages over SIP, the IWF should provide the ability to use IPSEC and/or any native-SIP authentication or other security mechanisms to secure the tunnelling messages. This allows administrative transparency. An H.323 signalling network may treat a SIP leg as "just another leg", while the operator of the SIP network may elect to provide this service over a public network, unbeknown to the H.323 network's operator, and do so securely with strong encryption. This allows the security considerations of the network using the tunnel to be clearly separated from the security considerations of the network providing the tunnel.

7.1.2 Media security

An IWF intended for intra-domain interworking may optionally provide mechanisms providing media security.

An IWF intended for inter-domain interworking should be aware of media security mechanisms by supporting

- access control lists (e.g. firewall functionality);
- differences in addressing policy (e.g. network address translation);
- packet level security (e.g. IPSEC).

7.2 Addressing and naming consideration

Applications such as emergency calling require specific location address information to be passed from the originating domain to the terminating domain. Where H.323 domains and SIP domains are connected together, it is important that such information be made available to the terminating side. In addition, it is important that address information received by the terminating side of the IWF is sufficient for the called party to be able to return a call to the calling party if so required.

7.3 Quality of service considerations

Interworking between H.323 and SIP at the signalling level may have implications for QoS mechanisms used to provide QoS for both the signalling and media within each domain. This remains for further study.

7.4 Management considerations

7.4.1 Reporting

The IWF should support configuration and status reporting of its service, network and security parameters.

7.4.2 Diagnostic test

The IWF should allow service and network element tests from authorized and authenticated administrative personnel. This should include self-diagnostic tests.

7.4.3 Fault management

The IWF should provide functionality that enables fault management processes to allow the detection and isolation of abnormal conditions affecting its operation.

8 Prioritized requirements

For the purposes of TIPHON, a Simple Call Service Application shall support the following scenarios:

- Interworking between a SIP domain and an H.323 domain;
- Administrative Control from a SIP Domain;
- Administrative Control from an H.323 Domain;
- Interworking between Administrative Domains with In-direct Peering;
- Interworking between Administrative Domains with Direct Peering;
- Control of Tunnels through an IWF.

Annex A:
Bibliography

- ITU-T Recommendation H.245: "Control protocol for multimedia communication".
- ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues".
- ETSI TS 101 321: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Open Settlement Protocol (OSP) for Inter-Domain pricing, authorization, and usage exchange".
- ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".
- RFC 2401 (1998): "Security Architecture for the Internet Protocol".
- IMTC aHIT!: "Interoperability Requirements for SIP and H.323 Interworking", March 2000.
- SIP-H.323 Interworking Requirements: "draft-agrawal-sip-h323-interworking-reqs-00.txt", Argrawal, et al, July 2000.
- Interworking Between SIP/DSP and H.323: "draft-singh-sip-h323-01.txt", Singh and Schulzrinne, May 2000.
- 3GPP TS 24.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP; stage 3 (Release 5)".
- PacketCable CMS to CMS Signalling Specification, PKT-SP-CMSS-D01-001010, October 2000.

History

Document history		
V1.1.1	December 2001	Publication