

Network Working Group
Request for Comments: 4123
Category: Informational

H. Schulzrinne
Columbia University
C. Agboh
July 2005

Session Initiation Protocol (SIP)-H.323 Interworking Requirements

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

IESG Note

This RFC is not a candidate for any level of Internet Standard. The IETF disclaims any knowledge of the fitness of this RFC for any purpose, and in particular notes that the decision to publish is not based on IETF review for such things as security, congestion control, or inappropriate interaction with deployed protocols. The RFC Editor has chosen to publish this document at its discretion. Readers of this document should exercise caution in evaluating its value for implementation and deployment. See [RFC3932] for more information.

Abstract

This document describes the requirements for the logical entity known as the Session Initiation Protocol (SIP)-H.323 Interworking Function (SIP-H.323 IWF) that will allow the interworking between SIP and H.323.

Table of Contents

1. Introduction	3
2. Definitions	3
3. Functionality within the SIP-H.323 IWF	4
4. Pre-Call Requirements	4
4.1. Registration with H.323 Gatekeeper	5
4.2. Registration with SIP Server	5
5. General Interworking Requirements	5
5.1. Basic Call Requirements	5
5.1.1. General Requirements	5
5.1.2. Address Resolution	6
5.1.3. Call with H.323 Gatekeeper	6
5.1.4. Call with SIP Registrar	6
5.1.5. Capability Negotiation	6
5.1.6. Opening of Logical Channels	7
5.2. IWF H.323 Features	7
5.3. Overlapped Sending	7
5.3.1. DTMF Support	7
6. Transport	8
7. Mapping between SIP and H.323	8
7.1. General Requirements	8
7.2. H.225.0 and SIP Call Signaling	8
7.3. Call Sequence	9
7.4. State Machine Requirements	9
8. Security Considerations	10
9. Examples and Scenarios	10
9.1. Introduction	10
9.2. IWF Configurations	11
9.3. Call Flows	11
9.3.1. Call from H.323 Terminal to SIP UA	11
9.3.2. Call from SIP UA to H.323 Terminal	12
10. Acknowledgments	12
11. Contributors	13
12. References	14
12.1. Normative References	14
12.2. Informative References	15

1. Introduction

The SIP-H.323 Interworking function (IWF) converts between SIP (Session Initiation Protocol) [RFC3261] and the ITU Recommendation H.323 protocol [H.323]. This document describes requirements for this protocol conversion.

2. Definitions

H.323 gatekeeper (GK): An H.323 gatekeeper is an optional component in an H.323 network. If it is present, it performs address translation, bandwidth control, admission control, and zone management.

H.323 network: In this document, we refer to the collection of all H.323-speaking components as the H.323 network.

SIP network: In this document, we refer to the collection of all SIP servers and user agents as the SIP network.

Interworking Function (IWF): This function performs interworking between H.323 and SIP. It belongs to both the H.323 and SIP networks.

SIP server: A SIP server can be a SIP proxy, redirect server, or registrar server.

Endpoint: An endpoint can call and be called. An endpoint is an entity from which the media such as voice, video, or fax originates or terminates. An endpoint can be H.323 terminal, H.323 Gateway, H.323 MCU [H.323], or SIP user agent (UA) [RFC3261].

Media-Switching Fabric (MSF): This is an optional logical entity within the IWF. The MSF switches media such as voice, video, or fax from one network association to another.

3. Functionality within the SIP-H.323 IWF

This section summarizes the functional requirements of the SIP-H.323 interworking function (IWF).

A SIP-H.323 IWF may be integrated into an H.323 gatekeeper or SIP server. Interworking should not require any optional components in either the SIP or H.323 network, such as H.323 gatekeepers. IWF redundancy in the network is beyond the scope of this document.

An IWF contains functions from the following list, inter alia:

- o Mapping of the call setup and teardown sequences;
- o Registering H.323 and SIP endpoints with SIP registrars and H.323 gatekeepers;
- o Resolving H.323 and SIP addresses;
- o Maintaining the H.323 and SIP state machines;
- o Negotiating terminal capabilities;
- o Opening and closing media channels;
- o Mapping media-coding algorithms for H.323 and SIP networks;
- o Reserving and releasing call-related resources;
- o Processing of mid-call signaling messages;
- o Handling of services and features.

The IWF should not process media. We assume that the same media transport protocols, such as RTP, are used in both the SIP and H.323 networks. Thus, media packets are exchanged directly between the endpoints. If a particular service requires the IWF to handle media, we assume that the IWF simply forwards media packets without modification from one network to the other, using a media-switching fabric (MSF). The conversion of media from one encoding or format to another is out of scope for SIP-H.323 protocol translation.

4. Pre-Call Requirements

The IWF function may use a translation table to resolve the H.323 and SIP addresses to IP addresses. This translation table can be updated by using an H.323 gatekeeper, a SIP proxy server, or a locally-maintained database.

4.1. Registration with H.323 Gatekeeper

An IWF may provide and update the H.323 gatekeeper with the addresses of SIP UAs. A SIP user agent can make itself known to the H.323 network by registering with an IWF serving as a registrar. The IWF creates an H.323 alias address and registers this alias, together with its own network address, with the appropriate GK.

The gatekeeper can then use this information to route calls to SIP UAs via the IWF, without being aware that the endpoint is not a "native" H.323 endpoint.

The IWF can register SIP UAs with one or more H.323 gatekeepers.

4.2. Registration with SIP Server

The IWF can provide information about H.323 endpoints to a SIP registrar. This allows the SIP proxy using this SIP registrar to direct calls to the H.323 endpoints via the IWF.

The IWF can easily obtain information about H.323 endpoints if it also serves as a gatekeeper. Other architectures require further study.

If the H.323 endpoints are known through E.164 (telephone number) addresses, the IWF can use IGREP [TGREP] or SLP [GWLOC] to inform the SIP proxy server of these endpoints.

The IWF only needs to register with multiple SIP registrars if the H.323 terminal is to appear under multiple, different addresses-of-record.

5. General Interworking Requirements

The IWF should use H.323 Version 2 or later and SIP according to RFC 3261 [RFC3261]. The protocol translation function must not require modifications or additions to either H.323 or SIP. However, it may not be possible to support certain features of each protocol across the IWF.

5.1. Basic Call Requirements

5.1.1. General Requirements

The IWF should provide default settings for translation parameters. The IWF specification must identify these defaults.

The IWF must release any call-related resource at the end of a call. SIP session timers [RFC4028] may be used on the SIP side.

5.1.2. Address Resolution

The IWF should support all the addressing schemes in H.323, including the H.323 URI [RFC3508], and the "sip", "sips", and "tel" URI schemes in SIP. It should support the DNS-based SIP server location mechanisms described in [RFC3263] and H.323 Annex O, which details how H.323 uses DNS and, in particular, DNS SRV records.

The IWF should register with the H.323 Gatekeeper and the SIP registrar when available.

The IWF may use any means to translate between SIP and H.323 addresses. Examples include translation tables populated by the gatekeeper, SIP registrar or other database, LDAP, DNS or TRIP.

5.1.3. Call with H.323 Gatekeeper

When an H.323 GK is present in the network, the IWF should resolve addresses with the help of the GK.

5.1.4. Call with SIP Registrar

The IWF applies normal SIP call routing and does not need to be aware whether there is a proxy server.

5.1.5. Capability Negotiation

The IWF should not make any assumptions about the capabilities of either the SIP user agent or the H.323 terminal. However, it may indicate a guaranteed-to-be-supported list of codecs of the H.323 terminal or SIP user agent before exchanging capabilities with H.323 (using H.245) and SIP (using SDP [RFC2327]). H.323 defines mandatory capabilities, whereas SIP currently does not. For example, the G.711 audio codec is mandatory for higher bandwidth H.323 networks.

The IWF should attempt to map the capability descriptors of H.323 and SDP in the best possible fashion. The algorithm for finding the best mapping between H.245 capability descriptors and the corresponding SDP is left for further study.

The IWF should be able to map the common audio, video, and application format names supported in H.323 to and from the equivalent RTP/AVP [RFC3550] names.

The IWF may use the SIP OPTIONS message to derive SIP UA capabilities. It may support mid-call renegotiation of media capabilities.

5.1.6. Opening of Logical Channels

The IWF should support the seamless exchange of messages for opening, reopening, changing, and closing of media channels during a call. The procedures for opening, reopening, closing, and changing the existing media sessions during a call are for further study.

The IWF should open media channels between the endpoints whenever possible. If this is not possible, then the channel can be opened at the MSF of the IWF.

The IWF should support unidirectional, symmetric bi-directional, and asymmetric bi-directional opening of channels.

The IWF may respond to the mode request and to the request for reopening and changing an existing logical channel and may support the flow control mechanism in H.323.

5.2. IWF H.323 Features

The IWF should support Fast Connect; i.e., H.245 tunneling in H.323 Setup messages. If IWF and GK are the same device, pre-granted ARQ should be supported. If pre-granted ARQ is supported, the IWF may perform the address resolution from H.323 GK using the LRQ/LCF exchange.

5.3. Overlapped Sending

An IWF should follow the recommendations outlined in [RFC3578] when receiving overlapped digits from the H.323 side. If the IWF receives overlapped dialed digits from the SIP network, it may use the Q.931 Setup, Setup Ack, and Information Message in H.323.

The IWF may support the transfer of digits during a call by using the appropriate SIP mechanism and UserInputIndication in H.245 (H.323).

5.3.1. DTMF Support

An IWF should support the mapping between DTMF and possibly other telephony tones carried in signaling messages.

6. Transport

The H.323 and SIP systems do not have to be in close proximity. The IP networks hosting the H.323 and SIP systems do not need to assure quality of service (QoS). In particular, the IWF should not assume that signaling messages have priority over packets from other applications. H.323 signaling over UDP (H.323 Annex E) is optional.

7. Mapping between SIP and H.323

7.1. General Requirements

- o The call message sequence of both protocols must be maintained.
- o The IWF must not set up or tear down calls on its own.
- o Signaling messages that do not have a match for the destination protocol should be terminated on the IWF, with the IWF taking the appropriate action for them. For example, SIP allows a SIP UA to discard an ACK request silently for a non-existent call leg.
- o If the IWF is required to generate a message on its own, IWF should use pre-configured default values for the message parameters.
- o The information elements and header fields of the respective messages are to be converted as follows:
 - * The contents of connection-specific information elements, such as Call Reference Value for H.323, are converted to similar information required by SIP or SDP, such as the SDP session ID and the SIP 'Call-ID'.
 - * The IWF generates protocol elements that are not available from the other side.

7.2. H.225.0 and SIP Call Signaling

- o The IWF must conform to the call signaling procedures recommended for the SIP side regardless of the behavior of the H.323 elements.
- o The IWF must conform to the call signaling procedures recommended for the H.323 side regardless of the behavior of the SIP elements.

- o The IWF serves as the endpoint for the Q.931 Call Signaling Channel to either an H.323 endpoint or H.323 Gatekeeper (in case of GK routed signaling). The IWF also acts as a SIP user agent client and server.
- o The IWF also establishes a Registration, Admission, Status (RAS) Channel to the H.323 GK, if available.
- o The IWF should process messages for H.323 supplementary services (FACILITY, NOTIFY, and the INFORMATION messages) only if the service itself is supported.

7.3. Call Sequence

The call sequence on both sides should be maintained in such a way that neither the H.323 terminal nor the SIP UA is aware of presence of the IWF.

7.4. State Machine Requirements

The state machine for IWF will follow the following general guidelines:

- o Unexpected messages in a particular state shall be treated as "error" messages.
- o All messages that do not change the state shall be treated as "non-triggering" or informational messages.
- o All messages that expect a change in state shall be treated as "triggering" messages.

For each state, an IWF specification must classify all possible protocol messages into the above three categories. It must specify the actions taken on the content of the message and the resulting state. Below is an example of such a table:

State: Idle

Possible Messages	Message Category	Action	Next state

All RAS msg.	Triggering	Add Reg.Info.	WaitForSetup
All H.245 msg.	Error	Send 4xx	Idle
SIP OPTIONS	Non Triggering	Return cap.	Idle
SIP INVITE	Triggering	Send SETUP	WaitForConnect

8. Security Considerations

Because the IWF whose requirements have been described in this document combines both SIP and H.323 functionality, security considerations for both of these protocols apply.

The eventual security solution for interworking must rely on the standard mechanisms in RFC3261 [RFC3261] and H.323, without extending them for the interworking function. Signaling security for H.323 is described in H.235 [H.235].

Because all data elements in SIP or H.323 have to terminate at the IWF, the resulting security cannot be expected to be end-to-end. Thus, the IWF terminates not only the signalling protocols but also the security in each domain. Therefore, users at the SIP or H.323 endpoint have to trust the IWF, like they would any other gateway, to authenticate the other side correctly. Similarly, they have to trust the gateway to respect the integrity of data elements and to apply appropriate security mechanisms on the other side of the IWF.

The IWF must not indicate the identity of a user on one side without first performing authentication. For example, if the SIP user was not authenticated, it would be inappropriate to use mechanisms on the H.323 side, such as H.323 Annex D, to indicate that the user identity had been authenticated.

An IWF must not accept 'sips' requests unless it can guarantee that the H.323 side uses equivalent H.235 [H.235] security mechanisms. Similarly, the IWF must not accept H.235 sessions unless it succeeds in using SIP-over-TLS (sips) on the SIP side of the IWF.

9. Examples and Scenarios

9.1. Introduction

We present some examples of call scenarios that will show the signaling messages received and transmitted. The following situations can occur:

- o Some signaling messages can be translated one-to-one.
- o In some cases, parameters on one side do not match those on the other side.
- o Some signaling messages do not have an equivalent message on the other side. In some cases, the IWF can gather further information and the signal on the other side. In some cases, only an error indication can be provided.

9.2. IWF Configurations

Below are some common architectures involving an IWF:

Basic Configuration: H.323 EP -- IWF -- SIP UA

Calls using H.323 GK: H.323 EP -- H.323 GK -- IWF -- SIP UA

Calls using SIP proxies: H.323 EP -- IWF -- SIP proxies -- SIP UA

Calls using both H.323 GK and SIP proxy: H.323 EP -- H.323 GK -- IWF
-- SIP proxies -- SIP UA

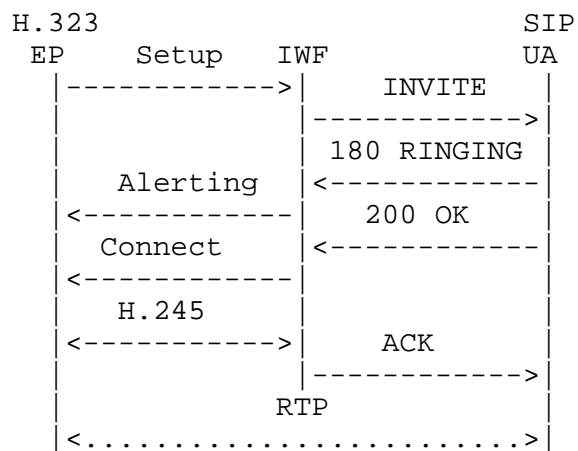
SIP trunking between H.323 networks: H.323 EP -- IWF -- SIP network
-- IWF -- H.323 EP

H.323 trunking between SIP networks: SIP EP -- IWF -- H.323 network
-- IWF -- SIP UA

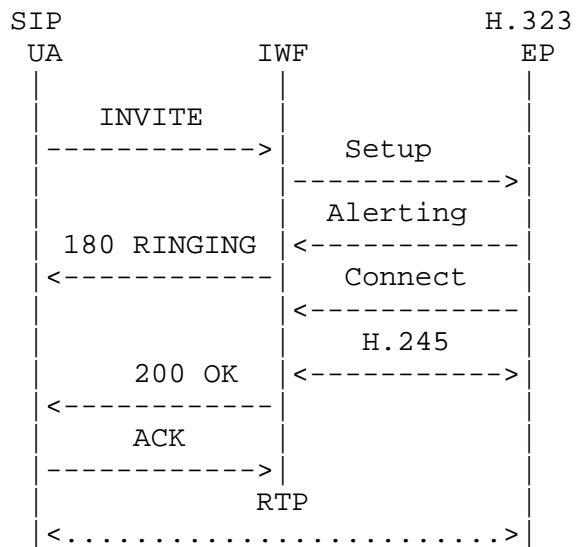
9.3. Call Flows

Some call flow examples for two different configurations and call scenarios are given below.

9.3.1. Call from H.323 Terminal to SIP UA



9.3.2. Call from SIP UA to H.323 Terminal



10. Acknowledgments

The authors would like to acknowledge the many contributors who discussed the SIP-H.323 interworking architecture and requirements on the IETF, SIP, and SG16 mailing lists. In particular, we would like to thank Joon Maeng, Dave Walker, and Jean-Francois Mule. Contributions to this document have also been made by members of the H.323, aHIT!, TIPHON, and SG16 forums.

11. Contributors

In addition to the editors, the following people provided substantial technical and written contributions to this document. They are listed alphabetically.

Hemant Agrawal
Telveverse Communications
1010 Stewart Drive
Sunnyvale, CA 94085
USA

EMail: hagrawal@telverse.com

Alan Johnston
MCI WorldCom
100 South Fourth Street
St. Louis, MO 63102
USA

EMail: alan.johnston@wcom.com

Vipin Palawat
Cisco Systems Inc.
900 Chelmsford Street
Lowell, MA 01851
USA

EMail: vpalawat@cisco.com

Radhika R. Roy
AT&T
Room C1-2B03
200 Laurel Avenue S.
Middletown, NJ 07748
USA

EMail: rrroy@att.com

Kundan Singh
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA

EMail: kns10@cs.columbia.edu

David Wang
Nuera Communications Inc.
10445 Pacific Center Court
San Diego, CA 92121
USA

EMail: dwang@nuera.com

12. References

12.1. Normative References

- [H.235] International Telecommunication Union, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals", Recommendation H.235, February 1998.
- [H.323] International Telecommunication Union, "Packet based multimedia communication systems", Recommendation H.323, July 2003.
- [RFC2327] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.
- [RFC3508] Levin, O., "H.323 Uniform Resource Locator (URL) Scheme Registration", RFC 3508, April 2003.

- [RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

12.2. Informative References

- [GWLOC] Zhao, W. and H. Schulzrinne, "Locating IP-to-Public Switched Telephone Network (PSTN) Telephony Gateways via SLP", work in progress, February 2004.
- [RFC3578] Camarillo, G., Roach, A., Peterson, J., and L. Ong, "Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to the Session Initiation Protocol (SIP)", RFC 3578, August 2003.
- [RFC3932] Alvestrand, H., "The IESG and RFC Editor Documents: Procedures", BCP 92, RFC 3932, October 2004.
- [RFC4028] Donovan, S. and J. Rosenberg, "Session Timers in the Session Initiation Protocol (SIP)", RFC 4028, April 2005.
- [TGREP] Bangalore, M., "A Telephony Gateway REGistration Protocol (TGREP)", work in progress, March 2004.

Authors' Addresses

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7042
EMail: hgs@cs.columbia.edu
URI: <http://www.cs.columbia.edu>

Charles Agboh
61 Bos Straat
3540 Herk-de-Stad
Belgium

Phone: +32479736250
EMail: charles.agboh@packetizer.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78 and at www.rfc-editor.org/copyright.html, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

