

# [MS-OCPSTN]:

## Session Initiation Protocol (SIP) for PSTN Calls Extensions

---

### Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](#) or the [Microsoft Community Promise](#). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the [Patent Map](#).
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights.** All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

**Tools.** The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

**Support.** For questions and support, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

## Revision Summary

Date	Revision History	Revision Class	Comments
4/4/2008	0.1	New	Initial version
4/25/2008	0.2	Minor	Updated based on feedback
6/27/2008	1.0	Major	Updated and revised the technical content.
8/15/2008	1.01	Minor	Revised and edited the technical content.
9/12/2008	1.02	Minor	Revised and edited the technical content.
12/12/2008	2.0	Major	Updated and revised the technical content.
2/13/2009	2.01	Minor	Revised and edited the technical content.
3/13/2009	2.02	Minor	Revised and edited the technical content.
7/13/2009	2.03	Major	Revised and edited the technical content
8/28/2009	2.04	Editorial	Revised and edited the technical content
11/6/2009	2.05	Editorial	Revised and edited the technical content
2/19/2010	2.06	Editorial	Revised and edited the technical content
3/31/2010	2.07	Major	Updated and revised the technical content
4/30/2010	2.08	Editorial	Revised and edited the technical content
6/7/2010	2.09	Editorial	Revised and edited the technical content
6/29/2010	2.10	Editorial	Changed language and formatting in the technical content.
7/23/2010	2.10	None	No changes to the meaning, language, or formatting of the technical content.
9/27/2010	3.0	Major	Significantly changed the technical content.
11/15/2010	3.0	None	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	3.0	None	No changes to the meaning, language, or formatting of the technical content.
3/18/2011	3.0	None	No changes to the meaning, language, or formatting of the technical content.
6/10/2011	3.0	None	No changes to the meaning, language, or formatting of the technical content.
1/20/2012	4.0	Major	Significantly changed the technical content.
4/11/2012	4.0	None	No changes to the meaning, language, or formatting of the technical content.
7/16/2012	4.0	None	No changes to the meaning, language, or formatting of the technical content.
10/8/2012	4.0.1	Editorial	Changed language and formatting in the technical content.
2/11/2013	4.0.1	None	No changes to the meaning, language, or formatting of the

<b>Date</b>	<b>Revision History</b>	<b>Revision Class</b>	<b>Comments</b>
			technical content.
7/30/2013	4.0.1	None	No changes to the meaning, language, or formatting of the technical content.
11/18/2013	4.0.1	None	No changes to the meaning, language, or formatting of the technical content.
2/10/2014	4.0.1	None	No changes to the meaning, language, or formatting of the technical content.
4/30/2014	4.1	Minor	Clarified the meaning of the technical content.
7/31/2014	4.2	Minor	Clarified the meaning of the technical content.
10/30/2014	4.2	None	No changes to the meaning, language, or formatting of the technical content.
3/30/2015	5.0	Major	Significantly changed the technical content.
9/4/2015	5.0	None	No changes to the meaning, language, or formatting of the technical content.
7/15/2016	5.0	None	No changes to the meaning, language, or formatting of the technical content.
9/14/2016	5.0	None	No changes to the meaning, language, or formatting of the technical content.
9/29/2016	5.0	None	No changes to the meaning, language, or formatting of the technical content.
4/27/2018	6.0	Major	Significantly changed the technical content.
7/24/2018	7.0	Major	Significantly changed the technical content.
8/28/2018	8.0	Major	Significantly changed the technical content.
6/18/2019	8.0	None	No changes to the meaning, language, or formatting of the technical content.

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Glossary .....	7
1.2	References .....	9
1.2.1	Normative References .....	9
1.2.2	Informative References .....	9
1.3	Overview .....	10
1.4	Relationship to Other Protocols .....	11
1.5	Prerequisites/Preconditions .....	11
1.6	Applicability Statement .....	11
1.7	Versioning and Capability Negotiation .....	11
1.8	Vendor-Extensible Fields .....	12
1.9	Standards Assignments.....	12
<b>2</b>	<b>Messages.....</b>	<b>13</b>
2.1	Transport.....	13
2.2	Message Syntax.....	13
2.2.1	isGateway.....	13
2.2.2	phone-context.....	13
2.2.3	ms-call-source .....	14
2.2.4	ms-early-media .....	14
2.2.5	Anonymous Phone URI .....	14
2.2.6	ms-bypass .....	14
2.2.7	ms-accepted-content-id.....	14
2.2.8	ms-trunking-peer .....	15
2.2.9	ms-mediation-generated .....	15
<b>3</b>	<b>Protocol Details .....</b>	<b>16</b>
3.1	isGateway Details.....	16
3.1.1	Abstract Data Model.....	16
3.1.2	Timers .....	16
3.1.3	Initialization.....	16
3.1.4	Higher-Layer Triggered Events .....	16
3.1.5	Message Processing Events and Sequencing Rules .....	16
3.1.6	Timer Events.....	16
3.1.7	Other Local Events.....	16
3.2	phone-context Details.....	16
3.2.1	Abstract Data Model.....	17
3.2.2	Timers .....	17
3.2.3	Initialization.....	17
3.2.4	Higher-Layer Triggered Events .....	17
3.2.5	Message Processing Events and Sequencing Rules .....	18
3.2.6	Timer Events.....	18
3.2.7	Other Local Events.....	18
3.3	ms-call-source Details .....	18
3.3.1	Abstract Data Model.....	18
3.3.2	Timers .....	18
3.3.3	Initialization .....	18
3.3.4	Higher-Layer Triggered Events .....	18
3.3.5	Message Processing Events and Sequencing Rules .....	19
3.3.6	Timer Events.....	19
3.3.7	Other Local Events.....	19
3.4	ms-early-media Details.....	19
3.4.1	Abstract Data Model.....	19
3.4.2	Timers .....	19
3.4.3	Initialization.....	19

3.4.4	Higher-Layer Triggered Events .....	19
3.4.5	Message Processing Events and Sequencing Rules .....	19
3.4.6	Timer Events.....	20
3.4.7	Other Local Events.....	20
3.5	Anonymous Phone URI Details .....	20
3.5.1	Abstract Data Model.....	20
3.5.2	Timers .....	20
3.5.3	Initialization.....	20
3.5.4	Higher-Layer Triggered Events .....	20
3.5.5	Message Processing Events and Sequencing Rules .....	20
3.5.6	Timer Events.....	20
3.5.7	Other Local Events.....	20
3.6	ms-bypass Details.....	20
3.6.1	Abstract Data Model.....	21
3.6.2	Timers .....	21
3.6.3	Initialization.....	21
3.6.4	Higher-Layer Triggered Events .....	21
3.6.5	Message Processing Events and Sequencing Rules .....	21
3.6.6	Timer Events.....	21
3.6.7	Other Local Events.....	21
3.7	ms-accepted-content-id Details.....	21
3.7.1	Abstract Data Model.....	21
3.7.2	Timers .....	22
3.7.3	Initialization.....	22
3.7.4	Higher-Layer Triggered Events .....	22
3.7.5	Message Processing Events and Sequencing Rules .....	22
3.7.6	Timer Events.....	22
3.7.7	Other Local Events.....	22
3.8	ms-trunking-peer Details .....	22
3.8.1	Abstract Data Model.....	22
3.8.2	Timers .....	22
3.8.3	Initialization.....	22
3.8.4	Higher-Layer Triggered Events .....	22
3.8.5	Message Processing Events and Sequencing Rules .....	22
3.8.6	Timer Events.....	22
3.8.7	Other Local Events.....	23
3.9	ms-mediation-generated Details .....	23
3.9.1	Abstract Data Model.....	23
3.9.2	Timers .....	23
3.9.3	Initialization.....	23
3.9.4	Higher-Layer Triggered Events .....	23
3.9.5	Message Processing Events and Sequencing Rules .....	23
3.9.6	Timer Events.....	23
3.9.7	Other Local Events.....	23
<b>4</b>	<b>Protocol Examples .....</b>	<b>24</b>
4.1	isGateway SIP Contact Header Parameter .....	24
4.1.1	Inbound Call .....	24
4.1.1.1	Step 3: INVITE Message Is Received by the UAC .....	24
4.1.1.2	Step 7: 200 Message Is Sent from the UAC.....	25
4.1.2	Outbound Call .....	26
4.1.2.1	Step 1: INVITE Message Is Sent from the UAC .....	26
4.1.2.2	Step 13: 200 Message Is Received by the UAC .....	27
4.2	phone-context SIP URI Parameter.....	28
4.2.1	Inbound Call .....	28
4.2.1.1	Step 3: INVITE Message Is Received by the UAC .....	28
4.2.1.2	Step 7: 200 Message Is Sent from the UAC.....	29
4.2.2	Outbound Call .....	30

4.2.2.1	Step 1: INVITE Message Is Sent from the UAC .....	30
4.2.2.2	Step 13: 200 Message Is Received by the UAC .....	31
4.3	ms-call-source SIP Header .....	32
4.3.1	Inbound Call .....	32
4.3.1.1	Step 2: INVITE Message Is Received by the UAC .....	32
4.3.1.2	Step 8: INVITE Message Is Received by the UAC .....	33
4.3.1.3	Step 9: 605 Message Is Sent from the UAC .....	33
4.3.1.4	Step 12: 200 Message Is Sent from the UAC .....	34
4.3.2	Outbound Call .....	34
4.4	ms-early-media SIP Supported Header Option Tag .....	34
4.4.1	Inbound Call .....	34
4.4.2	Outbound Call .....	35
4.4.2.1	Step 1: INVITE Is Sent from the UAC .....	35
4.4.2.2	Step 7: 183 Message Is Received by the UAC .....	36
4.4.2.3	Step 13: 200 Message Is Received by the UAC .....	37
4.5	ms-bypass SIP Supported Header Option Tag .....	38
4.5.1	Inbound Call .....	38
4.5.1.1	Step 6: INVITE Message Is Received by the Protocol Client .....	39
4.5.1.2	Step 17: 200 Message Is Sent by the Protocol Client .....	40
4.5.2	Outbound Call .....	41
4.5.2.1	Step 1: INVITE Message Is Sent by the Protocol Client .....	42
4.5.2.2	Step 13: 200 OK Message Is Received by the Protocol Client .....	44
4.6	ms-accepted-content-id SIP Header .....	45
4.6.1	Inbound Call .....	45
4.6.1.1	Step 6: INVITE Message Is Received by the Protocol Client .....	45
4.6.1.2	Step 17: 200 Message Is Sent by the Protocol Client .....	47
4.6.2	Outbound Call .....	48
4.6.2.1	Step 1: INVITE Message Is Sent by the Protocol Client .....	48
4.6.2.2	Step 13: 200 Message Is Received by the Protocol Client .....	51
4.7	ms-trunking-peer SIP Header .....	51
4.7.1	Inbound Call .....	52
4.7.1.1	Step 6: INVITE Message Is Received by the Protocol Client .....	52
4.7.2	Outbound Call .....	53
4.7.2.1	Step 13: 200 Message Is Received by the Protocol Client .....	54
4.8	ms-mediation-generated SIP Header .....	54
4.8.1	Outbound Call .....	55
4.8.1.1	Step 5: 183 Message Is Received by the Protocol Client .....	55
4.8.1.2	Step 10: 180 Message Is Received by the Protocol Client .....	56
<b>5</b>	<b>Security .....</b>	<b>57</b>
5.1	Security Considerations for Implementers .....	57
5.2	Index of Security Parameters .....	57
<b>6</b>	<b>Appendix A: Product Behavior .....</b>	<b>58</b>
<b>7</b>	<b>Change Tracking .....</b>	<b>60</b>
<b>8</b>	<b>Index .....</b>	<b>61</b>

# 1 Introduction

The **Session Initiation Protocol (SIP)** for public switched telephone network (PSTN) Calls Extensions protocol consists of proprietary extensions applicable for interfacing a protocol client with other traditional telephony networks, such as the public switched telephone network (PSTN) and an enterprise private branch exchange (PBX) or IP-PBX.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

## 1.1 Glossary

This document uses the following terms:

**200 OK:** A response to indicate that the request has succeeded.

**answer:** A message that is sent in response to an **offer** that is received from an offerer.

**Augmented Backus-Naur Form (ABNF):** A modified version of Backus-Naur Form (BNF), commonly used by Internet specifications. ABNF notation balances compactness and simplicity with reasonable representational power. ABNF differs from standard BNF in its definitions and uses of naming rules, repetition, alternatives, order-independence, and value ranges. For more information, see [\[RFC5234\]](#).

**call:** A communication between peers that is configured for a multimedia conversation.

**dial plan:** The rules that govern the translation of dial strings into **SIP** and tel **URIs**, either global or local, as described in [\[RFC3966\]](#).

**dial string:** The numbers, symbols, and pauses that users enter to place a phone call. It is consumed by one or more network entities and understood in the context of the configuration of those entities. It is used to generate an address-of-record or identifier to route a **call**.

**dialog:** A peer-to-peer **Session Initiation Protocol (SIP)** relationship that exists between two user agents and persists for a period of time. A dialog is established by **SIP messages**, such as a 2xx response to an INVITE request, and is identified by a call identifier, a local tag, and a remote tag.

**domain:** A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a domain controller (DC) and host a member list that identifies all members of the domain, as well as optionally hosting the Active Directory service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5 and [\[MS-ADTS\]](#).

**E.164:** An international public telecommunication numbering plan that is used in the public switched telephone network (PSTN) and some data networks. It defines the format of telephone numbers. E.164 numbers can have a maximum of 15 digits and typically are written with a plus sign (+) prefix.

**early media:** Media, such as audio and video, that is exchanged before a specific session is accepted by the called user. During a dialog, early media occurs when the initial INVITE is sent, until the **user agent server (UAS)** generates a final response.

**fully qualified domain name (FQDN):** An unambiguous domain name that gives an absolute location in the Domain Name System's (DNS) hierarchy tree, as defined in [\[RFC1035\]](#) section 3.1 and [\[RFC2181\]](#) section 11.

**gateway:** A network edge device that bridges Microsoft Office Communications Server protocols with legacy telephony networks protocols.

**INVITE:** A **Session Initiation Protocol (SIP)** method that is used to invite a user or a service to participate in a session.

**IP-PBX:** A **PBX** that supports Voice over IP (VoIP).

**Multipurpose Internet Mail Extensions (MIME):** A set of extensions that redefines and expands support for various types of content in email messages, as described in [\[RFC2045\]](#), [\[RFC2046\]](#), and [\[RFC2047\]](#).

**offer:** A message that is sent by an offerer.

**P-Asserted-Identity (PAI):** A Session Initiation Protocol (SIP) header field, as described in [\[RFC3325\]](#), that is used by trusted entities to carry the identity of the user who is sending an SIP message as it was verified by authentication.

**private branch exchange (PBX):** A server-based telephony solution that services a specific organization or office.

**proxy:** A computer, or the software that runs on it, that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a go-between that represents all internal computers, the proxy helps protect network identities while also providing access to the Internet.

**public switched telephone network (PSTN):** Public switched telephone network is the voice-oriented public switched telephone network. It is circuit-switched, as opposed to the packet-switched networks.

**SDP answer:** A **Session Description Protocol (SDP)** message that is sent by an answerer in response to an offer that is received from an offerer.

**SDP offer:** A **Session Description Protocol (SDP)** message that is sent by an offerer.

**Session Description Protocol (SDP):** A protocol that is used for session announcement, session invitation, and other forms of multimedia session initiation. For more information see [\[MS-SDP\]](#) and [\[RFC3264\]](#).

**Session Initiation Protocol (SIP):** An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. **SIP** is defined in [\[RFC3261\]](#).

**SIP message:** The data that is exchanged between **Session Initiation Protocol (SIP)** elements as part of the protocol. An SIP message is either a request or a response.

**SIP transaction:** A **SIP transaction** occurs between a **UAC** and a **UAS**. The **SIP transaction** comprises all messages from the first request sent from the **UAC** to the **UAS** up to a final response (non-1xx) sent from the **UAS** to the **UAC**. If the request is **INVITE**, and the final response is a non-2xx, the **SIP transaction** also includes an ACK to the response. The ACK for a 2xx response to an **INVITE** request is a separate **SIP transaction**.

**Uniform Resource Identifier (URI):** A string that identifies a resource. The URI is an addressing mechanism defined in Internet Engineering Task Force (IETF) Uniform Resource Identifier (URI): Generic Syntax [\[RFC3986\]](#).

**user agent client (UAC):** A logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of **UAC** lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a **UAC** for the duration of that transaction. If it receives a request later, it assumes the role of a **user agent server (UAS)** for the processing of that transaction.



**user agent server (UAS):** A logical entity that generates a response to a **Session Initiation Protocol (SIP)** request. The response either accepts, rejects, or redirects the request. The role of the UAS lasts only for the duration of that transaction. If a process responds to a request, it acts as a UAS for that transaction. If it initiates a request later, it assumes the role of a **user agent client (UAC)** for that transaction.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [\[RFC2119\]](#). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## 1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](#).

### 1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[MS-SDPEXT] Microsoft Corporation, "[Session Description Protocol \(SDP\) Version 2.0 Extensions](#)".

[RFC2045] Freed, N., and Borenstein, N., "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996, <http://www.rfc-editor.org/rfc/rfc2045.txt>

[RFC2111] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2111, March 1997, <http://www.rfc-editor.org/rfc/rfc2111.txt>

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/rfc/rfc2119.txt>

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, June 2002, <http://www.ietf.org/rfc/rfc3261.txt>

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004, <http://www.rfc-editor.org/rfc/rfc3966.txt>

### 1.2.2 Informative References

[MS-SIPAE] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Authentication Extensions](#)".

[MS-SIPREG] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Registration Extensions](#)".

[MS-SIPRE] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Routing Extensions](#)".

[RFC3262] Rosenberg, J., and Schulzrinne, H., "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)", RFC 3262, June 2002, <http://www.ietf.org/rfc/rfc3262.txt>

[RFC3263] Rosenberg, J., and Schulzrinne, H., "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002, <http://www.ietf.org/rfc/rfc3263.txt>

[RFC3264] Rosenberg, J., and Schulzrinne, H., "An Offer/Answer Model with the Session Description Protocol (SDP)", RFC 3264, June 2002, <http://www.rfc-editor.org/rfc/rfc3264.txt>

[RFC3325] Jennings, C., Peterson, J., and Watson, M., "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002, <http://www.rfc-editor.org/rfc/rfc3325.txt>

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003, <http://www.ietf.org/rfc/rfc3515.txt>

[RFC3891] Mahy, R., Biggs, B., and Dean, R., "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004, <http://www.rfc-editor.org/rfc/rfc3891.txt>

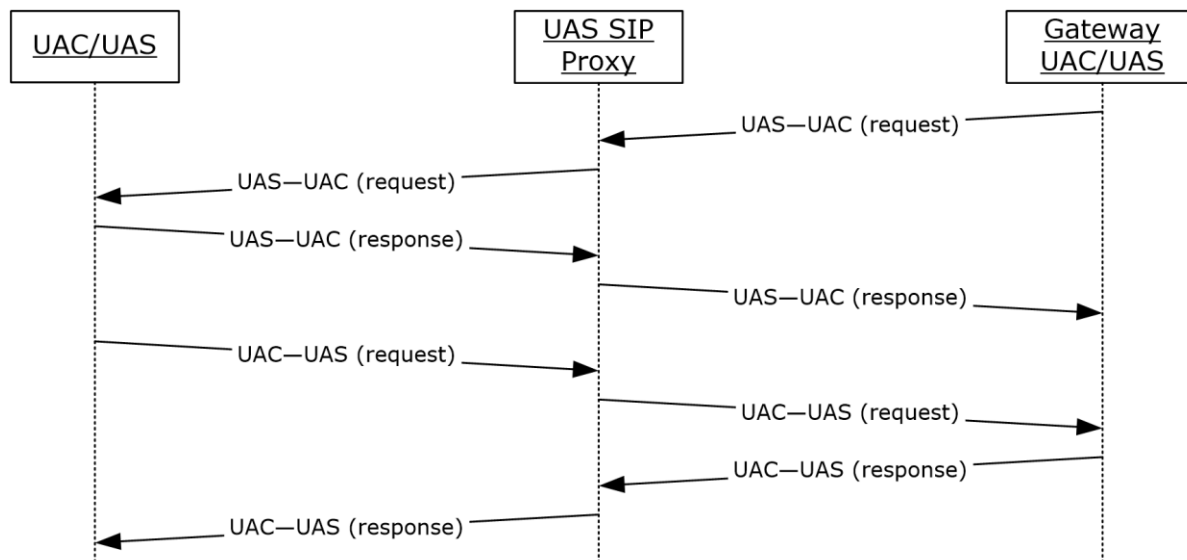
[RFC3892] Sparks, R., "The Session Initiation Protocol (SIP) Referred-By Mechanism", RFC 3892, September 2004, <http://www.rfc-editor.org/rfc/rfc3892.txt>

[RFC5234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, <http://www.rfc-editor.org/rfc/rfc5234.txt>

### 1.3 Overview

This protocol adds extensions to the **Session Initiation Protocol (SIP)**, for interfacing a protocol client with other traditional telephony networks, such as a **public switched telephone network (PSTN)** and an enterprise **private branch exchange (PBX)** or **IP-PBX**.

The logical entities that are affected by these extensions are protocol client, server (**proxy**), and **gateway** entities. The protocol client and the gateway can function as a **user agent client (UAC)** or **user agent server (UAS)**, depending on their role in the **SIP transaction**, as illustrated in the following diagram.



**Figure 1: SIP transaction**

The extensions do the following:

- Enable a SIP user agent (SIP UA) to be aware that a remote SIP UA in a SIP **dialog** is a gateway, as described in section [2.2.1](#) and section [3.1](#). This information can be rendered to the user interface (UI) to provide a better user experience (UX).
- Enable a SIP **URI** to hold an address of a **dial string** that is given by a user, as described in section [2.2.2](#) and section [3.2](#).

- Enable a SIP UAS to detect a redundant **call** that is triggered as a result of a loop, as described in section [2.2.3](#) and section [3.3](#). A loop occurs when a call is forked to a PBX that forks the call back, using a new SIP dialog.
- Enable a SIP UA to indicate that it is willing to receive an **SDP answer** through a non-reliable 183 provisional response to an **INVITE** message, as described in section [2.2.4](#) and section [3.4](#). Note that the standard recommends sending an SDP answer for **early media** only through a reliable provisional response, as described in [\[RFC3262\]](#).
- Define an anonymous phone URI, as described in section [2.2.5](#) and section [3.5](#), as an alternative to the standard anonymous SIP URI, as described in [\[RFC3261\]](#). Note that the standard anonymous SIP URI is not supported.
- Enable a SIP UA in the protocol network to indicate that it supports media bypass functionality, as described in section [2.2.6](#) and section [3.6](#). Media bypass has the media from the protocol network entity involved in a PSTN call going directly to the gateway used to interface with the PSTN for that call, without traversing any intermediate element in the protocol network.
- Enable a SIP UA in the protocol network to reference the appropriate **Session Description Protocol (SDP)** that was selected from a received **offer** when sending a **SIP message** with an **answer** to the offer, as described in section [2.2.7](#) and section [3.7](#).
- Identify the specific gateway used to interface with the PSTN for a PSTN call, as described in section [2.2.8](#) and section [3.8](#).

#### 1.4 Relationship to Other Protocols

This protocol uses the protocols as described in [\[MS-SIPAE\]](#), [\[MS-SIPREGE\]](#), [\[MS-SIPRE\]](#), and [\[MS-SDPEXT\]](#) as well as the following Internet Engineering Task Force (IETF) **Session Initiation Protocol (SIP)** specifications:

- SIP: Session Initiation Protocol, as described in [\[RFC3261\]](#).
- Session Initiation Protocol (SIP): Locating SIP Servers, as described in [\[RFC3263\]](#).
- the Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, as described in [\[RFC3325\]](#).
- the Session Initiation Protocol (SIP) Refer Method, as described in [\[RFC3515\]](#).
- the Session Initiation Protocol (SIP) "Replaces" Header, as described in [\[RFC3891\]](#).
- the Session Initiation Protocol (SIP) Referred-By Mechanism, as described in [\[RFC3892\]](#).
- an Offer/Answer Model with the Session Description Protocol (SDP), as described in [\[RFC3264\]](#).

#### 1.5 Prerequisites/Preconditions

None.

#### 1.6 Applicability Statement

This protocol is applicable for interfacing a protocol client with other traditional telephony networks, such as a **PSTN** and an enterprise **PBX** or **IP-PBX**.

## 1.7 Versioning and Capability Negotiation

This protocol does not have protocol versioning. Instead, explicit capability negotiation is done by using the **Supported** header to indicate support of various features. The **Supported** header is the standard **SIP** mechanism for doing capability negotiation.

## 1.8 Vendor-Extensible Fields

None.

## 1.9 Standards Assignments

None.

## 2 Messages

### 2.1 Transport

This protocol relies on **SIP** transport.

### 2.2 Message Syntax

This protocol uses the **SIP message** format, as specified in [\[RFC3261\]](#) section 7, and extends definitions of **URI** parameters and headers by adding new values for parameter and header names as well as their corresponding values.

#### 2.2.1 isGateway

The **isGateway** parameter is defined by this protocol as a new **Contact** header field parameter. The original **Augmented Backus-Naur Form (ABNF)**, as defined in [\[RFC5234\]](#), for the **Contact** header field, as specified in [\[RFC3261\]](#) section 25, is extended as follows. The **SIP Contact** header field extension is the second line.

```
contact-params = c-p-q / c-p-expires
                / c-p-gw
                / contact-extension
c-p-gw = "isGateway"
```

The syntax of the **Contact** header field with the **SIP Contact** header field extension is illustrated as follows. The extension is the final `;isGateway`.

```
CONTACT: <sip:a@example.com;gruu;opaque=svr:MediationServer:xxx;grid=yyy>;isGateway
```

#### 2.2.2 phone-context

This protocol extends the semantics of the *phone-context* parameter but does not change its syntax, as specified in [\[RFC3966\]](#). The *phone-context* value for a **dial string** is the provisioned location profile name of the user.

The *phone-context* extension defines the following two *phone-context* names:

- "dialstring"
- "enterprise"

The first one is used if a user location profile name is not provisioned, and the second is used if a **SIP URI** holds a phone number in a non-**E.164** format that is a result of applying enterprise **dial plan** rules.

The syntax of a SIP URI with a *phone-context* parameter is illustrated as follows:

```
sip:12345;phone-context=lp1@example.com;user=phone
```

In the previous line, `example.com` is the host part of the SIP URI. It is not affected by the *phone-context* parameter.

### 2.2.3 ms-call-source

The **ABNF**, as defined in [\[RFC5234\]](#), for the **ms-call-source** SIP header is as follows:

```
Ms-Call-Source = "Ms-Call-Source" HCOLON ("ms-rtc" / "non-ms-rtc")
```

The supported tokens for the **ms-call-source** header are "ms-rtc" and "non-ms-rtc". The first token designates that the **call** originated from a protocol server network, and the latter means that the call originated from a non-protocol server network, such as a **PSTN** or **IP-PBX**.

The syntax of this header is illustrated as follows:

```
Ms-Call-Source: ms-rtc
```

### 2.2.4 ms-early-media

The **ms-early-media** option tag is a proprietary option tag for the **SIP Supported** header, as specified in [\[RFC3261\]](#) section 20.37.

The syntax of the **ms-early-media** tag in the **Supported** header is illustrated as follows:

```
supported: ms-early-media
```

### 2.2.5 Anonymous Phone URI

The anonymous phone **URI** is an alternative to the standard anonymous **SIP** URI, as specified in [\[RFC3261\]](#). The user part of the SIP URI is set with the value "anonymous" and the parameter *user=phone* is added to the URI.

The syntax of a SIP URI with these settings is illustrated as follows:

```
sip:anonymous@contoso.com;user=phone
```

### 2.2.6 ms-bypass

The **ms-bypass** option tag is a proprietary option tag for the **SIP Supported** header, as specified in [\[RFC3261\]](#) section 20.37.

### 2.2.7 ms-accepted-content-id

The **ABNF**, as defined in [\[RFC5234\]](#), for the **ms-accepted-content-id** **SIP** header is as follows:

```
ms-accepted-content-id = "ms-accepted-content-id" HCOLON content-id
```

The **content-id** element is specified in [\[RFC2045\]](#) section 7 and [\[RFC2111\]](#) section 2. Note that the **ms-accepted-content-id** header includes the value of the **Content-ID MIME** header associated with the selected **SDP offer**.

The syntax of the **ms-accepted-content-id** header is illustrated as follows:

```
ms-accepted-content-id: <da6e05c91d6b4132afa14d8b528732e6>
```

## 2.2.8 ms-trunking-peer

The **ABNF**, as defined in [\[RFC5234\]](#), for the **ms-trunking-peer SIP** header is as follows:

```
ms-trunking-peer = "ms-trunking-peer" HCOLON host *1(SEMI trunkname) *1(SEMI User-Agent)
trunkname = "trunk" EQUAL hostname
User-Agent = "User-Agent" EQUAL quoted-string
```

The **host**, **hostname**, and **quoted-string** elements are specified in [\[RFC3261\]](#) section 25.

The syntax of the **ms-trunking-peer** header is illustrated as follows:

```
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
```

## 2.2.9 ms-mediation-generated

The **ABNF**, as defined in [\[RFC5234\]](#), for the **ms-mediation-generated SIP** header [<1>](#) is as follows:

```
ms-mediation-generated = "ms-mediation-generated" HCOLON "yes"
```

The syntax of the **ms-mediation-generated** header is illustrated as follows:

```
ms-mediation-generated: yes
```

## 3 Protocol Details

### 3.1 isGateway Details

#### UAC Behavior

If a **UAC** has a **gateway** role, it MUST insert the **isGateway** parameter in the **Contact** header. Otherwise, it MUST NOT insert this parameter in the **Contact** header.

#### UAS Behavior

If a **UAS** receives a **SIP message** with a **Contact** header that includes an **isGateway** parameter, it SHOULD render it to the application. The application MAY display this information to the user.

#### Proxy Behavior

This parameter does not affect a **SIP proxy**.

#### 3.1.1 Abstract Data Model

None.

#### 3.1.2 Timers

None.

#### 3.1.3 Initialization

None.

#### 3.1.4 Higher-Layer Triggered Events

None.

#### 3.1.5 Message Processing Events and Sequencing Rules

None.

#### 3.1.6 Timer Events

None.

#### 3.1.7 Other Local Events

None.

### 3.2 phone-context Details

#### UAC Behavior

A **UAC** that is about to send an **INVITE** message to an address of a **dial string** MUST use the following logic. If a UAC cannot resolve the dial string to a **SIP URI** with an **E.164** number of a remote party, based on local provisioning, it MUST set the SIP URI of the **Request URI** header with a phone number and a *phone-context* of the phone number in the user part of the SIP URI, as specified in [\[RFC3966\]](#) section 5.1.5. The value of the *phone-context* SIP URI parameter holds the location



profile name of the user if the dial string could not be resolved or the resolution of the dial string is to a non-E.164 number. If a user profile name is not provisioned and the dial string is not an E.164 number, the user agent MUST set *phone-context* to the default predefined **dialstring** name.

Callback presents another case where an outgoing **call** can have a **Request URI** and **To URI** containing a *phone-context* parameter. An incoming call to a UA can have a **P-Asserted-Identity (PAI)** header containing a non-E.164 number with a *phone-context* of "dialstring". Alternatively an incoming call to a UA can have a **P-Asserted-Identity** header containing a non-E.164 number with a *phone-context* of "enterprise". If the callback feature is implemented in the UA, the value of the **P-Asserted-Identity** header SHOULD be used to populate the **Request URI** and **To URI** fields in the INVITE triggered by the callback.

A UAC SHOULD<2> set a valid SIP URI in the **From** header. If the SIP URI is in a phone number format, *user=phone*, the phone number SHOULD<3> be in either E.164 format or a private number with a *phone-context* that is set with the location profile of the UAC.

### UAS Behavior

If a **UAS** has a **gateway** role, it SHOULD include a **P-Asserted-Identity** in the **200 OK** that it sends in response to an initial INVITE used to establish a **dialog**. This 200 OK is derived by using the **Request URI** from the initial INVITE used to establish the dialog. If this **Request URI** is used, and it contains an E.164 number in the user part, the UAS SHOULD copy it to the PAI. If this **Request URI** is used, and it contains a non-E.164 number in the user part, the UAS SHOULD copy it to the P-Asserted-Identity (PAI) and the *phone-context* SHOULD be set to the location profile of the UAS.

### Proxy Behavior

A SIP **proxy** that receives a SIP URI with a *phone-context* in the **Request URI** MUST try to match the *phone-context* name with a list of provisioned **dial plan** names. If there is a match, it MUST convert the SIP URI based on the rules that are defined in the matched dial plan. Otherwise if there is no match, it SHOULD use other proxy logic to route this URI.

A **P-Preferred-Identity** header is a SIP header field, as described in section 9.2 of [\[RFC3325\]](#), which carries the preferred identity for the user sending the **SIP message**. This header field is sent by a UA to a trusted proxy to be inserted as the value in the P-Asserted-Identity (PAI) header field.

A SIP proxy that receives an INVITE that contains a *phone-context* in the **From URI** SHOULD<4> try to match the *phone-context* name with a list of provisioned dial plan names. If there is a match, and the INVITE does not contain a P-Asserted-Identity (PAI) or **P-Preferred-Identity** header, the proxy SHOULD<5> apply the rules defined in the matched dial plan and add a P-Asserted-Identity (PAI) with the result of the translation. If the result of the translation is not an E.164 number, the proxy SHOULD<6> insert a *phone-context* with the value "enterprise".

### 3.2.1 Abstract Data Model

None.

### 3.2.2 Timers

None.

### 3.2.3 Initialization

None.

### 3.2.4 Higher-Layer Triggered Events

None.

### 3.2.5 Message Processing Events and Sequencing Rules

None.

### 3.2.6 Timer Events

None.

### 3.2.7 Other Local Events

None.

## 3.3 ms-call-source Details

### UAC Behavior

If the **UAC** is a **gateway**, it MUST insert an **ms-call-source** header in the **SIP INVITE** message that is sent to a **UAS** with the value "ms-rtc".

If the UAC is a gateway, it MUST insert an **ms-call-source** header in the SIP INVITE message that is sent to the **PSTN** with the value "non-ms-rtc".

If the UAC is not a gateway, it MUST NOT insert an **ms-call-source** header in an INVITE message.

### UAS Behavior

If a UAS receives an INVITE message with an **ms-call-source** header while in alerting state in another SIP **dialog**, it MUST reject the INVITE message with a 605 error code. Otherwise, it processes the INVITE as a regular INVITE message.

### Proxy Behavior

If a SIP **proxy** receives an INVITE with an **ms-call-source** header and the **call** is forwarded to a different user based on the forwarding rules of the original user, it MUST strip the header.

If a SIP proxy receives an INVITE with an **ms-call-source** header and it forwards the INVITE to a user who is not provisioned to receive loop calls, as described in section [1.3](#), it MUST strip this header.

If a SIP proxy receives a 605 message to an INVITE message that includes the **ms-call-source header**, it MUST send back a 480 message to the previous hop.

### 3.3.1 Abstract Data Model

None.

### 3.3.2 Timers

None.

### 3.3.3 Initialization

None.

### 3.3.4 Higher-Layer Triggered Events

None.

### 3.3.5 Message Processing Events and Sequencing Rules

None.

### 3.3.6 Timer Events

None.

### 3.3.7 Other Local Events

None.

## 3.4 ms-early-media Details

### UAC Behavior

If a **UAC** supports an **SDP answer** in a non-reliable 183 provisional response to an **INVITE** message, it **MUST** send a **SIP Supported** header with the **ms-early-media** option tag. The **SDP** content and the procedure for starting **early media** are specified in [\[MS-SDPEXT\]](#) section 3.1.5.12.

### UAS Behavior

A **UAS** with a **gateway** role that receives an **INVITE** with a **Supported** header that includes an **ms-early-media** option tag **MUST** send an unreliable 183 provisional response with an **SDP answer**. The **SDP** content and the procedure for starting early media are specified in [\[MS-SDPEXT\]](#) section 3.1.5.12.

A **UAS** with a non-gateway role that receives an **INVITE** with a **Supported** header that includes an **ms-early-media** option tag **MAY** send an unreliable 183 provisional response with an **SDP answer**. The **SDP** content and the procedure for starting early media are specified in [\[MS-SDPEXT\]](#) section 3.1.5.12.

### Proxy Behavior

There is no special handling for this extension for a **SIP proxy**.

### 3.4.1 Abstract Data Model

None.

### 3.4.2 Timers

None.

### 3.4.3 Initialization

None.

### 3.4.4 Higher-Layer Triggered Events

None.

### 3.4.5 Message Processing Events and Sequencing Rules

None.

### 3.4.6 Timer Events

None.

### 3.4.7 Other Local Events

None.

## 3.5 Anonymous Phone URI Details

The special **URI** "anonymous@host;user=phone" in the **From** header field MUST be used to denote an anonymous user. <7> The *host* portion contains the IP address, **fully qualified domain name (FQDN)**, or **domain** of the user. The encoding for an anonymous user that uses "anonymous.invalid" in the *host* portion MUST NOT be used.

### 3.5.1 Abstract Data Model

None.

### 3.5.2 Timers

None.

### 3.5.3 Initialization

None.

### 3.5.4 Higher-Layer Triggered Events

None.

### 3.5.5 Message Processing Events and Sequencing Rules

None.

### 3.5.6 Timer Events

None.

### 3.5.7 Other Local Events

None.

## 3.6 ms-bypass Details

A user agent (UA) supporting media bypass SHOULD <8> include a **Session Initiation Protocol (SIP) Supported** header with the **ms-bypass** option tag whenever it advertises the options it supports. Media bypass has the media from the protocol network entity involved in a **public switched telephone network (PSTN)** call going directly to the gateway used to interface with the PSTN for that call, without traversing any intermediate element in the protocol network.

### 3.6.1 Abstract Data Model

None.

### 3.6.2 Timers

None.

### 3.6.3 Initialization

None.

### 3.6.4 Higher-Layer Triggered Events

None.

### 3.6.5 Message Processing Events and Sequencing Rules

None.

### 3.6.6 Timer Events

None.

### 3.6.7 Other Local Events

None.

## 3.7 ms-accepted-content-id Details

This section describes the **ms-accepted-content-id** **SIP** header. <9>

### UAC Behavior

A **UAC** MUST include a **Content-ID MIME** header with each **Multipurpose Internet Mail Extensions (MIME)** type of "application/SDP" and "application/gw-sdp" that it sends in an **offer**. The **SDP** content is specified in [\[MS-SDPEXT\]](#) section 3.

### UAS Behavior

A **UAS** MUST include an **ms-accepted-content-id** SIP header in a **SIP message** containing an **SDP answer** if the selected SDP from the offer with which the **answer** is associated contained a **Content-ID MIME** header. The value of the **Content-ID MIME** header from the selected SDP in the offer MUST be copied as the value for the **ms-accepted-content-id** header.

### Proxy Behavior

This parameter does not affect a SIP proxy.

### 3.7.1 Abstract Data Model

None.

### **3.7.2 Timers**

None.

### **3.7.3 Initialization**

None.

### **3.7.4 Higher-Layer Triggered Events**

None.

### **3.7.5 Message Processing Events and Sequencing Rules**

None.

### **3.7.6 Timer Events**

None.

### **3.7.7 Other Local Events**

None.

## **3.8 ms-trunking-peer Details**

The **ms-trunking-peer Session Initiation Protocol (SIP)** header is included by a SIP UA that has a **gateway** role. It is used to identify the specific gateway used to interface with the **public switched telephone network (PSTN)** for a PSTN **call**.<10>

### **3.8.1 Abstract Data Model**

None.

### **3.8.2 Timers**

None.

### **3.8.3 Initialization**

None.

### **3.8.4 Higher-Layer Triggered Events**

None.

### **3.8.5 Message Processing Events and Sequencing Rules**

None.

### **3.8.6 Timer Events**

None.

### 3.8.7 Other Local Events

None.

## 3.9 ms-mediation-generated Details

The **ms-mediation-generated Session Initiation Protocol (SIP)** header is included by a SIP UA that has a **gateway** role. [<11>](#) It is used in provisional responses to indicate that the response was auto-generated by the UA and is not forwarded from a gateway used to interface with the **public switched telephone network (PSTN)** for a PSTN **call**.

### 3.9.1 Abstract Data Model

None.

### 3.9.2 Timers

None.

### 3.9.3 Initialization

None.

### 3.9.4 Higher-Layer Triggered Events

None.

### 3.9.5 Message Processing Events and Sequencing Rules

None.

### 3.9.6 Timer Events

None.

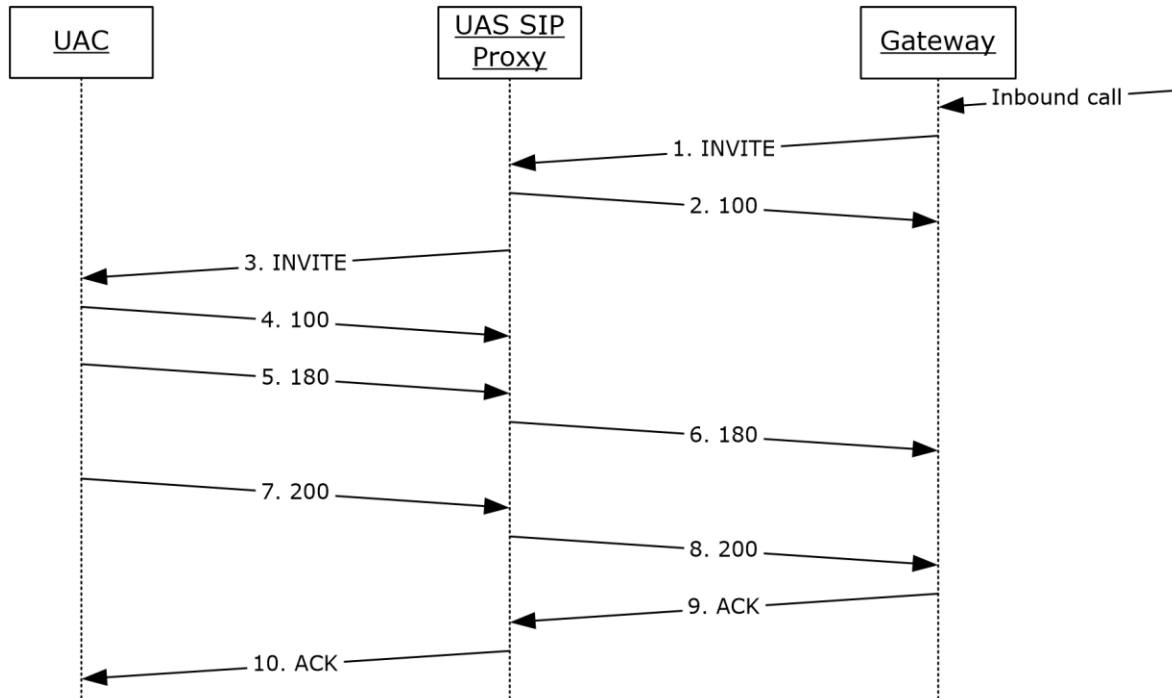
### 3.9.7 Other Local Events

None.

## 4 Protocol Examples

### 4.1 isGateway SIP Contact Header Parameter

#### 4.1.1 Inbound Call



**Figure 2: Inbound call**

The preceding figure includes only one message in each direction because other messages repeat the same values.

The messages in the following subsections illustrate the use of the **Contact** header **isGateway** parameter in messages that are sent from and received by a protocol client.

##### 4.1.1.1 Step 3: INVITE Message Is Received by the UAC

```
INVITE sip:10.56.66.167:1501;transport=tls;ms-opaque=56d3073f52;ms-received-cid=8000
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-
identity=C8yb10ausk5JrrJOeabpGevnl7YoohtFBsEB3Oy33pmWwR9xH_oTAlgAA;ms-route-
sig=ea0mlvIX8ijETotqsV9nVQESDR_2qwR9xH_oTAlgAA>;tag=D78DE2B2FF72EB24FDA98B88DCC879B2
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-
internal-info="daqI8alfcNqkUHDJyMoUxdQudrDTCwR9xH7 OEdQAA"
Authentication-Info: Kerberos
rspauth="602306092A864886F71201020201011100FFFFFFFF1125B31E1322F6E6A4E65212D8DEDCA4",
srand="A8085D66", snum="58", opaque="C216B7E9", qop="auth",
targetname="sip/media.example.com", realm="SIP Communications Service"
Max-Forwards: 69
Content-Length: 1606
Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bK27555a4e;ms-received-port=2861;ms-
received-cid=8900
```

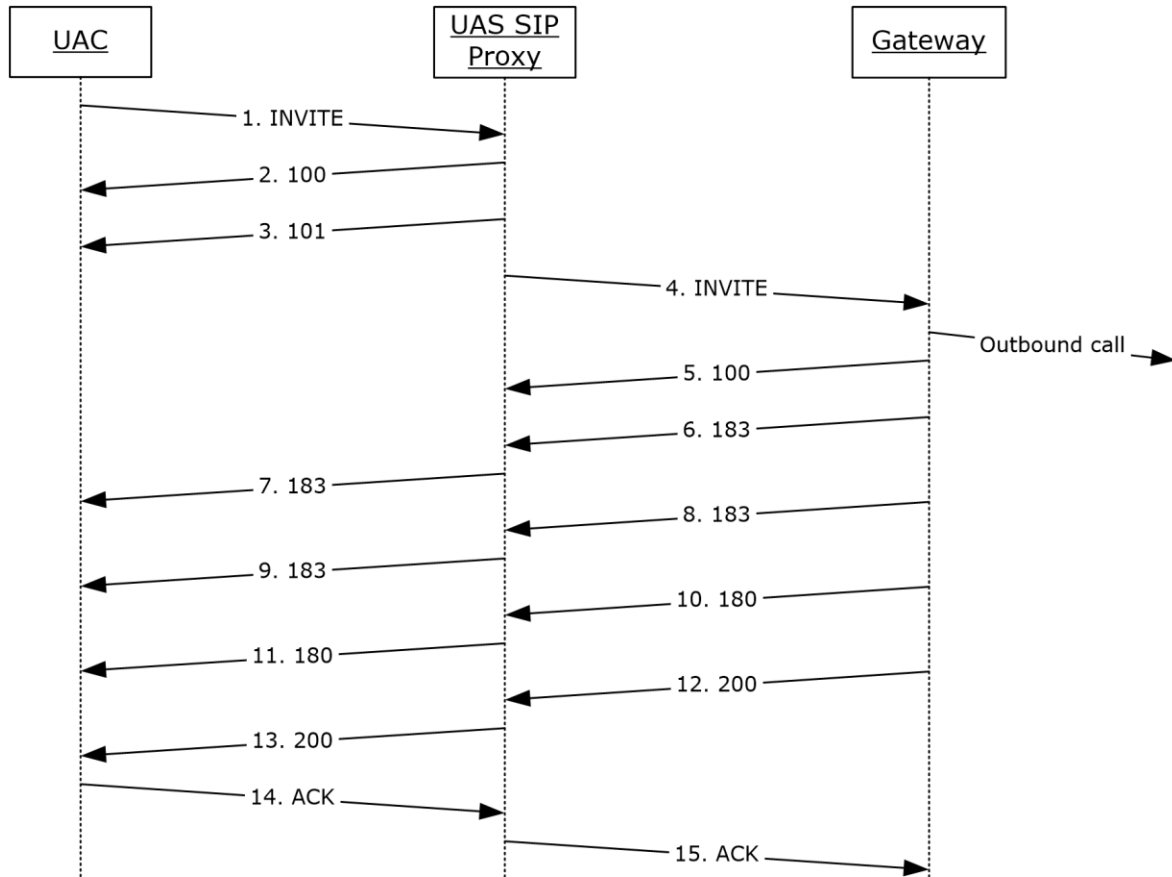


From: <sip:anonymous@server1.example.com;user=phone>;epid=571F84BB45;tag=ed77bad0f0  
To: <sip:7275036;phone-context=normal-loc@server1.example.com;user=phone>;epid=782abb8f70  
CSeq: 6 INVITE  
Call-ID: 46bac89b-3f5f-4f1f-bb0b-e791706e2401  
Contact:  
<sip:server1.example.com@server1.example.com;gruu;opaque=srvr:MediationServer:ANaNrdcy8Em  
B-dKmljqX-wAA;grid=9b192c6b829d4373adb88ea9ef4dff03>;isGateway  
Supported: replaces  
Supported: gruu-10  
User-Agent: RTCC/3.0.0.0 MediationServer  
Content-Type: application/sdp; charset=utf-8

#### 4.1.1.2 Step 7: 200 Message Is Sent from the UAC

SIP/2.0 200 OK  
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-internal-info="daqI8alfcNQkUHDJyMoUxdQuodrDTCwR9xH7\_OEdQAA"  
Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bK27555a4e;ms-received-port=2861;ms-received-cid=8900  
From: <sip:anonymous@server1.example.com;user=phone>;epid=571F84BB45;tag=ed77bad0f0  
To: "" <sip:7275036;phone-context=normal-loc@server1.example.com;user=phone>;epid=782abb8f70;tag=8827660e0c  
Call-ID: 46bac89b-3f5f-4f1f-bb0b-e791706e2401  
CSeq: 6 INVITE  
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-identity=C8ybl0ausk5JrrJOeabpGevnl7YoohtFBsEB3Oy33pmWwR9xH\_oTAlgAA;ms-route-sig=ea0mlvIX8ijETotqsV9nVQESDR\_2qwR9xH\_oTAlgAA>;tag=D78DE2B2FF72EB24FDA98B88DCC879B2  
Contact: <sip:alice@server1.example.com;opaque=user:epid:reTyjuqAaVmcCIO4qlA4vwAA;gruu>  
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)  
P-Preferred-Identity: <sip:alice@server1.example.com>, <tel:+15555550103>  
Proxy-Authorization: Kerberos qop="auth", realm="SIP Communications Service", opaque="C216B7E9", crand="dde2ad45", cnum="44", targetname="sip/server1.example.com", response="602306092a864886f71201020201011100ffffffff77de9d7a16f9693a9cc29ed8d6735499"  
Content-Type: application/sdp

## 4.1.2 Outbound Call



**Figure 3: Outbound call**

The preceding figure includes only one message in each direction because other messages repeat the same values.

The messages in the following subsections illustrate the use of the **Contact** header **isGateway** parameter in messages that are sent from and received by a **UAC**.

### 4.1.2.1 Step 1: INVITE Message Is Sent from the UAC

```
INVITE sip:+15555550103@server1.example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.66.167:1501
Max-Forwards: 70
From: <sip:alice@server1.example.com>;tag=85e83db3c6;epid=782abb8f70
To: <sip:+15555550103@server1.example.com;user=phone>
Call-ID: accd397afad9439d880f45cfce04bd66
CSeq: 1 INVITE
Contact: <sip:alice@server1.example.com;opaque=user:epid:reTyjuqAaVmcCIO4qlA4vwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
Ms-Conversation-ID: AchdT5LJJvFktNrrSjejQUAy0wgfoA==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
```

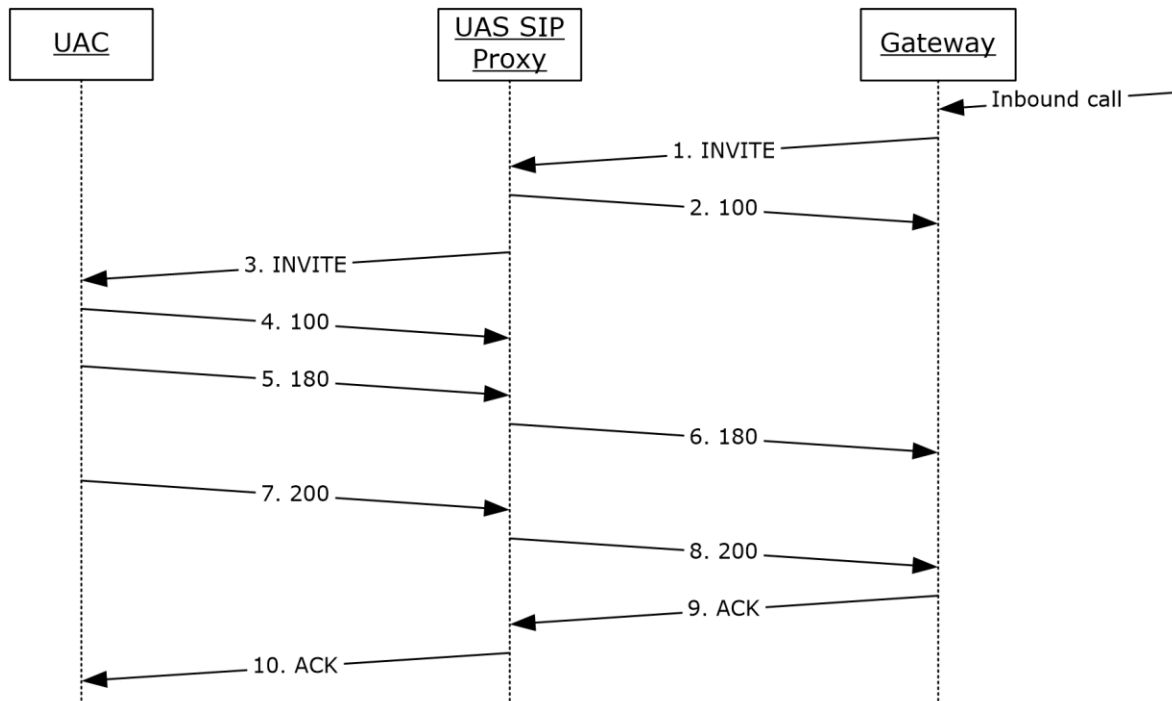
P-Preferred-Identity: <sip:alice@server1.example.com>, <tel:+15555550103>  
Supported: ms-conf-invite  
Proxy-Authorization: Kerberos qop="auth", realm="SIP Communications Service",  
opaque="C216B7E9", crand="aeee0f50", cnum="35", targetname="sip/server1.example.com",  
response="602306092a864886f71201020201011100fffffffffec51ac48141bf21d6a1487eaca68cca6"  
Content-Type: application/sdp  
Content-Length: 1076

#### 4.1.2.2 Step 13: 200 Message Is Received by the UAC

```
SIP/2.0 200 OK
Authentication-Info: Kerberos
rspauth="602306092A864886F71201020201011100FFFFFFFFF0714800DE2F658803052D07C86052224",
srand="B997073B", snum="50", opaque="C216B7E9", qop="auth",
targetname="sip/server1.example.com", realm="SIP Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:1501;ms-received-port=1501;ms-received-cid=8000
FROM: "alice"<sip:alice@server1.example.com>;tag=85e83db3c6;epid=782abb8f70
TO: <sip:+15555550103@server1.example.com;user=phone>;epid=571F84BB45;tag=a0f83282b
CSEQ: 1 INVITE
CALL-ID: accd397afad9439d880f45cfce04bd66
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-route-
sig=eab5PYPD_tLMiadtWiQ5tem-72y4vocRve_oTAlgAA>
CONTACT:
<sip:server1.example.com@server1.example.com;gruu;opaque=svr:MediationServer:ANaNRdcy8Em
B-dKmljqX-wAA;grid=439be8c54ef04ce0baa8842286f86c53>;isGateway
CONTENT-LENGTH: 1412
SUPPORTED: gruu-10
SUPPORTED: replaces
CONTENT-TYPE: application/sdp; charset=utf-8
ALLOW: UPDATE
P-ASSERTED-IDENTITY: <sip:+15555550103@server1.example.com;user=phone>
SERVER: RTCC/3.0.0.0 MediationServer
ALLOW: Ack, Cancel, Bye, Invite, Refer
```

## 4.2 phone-context SIP URI Parameter

### 4.2.1 Inbound Call



**Figure 4: Inbound call**

The preceding figure includes one message in each direction because other messages repeat the same values.

The messages in the following subsections illustrate the use of the *phone-context* parameter in messages that are sent from and received by the **UAC**.

#### 4.2.1.1 Step 3: INVITE Message Is Received by the UAC

A **UAS proxy** replaces the **Request URI** header with the *phone-context* parameter that is received from the **gateway**. However, the **To** header is not replaced and holds the **SIP URI** with the *phone-context* that was inserted by the gateway.

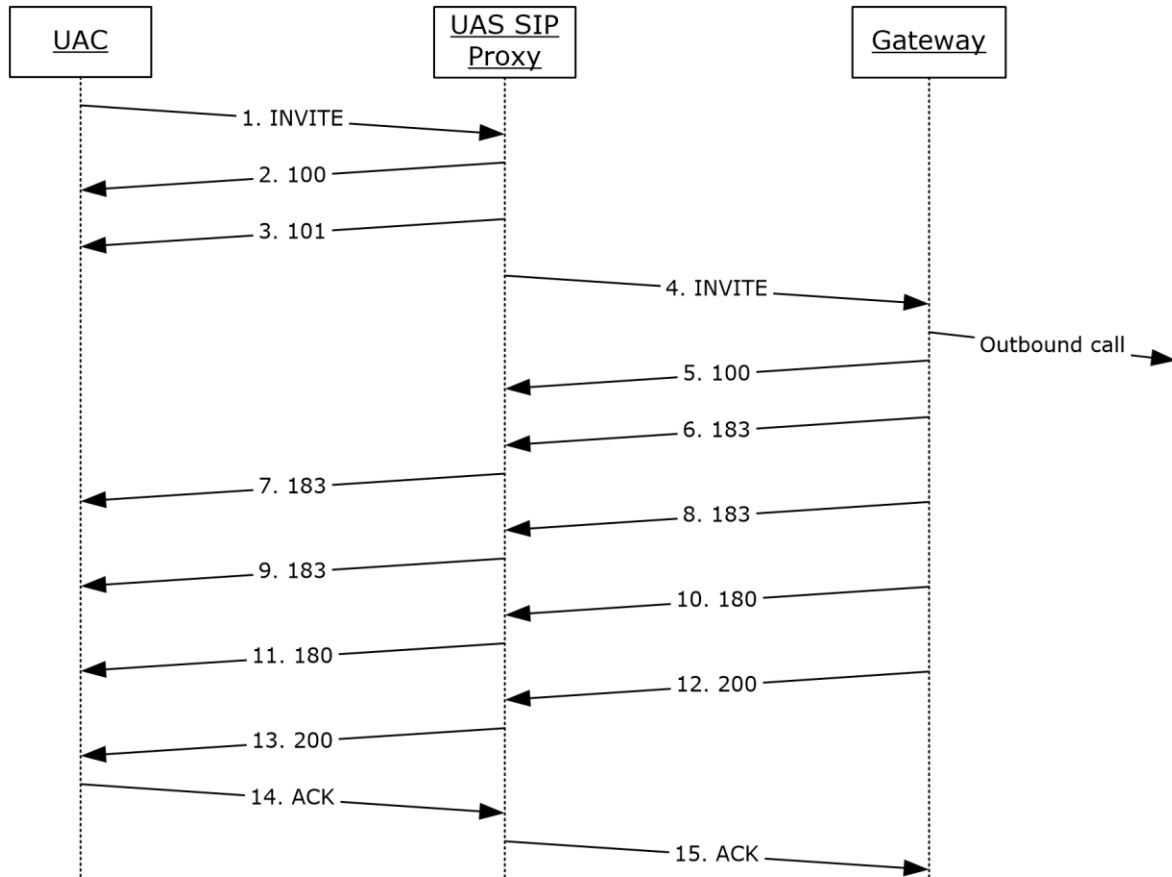
```
INVITE sip:10.56.66.167:1501;transport=tls;ms-opaque=56d3073f52;ms-received-cid=8000
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-
identity=C8ybl0ausk5JrrJOeabpGevnl7YoohtFBsEB3Oy33pmWwR9xH_oTAlgAA;ms-route-
sig=ea0mlvIX8ijETotqsV9nVQESDR_2qwR9xH_oTAlgAA>;tag=D78DE2B2FF72EB24FDA98B88DCC879B2
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-
internal-info="daqI8a1fcNQkUHDJyMoUxdQuDrDTCwR9xH7_OEdQAA"
Authentication-Info: Kerberos
rspauth="602306092A864886F71201020201011100FFFFFFFF1125B31E1322F6E6A4E65212D8DEDCA4",
srand="A8085D66", snum="58", opaque="C216B7E9", qop="auth",
targetname="sip/server1.example.com", realm="SIP Communications Service"
Max-Forwards: 69
Content-Length: 1606
Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bK27555a4e;ms-received-port=2861;ms-
received-cid=8900
From: <sip:+1555550103@server1.example.com;user=phone>;epid=571F84BB45;tag=ed77bad0f0
```

To: <sip:7275036;phone-context=normal-loc@server1.example.com;user=phone>;epid=782abb8f70  
CSeq: 6 INVITE  
Call-ID: 46bac89b-3f5f-4f1f-bb0b-e791706e2401  
Contact:  
<sipserver1.example.com@server1.example.com;gruu;opaque=srvr:MediationServer:ANaNrdcy8EmB  
-dKmljqX-wAA;grid=9b192c6b829d4373adb88ea9ef4dff03>;isGateway  
Supported: replaces  
Supported: gruu-10  
User-Agent: RTCC/3.0.0.0 MediationServer  
Content-Type: application/sdp; charset=utf-8

#### 4.2.1.2 Step 7: 200 Message Is Sent from the UAC

SIP/2.0 200 OK  
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-internal-info="daqI8alfcNqkUHDJyMoUxdQuDrDTCwR9xH7\_OEdQAA"  
Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bK27555a4e;ms-received-port=2861;ms-received-cid=8900  
From: <sip:+15555550103@server1.example.com;user=phone>;epid=571F84BB45;tag=ed77bad0f0  
To: "" <sip:7275036;phone-context=normal-loc@server1.example.com;user=phone>;epid=782abb8f70;tag=8827660e0c  
Call-ID: 46bac89b-3f5f-4f1f-bb0b-e791706e2401  
CSeq: 6 INVITE  
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-identity=C8yb10ausk5JrrJOeabpGevnl7YoohctFBsEB3Oy33pmWwR9xH\_oTAlgAA;ms-route-sig=ea0mlvIX8ijETotqsV9nVQESDR\_2qwR9xH\_oTAlgAA>;tag=D78DE2B2FF72EB24FDA98B88DCC879B2  
Contact: <sip:alice@server1.example.com;opaque=user:epid:reTyjuqAaVmcCIO4qlA4vwAA;gruu>  
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)  
P-Preferred-Identity: <sip:alice@server1.example.com>, <tel:+15555550106>  
Proxy-Authorization: Kerberos qop="auth", realm="SIP Communications Service", opaque="C216B7E9", crand="dde2ad45", cnum="44", targetname="sip/server1.example.com", response="602306092a864886f71201020201011100ffffffffff77de9d7a16f9693a9cc29ed8d6735499"  
Content-Type: application/sdp

## 4.2.2 Outbound Call



**Figure 5: Outbound call**

The preceding figure includes one message in each direction because other messages repeat the same values.

The messages in the following subsections illustrate the use of the *phone-context* parameter in messages that are sent from and received by a **UAC**.

### 4.2.2.1 Step 1: INVITE Message Is Sent from the UAC

```
INVITE sip:72181;phone-context=dialstring@example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.64.148:4031
Max-Forwards: 70
From: <sip:test2@example.com>;tag=cefe741803;epid=7d725e08a1
To: <sip:72181;phone-context=dialstring@example.com;user=phone>
Call-ID: a6a53b0e3b7d40a3b445dc4d9249b6fe
CSeq: 1 INVITE
Contact: <sip:test2@example.com;opaque=user:epid:00NaA0AXIFCRDgr367kcHwAA;gruu>
User-Agent: UCCP/2.0.6362.36 OC/2.0.6362.36 (Client)
Ms-Conversation-ID: Achis3b6kqiLEhnZR/+DMH2N7CO9hg==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
```

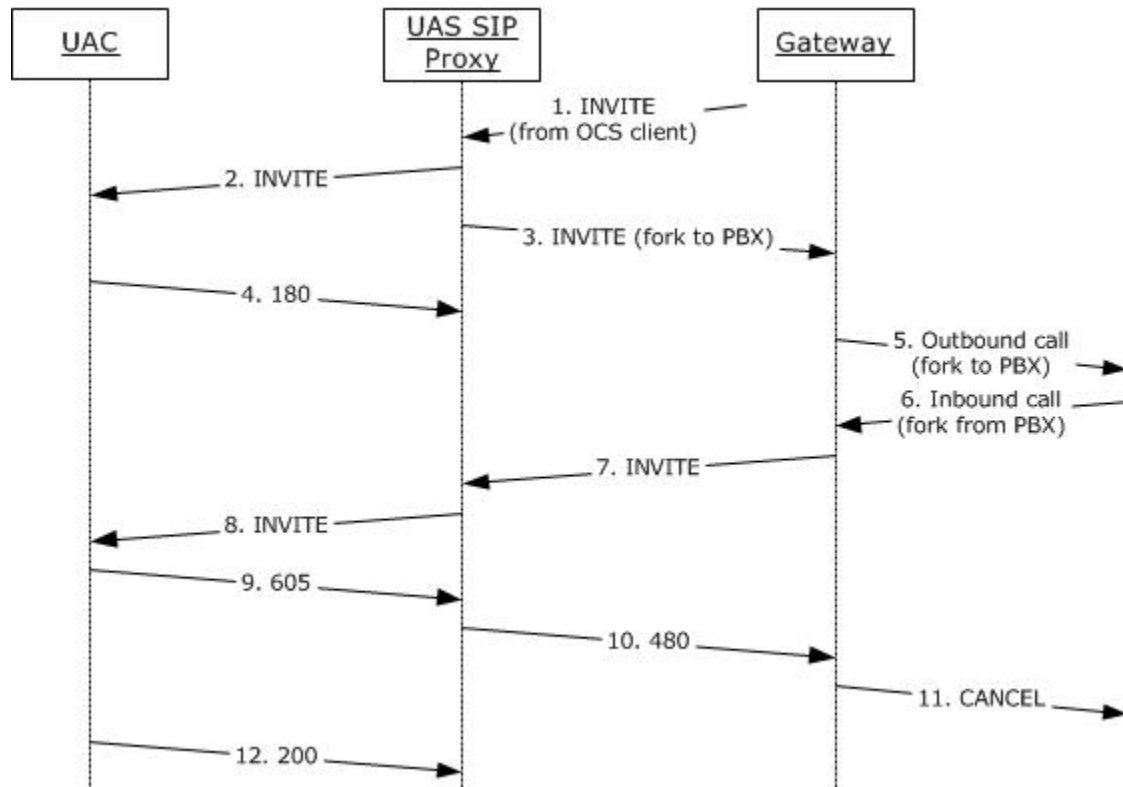
P-Preferred-Identity: <sip:test2@example.com>, <tel:+15555550100>  
Supported: ms-conf-invite  
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",  
opaque="9ACB05CE", crand="05c62674", cnum="10", targetname="server1.example.com",  
response="01000000b09f0702d4e4e934e25e6f9b"  
Content-Type: application/sdp

#### 4.2.2.2 Step 13: 200 Message Is Received by the UAC

```
SIP/2.0 200 OK
Authentication-Info: NTLM rspauth="01000000653865359728F3C8E25E6F9B", srand="8A3F6211",
snum="19", opaque="9ACB05CE", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Via: SIP/2.0/TLS 10.56.64.148:4031;ms-received-port=4031;ms-received-cid=500
FROM: "test2"<sip:test2@example.com>;tag=cefe741803;epid=7d725e08a1
TO: <sip:72181;phone-
context=dialstring@example.com;user=phone>;epid=6477F45221;tag=a5c53ff9d6
CSEQ: 1 INVITE
CALL-ID: a6a53b0e3b7d40a3b445dc4d9249b6fe
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-route-
sig=aaabLHUMznhhFXTzutN9dwpQ-RmwQYZA_UIeyt1QAA>
CONTACT: <sip:SH13-
LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXhNJb1ZwQfgAA;gri
d=f1f9379bd9334f65aa1dfb77bed58905>;isGateway
CONTENT-LENGTH: 740
SUPPORTED: gruu-10
SUPPORTED: replaces
CONTENT-TYPE: application/sdp; charset=utf-8
```

## 4.3 ms-call-source SIP Header

### 4.3.1 Inbound Call



**Figure 6: Inbound call**

The preceding figure includes only key messages that are described in this section.

The messages in the following subsections illustrate the use of the **ms-call-source** header in messages that are sent from and received by a **UAC**.

#### 4.3.1.1 Step 2: INVITE Message Is Received by the UAC

This **call** originates from a protocol client; therefore, it does not include an **ms-call-source** header.

```
INVITE sip:10.56.66.167:3080;transport=tls;ms-opaque=0e2b3bcc10;ms-received-cid=300
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-to;ms-role-rs-
from;lr;ms-route-sig=aalPYPsX-
ubLAoi5ZiOqMHlGcU3l0xkBBiLt2WZQAA>;tag=8951C70C798E10EA48EB96EAA4B379BC
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bK76F2CFD5.31901062;branched=TRUE;ms-
internal-info="aaC8UGYE_vlAjm36glJ1-v1NQi15UxxBBihbkIPAAA"
Authentication-Info: NTLM rspauth="0100000044415441C22E2F66F9C08F09", srand="4CB6D6F5",
snum="31", opaque="FB347BC6", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Max-Forwards: 69
Content-Length: 1074
Via: SIP/2.0/TLS 10.56.64.148:3981;ms-received-port=3981;ms-received-cid=200
P-Asserted-Identity: "test2"<sip:test2@example.com>,<tel:+15555550100>
From: "test2"<sip:test2@example.com>;tag=08399379aa;epid=7d725e08a1
To: <sip:test1@example.com>;epid=782abb8f70
Call-ID: ee22d219e9f44441bbac7b304ddc1096
```



```
CSeq: 1 INVITE
Contact: <sip:test2@example.com;opaque=user:epid:00NaA0AXIFCRDgr367kcHwAA;gruu>
User-Agent: UCCP/2.0.6362.36 OC/2.0.6362.36 (Client)
Ms-Conversation-ID: AchisczVZkuxUO7mTZieBaNoXIHJ8g==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
Supported: ms-conf-invite
Content-Type: application/sdp
```

#### 4.3.1.2 Step 8: INVITE Message Is Received by the UAC

This **call** originates from the **private branch exchange (PBX)**; therefore, it includes an **ms-call-source** header.

```
INVITE sip:10.56.66.167:3080;transport=tls;ms-opaque=0e2b3bcc10;ms-received-cid=300
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-
identity=B5buGzyhwo49ocK0aabbgxdAqaQRu_k9cZxy4WI-659Sq6MHw6Lt2WZQAA;ms-route-
sig=aa3Oeh935IYJmaV5AyTn4katb_Zd-6MHw6Lt2WZQAA>;tag=8951c70c798e10ea48eb96eaa4b379bc
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bKD300E89E.BA307C3A;branched=TRUE;ms-
internal-info="aaKlz4lwQeqhL-R5X7wnN8hEhuJwK6MHw6hbkiPAAA"
Authentication-Info: NTLM rspauth="0100000000000000A761D372F9C08F09", srand="51ED7291",
snum="32", opaque="FB347BC6", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Max-Forwards: 69
Content-Length: 934
Via: SIP/2.0/TLS 10.198.92.126:4757;branch=z9hG4bK557e25e3;ms-received-port=4757;ms-
received-cid=700
From: <sip:2160;phone-
context=dialstring@example.com;user=phone>;epid=6477F45221;tag=a3a3579bb
To: <sip:+1555550108@example.com;user=phone>;epid=782abb8f70
CSeq: 179 INVITE
Call-ID: 729ab37d-c0f5-4ad7-b7e0-8f3dad99065
Contact: <sip:SH13-
LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXhNJb1ZwQfgAA;gri
d=2cfb52f9fd4b4930a6f0a82dbfcd39e4>;isGateway
Supported: replaces
Supported: gruu-10
User-Agent: RTCC/3.0.0.0 MediationServer
Content-Type: application/sdp; charset=utf-8
Allow: UPDATE
Allow: Ack, Cancel, Bye, Invite, Refer
Ms-Call-Source: non-ms-rtc
```

#### 4.3.1.3 Step 9: 605 Message Is Sent from the UAC

This **INVITE** is rejected with a 605 Decline because it originated as a result of a loop in the **private branch exchange (PBX)**.

```
SIP/2.0 605 Decline Everywhere
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bKD300E89E.BA307C3A;branched=TRUE;ms-
internal-info="aaKlz4lwQeqhL-R5X7wnN8hEhuJwK6MHw6hbkiPAAA"
Via: SIP/2.0/TLS 10.198.92.126:4757;branch=z9hG4bK557e25e3;ms-received-port=4757;ms-
received-cid=700
From: <sip:2160;phone-
context=dialstring@example.com;user=phone>;epid=6477F45221;tag=a3a3579bb
To: "" <sip:+1555550108@example.com;user=phone>;epid=782abb8f70;tag=b9bc5b444c
Call-ID: 729ab37d-c0f5-4ad7-b7e0-8f3dad99065
CSeq: 179 INVITE
```

```
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-identity=B5buGzyhwo49ocK0aabbgxdAqaQRu_k9cZxy4WI-659Sq6MHw6Lt2WZQAA;ms-route-sig=aa30eh935IYJmaV5AyTn4katb_Zd-6MHw6Lt2WZQAA>;tag=8951c70c798e10ea48eb96eaa4b379bc
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
Ms-client-diagnostics: 52034; reason="Rejected Duplicate call from PBX"
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service", opaque="FB347BC6", crand="b062a12e", cnum="29", targetname="server1.example.com", response="01000000730069006642f8a9f9c08f09"
Content-Length: 0
```

#### 4.3.1.4 Step 12: 200 Message Is Sent from the UAC

The first **INVITE** from a protocol client is accepted and the following **200 OK** is sent.

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bK76F2CFD5.31901062;branched=TRUE;ms-internal-info="aaC8UGYE_vlAjm36glJ1-v1NQi15UxkBBihbkIPAAA"
Via: SIP/2.0/TLS 10.56.64.148:3981;ms-received-port=3981;ms-received-cid=200
From: "test2"<sip:test2@example.com>;tag=08399379aa;epid=7d725e08a1
To: "" <sip:test1@example.com>;epid=782abb8f70;tag=281b612cd0
Call-ID: ee22d219e9f44441bbac7b304ddc1096
CSeq: 1 INVITE
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-to;ms-role-rs-from;lr;ms-route-sig=aalPYPSx-ubLAoi5ZiOqMh1GcU3l0xkBBiLt2WZQAA>;tag=8951c70c798e10ea48eb96eaa4b379bc
Contact: <sip:test1@example.com;opaque=user:epid:reTyjuqAaVmccIO4qlA4vwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
P-Preferred-Identity: <sip:test1@example.com>, <tel:+15555550100>
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service", opaque="FB347BC6", crand="1b602324", cnum="30", targetname="server1.example.com", response="010000006895aa03478d7d34f9c08f09"
Content-Type: application/sdp
```

### 4.3.2 Outbound Call

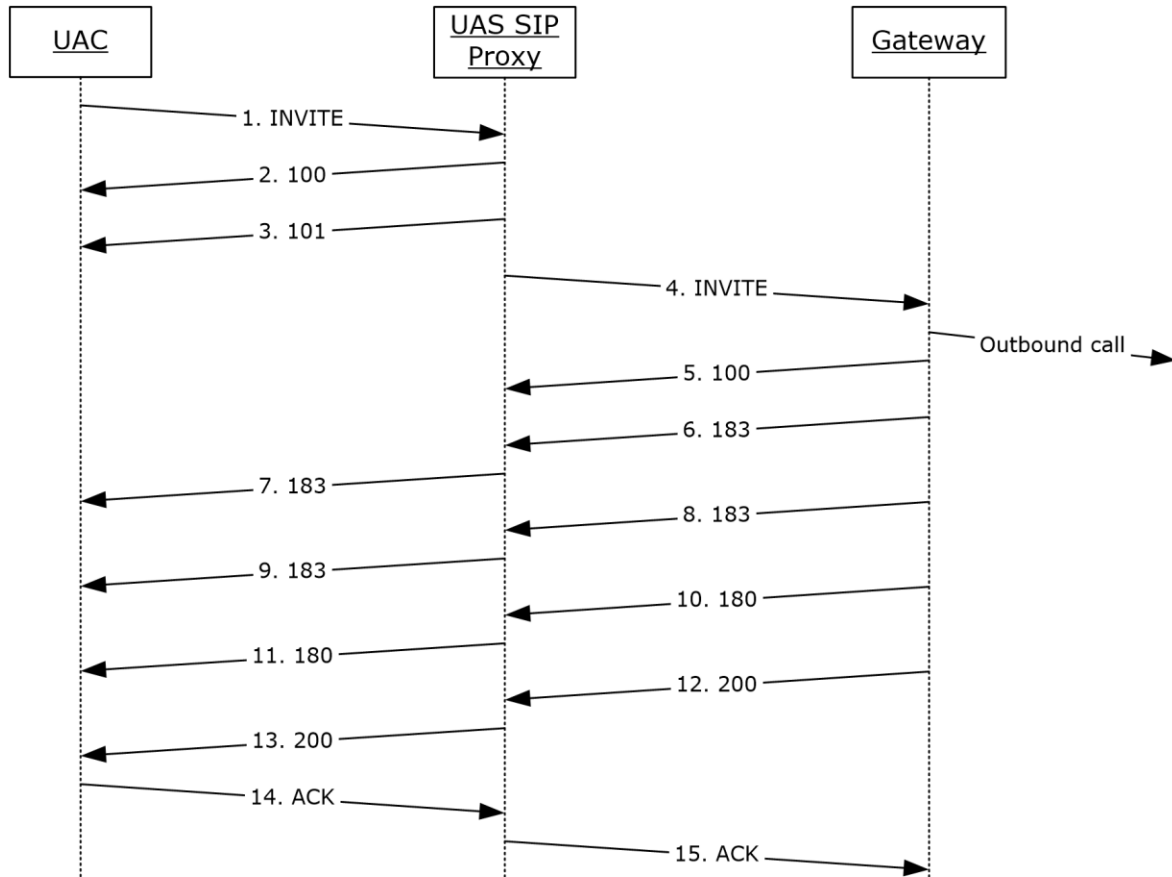
The **ms-call-source** header is not sent or received by a **UAC** in this scenario.

## 4.4 ms-early-media SIP Supported Header Option Tag

### 4.4.1 Inbound Call

The **ms-early-media** tag is not sent or received by a **UAC** in this scenario.

## 4.4.2 Outbound Call



**Figure 7: Outbound call**

The preceding figure includes only key messages that are described in this section.

The following messages illustrate the use of the **ms-early-media** option tag in messages that are sent from and received by a **UAC**.

### 4.4.2.1 Step 1: INVITE Is Sent from the UAC

The following **INVITE** includes an **ms-early-media** option tag in a **Supported** header and an **SDP offer**.

```
INVITE sip:+15555550100@example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.66.167:3137
Max-Forwards: 70
From: <sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
To: <sip:+15555550100@example.com;user=phone>
Call-ID: ca22890914c34bf8a7439dfe1e834420
CSeq: 1 INVITE
Contact: <sip:test1@example.com;opaque=user:epid:reTyjuqAaVmcCIO4qlA4vwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
Ms-Conversation-ID: Achit1olq5CCFcXhRKeZABfaZzvWNw==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
```

```

P-Preferred-Identity: <sip:test1@example.com>, <tel:+15555550101>
Supported: ms-conf-invite
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",
opaque="B25450B8", crand="620d1d6e", cnum="79", targetname="server1.example.com",
response="0100000008aab30387f6e10ef27db686"
Content-Type: application/sdp
Content-Length: 1076
v=0
o=- 0 0 IN IP4 10.56.66.167
s=session
c=IN IP4 10.56.66.167
b=CT:99980
t=0 0
m=audio 50016 RTP/AVP 114 111 112 115 116 4 8 0 97 101
k=base64:BCw/3c0RQ/ndiix3QiLgO9s3z1ZhEcLU3ZC85C74zuNSmyIrx11eIA4kErwh
a=candidate:Hfb3G/XvuV5G7gXYnDfWjyyZ8aIUbsPUhQRkndBg3vU 1 x4Ykst3u0Cf7mAW0moKnMQ UDP
0.900 10.56.66.167 50016
a=candidate:Hfb3G/XvuV5G7gXYnDfWjyyZ8aIUbsPUhQRkndBg3vU 2 x4Ykst3u0Cf7mAW0moKnMQ UDP
0.900 10.56.66.167 50008
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:aAzhJhKx1bOgjuVWNfI8C4f1K91E5SJb6vFIAWP|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:VqAkQvuZOMKHluaXvi+8kjiJlRsiyngtcuh2AA5k|2^31|1:1
a=maxptime:200
a=rtcp:50008
a=rtpmap:114 x-msrta/16000
a=fmtp:114 bitrate=29000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:116 AAL2-G726-32/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional

```

#### 4.4.2.2 Step 7: 183 Message Is Received by the UAC

The following 183 Session Progress message includes an **SDP answer**.

```

SIP/2.0 183 Session Progress
Authentication-Info: NTLM rspauth="010000000000000008AC67ADF27DB686", srand="DF9D53C4",
snum="103", opaque="B25450B8", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:3137;ms-received-port=3137;ms-received-cid=100
FROM: "test1"<sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
TO: <sip:+15555550100@example.com;user=phone>;epid=6477F45221;tag=b5bb1243e3
CSEQ: 1 INVITE
CALL-ID: ca22890914c34bf8a7439dfe1e834420
CONTENT-LENGTH: 740
CONTENT-TYPE: application/sdp; charset=utf-8
SERVER: RTCC/3.0.0.0 MediationServer
v=0
o=- 0 0 IN IP4 10.198.92.126
s=session
c=IN IP4 10.198.92.126
b=CT:1000
t=0 0
m=audio 60625 RTP/SAVP 111 115 8 97 101
c=IN IP4 10.198.92.126

```

```

a=rtcp:60532
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 1 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60625
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 2 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60532
a=crypto:2 AES CM 128 HMAC SHA1 80
inline:Pb+rI3y4U1xd47P8USsgDc/znOiBIv5s0Ev2abRT|2^31|1:1
a=label:main-audio
a=encryption:rejected
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:8 PCMA/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20

```

#### 4.4.2.3 Step 13: 200 Message Is Received by the UAC

The following **200 OK** message repeats the **SDP answer** that was sent in the preceding 183 Session Progress message.

```

SIP/2.0 200 OK
Authentication-Info: NTLM rspauth="010000003240756E24DFD336F27DB686", srand="C1DF9895",
snum="105", opaque="B25450B8", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:3137;ms-received-port=3137;ms-received-cid=100
FROM: "test1"<sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
TO: <sip:+15555550100@example.com;user=phone>;epid=6477F45221;tag=b5bb1243e3
CSEQ: 1 INVITE
CALL-ID: ca22890914c34bf8a7439dfe1e834420
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-route-
sig=aaelhWZJsyQvUcPVgXY5rCBgN5MnVHAhdiIeyt1QAA>
CONTACT: <sip:SH13-
LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXhNJb1ZwQfgAA;gri
d=b6796217d6ea465cbe261a778c10d5c0>;isGateway
CONTENT-LENGTH: 740
SUPPORTED: gruu-10
SUPPORTED: replaces
CONTENT-TYPE: application/sdp; charset=utf-8
ALLOW: UPDATE
P-ASSERTED-IDENTITY: <sip:+17036508897@example.com;user=phone>
SERVER: RTCC/3.0.0.0 MediationServer
ALLOW: Ack, Cancel, Bye, Invite, Refer
v=0
o=- 0 0 IN IP4 10.198.92.126
s=session
c=IN IP4 10.198.92.126
b=CT:1000
t=0 0
m=audio 60625 RTP/SAVP 111 115 8 97 101
c=IN IP4 10.198.92.126
a=rtcp:60532
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 1 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60625
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 2 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60532
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:Pb+rI3y4U1xd47P8USsgDc/znOiBIv5s0Ev2abRT|2^31|1:1
a=label:main-audio
a=encryption:rejected
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:115 x-msrta/8000

```

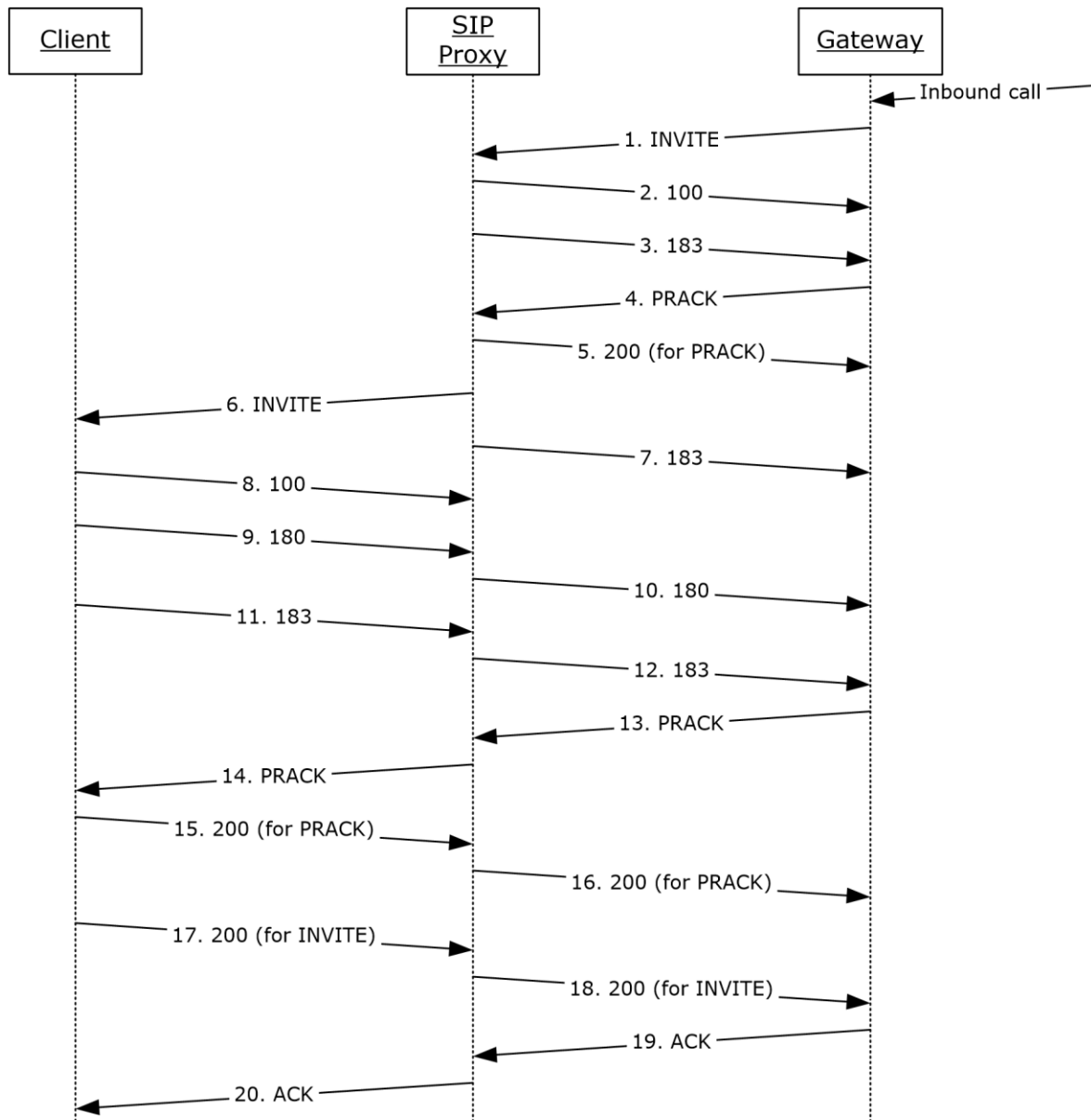
```

a=fmtp:115 bitrate=11800
a=rtpmap:8 PCMA/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20

```

## 4.5 ms-bypass SIP Supported Header Option Tag

### 4.5.1 Inbound Call



**Figure 8: Inbound call**

The messages in the following subsections illustrate the use of the **ms-bypass** option tag in a **Supported** header in messages that are sent from and received by a protocol client.

#### 4.5.1.1 Step 6: INVITE Message Is Received by the Protocol Client

```
INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f6d3a;ms-received-cid=475300
SIP/2.0
Record-Route:
<sip:PROXY.company1:5061;transport=tls;opaque=state:F:CI.R475300:Ieh.gU65xODvWq j78KvdcC-
dRxH71EBsv8oECfECdsWTe7QW4niMEtoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzxxvkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40
Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-
internal-info="cehce-xXzqcRs3A ZSAwy8D4JLgyqxDKREgfiVft6noRjHnKsZUY47CgAA"
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="CC46B5FD", snum="26",
rspauth="d6179291f72761e057a67adb7288fd256c2ble4d", targetname="PROXY.company1", realm="SIP
Communications Service", version=4
Max-Forwards: 69
Content-Length: 3161
Via: SIP/2.0/TLS 10.1.1.102:57350;branch=z9hG4bKe82f3c;ms-received-port=57350;ms-received-
cid=475900
From: <sip:4259876543;phone-
context=Location1@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223ea
To: <sip:+14251234567@company1;user=phone>;epid=54dd5867e8
CSeq: 35 INVITE
Call-ID: df601b2d-e42e-4677-b921-c9dbf4e25940
Contact:
<sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=bd9
c42fc618147d0af4d8f84f718910b>;isGateway
Supported: replaces
Supported: ms-safe-transfer
Supported: ms-bypass
Supported: ms-dialog-route-set-update
Supported: timer
Supported: 100rel
Supported: gruu-10
User-Agent: Mediation Server
Content-Type: multipart/alternative; boundary=9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J
Allow: ACK
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Session-Expires: 1800
Min-SE: 90
Allow: CANCEL, BYE, INVITE, REFER, NOTIFY, PRACK, UPDATE
P-Asserted-Identity: <sip:+4259876543@company1;user=phone>
History-Info: <sip:user112@company1>;index=1
--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J
Content-Type: application/sdp
Content-ID: <72e03bb9-6acc-453b-ae09-4b8671344d83>
Content-Disposition: Session;handling=optional;ms-proxy-2007fallback
v=0
o=- 1 0 IN IP4 10.1.1.102
s=session
c=IN IP4 10.1.1.102
b=CT:1000000
t=0 0
m=audio 56568 RTP/AVP 0 8 115 13 118 97 101
c=IN IP4 10.1.1.102
a=rtcp:56569
a=candidate:wPBogiU8NLp21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 1 0tKavBj1axiy4rc19atywg UDP 0.830
10.1.1.102 56568
a=candidate:wPBogiU8NLp21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 2 0tKavBj1axiy4rc19atywg UDP 0.830
10.1.1.102 56569
a=candidate:bgLnsM3DP4aSPQloj2Ak1IUYeGDPsldLRetvScj5izM 1 5VdtqvYZImPIpht0Tx5Mcg TCP 0.150
10.3.0.7 59954
```

```

a=candidate:bglnsm3DP4aSPQloj2Ak1IUYeGDPslDLRetvScj5izM 2 5VdtqvYZImPIpTh0Tx5Mcg TCP 0.150
10.3.0.7 59954
a=candidate:hdj57XrOXJwib/pE8R3lzSwmFwi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIXlAqv0bFA UDP 0.450
10.3.0.7 55690
a=candidate:hdj57XrOXJwib/pE8R3lzSwmFwi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIXlAqv0bFA UDP 0.450
10.3.0.7 57652
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 1 8yhh8eM+TlZ9w0CbEkzWfA TCP 0.250
10.1.1.102 207 52082
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 2 8yhh8eM+TlZ9w0CbEkzWfA TCP 0.250
10.1.1.102 52082
a=label:main-audio
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltvDv|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:tbZ34R5hvhfBSSvLMD0/uiQ7AWOCJD5Hj+Q58HQm|2^31
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/sdpContent-ID: <d05db498-7556-
445d-86e3-bfeb36fd52e9>

v=0o=- 2 0 IN IP4 10.1.1.102s=sessionc=IN IP4 10.1.1.102b=CT:100000t=0 0m=audio 50352
RTP/AVP 0 8 115 13 118 97 101c=IN IP4 10.1.1.102a=rtcp:50353a=ice-ufraq:LxLAA=ice-
pwd:3470M/yHdvxSWmMqhs+jJF2Ea=candidate:1 1 UDP 2130706431 10.1.1.102 50352 typ
hosta=candidate:1 2 UDP 2130705918 10.1.1.102 50353 typ host
a=candidate:2 1 tcp-pass 6555135 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:2 2 tcp-pass 6555134 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:3 1 UDP 16647679 10.0.3.7 52516 typ relay raddr 10.1.1.102 rport 55636
a=candidate:3 2 UDP 16647678 10.0.3.7 58728 typ relay raddr 10.1.1.102 rport 55637
a=candidate:4 1 tcp-act 7076863 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:4 2 tcp-act 7076350 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:5 1 tcp-act 1684798975 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=candidate:5 2 tcp-act 1684798462 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=label:main-audioa=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltvDv|2^31|1:1a=crypto:3 AES_CM_128_HMAC_SHA1_80
inline:tbZ34R5hvhfBSSvLMD0/uiQ7AWOCJD5Hj+Q58HQm|2^31a=rtpmap:0 PCMU/8000a=rtpmap:8
PCMA/8000a=rtpmap:115 x-msrta/8000a=fmtp:115 bitrate=11800a=rtpmap:13 CN/8000a=rtpmap:118
CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/gw-sdp; x-bypassid=9CD08A01-E998-
456a-AC8A-D028930E5933Content-ID: <466ac626-be34-4f8d-ba0d-c7bacf53c0ac>Content-Disposition:
Session;handling=optional

v=0o=Gateway 94331345 94331031 IN IP4 10.1.2.12s=sessionc=IN IP4 10.1.2.12t=0 0m=audio 6430
RTP/SAVP 0 8 4 2 3 13 101c=IN IP4 10.1.2.12a=rtcp:6431a=x-bypassid:9CD08A01-E998-456a-AC8A-
D028930E5933a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:uch9eRm5IMoOhC+jNRprVaEuvK2JN0upP2+9ciM9|2^31|129:1a=sendrecv=rtpmap:0
PCMU/8000a=rtpmap:8 PCMA/8000a=rtpmap:4 G723/8000a=fmtp:4 annexa=yesar=rtpmap:2 G726-
32/8000a=rtpmap:3 GSM/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-15a=ptime:20a=x-
mediasettings:signalboostunsupported

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J--

```

#### 4.5.1.2 Step 17: 200 Message Is Sent by the Protocol Client

```

SIP/2.0 200 OKVia: SIP/2.0/TLS
10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-internal-
info="cehce-xXzqcRs3A_ZSAwy8D4JLgyqxDKREgIVft6noRjHnKsZUY47CgAA"Via: SIP/2.0/TLS

```



```

10.1.1.102:57350;branch=z9hG4bKe82f3c;ms-received-port=57350;ms-received-cid=475900From:
<sip:4259876543;phone-
context=Location1@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223eaTo:
<sip:+14251234567@company1;user=phone>;epid=54dd5867e8;tag=c608fec21aCall-ID: df601b2d-
e42e-4677-b921-c9dbf4e25940CSeq: 35 INVITERecord-Route:
<sip:PROXY.company1:5061;transport=tls;opaque=state:F:ci.R475300:Ieh.gU65xODvqw_j78KvdcC-
dRxH71EBsv8oECfECdswTe7QW4niMEtoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzsvkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40Contact:
<sip:user112@company1;opaque=user:epid:jVxLXKl9112yFm93r_ArNgAA;gruu>User-Agent: Client
1.0Supported: histinfoSupported: ms-safe-transferAllow: INVITE, BYE, ACK, CANCEL, INFO,
UPDATE, REFER, NOTIFY, BENOTIFY, OPTIONSSession-Expires: 720;refresher=uacms-accepted-
content-id: <466ac626-be34-4f8d-ba0d-c7bacf53c0ac>P-Preferred-Identity:
<sip:user112@company1>, <tel:+14251234567>Supported: ms-bypassSupported: replacesProxy-
Authorization: TLS-DSK qop="auth", realm="SIP Communications Service", opaque="F755045D",
targetname="PROXY.company1", crand="bdaff021", cnum="26",
response="ec06b619fdde8d00dae6a5e3ef008db607f08538"Content-Type: application/sdpContent-
Length: 362
v=0o=- 0 0 IN IP4 192.168.1.114s=sessionc=IN IP4 192.168.1.114b=CT:99980t=0 0m=audio
10228 RTP/SAVP 0 8 4 101a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:coOkWf6dIPsrYkRXi7QkjHb4nlZwOQyZn0wWwBZR|2^31|1:1a=maxptime:200a=rtpmap:0
PCMU/8000a=rtpmap:8 PCMA/8000a=rtpmap:4 G723/8000a=rtpmap:101 telephone-
event/8000a=fmtp:101 0-16a=x-bypass

```

## 4.5.2 Outbound Call

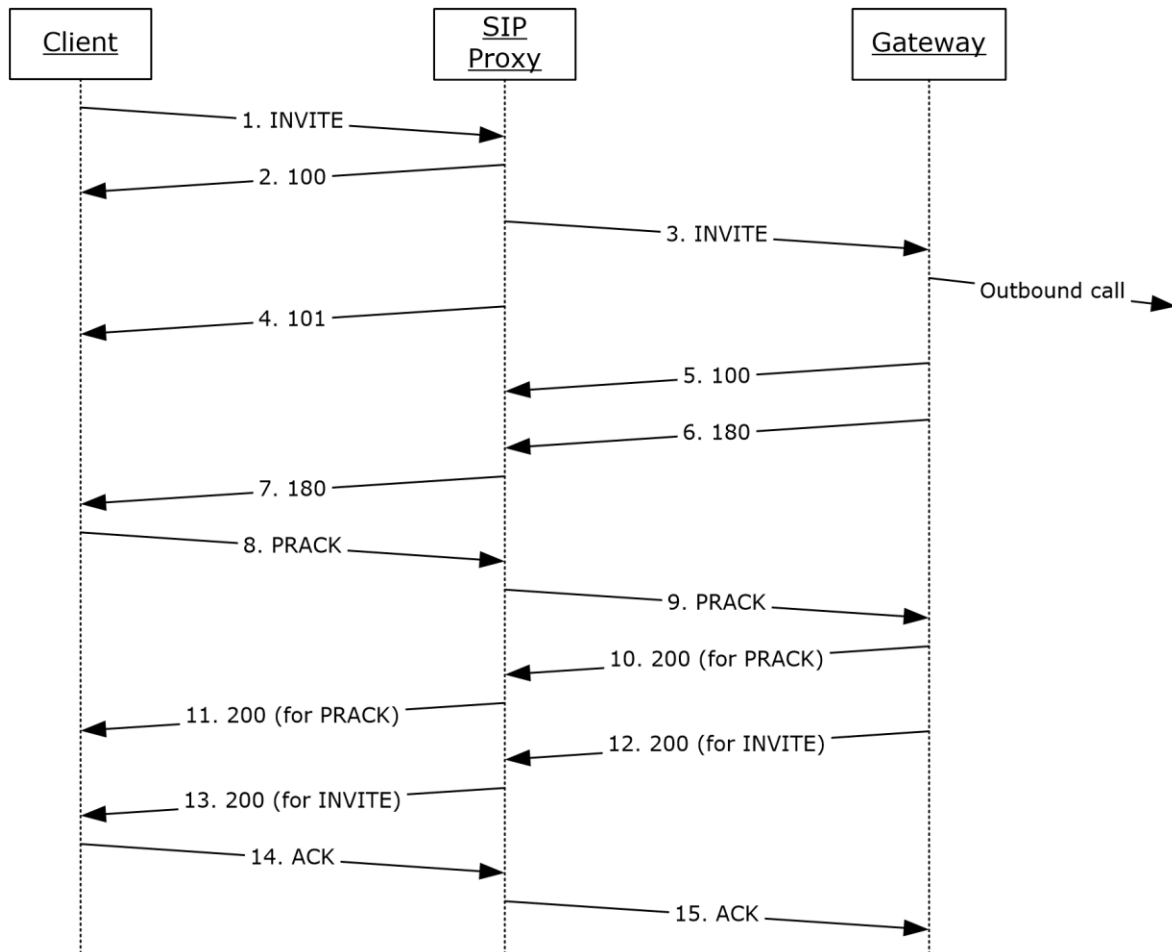


Figure 9: Outbound call

The messages in the following subsections illustrate the use of the **ms-bypass** option tag in a **Supported** header in messages that are sent from and received by a protocol client.

#### 4.5.2.1 Step 1: INVITE Message Is Sent by the Protocol Client

```
INVITE sip:+14258901234@company1;user=phone SIP/2.0
Via: SIP/2.0/TLS 192.168.1.114:4535
Max-Forwards: 70
From: <sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
To: <sip:+14258901234@company1;user=phone>
Call-ID: e571df11a45947f1a5b90da8d957b8ae
CSeq: 1 INVITE
Contact: <sip:user112@company1;opaque=user:epid:jVxLXK19112yFm93r ArNgAA;gruu>
User-Agent: Client 1.0
Ms-Conversation-ID: AcrCQkQ2CGV+fQQpS5OprWuDL+KaYQ==
Supported: timer
Supported: histinfo
Supported: ms-safe-transfer
Supported: ms-sender
Supported: ms-early-media
Supported: 100rel
ms-keep-alive: UAC;hop-hop=yes
Allow: INVITE, BYE, ACK, CANCEL, INFO, UPDATE, REFER, NOTIFY, BENOTIFY, OPTIONS
P-Preferred-Identity: <sip:user112@company1>, <tel:+14251234567>
Supported: ms-bypass
Supported: replaces
Supported: ms-conf-invite
Proxy-Authorization: TLS-DSK qop="auth", realm="SIP Communications Service",
opaque="F755045D", targetname="PROXY.company1", crand="738839d3", cnum="12",
response="2b5e54b5d29a1493e07894772e5ce0dcca06bdf3"
Content-Type: multipart/alternative;boundary="----- NextPart 000 0003 01CAC1FF.366488E0"
Content-Length: 3052

-----_NextPart_000_0003_01CAC1FF.366488E0

Content-Type: application/sdp
Content-Transfer-Encoding: 7bit
Content-ID: <2dd1547f1a2043c2a622586b444229e2>
Content-Disposition: session; handling=optional; ms-proxy-2007fallback

v=0
o=- 0 0 IN IP4 192.168.1.114
s=session
c=IN IP4 192.168.1.114
b=CT:99980
t=0 0
m=audio 25486 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFIVXLwt+YRbaobG+X43A 1 4Q/jKJde54nbJ5sfchXniA UDP 0.830
192.168.1.114 25486
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFIVXLwt+YRbaobG+X43A 2 4Q/jKJde54nbJ5sfchXniA UDP 0.830
192.168.1.114 25487
a=candidate:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeoLhFH8L6sN1M 1 wiGTb6hg53yn1/Keu8TGSg TCP 0.190
10.3.0.7 57587
a=candidate:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeoLhFH8L6sN1M 2 wiGTb6hg53yn1/Keu8TGSg TCP 0.190
10.3.0.7 57587
a=candidate:+LqcUBIcwtUej3u0lhJq7UET5SYTrNNWvpIzn7S4lho 1 X3SHHBGYzFqLK8TzSd5vNQ UDP 0.490
10.3.0.7 51247
a=candidate:+LqcUBIcwtUej3u0lhJq7UET5SYTrNNWvpIzn7S4lho 2 X3SHHBGYzFqLK8TzSd5vNQ UDP 0.490
10.3.0.7 50976
a=candidate:DzxxkqWh6pd3wMmObq9itqTbhQ6yI4DLm1I8ZRbI3J6c 1 AUw+lgvF2GlnnLiF4otDhg TCP 0.250
192.168.1.114 50007
a=candidate:DzxxkqWh6pd3wMmObq9itqTbhQ6yI4DLm1I8ZRbI3J6c 2 AUw+lgvF2GlnnLiF4otDhg TCP 0.250
192.168.1.114 50007
```

a=cryptoscale:1 client AES\_CM\_128\_HMAC\_SHA1\_80  
inline:OY1qCCFx84fwIkrR39XpPDA2HuNdtAB+6ekKly5a|2^31|1:1  
a=crypto:2 AES\_CM\_128\_HMAC\_SHA1\_80 inline:b28SzCBSdH7eBr13AhecN34gKh8OeCYQG6IMwxbC|2^31|1:1  
a=crypto:3 AES\_CM\_128\_HMAC\_SHA1\_80 inline:8LUckwDobd31ORi6KGZLYf+My7wvCwftc5Nw7G79|2^31

a=maxptime:200  
a=rtpmap:114 x-msrta/16000  
a=fmtp:114 bitrate=29000  
a=rtpmap:9 G722/8000  
a=rtpmap:112 G7221/16000  
a=fmtp:112 bitrate=24000  
a=rtpmap:111 SIREN/16000  
a=fmtp:111 bitrate=16000  
a=rtpmap:0 PCMU/8000  
a=rtpmap:8 PCMA/8000  
a=rtpmap:116 AAL2-G726-32/8000  
a=rtpmap:115 x-msrta/8000  
a=fmtp:115 bitrate=11800  
a=rtpmap:4 G723/8000  
a=rtpmap:97 RED/8000  
a=rtpmap:13 CN/8000  
a=rtpmap:118 CN/16000  
a=rtpmap:101 telephone-event/8000  
a=fmtp:101 0-16  
a=encryption:optional  
a=x-bypassid:9CD08A01-E998-456a-AC8A-D028930E5933

-----\_NextPart\_000\_0003\_01CAC1FF.366488E0  
Content-Type: application/sdp  
Content-Transfer-Encoding: 7bit  
Content-ID: <3d45476919eb4c81be0c4e19c730c655>  
Content-Disposition: session; handling=optional

v=0  
o=- 0 0 IN IP4 192.168.1.114  
s=session  
c=IN IP4 192.168.1.114  
b=CT:99980  
t=0 0  
m=audio 28238 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101  
a=ice-ufrag:ayqK  
a=ice-pwd:ckRbkr221v38PhlmqvzmVe5n  
a=candidate:1 1 UDP 2130706431 192.168.1.114 28238 typ host  
a=candidate:1 2 UDP 2130705918 192.168.1.114 28239 typ host  
a=candidate:2 1 TCP-PASS 6556159 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031  
a=candidate:2 2 TCP-PASS 6556158 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031  
a=candidate:3 1 UDP 16648703 10.3.0.7 50217 typ relay raddr 192.168.1.114 rport 50006  
a=candidate:3 2 UDP 16648702 10.3.0.7 58942 typ relay raddr 192.168.1.114 rport 50007  
a=candidate:4 1 TCP-ACT 7076863 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031  
a=candidate:4 2 TCP-ACT 7076350 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031  
a=candidate:5 1 TCP-ACT 1684798975 192.168.1.114 50031 typ srflx raddr 192.168.1.114 rport 50031  
a=candidate:5 2 TCP-ACT 1684798462 192.168.1.114 50031 typ srflx raddr 192.168.1.114 rport 50031  
a=cryptoscale:1 client AES\_CM\_128\_HMAC\_SHA1\_80  
inline:OY1qCCFx84fwIkrR39XpPDA2HuNdtAB+6ekKly5a|2^31|1:1  
a=crypto:2 AES CM 128 HMAC SHA1 80 inline:b28SzCBSdH7eBr13AhecN34gKh8OeCYQG6IMwxbC|2^31|1:1  
a=crypto:3 AES CM 128 HMAC SHA1 80 inline:8LUckwDobd31ORi6KGZLYf+My7wvCwftc5Nw7G79|2^31  
a=maxptime:200  
a=rtpmap:114 x-msrta/16000  
a=fmtp:114 bitrate=29000  
a=rtpmap:9 G722/8000  
a=rtpmap:112 G7221/16000  
a=fmtp:112 bitrate=24000  
a=rtpmap:111 SIREN/16000  
a=fmtp:111 bitrate=16000  
a=rtpmap:0 PCMU/8000  
a=rtpmap:8 PCMA/8000  
a=rtpmap:116 AAL2-G726-32/8000

```
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:4 G723/8000
a=rtpmap:97 RED/8000
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional
a=x-bypassid:9CD08A01-E998-456a-AC8A-D028930E5933
```

```
-----=_NextPart_000_0003_01CAC1FF.366488E0--
```

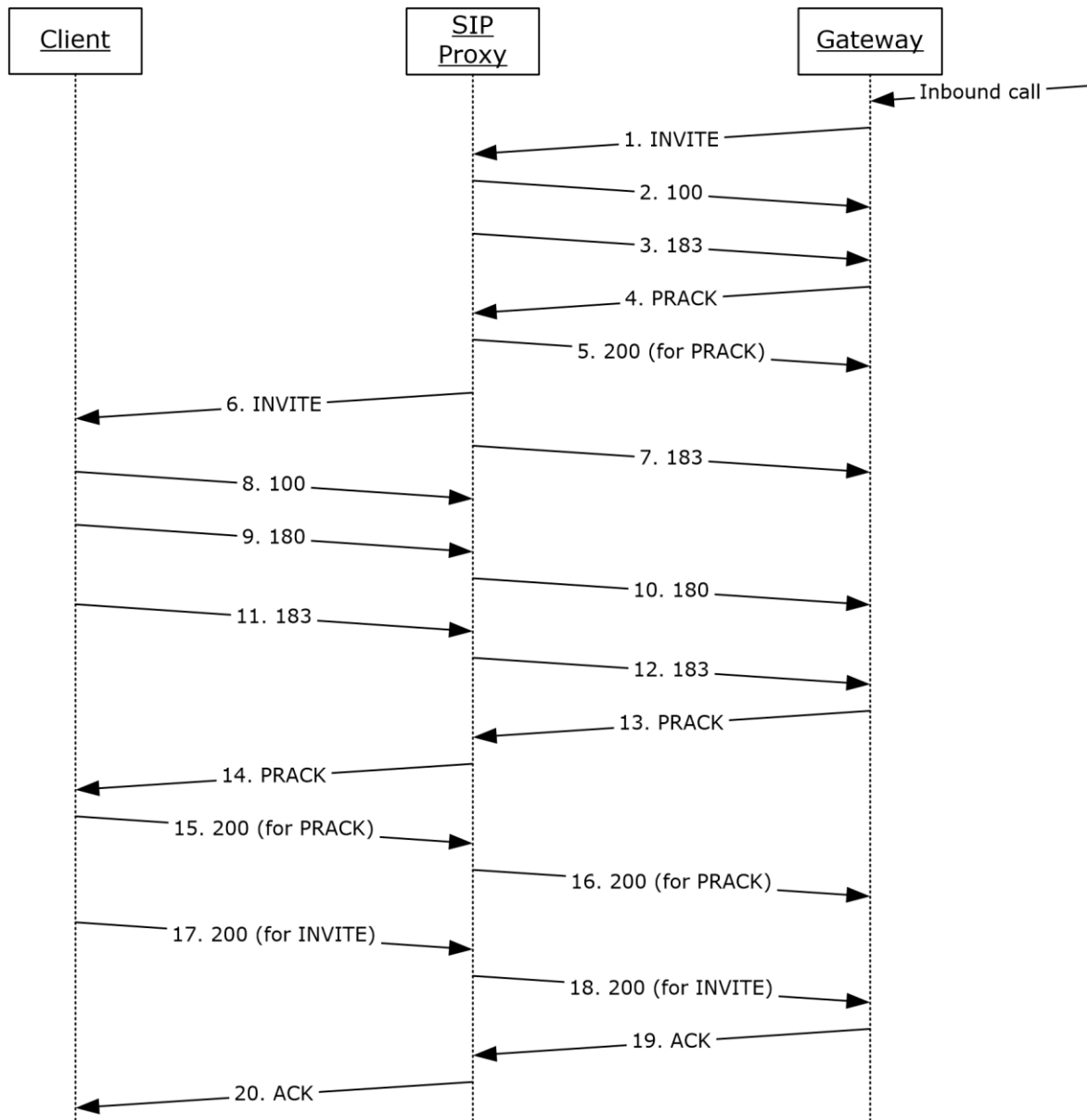
#### 4.5.2.2 Step 13: 200 OK Message Is Received by the Protocol Client

```
SIP/2.0 200 OK
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="1D9666D9", snum="17",
rspauth="3359c8ac2e6229b2eb9738ac707dc8c3e54f65f0", targetname="PROXY.company1", realm="SIP
Communications Service", version=4
Via: SIP/2.0/TLS 192.168.1.114:4535;ms-received-port=4535;ms-received-cid=475300
FROM: "user112"<sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
TO: <sip:+14258901234@company1;user=phone>;tag=201fec487e;epid=CDCFEF8F18
CSEQ: 1 INVITE
CALL-ID: e571df11a45947f1a5b90da8d957b8ae
RECORD-ROUTE: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300;lr;ms-route-
sig=dcw0SbeehYaHu9dRxfCQNPNLaiGM-c5DzikYU7AfKG2hHch3QtgY3jngAA>
CONTACT:
<sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=462
36573d0ae4a339d83726b2bf7f7ab>;isGateway
CONTENT-LENGTH: 422
SUPPORTED: replaces
SUPPORTED: ms-safe-transfer
SUPPORTED: ms-bypass
SUPPORTED: ms-dialog-route-set-update
SUPPORTED: gruu-10
SUPPORTED: timer
SUPPORTED: 100rel
CONTENT-TYPE: application/gw-sdp
ALLOW: ACK
P-ASSERTED-IDENTITY: <sip:+14258901234@company1;user=phone>
SERVER: Mediation Server
Ms-Accepted-Content-ID: <3d45476919eb4c81be0c4e19c730c655>
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresher=uas
Min-SE: 90

v=0
o=Gateway 1303417666 1303417345 IN IP4 10.1.2.12
s=session
c=IN IP4 10.1.2.12
t=0 0
m=audio 6390 RTP/SAVP 0 13 101
c=IN IP4 10.1.2.12
a=rtcp:6391
a=x-bypass
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:bN1zDJ0LC8QYNvMIohDtGkWD/rCastpGbz5ObNo|2^31|244:1
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=x-mediasettings:signalboostunsupported
```

## 4.6 ms-accepted-content-id SIP Header

### 4.6.1 Inbound Call



**Figure 10: Inbound call**

The following messages illustrate the use of the **ms-accepted-content-id Session Initiation Protocol (SIP)** header in messages that are sent from and received by a protocol client.

#### 4.6.1.1 Step 6: INVITE Message Is Received by the Protocol Client

INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f6d3a;ms-received-cid=475300  
SIP/2.0  
Record-Route:  
<sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300:Ieh.gU65xODvWvj78KvdcC-  
dRxh71EBsv8oECfECdswTe7QW4niMEtoTOi\_iwBgjHnKsZgY3jngAA;lr;ms-route-  
sig=dcrEzxxvkq3iKgc2ApWyiXbCYC7NNwE-  
pYCYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40  
Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-  
internal-info="cehce-xXzqcRs3A\_ZSAwy8D4JLgyqxDKREgfIVFt6noRjHnKsZUY47CgAA"  
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="CC46B5FD", snum="26",  
rspauth="d6179291f72761e057a67adb7288fd256c2b1e4d", targetname="PROXY.company1", realm="SIP  
Communications Service", version=4  
Max-Forwards: 69  
Content-Length: 3161  
Via: SIP/2.0/TLS 10.1.1.102:57350;branch=z9hG4bKe82f3c;ms-received-port=57350;ms-received-  
cid=475900  
From: <sip:4259876543;phone-  
context=Location1@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223ea  
To: <sip:+14251234567@company1;user=phone>;epid=54dd5867e8  
CSeq: 35 INVITE  
Call-ID: df601b2d-e42e-4677-b921-c9dbf4e25940  
Contact:  
<sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=bd9  
c42fc618147d0af4d8f84f718910b>;isGateway  
Supported: replaces  
Supported: ms-safe-transfer  
Supported: ms-bypass  
Supported: ms-dialog-route-set-update  
Supported: timer  
Supported: 100rel  
Supported: gruu-10  
User-Agent: Mediation Server  
Content-Type: multipart/alternative; boundary=9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J  
Allow: ACK  
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"  
Session-Expires: 1800  
Min-SE: 90  
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE  
P-Asserted-Identity: <sip:+4259876543@company1;user=phone>  
History-Info: <sip:user112@company1>;index=1  
--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J  
Content-Type: application/sdp  
Content-ID: <72e03bb9-6acc-453b-ae09-4b8671344d83>  
Content-Disposition: Session;handling=optional;ms-proxy-2007fallback  
v=0  
o=- 1 0 IN IP4 10.1.1.102  
s=session  
c=IN IP4 10.1.1.102  
b=CT:1000000  
t=0 0  
m=audio 56568 RTP/AVP 0 8 115 13 118 97 101  
c=IN IP4 10.1.1.102  
a=rtcp:56569  
a=candidate:wPBogiU8NLp21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 1 0tKavBj1axiy4rc19atywg UDP 0.830  
10.1.1.102 56568  
a=candidate:wPBogiU8NLp21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 2 0tKavBj1axiy4rc19atywg UDP 0.830  
10.1.1.102 56569  
a=candidate:bgLnsM3DP4aSPQ1oj2Ak1IUYeGDPsldLRetvScj5izM 1 5VdtqvYZImPIpht0Tx5Mcg TCP 0.150  
10.3.0.7 59954  
a=candidate:bgLnsM3DP4aSPQ1oj2Ak1IUYeGDPsldLRetvScj5izM 2 5VdtqvYZImPIpht0Tx5Mcg TCP 0.150  
10.3.0.7 59954  
a=candidate:hdj57XrOXJwib/pE8R31zSwmfWi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450  
10.3.0.7 55690  
a=candidate:hdj57XrOXJwib/pE8R31zSwmfWi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450  
10.3.0.7 57652  
a=candidate:JqHr0VQ3SBc1eDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 1 8yhh8eM+T1Z9w0CbEkzwfA TCP 0.250  
10.1.1.102 207 52082  
a=candidate:JqHr0VQ3SBc1eDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 2 8yhh8eM+T1Z9w0CbEkzwfA TCP 0.250  
10.1.1.102 52082

```

a=label:main-audio
a=cryptoscale:1 client AES_CM 128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1
a=crypto:2 AES_CM 128_HMAC_SHA1_80 inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltvdv|2^31|1:1
a=crypto:3 AES_CM 128_HMAC_SHA1_80 inline:tbZ34R5hvhfBSsVLMd0/uiQ7AWOCJD5Hj+Q58HQm|2^31
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/sdpContent-ID: <d05db498-7556-445d-86e3-bfeb36fd52e9>

v=0o=- 2 0 IN IP4 10.1.1.102s=sessionc=IN IP4 10.1.1.102b=CT:100000t=0 0m=audio 50352
RTP/AVP 0 8 115 13 118 97 101c=IN IP4 10.1.1.102a=rtcp:50353a=ice-ufraq:LxLAA=ice-
pwd:3470M/yHdvxSWmMqhs+jJF2Ea=candidate:1 1 UDP 2130706431 10.1.1.102 50352 typ
hosta=candidate:1 2 UDP 2130705918 10.1.1.102 50353 typ host
a=candidate:2 1 tcp-pass 6555135 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:2 2 tcp-pass 6555134 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:3 1 UDP 16647679 10.0.3.7 52516 typ relay raddr 10.1.1.102 rport 55636
a=candidate:3 2 UDP 16647678 10.0.3.7 58728 typ relay raddr 10.1.1.102 rport 55637
a=candidate:4 1 tcp-act 7076863 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:4 2 tcp-act 7076350 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:5 1 tcp-act 1684798975 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=candidate:5 2 tcp-act 1684798462 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=label:main-audioa=cryptoscale:1 client AES_CM 128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1a=crypto:2 AES_CM 128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltvdv|2^31|1:1a=crypto:3 AES_CM 128_HMAC_SHA1_80
inline:tbZ34R5hvhfBSsVLMd0/uiQ7AWOCJD5Hj+Q58HQm|2^31a=rtpmap:0 PCMU/8000a=rtpmap:8
PCMA/8000a=rtpmap:115 x-msrta/8000a=fmtp:115 bitrate=11800a=rtpmap:13 CN/8000a=rtpmap:118
CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/gw-sdp; x-bypassid=9CD08A01-E998-
456a-AC8A-D028930E5933Content-ID: <466ac626-be34-4f8d-ba0d-c7bacf53c0ac>Content-Disposition:
Session;handling=optional

v=0o=Gateway 94331345 94331031 IN IP4 10.1.2.12s=sessionc=IN IP4 10.1.2.12t=0 0m=audio 6430
RTP/SAVP 0 8 4 2 3 13 101c=IN IP4 10.1.2.12a=rtcp:6431a=x-bypassid:9CD08A01-E998-456a-AC8A-
D028930E5933a=crypto:1 AES_CM 128_HMAC_SHA1_80
inline:uch9eRm5IMoOhc+jNRprVaEuvK2JN0upP2+9ciM9|2^31|129:1a=sendrecv a=rtpmap:0
PCMU/8000a=rtpmap:8 PCMA/8000a=rtpmap:4 G723/8000a=fmtp:4 annexa=yes a=rtpmap:2 G726-
32/8000a=rtpmap:3 GSM/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-15a=ptime:20a=x-
mediasettings:signalboostunsupported

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J-

```

#### 4.6.1.2 Step 17: 200 Message Is Sent by the Protocol Client

```

SIP/2.0 200 OKVia: SIP/2.0/TLS
10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-internal-info="cehce-
xXzqcRs3A ZSAwy8D4JLgyqxDKREgfIVFt6noRjHnKsZUY47CgAA"Via: SIP/2.0/TLS
10.1.1.102:57350;branch=z9hG4bK8e2f3c;ms-received-port=57350;ms-received-cid=475900From:
<sip:4259876543;phone-
context=Location1@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223eaTo:
<sip:+14251234567@company1;user=phone>;epid=54dd5867e8;tag=c608fec21aCall-ID: df601b2d-e42e-
4677-b921-c9dbf4e25940CSeq: 35 INVITERecord-Route:
<sip:PROXY.company1:5061;transport=tls;opaque=state:F:ci.R475300:Ieh.gU65xODvWq j78KvdcC-
dRxH7lEBsv8oECfECdswTe7QW4niMetoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzvxvkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40Contact:
<sip:user112@company1;opaque=user:epid:jvLXK19112yFm93r_ArNgAA;gruu>User-Agent: Client

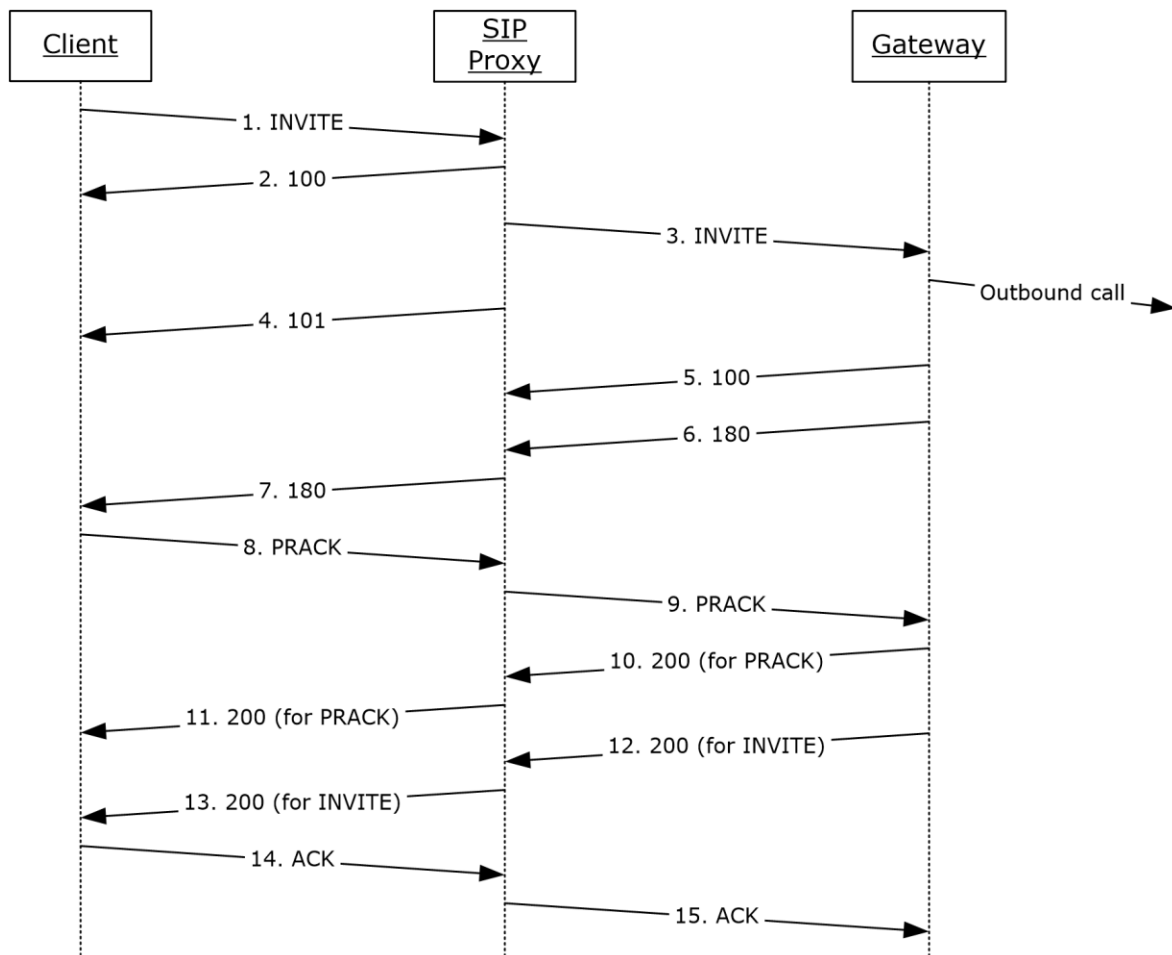
```

```

1.0Supported: histinfoSupported: ms-safe-transferAllow: INVITE, BYE, ACK, CANCEL, INFO,
UPDATE, REFER, NOTIFY, BENOTIFY, OPTIONSSession-Expires: 720;refresher=uacms-accepted-
content-id: <466ac626-be34-4f8d-ba0d-c7bacf53c0ac>P-Preferred-Identity:
<sip:user112@company1>, <tel:+14251234567>Supported: ms-bypassSupported: replacesProxy-
Authorization: TLS-DSK qop="auth", realm="SIP Communications Service", opaque="F755045D",
targetname="PROXY.company1", crand="bdaff021", cnum="26",
response="ec06b619fdde8d00dae6a5e3ef008db607f08538"Content-Type: application/sdpContent-
Length: 362
v=0o=- 0 0 IN IP4 192.168.1.114s=sessionc=IN IP4 192.168.1.114b=CT:99980t=0 0m=audio 10228
RTP/SAVP 0 8 4 101a=crypto:1 AES CM 128 HMAC SHA1 80
inline:coOkWf6dIPsrYkRXi7QkjHb4nlZwOQyZn0wWwBZR|2^31|1:1a=maxptime:200a=rtpmap:0
PCMU/8000a=rtpmap:8 PCMA/8000a=rtpmap:4 G723/8000a=rtpmap:101 telephone-event/8000a=fmtp:101
0-16a=x-bypass

```

## 4.6.2 Outbound Call



**Figure 11: Outbound call**

The messages in the following subsections illustrate the use of the **ms-accepted-content-id** **Session Initiation Protocol (SIP)** header in messages that are sent from and received by a protocol client.

### 4.6.2.1 Step 1: INVITE Message Is Sent by the Protocol Client



INVITE sip:+14258901234@company1;user=phone SIP/2.0

Via: SIP/2.0/TLS 192.168.1.114:4535  
Max-Forwards: 70  
From: <sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8  
To: <sip:+14258901234@company1;user=phone>  
Call-ID: e571df11a45947f1a5b90da8d957b8ae  
CSeq: 1 INVITE  
Contact: <sip:user112@company1;opaque=user:epid:jVxLXKl9112yFm93r\_ArNgAA;gruu>  
User-Agent: Client 1.0  
Ms-Conversation-ID: AcrCQkQ2CGV+fQQpS5OprWuDL+KaYQ==  
Supported: timer  
Supported: histinfo  
Supported: ms-safe-transfer  
Supported: ms-sender  
Supported: ms-early-media  
Supported: 100rel  
ms-keep-alive: UAC;hop-hop=yes  
Allow: INVITE, BYE, ACK, CANCEL, INFO, UPDATE, REFER, NOTIFY, BENOTIFY, OPTIONS  
P-Preferred-Identity: <sip:user112@company1>, <tel:+14251234567>  
Supported: ms-bypass  
Supported: replaces  
Supported: ms-conf-invite  
Proxy-Authorization: TLS-DSK qop="auth", realm="SIP Communications Service",  
opaque="F755045D", targetname="PROXY.company1", crand="738839d3", cnum="12",  
response="2b5e54b5d29a1493e07894772e5ce0dcca06bdf3"  
Content-Type: multipart/alternative;boundary="----- NextPart 000 0003 01CAC1FF.366488E0"  
Content-Length: 3052

-----\_NextPart\_000\_0003\_01CAC1FF.366488E0

Content-Type: application/sdp  
Content-Transfer-Encoding: 7bit  
Content-ID: <2dd1547f1a2043c2a622586b444229e2>  
Content-Disposition: session; handling=optional; ms-proxy-2007fallback

v=0  
o=- 0 0 IN IP4 192.168.1.114  
s=session  
c=IN IP4 192.168.1.114  
b=CT:99980  
t=0 0  
m=audio 25486 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101  
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFIVXLwt+YRbaobG+X43A 1 4Q/jKJde54nbJ5sfchXniA UDP 0.830  
192.168.1.114 25486  
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFIVXLwt+YRbaobG+X43A 2 4Q/jKJde54nbJ5sfchXniA UDP 0.830  
192.168.1.114 25487  
a=candidate:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeoLhFH8L6sN1M 1 wiGTb6hg53yn1/Keu8TGSg TCP 0.190  
10.3.0.7 57587  
a=candidate:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeoLhFH8L6sN1M 2 wiGTb6hg53yn1/Keu8TGSg TCP 0.190  
10.3.0.7 57587  
a=candidate:+LqcUBIcwtUej3u0lhJq7UET5SYTrNNWvpIzn7S4lho 1 X3SHHBGYzFqLK8TzSd5vNQ UDP 0.490  
10.3.0.7 51247  
a=candidate:+LqcUBIcwtUej3u0lhJq7UET5SYTrNNWvpIzn7S4lho 2 X3SHHBGYzFqLK8TzSd5vNQ UDP 0.490  
10.3.0.7 50976  
a=candidate:DzxxkqWh6pd3wMmObq9itqTbhQ6yI4DLm1I8ZRbI3J6c 1 AUw+lgvF2GlnnLiF4otDhg TCP 0.250  
192.168.1.114 50007  
a=candidate:DzxxkqWh6pd3wMmObq9itqTbhQ6yI4DLm1I8ZRbI3J6c 2 AUw+lgvF2GlnnLiF4otDhg TCP 0.250  
192.168.1.114 50007  
a=cryptoscale:1 client AES CM 128 HMAC SHA1 80  
inline:OY1qCCFx84fwIkrR39XpPDA2HuNdtAB+6ekKly5a|2^31|1:1  
a=crypto:2 AES CM 128 HMAC SHA1 80 inline:b28SzsCBSdH7eBr13AhecN34gKh8OeCYQG6IMwxbC|2^31|1:1  
a=crypto:3 AES\_CM\_128\_HMAC\_SHA1\_80 inline:8LUckwDobd31ORi6KGZLYf+My7wvCwftc5Nw7G79|2^31  
  
a=maxptime:200  
a=rtpmap:114 x-msrta/16000  
a=fmtp:114 bitrate=29000  
a=rtpmap:9 G722/8000

```

a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 AAL2-G726-32/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:4 G723/8000
a=rtpmap:97 RED/8000
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional
a=x-bypassid:9CD08A01-E998-456a-AC8A-D028930E5933

----- NextPart 000 0003 01CAC1FF.366488E0
Content-Type: application/sdp
Content-Transfer-Encoding: 7bit
Content-ID: <3d45476919eb4c81be0c4e19c730c655>
Content-Disposition: session; handling=optional

v=0
o=- 0 0 IN IP4 192.168.1.114
s=session
c=IN IP4 192.168.1.114
b=CT:99980
t=0 0
m=audio 28238 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101
a=ice-frag:aygK
a=ice-pwd:ckRbkR22lv38PhlmqvzmVe5n
a=candidate:1 1 UDP 2130706431 192.168.1.114 28238 typ host
a=candidate:1 2 UDP 2130705918 192.168.1.114 28239 typ host
a=candidate:2 1 TCP-PASS 6556159 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:2 2 TCP-PASS 6556158 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:3 1 UDP 16648703 10.3.0.7 50217 typ relay raddr 192.168.1.114 rport 50006
a=candidate:3 2 UDP 16648702 10.3.0.7 58942 typ relay raddr 192.168.1.114 rport 50007
a=candidate:4 1 TCP-ACT 7076863 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:4 2 TCP-ACT 7076350 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:5 1 TCP-ACT 1684798975 192.168.1.114 50031 typ srflx raddr 192.168.1.114 rport 50031
a=candidate:5 2 TCP-ACT 1684798462 192.168.1.114 50031 typ srflx raddr 192.168.1.114 rport 50031
a=cryptoscale:1 client AES CM 128 HMAC SHA1 80
inline:OY1qCCF84fwIkrR39XpPDA2HuNdtAB+6ekKly5a|2^31|1:1
a=crypto:2 AES CM 128 HMAC SHA1 80 inline:b28SzCBSdh7eBr13AhecN34gKh8OeCYQG6IMwxbC|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:8LUckwDobd31ORi6KGZLYf+My7wvCwftc5Nw7G79|2^31
a=maxptime:200
a=rtpmap:114 x-msrta/16000
a=fmtp:114 bitrate=29000
a=rtpmap:9 G722/8000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 AAL2-G726-32/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:4 G723/8000
a=rtpmap:97 RED/8000
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional

```

a=x-bypassid:9CD08A01-E998-456a-AC8A-D028930E5933

-----\_NextPart\_000\_0003\_01CAC1FF.366488E0--

#### 4.6.2.2 Step 13: 200 Message Is Received by the Protocol Client

```
SIP/2.0 200 OK
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="1D9666D9", snum="17",
rspauth="3359c8ac2e6229b2eb9738ac707dc8c3e54f65f0", targetname="PROXY.company1", realm="SIP
Communications Service", version=4
Via: SIP/2.0/TLS 192.168.1.114:4535;ms-received-port=4535;ms-received-cid=475300
FROM: "user112"<sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
TO: <sip:+14258901234@company1;user=phone>;tag=201fec487e;epid=CDCFEF8F18
CSEQ: 1 INVITE
CALL-ID: e571df11a45947f1a5b90da8d957b8ae
RECORD-ROUTE: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300;lr;ms-route-
sig=dcw0SbeehYaHu9dRxfcQNPNLaiGM-c5DzikYU7AfKG2hHch3QtgY3jngAA>
CONTACT:
<sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=462
36573d0ae4a339d83726b2bf7f7ab>;isGateway
CONTENT-LENGTH: 422
SUPPORTED: replaces
SUPPORTED: ms-safe-transfer
SUPPORTED: ms-bypass
SUPPORTED: ms-dialog-route-set-update
SUPPORTED: gruu-10
SUPPORTED: timer
SUPPORTED: 100rel
CONTENT-TYPE: application/gw-sdp
ALLOW: ACK
P-ASSERTED-IDENTITY: <sip:+14258901234@company1;user=phone>
SERVER: Mediation Server
Ms-Accepted-Content-ID: <3d45476919eb4c81be0c4e19c730c655>
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresher=uas
Min-SE: 90

v=0
o=Gateway 1303417666 1303417345 IN IP4 10.1.2.12
s=session
c=IN IP4 10.1.2.12
t=0 0
m=audio 6390 RTP/SAVP 0 13 101
c=IN IP4 10.1.2.12
a=rtcp:6391
a=x-bypass
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:bn1zDJ0LC8QYNvMIIdohDtGkWD/rCastpGbz50bNo|2^31|244:1
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=x-mediasettings:signalboostunsupported
```

#### 4.7 ms-trunking-peer SIP Header

The messages in the following subsections illustrate the use of the **ms-trunking-peer Session Initiation Protocol (SIP)** header in messages that are sent from and received by a protocol client.

## 4.7.1 Inbound Call

The message in the following subsection illustrates the use of the **ms-trunking-peer SIP** header for inbound calls. For a diagram of the inbound **call**, see the figure in section [4.6.1](#).

### 4.7.1.1 Step 6: INVITE Message Is Received by the Protocol Client

```
INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f6d3a;ms-received-cid=475300
SIP/2.0
Record-Route:
<sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300:Ieh.gU65xODvqw_j78KvdcC-
dRxH7lEBsv8oECfECdswTe7QW4niMEtoTOi iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzvxvkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40
Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-
internal-info="cehce-xXzqcRs3A_ZSAwy8D4JLgyqxDKREgfIVFt6noRjHnKsZUY47CgAA"
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="CC46B5FD", snum="26",
rspauth="d6179291f72761e057a67adb7288fd256c2b1e4d", targetname="PROXY.company1", realm="SIP
Communications Service", version=4
Max-Forwards: 69
Content-Length: 3161
Via: SIP/2.0/TLS 10.1.1.102:57350;branch=z9hG4bKe82f3c;ms-received-port=57350;ms-received-
cid=475900
From: <sip:4259876543;phone-
context=Location1@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223ea
To: <sip:+14251234567@company1;user=phone>;epid=54dd5867e8
CSeq: 35 INVITE
Call-ID: df601b2d-e42e-4677-b921-c9dbf4e25940
Contact:
<sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=bd9
c42fc618147d0af4d8f84f718910b>;isGateway
Supported: replaces
Supported: ms-safe-transfer
Supported: ms-bypass
Supported: ms-dialog-route-set-update
Supported: timer
Supported: 100rel
Supported: gruu-10
User-Agent: Mediation Server
Content-Type: multipart/alternative; boundary=9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J
Allow: ACK
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Session-Expires: 1800
Min-SE: 90
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
P-Asserted-Identity: <sip:+4259876543@company1;user=phone>
History-Info: <sip:user112@company1>;index=1
--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J
Content-Type: application/sdp
Content-ID: <72e03bb9-6acc-453b-ae09-4b8671344d83>
Content-Disposition: Session;handling=optional;ms-proxy-2007fallback
v=0
o=- 1 0 IN IP4 10.1.1.102
s=session
c=IN IP4 10.1.1.102
b=CT:1000000
t=0 0
m=audio 56568 RTP/AVP 0 8 115 13 118 97 101
c=IN IP4 10.1.1.102
a=rtcp:56569
a=candidate:wPBogiU8NLP21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 1 0tKavBj1axiy4rc19atywg UDP 0.830
10.1.1.102 56568
a=candidate:wPBogiU8NLP21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 2 0tKavBj1axiy4rc19atywg UDP 0.830
10.1.1.102 56569
```

```

a=candidate:bglnsm3DP4aSPQloj2Ak1IUYeGDPslDLRetvScj5izM 1 5VdtqvYZImPIpTh0Tx5Mcg TCP 0.150
10.3.0.7 59954
a=candidate:bglnsm3DP4aSPQloj2Ak1IUYeGDPslDLRetvScj5izM 2 5VdtqvYZImPIpTh0Tx5Mcg TCP 0.150
10.3.0.7 59954
a=candidate:hdj57XrOXJwib/pE8R31zSwmfWi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIXlAqv0bFA UDP 0.450
10.3.0.7 55690
a=candidate:hdj57XrOXJwib/pE8R31zSwmfWi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIXlAqv0bFA UDP 0.450
10.3.0.7 57652
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 1 8yhh8eM+TlZ9w0CbEkzWfA TCP 0.250
10.1.1.102 207 52082
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 2 8yhh8eM+TlZ9w0CbEkzWfA TCP 0.250
10.1.1.102 52082
a=label:main-audio
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVzllNEk3EJ6T3|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltdvd|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:tbZ34R5hvhfBSSvLMD0/uiQ7AWOCJD5Hj+Q58HQm|2^31
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:13 CN/8000
a=rtpmap:118 CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/sdpContent-ID: <d05db498-7556-
445d-86e3-bfeb36fd52e9>

v=0o=- 2 0 IN IP4 10.1.1.102s=sessionc=IN IP4 10.1.1.102b=CT:100000t=0 0m=audio 50352
RTP/AVP 0 8 115 13 118 97 101c=IN IP4 10.1.1.102a=rtcp:50353a=ice-ufraq:LxLAa=ice-
pwd:3470M/yHdvxSWmQhs+jJF2Ea=candidate:1 1 UDP 2130706431 10.1.1.102 50352 typ
hosta=candidate:1 2 UDP 2130705918 10.1.1.102 50353 typ host
a=candidate:2 1 tcp-pass 6555135 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:2 2 tcp-pass 6555134 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:3 1 UDP 16647679 10.0.3.7 52516 typ relay raddr 10.1.1.102 rport 55636
a=candidate:3 2 UDP 16647678 10.0.3.7 58728 typ relay raddr 10.1.1.102 rport 55637
a=candidate:4 1 tcp-act 7076863 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:4 2 tcp-act 7076350 10.0.3.7 55634 typ relay raddr 10.1.1.102 rport 53970
a=candidate:5 1 tcp-act 1684798975 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=candidate:5 2 tcp-act 1684798462 10.1.1.102 53970 typ srflx raddr 10.1.1.102 rport
53970a=label:main-audioa=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:f6V1oCUyKIzjLEBRg46FFt7BenyVzllNEk3EJ6T3|2^31|1:1a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtMltdvd|2^31|1:1a=crypto:3 AES_CM_128_HMAC_SHA1_80
inline:tbZ34R5hvhfBSSvLMD0/uiQ7AWOCJD5Hj+Q58HQm|2^31a=rtpmap:0 PCMU/8000a=rtpmap:8
PCMA/8000a=rtpmap:115 x-msrta/8000a=fmtp:115 bitrate=11800a=rtpmap:13 CN/8000a=rtpmap:118
CN/16000a=rtpmap:97 RED/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-16,36

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3JContent-Type: application/gw-sdp; x-bypassid=9CD08A01-E998-
456a-AC8A-D028930E5933Content-ID: <466ac626-be34-4f8d-ba0d-c7bacf53c0ac>Content-Disposition:
Session;handling=optional

v=0o=Gateway 94331345 94331031 IN IP4 10.1.2.12s=sessionc=IN IP4 10.1.2.12t=0 0m=audio 6430
RTP/SAVP 0 8 4 2 3 13 101c=IN IP4 10.1.2.12a=rtcp:6431a=x-bypassid:9CD08A01-E998-456a-AC8A-
D028930E5933a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:uch9eRm5IMoOhc+jNRprVaEuvK2JN0upP2+9ciM9|2^31|129:1a=sendrecv a=rtpmap:0
PCMU/8000a=rtpmap:8 PCMA/8000a=rtpmap:4 G723/8000a=fmtp:4 annexa=yes a=rtpmap:2 G726-
32/8000a=rtpmap:3 GSM/8000a=rtpmap:101 telephone-event/8000a=fmtp:101 0-15a=ptime:20a=x-
mediasettings:signalboostunsupported

--9dvaKhfhPJxCOyObvB70o0f2xfgiXN3J-

```

## 4.7.2 Outbound Call

The message in the following subsection illustrates the use of the **ms-trunking-peer SIP** header for outbound calls. For a diagram of the outbound **call**, see the figure in section [4.6.2](#).

### 4.7.2.1 Step 13: 200 Message Is Received by the Protocol Client

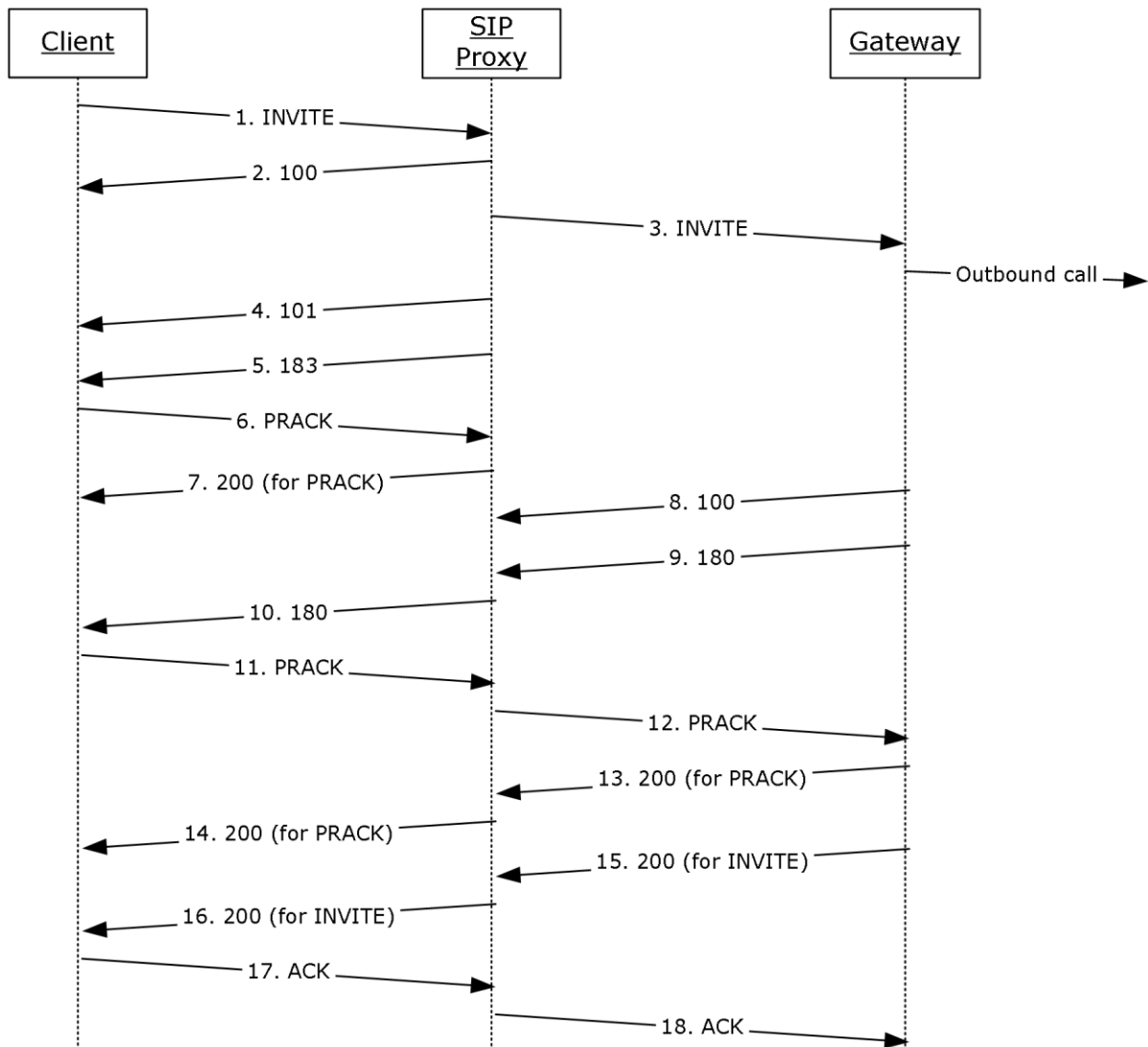
```
SIP/2.0 200 OK
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srand="1D9666D9", snum="17",
rspauth="3359c8ac2e6229b2eb9738ac707dc8c3e54f65f0", targetname="PROXY.company1", realm="SIP
Communications Service", version=4
Via: SIP/2.0/TLS 192.168.1.114:4535;ms-received-port=4535;ms-received-cid=475300
FROM: "user112"<sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
TO: <sip:+14258901234@company1;user=phone>;tag=201fec487e;epid=CDCFEF8F18
CSEQ: 1 INVITE
CALL-ID: e571df11a45947f1a5b90da8d957b8ae
RECORD-ROUTE: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300;lr;ms-route-
sig=dcw0SbeehYaHu9dRxfCQNPNLaiGM-c5DzikYU7AfKG2hHch3QtgY3jngAA>
CONTACT:
<sip:ms5.company1@company1;gruu;opaque=svr:MediationServer:XzRY6u68aVipMcYVfYs0hQAA;grid=462
36573d0ae4a339d83726b2bf7f7ab>;isGateway
CONTENT-LENGTH: 422
SUPPORTED: replaces
SUPPORTED: ms-safe-transfer
SUPPORTED: ms-bypass
SUPPORTED: ms-dialog-route-set-update
SUPPORTED: gruu-10
SUPPORTED: timer
SUPPORTED: 100rel
CONTENT-TYPE: application/gw-sdp
ALLOW: ACK
P-ASSERTED-IDENTITY: <sip:+14258901234@company1;user=phone>
SERVER: Mediation Server
Ms-Accepted-Content-ID: <3d45476919eb4c81be0c4e19c730c655>
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresher=uas
Min-SE: 90

v=0
o=Gateway 1303417666 1303417345 IN IP4 10.1.2.12
s=session
c=IN IP4 10.1.2.12
t=0 0
m=audio 6390 RTP/SAVP 0 13 101
c=IN IP4 10.1.2.12
a=rtcp:6391
a=x-bypass
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:bN1zDJ0LC8QYNvMIohDtGkWD/rCastpGbZ5ObNo|2^31|244:1
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=x-mediasettings:signalboostunsupported
```

## 4.8 ms-mediation-generated SIP Header

The messages in the following subsections illustrate the use of the ms-mediation-generated Session Initiation Protocol (SIP) header in messages that are sent from and received by a protocol client.

## 4.8.1 Outbound Call



**Figure 12: Outbound Call**

The message in the following subsection illustrates the use of the ms-mediation-generated SIP header for outbound calls. For a diagram of the outbound call, see the preceding figure.

### 4.8.1.1 Step 5: 183 Message Is Received by the Protocol Client

```
SIP/2.0 183 Session Progress
Authentication-Info: NTLM rspauth="010000000000000008AC67ADF27DB686", srand="DF9D53C4",
snum="103", opaque="B25450B8", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:3137;ms-received-port=3137;ms-received-cid=100
FROM: "test1"<sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
```

```
TO: <sip:+15555550100@example.com;user=phone>;epid=6477F45221;tag=b5bb1243e3
CSEQ: 1 INVITE
CALL-ID: ca22890914c34bf8a7439dfe1e834420
ms-mediation-generated: yes
CONTENT-LENGTH: 740
CONTENT-TYPE: application/sdp; charset=utf-8
SERVER: RTCC/3.0.0.0 MediationServer
v=0
o=- 0 0 IN IP4 10.198.92.126
s=session
c=IN IP4 10.198.92.126
b=CT:1000
t=0 0
m=audio 60625 RTP/SAVP 111 115 8 97 101
c=IN IP4 10.198.92.126
a=rtcp:60532
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 1 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60625
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 2 Bx2Is+Wi/HJbdQKM3FIBKg UDP
0.900 10.198.92.126 60532
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:Pb+rI3y4U1xd47P8USsgDc/znOiBIv5s0Ev2abRT|2^31|1:1
a=label:main-audio
a=encryption:rejected
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:8 PCMA/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```

#### 4.8.1.2 Step 10: 180 Message Is Received by the Protocol Client

```
SIP/2.0 180 Ringing
Authentication-Info: NTLM rspauth="010000000000000008AC67ADF27DB686", srand="DF9D53C4",
snum="103", opaque="B25450B8", qop="auth", targetname="server1.example.com", realm="SIP
Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:3137;ms-received-port=3137;ms-received-cid=100
FROM: "test1"<sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
TO: <sip:+15555550100@example.com;user=phone>;epid=6477F45221;tag=b5bb1243e3
CSEQ: 1 INVITE
CALL-ID: ca22890914c34bf8a7439dfe1e834420
CONTENT-LENGTH: 0
```



## **5 Security**

### **5.1 Security Considerations for Implementers**

None.

### **5.2 Index of Security Parameters**

None.

## 6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

- Microsoft Office Communicator 2007
- Microsoft Office Communicator 2007 R2
- Microsoft Office Communications Server 2007
- Microsoft Office Communications Server 2007 R2
- Microsoft Lync 2010
- Microsoft Lync Server 2010
- Microsoft Lync Client 2013/Skype for Business
- Microsoft Lync Server 2013
- Microsoft Skype for Business 2016
- Microsoft Skype for Business Server 2015
- Microsoft Skype for Business 2019
- Microsoft Skype for Business Server 2019

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

[<1> Section 2.2.9](#): This header is not available in Office Communicator 2007, Office Communicator 2007 R2, Office Communications Server 2007, Office Communications Server 2007 R2, Lync 2010, or Lync Server 2010.

[<2> Section 3.2](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

[<3> Section 3.2](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

[<4> Section 3.2](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

[<5> Section 3.2](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

[<6> Section 3.2](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

[<7> Section 3.5](#): Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<8> [Section 3.6](#): Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<9> [Section 3.7](#): Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<10> [Section 3.8](#): Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<11> [Section 3.9](#): This behavior is not supported in Office Communicator 2007, Office Communicator 2007 R2, Lync 2010, Office Communications Server 2007, Office Communications Server 2007 R2, or Lync Server 2010.

## 7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

## 8 Index

### A

Abstract data model

- [anonymous phone URI](#) 20
- [isGateway parameter](#) 16
- [ms-accepted-content-id header](#) 21
- [ms-bypass option tag](#) 21
- [ms-call-source header](#) 18
- [ms-early-media option tag](#) 19
- [ms-mediation-generated header](#) 23
- [ms-trunking-peer header](#) 22
- [phone-context parameter](#) 17

[Anonymous phone URI](#) 20

- [abstract data model](#) 20
- [higher-layer triggered events](#) 20
- [initialization](#) 20
- [local events](#) 20
- [message processing](#) 20
- [timer events](#) 20
- [timers](#) 20

[Anonymous Phone URI message](#) 14

[Applicability](#) 11

### C

[Capability negotiation](#) 11

[Change tracking](#) 60

Contact header

- [isGateway parameter](#) 16

### E

[Examples](#) 24

- [isGateway SIP contact header parameter](#) 24

- [ms-accepted-content-id SIP header](#) 45

ms-bypass option tag

- [inbound call](#) 38

- [outbound call](#) 41

- [ms-bypass SIP supported header option tag](#) 38

- [ms-call-source SIP header](#) 32

- [ms-early-media SIP supported header option tag](#) 34

- [ms-mediation-generated SIP header](#) 54

- [ms-trunking-peer SIP header](#) 51

- [phone-context SIP URI parameter](#) 28

Supported header

- ms-bypass option tag

  - [inbound call](#) 38

  - [outbound call](#) 41

### F

[Fields - vendor-extensible](#) 12

### G

[Glossary](#) 7

### H

Higher-layer triggered events

- [anonymous phone URI](#) 20

- [isGateway parameter](#) 16

- [ms-accepted-content-id header](#) 22

- [ms-bypass option tag](#) 21

- [ms-call-source header](#) 18

- [ms-early-media option tag](#) 19

- [ms-mediation-generated header](#) 23

- [ms-trunking-peer header](#) 22

- [phone-context parameter](#) 17

### I

[Implementer - security considerations](#) 57

inbound call examples

- isGateway SIP contact header parameter

  - [200 message sent from UAC](#) 25

  - [INVITE message received by UAC](#) 24

- ms-accepted-content-id SIP header

  - [200 message sent by protocol client](#) 47

  - [INVITE message received by protocol client](#) 45

- ms-bypass SIP supported header option tag

  - [200 message sent by protocol client](#) 40

  - [INVITE message received by protocol client](#) 39

- ms-call-source SIP header

  - [200 message sent from UAC](#) 34

  - [605 message sent from UAC](#) 33

  - [INVITE message received by UAC - step 2](#) 32

  - [INVITE message received by UAC - step 8](#) 33

- ms-trunking-peer SIP header

  - [INVITE message received by protocol client](#) 52

- phone-context SIP URI parameter

  - [200 message sent from UAC](#) 29

  - [INVITE message received by UAC](#) 28

[Index of security parameters](#) 57

[Informative references](#) 9

Initialization

- [anonymous phone URI](#) 20

- [isGateway parameter](#) 16

- [ms-accepted-content-id](#) 22

- [ms-bypass option tag](#) 21

- [ms-call-source header](#) 18

- [ms-early-media option tag](#) 19

- ms-mediation-generated header ([section 3.9.3](#) 23, [section 6](#) 58)

- [ms-trunking-peer](#) 22

- [phone-context parameter](#) 17

[Introduction](#) 7

[isGateway](#) 16

- [abstract data model](#) 16

- [higher-layer triggered events](#) 16

- [initialization](#) 16

- [local events](#) 16

- [message processing](#) 16

- [timer events](#) 16

- [timers](#) 16

[isGateway message](#) 13

[isGateway SIP contact header parameter example](#) 24

- [inbound call](#) 24

  - [200 message sent from UAC](#) 25

  - [INVITE message received by UAC](#) 24

- [outbound call](#) 26

  - [200 message received by UAC](#) 27

  - [INVITE message sent from UAC](#) 26

## L

### Local events

- [anonymous phone URI](#) 20
- [isGateway parameter](#) 16
- [ms-accepted-content-id header](#) 22
- [ms-bypass option tag](#) 21
- [ms-call-source header](#) 19
- [ms-early-media option tag](#) 20
- [ms-trunking-peer header](#) 23
- [phone-context parameter](#) 18

## M

### Message processing

- [anonymous phone URI](#) 20
- [isGateway parameter](#) 16
- [ms-accepted-content-id header](#) 22
- [ms-bypass option tag](#) 21
- [ms-call-source header](#) 19
- [ms-early-media option tag](#) 19
- [ms-mediation-generated header](#) 23
- [ms-trunking-peer header](#) 22
- [phone-context parameter](#) 18

### Message syntax

### Messages

- [Anonymous Phone URI](#) 14
- [isGateway](#) 13
- [ms-accepted-content-id](#) 14
- [ms-bypass](#) 14
- [ms-call-source](#) 14
- [ms-early-media](#) 14
- [ms-mediation-generated](#) 15
- [ms-trunking-peer](#) 15
- [phone-context](#) 13
- [syntax](#) 13
- [transport](#) 13

### ms-accepted-content-id

- [abstract data model](#) 21
- [higher-layer triggered events](#) 22
- [initialization](#) 22
- [local events](#) 22
- [message processing](#) 22
- [timer events](#) 22
- [timers](#) 22

### ms-accepted-content-id message

### ms-accepted-content-id SIP header example

- [inbound call](#) 45
  - [200 message sent by protocol client](#) 47
  - [INVITE message received by protocol client](#) 45
- [outbound call](#) 48
  - [200 message received by protocol client](#) 51
  - [INVITE message sent by protocol client](#) 48

### ms-bypass

- [abstract data model](#) 21
- example
  - [inbound call](#) 38
  - [outbound call](#) 41
- [higher-layer triggered events](#) 21
- [initialization](#) 21
- [local events](#) 21
- [message processing](#) 21
- [timer events](#) 21
- [timers](#) 21

### ms-bypass message

### ms-bypass SIP supported header option tag example

- 38
  - [inbound call](#) 38
    - [200 message sent by protocol client](#) 40
    - [INVITE message received by protocol client](#) 39
  - [outbound call](#) 41
    - [200 OK message received by protocol client](#) 44
    - [INVITE message sent by protocol client](#) 42

### ms-call-source (section 3.3 18, section 3.4 19)

- [abstract data model](#) 18
- [higher-layer triggered events](#) 18
- [initialization](#) 18
- [local events](#) 19
- [message processing](#) 19
- [timer events](#) 19
- [timers](#) 18

### ms-call-source message

### ms-call-source SIP header example

- [inbound call](#) 32
  - [605 message sent from UAC](#) 33
  - [I200 message sent from UAC](#) 34
  - [INVITE message received by UAC – step 2](#) 32
  - [INVITE message received by UAC – step 8](#) 33
- [outbound call](#) 34

### ms-early-media

- [abstract data model](#) 19
- [higher-layer triggered events](#) 19
- [initialization](#) 19
- [local events](#) 20
- [message processing](#) 19
- [timer events](#) 20
- [timers](#) 19

### ms-early-media message

### ms-early-media SIP supported header option tag

- example 34
  - [inbound call](#) 34
  - [outbound call](#) 35
    - [183 message received by UAC](#) 36
    - [200 message received by UAC](#) 37
    - [INVITE sent from UAC](#) 35

### ms-mediation-generated

- [abstract data model](#) 23
- [higher-layer triggered events](#) 23
- initialization ([section 3.9.3](#) 23, [section 6](#) 58)
- [message processing](#) 23
- [other local events](#) 23
- [timer events](#) 23
- [timers](#) 23

### ms-mediation-generated message

### ms-mediation-generated SIP header example

- [outbound call](#) 55
  - [180 message received by protocol client](#) 56
  - [183 message received by protocol client](#) 55

### ms-trunking-peer

- [abstract data model](#) 22
- [higher-layer triggered events](#) 22
- [initialization](#) 22
- [local events](#) 23
- [message processing](#) 22
- [timer events](#) 22
- [timers](#) 22

### ms-trunking-peer message

### ms-trunking-peer SIP header example

- [inbound call](#) 52

[INVITE message received by protocol client](#) 52  
[outbound call](#) 53  
[200 message received by protocol client](#) 54

## N

[Normative references](#) 9

## O

Other local events

[ms-mediation-generated header](#) 23  
outbound call examples  
isGateway SIP contact header parameter  
[200 message received by UAC](#) 27  
[INVITE message sent from UAC](#) 26  
ms-accepted-content-id SIP header  
[200 message received by protocol client](#) 51  
[INVITE message sent by protocol client](#) 48  
ms-bypass SIP supported header option tag  
[200 OK message received by protocol client](#) 44  
[INVITE message sent by protocol client](#) 42  
ms-early-media SIP supported header option tag  
[183 message received by UAC](#) 36  
[200 message received by UAC](#) 37  
[INVITE sent from UAC](#) 35  
ms-mediation-generated SIP header  
[180 message received by protocol client](#) 56  
[183 message received by protocol client](#) 55  
ms-trunking-peer SIP header  
[200 message received by protocol client](#) 54  
phone-context SIP URI parameter  
[200 message received by UAC](#) 31  
[INVITE message sent from UAC](#) 30  
[Overview \(synopsis\)](#) 10

## P

[Parameters - security index](#) 57  
[phone-context](#) 16  
[abstract data model](#) 17  
[higher-layer triggered events](#) 17  
[initialization](#) 17  
[local events](#) 18  
[message processing](#) 18  
[timer events](#) 18  
[timers](#) 17  
[phone-context message](#) 13  
[phone-context SIP URI parameter example](#) 28  
[inbound call](#) 28  
[200 message sent from UAC](#) 29  
[INVITE message received by UAC](#) 28  
[outbound call](#) 30  
[200 message received by UAC](#) 31  
[INVITE message sent from UAC](#) 30  
[Preconditions](#) 11  
[Prerequisites](#) 11  
[Product behavior](#) 58

## R

[References](#) 9  
[informative](#) 9  
[normative](#) 9  
[Relationship to other protocols](#) 11

## S

Security  
[implementer considerations](#) 57  
[parameter index](#) 57  
SIP headers  
[ms-accepted-content-id](#) 21  
[ms-bypass option tag](#) 20  
[ms-call-source](#) 18  
[ms-early-media option tag](#) 19  
[ms-mediation-generated](#) 23  
[ms-trunking-peer](#) 22  
SIP URI  
[phone-context parameter](#) 16  
[Standards assignments](#) 12  
Supported header  
ms-bypass option tag  
example  
[inbound call](#) 38  
[outbound call](#) 41

## T

Timer events  
[anonymous phone URI](#) 20  
[isGateway parameter](#) 16  
[ms-accepted-content-id header](#) 22  
[ms-bypass option tag](#) 21  
[ms-call-source header](#) 19  
[ms-early-media option tag](#) 20  
[ms-mediation-generated header](#) 23  
[ms-trunking-peer header](#) 22  
[phone-context parameter](#) 18  
Timers  
[anonymous phone URI](#) 20  
[isGateway parameter](#) 16  
[ms-accepted-content-id header](#) 22  
[ms-bypass option tag](#) 21  
[ms-call-source header](#) 18  
[ms-early-media option tag](#) 19  
[ms-mediation-generated header](#) 23  
[ms-trunking-peer header](#) 22  
[phone-context parameter](#) 17  
[Tracking changes](#) 60  
[Transport](#) 13

## V

[Vendor-extensible fields](#) 12  
[Versioning](#) 11