

[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 for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **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 may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: <http://www.microsoft.com/interop/osp>) or the Community Promise (available here: <http://www.microsoft.com/interop/cp/default.mspx>). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplq@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events 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 specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do 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 are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial version
04/25/2008	0.2		Updated based on feedback
06/27/2008	1.0		Updated and revised the technical content.
08/15/2008	1.01		Revised and edited the technical content.
09/12/2008	1.02		Revised and edited the technical content.
12/12/2008	2.0		Updated and revised the technical content.
02/13/2009	2.01		Revised and edited the technical content.
03/13/2009	2.02		Revised and edited the technical content.
07/13/2009	2.03	Major	Revised and edited the technical content
08/28/2009	2.04	Editorial	Revised and edited the technical content
11/06/2009	2.05	Editorial	Revised and edited the technical content
02/19/2010	2.06	Editorial	Revised and edited the technical content
03/31/2010	2.07	Major	Updated and revised the technical content
04/30/2010	2.08	Editorial	Revised and edited the technical content
06/07/2010	2.09	Editorial	Revised and edited the technical content
06/29/2010	2.10	Editorial	Changed language and formatting in the technical content.
07/23/2010	2.10	No change	No changes to the meaning, language, or formatting of the technical content.
09/27/2010	3.0	Major	Significantly changed the technical content.
11/15/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction	6
1.1 Glossary	6
1.2 References	7
1.2.1 Normative References	7
1.2.2 Informative References	7
1.3 Protocol Overview (Synopsis)	8
1.4 Relationship to Other Protocols	10
1.5 Prerequisites/Preconditions	10
1.6 Applicability Statement	10
1.7 Versioning and Capability Negotiation	10
1.8 Vendor-Extensible Fields	11
1.9 Standards Assignments	11
2 Messages	12
2.1 Transport	12
2.2 Message Syntax	12
2.2.1 isGateway: SIP Contact Header Parameter	12
2.2.2 phone-context: SIP URI Parameter	12
2.2.3 ms-call-source: SIP Header	12
2.2.4 ms-early-media: SIP Supported Header Option Tag	12
2.2.5 ms-bypass: SIP Supported Header Option Tag	13
2.2.6 ms-accepted-content-id: SIP Header	13
2.2.7 ms-trunking-peer: SIP Header	13
3 Protocol Details	14
3.1 isGateway Contact Header Parameter	14
3.1.1 Abstract Data Model	14
3.1.2 Timers	14
3.1.3 Initialization	14
3.1.4 Higher-Layer Triggered Events	14
3.1.5 Message Processing Events and Sequencing Rules	14
3.1.6 Timer Events	14
3.1.7 Other Local Events	14
3.2 phone-context SIP URI Parameter	14
3.2.1 Abstract Data Model	15
3.2.2 Timers	16
3.2.3 Initialization	16
3.2.4 Higher-Layer Triggered Events	16
3.2.5 Message Processing Events and Sequencing Rules	16
3.2.6 Timer Events	16
3.2.7 Other Local Events	16
3.3 ms-call-source SIP Header	16
3.3.1 Abstract Data Model	17
3.3.2 Timers	17
3.3.3 Initialization	17
3.3.4 Higher-Layer Triggered Events	17
3.3.5 Message Processing Events and Sequencing Rules	17
3.3.6 Timer Events	17
3.3.7 Other Local Events	17
3.4 ms-early-media: SIP Supported Header Option Tag	17

3.4.1	Abstract Data Model	17
3.4.2	Timers	18
3.4.3	Initialization	18
3.4.4	Higher-Layer Triggered Events.....	18
3.4.5	Message Processing Events and Sequencing Rules.....	18
3.4.6	Timer Events	18
3.4.7	Other Local Events	18
3.5	Anonymous Phone URI	18
3.5.1	Abstract Data Model	18
3.5.2	Timers	18
3.5.3	Initialization	18
3.5.4	Higher-Layer Triggered Events.....	18
3.5.5	Message Processing Events and Sequencing Rules.....	18
3.5.6	Timer Events	19
3.5.7	Other Local Events	19
3.6	ms-bypass: SIP Supported Header Option Tag	19
3.6.1	Abstract Data Model	19
3.6.2	Timers	19
3.6.3	Initialization	19
3.6.4	Higher-Layer Triggered Events.....	19
3.6.5	Message Processing Events and Sequencing Rules.....	19
3.6.6	Timer Events	19
3.6.7	Other Local Events	19
3.7	ms-accepted-content-id: SIP Header.....	19
3.7.1	Abstract Data Model	20
3.7.2	Timers	20
3.7.3	Initialization	20
3.7.4	Higher-Layer Triggered Events.....	20
3.7.5	Message Processing Events and Sequencing Rules.....	20
3.7.6	Timer Events	20
3.7.7	Other Local Events	20
3.8	ms-trunking-peer: SIP Header.....	20
3.8.1	Abstract Data Model	20
3.8.2	Timers	20
3.8.3	Initialization	20
3.8.4	Higher-Layer Triggered Events.....	20
3.8.5	Message Processing Events and Sequencing Rules.....	21
3.8.6	Timer Events	21
3.8.7	Other Local Events	21
4	Protocol Examples.....	22
4.1	isGateway Contact Header Parameter.....	22
4.1.1	Inbound Call.....	22
4.1.1.1	Step 3: INVITE Message is Received by UAC	22
4.1.1.2	Step 7: 200 Message is Sent From UAC.....	23
4.1.2	Outbound Call.....	24
4.1.2.1	Step 1: INVITE Message is Sent From UAC	24
4.1.2.2	Step 12: 200 Message is Received by UAC.....	25
4.2	phone-context SIPURI Parameter.....	26
4.2.1	Inbound Call.....	26
4.2.1.1	Step 3: INVITE Message is Received by UAC	26
4.2.1.2	Step 7: 200 Message is Sent From UAC.....	27
4.2.2	Outbound Call.....	28

4.2.2.1	Step 1: INVITE Message is Sent From UAC	28
4.2.2.2	Step 12: 200 Message is Received by UAC.....	29
4.3	ms-call-source SIP Header	30
4.3.1	Inbound Call	30
4.3.1.1	Step 2: INVITE Message is Received by UAC	30
4.3.1.2	Step 8: INVITE Message is Received by UAC	31
4.3.1.3	Step 9: 605 Message is Sent From UAC.....	31
4.3.1.4	Step 12: 200 Message is Sent From UAC	32
4.3.2	Outbound Call.....	32
4.4	ms-early-media Supported Header Option Tag	32
4.4.1	Inbound Call	32
4.4.2	Outbound Call.....	33
4.4.2.1	Step 1: INVITE is Sent From UAC	33
4.4.2.2	Step 7: 183 Message is Received by UAC.....	34
4.4.2.3	Step 12: 200 Message is Received by UAC.....	35
4.5	ms-bypass: SIP Supported Header Option Tag	36
4.5.1	Inbound Call	37
4.5.1.1	Step 6: Invite Message is Received by Client.....	37
4.5.1.2	Step 17: 200 Message is Sent by Client.....	39
4.5.2	Outbound Call.....	40
4.5.2.1	Step 1: Invite Message is Sent by Client.....	40
4.5.2.2	Step 13: 200 OK Message is Received by Client.....	43
4.6	ms-accepted-content-id: SIP Header.....	44
4.6.1	Inbound Call	44
4.6.1.1	Step 6: Invite Message is Received by Client.....	45
4.6.1.2	Step 17: 200 Message is Sent by Client.....	46
4.6.2	Outbound Call.....	47
4.6.2.1	Step 1: Invite Message is Sent by Client.....	48
4.6.2.2	Step 13: 200 Message is Received by Client.....	50
4.7	ms-trunking-peer: SIP Header.....	51
4.7.1	Inbound Call	51
4.7.1.1	Step 6: Invite Message is Received by Client.....	51
4.7.2	Outbound Call.....	53
4.7.2.1	Step 13: 200 Message is Received by Client.....	53
5	Security.....	55
5.1	Security Considerations for Implementers.....	55
5.2	Index of Security Parameters	55
6	Appendix A: Product Behavior.....	56
7	Change Tracking.....	58
8	Index	59

1 Introduction

This document specifies 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.

1.1 Glossary

The following terms are defined in [\[MS-GLOS\]](#):

Augmented Backus-Naur Form (ABNF)
domain
domain name
fully qualified domain name (FQDN)

The following terms are defined in [\[MS-OFCGLOS\]](#):

200 OK
answer
call
dial plan
dialog
INVITE
MIME (Multipurpose Internet Mail Extensions)
offer
private branch exchange (PBX)
proxy
public switched telephone network (PSTN)
SDP answer
SDP offer
Session Description Protocol (SDP)
Session Initiation Protocol (SIP)
SIP message
SIP transaction
URI (Uniform Resource Identifier)
user agent client (UAC)
user agent server (UAS)

The following terms are specific to this document:

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.

E.164: An international public telecommunication numbering plan that is used in the public switched telephone network (PSTN) and some data networks, as described in [E164]. 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.

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

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

P-Asserted-Identity: 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.

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

1.2 References

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. We will assist you in finding the relevant information. Please check the archive site, <http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624>, as an additional source.

[MS-SDPEXT] Microsoft Corporation, "[Session Description Protocol \(SDP\) Version 2.0 Protocol Extensions](#)", June 2008.

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

[RFC2111] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", March 1997, <http://www.ietf.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.ietf.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.ietf.org/rfc/rfc3966.txt>

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "[Windows Protocols Master Glossary](#)", March 2007.

[MS-OFCGLOS] Microsoft Corporation, "[Microsoft Office Master Glossary](#)", June 2008.

[MS-SIPAE] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Authentication Extensions](#)", June 2008.

[MS-SIPRE] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Routing Extensions](#)", June 2008.

[MS-SIPREGE] Microsoft Corporation, "[Session Initiation Protocol \(SIP\) Registration Extensions](#)", June 2008.

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

[RFC3325] Jennings, C., Peterson, J., Watson, M., "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002, <http://www.ietf.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., Dean, R., "The Session Initiation Protocol (SIP) 'Replaces' Header", RFC 3891, September 2004, <http://www.ietf.org/rfc/rfc3891.txt>

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

1.3 Protocol Overview (Synopsis)

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 following extensions are specified in this protocol:

- **isGateway:** Contact SIP header parameter
- **phone-context:** SIP **URI** parameter as a context for a **dial string**, which is a phone number
- **ms-call-source:** SIP header
- **ms-early-media:** SIP **Supported** header option tag
- **anonymous:** Phone **URI**
- **ms-bypass:** SIP **Supported** header option tag
- **ms-accepted-content-id:** SIP header

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.

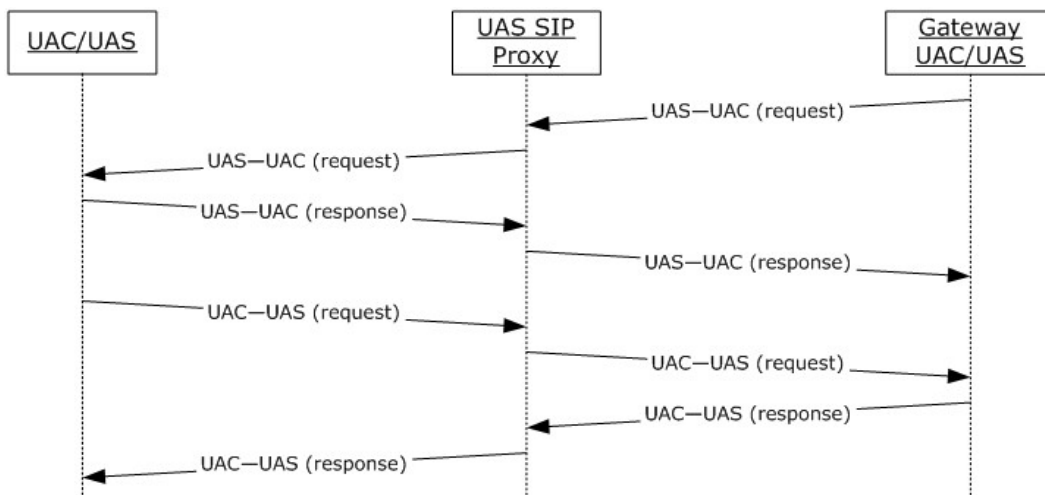


Figure 1: SIP transaction

This protocol defines a new **Contact** header parameter named **isGateway**. A SIP user agent (SIP UA) that uses this parameter in its **Contact** header indicates that it has a gateway role. This extension enables a SIP UA to be aware that a remote SIP UA in a SIP **dialog** is a gateway. This information can be rendered to the user interface (UI) to provide a better user experience (UX).

This protocol extends the semantics of a **phone-context** parameter, described in [\[RFC3966\]](#) sections 5 and 9. This extension enables a SIP **URI (Uniform Resource Identifier)** to hold an address of a dial string that is given by a user. 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.

This protocol defines a new SIP header, named **ms-call-source**. The purpose of this extension is to enable a SIP UAS to detect a redundant **call** that is triggered as a result of a loop. A loop occurs when a call is forked to a PBX that forks the call back, using a new SIP dialog. To detect a loop, this extension specifies a new **ms-call-source** header, which indicates the origin network of the call. The supported tokens for this 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 PBX or IP-PBX.

This protocol defines a new option tag, named **ms-early-media**, to the **Supported** header. This extension enables 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

Note: the standard recommends sending an SDP answer for **early media** only through a reliable provisional response.

This protocol defines an anonymous phone URI as an alternative to the standard anonymous SIP URI, described 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. An example of a SIP URI with these settings is as follows:

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

Note: the standard anonymous SIP URI is not supported.

This protocol defines a new option tag, named **ms-bypass**, to the **Supported** header. This extension enables a SIP UA in the protocol network to indicate that it supports media bypass functionality. 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.

This protocol defines a new SIP header, named **ms-accepted-content-id**. This extension enables 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. This header includes the value of the **Content-ID MIME** header associated with the selected SDP offer.

This protocol defines a new SIP header, named **ms-trunking-peer**. This header is used to identify the specific gateway used to interface with the PSTN for a PSTN call.

1.4 Relationship to Other Protocols

This protocol uses [\[MS-SIPAE\]](#), [\[MS-SIPREGE\]](#), [\[MS-SIPRE\]](#), [\[MS-SDPEXT\]](#) and the following IETF SIP specifications:

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

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 as specified in this section 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: SIP Contact Header Parameter

This protocol defines a new **Contact** header field parameter and its value. The original **Augmented Backus-Naur Form (ABNF)** for the **Contact** header field 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 following example is a **Contact** header field with the SIP **Contact** header field extension. The extension in the example is the final ";isGateway".

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

2.2.2 phone-context: SIP URI Parameter

This protocol extends the semantics of the **phone-context** parameter but does not change its syntax, as defined in [\[RFC3966\]](#).

The following example is a SIP URI with a **phone-context** parameter:

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

2.2.3 ms-call-source: SIP Header

The ABNF for the **ms-call-source** header is as follows:

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

2.2.4 ms-early-media: SIP Supported Header Option Tag

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

An example of the **ms-early-media** tag in the **Supported** header is as follows:

supported: ms-early-media

2.2.5 ms-bypass: SIP Supported Header Option Tag

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

2.2.6 ms-accepted-content-id: SIP Header

The ABNF for the **ms-accepted-content-id** header is as follows:

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

Content-id is as defined in [\[RFC2045\]](#) section 7 and [\[RFC2111\]](#) section 2.

An example of the **ms-accepted-content-id** header is as follows:

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

2.2.7 ms-trunking-peer: SIP Header

The ABNF for the **ms-trunking-peer** header is as follows:

```
ms-trunking-peer = "ms-trunking-peer" HCOLON host *1(SEMI User-Agent)
```

Host and **User-Agent** are as defined in [\[RFC3261\]](#) section 25.

An example of the **ms-trunking-peer** header is as follows:

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

3 Protocol Details

3.1 isGateway Contact Header Parameter

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 can 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 SIP URI Parameter

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

defined in [\[RFC3966\]](#) section 5.1.5. The **phone-context** value 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 UA 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**. 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<1> 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<2> be in either E.164 format or a private number with a **phone-context** that is set with the location profile of the UAC. An example of a SIP URI with a **phone-context** is the following:

```
sip:1234;phone-context=site-A@example.com;user=phone
```

Note: In the previous example, "example.com" is the **domain name** of the SIP URI. It is not affected by the **phone-context** parameter.

UAS Behavior

If a UAS has a gateway role, it SHOULD include a P-Asserted-Identity (PAI) in the **200 OK** that it sends in response to an initial INVITE used to establish a dialog. This 200 OK is typically derived 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 portion, 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 portion, the UAS SHOULD copy it to the 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 user agent to a trusted proxy to be inserted as the value in the **P-Asserted-Identity** header field.

A SIP proxy that receives an INVITE that contains a **phone-context** in the **From URI**, SHOULD<3> 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<4> apply the rules defined in the matched dial plan and add a PAI with the result of the translation. If the result of the translation is not an E.164 number, the proxy SHOULD<5> 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 SIP Header

UAC Behavior

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

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

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

UAS Behavior

If a UAS receives an INVITE message with a **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 a **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 a **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: SIP Supported Header Option Tag

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, which receives an INVITE with a **Supported** header that includes a **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, which 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

This section follows the product behavior as given in this footnote. [<6>](#)

The special **URI** "anonymous@host;user=phone" in the **From** header field MUST be used to denote an anonymous user; the **host** portion contains the appropriate 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: SIP Supported Header Option Tag

A UA supporting media bypass SHOULD [<7>](#) include a SIP **Supported** header with the **ms-bypass** option tag whenever it advertises the options it supports.

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: SIP Header

This section follows the product behavior described in footnote [<8>](#).

UAC Behavior

A UAC MUST include a **Content-ID MIME** header with each **MIME (Multipurpose Internet Mail Extensions)** type of "application/SDP" and "application/gw-sdp" that it sends in an offer. The SDP content is as 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.

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: SIP Header

This section follows the product behavior described in footnote [<9>](#).

The **ms-trunking-peer** 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 PSTN for a PSTN call.

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.

4 Protocol Examples

4.1 isGateway Contact Header Parameter

4.1.1 Inbound Call

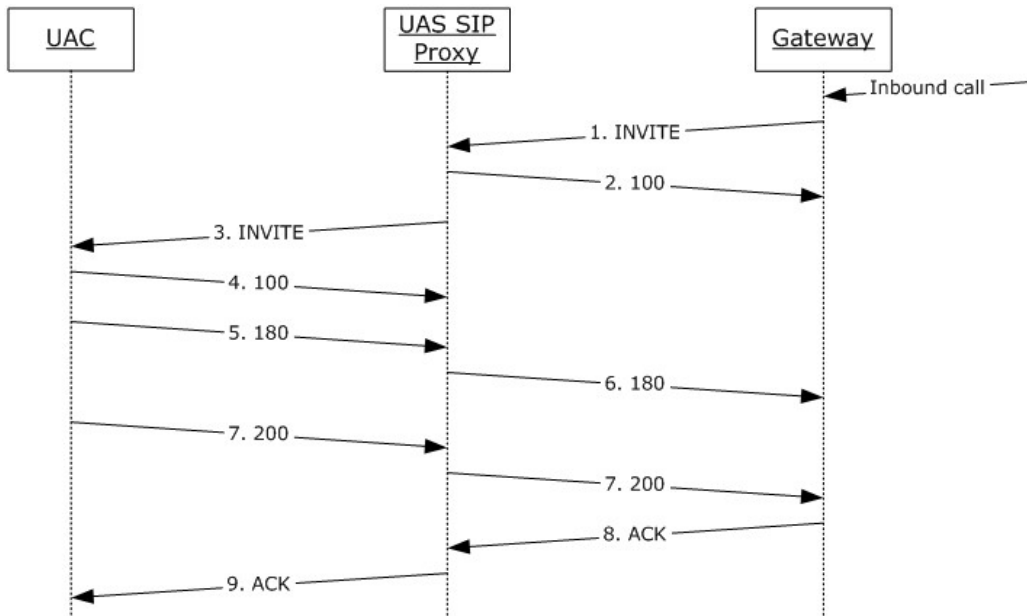


Figure 2: Inbound Call

This illustration 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 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=C8ybl0ausk5JrrJOeabpGevnl7YoohtFBsEB30y33pmWwR9xH_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: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

4.1.1.2 Step 7: 200 Message is Sent From UAC

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-internal-
info="daqI8a1fcNqkUHDJyMoUxdQuDrDTCwR9xH7_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=C8ybl0ausk5JrrJ0eabpGevnl7YoohtFBsEB30y33pmWwR9xH_oTAlgAA;ms-route-
sig=ea0mlvIX8ijETotqsV9nVQESDR_2qwr9xH_oTAlgAA>;tag=D78DE2B2FF72EB24FDA98B88DCC879B2
Contact: <sip:alice@server1.example.com;opaque=user:epid:reTyjuqAaVmcCIO4q1A4vwAA;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="602306092a864886f71201020201011100fffffffff77de9d7a16f9693a9cc29ed8d6735499"
Content-Type: application/sdp
```

4.1.2 Outbound Call

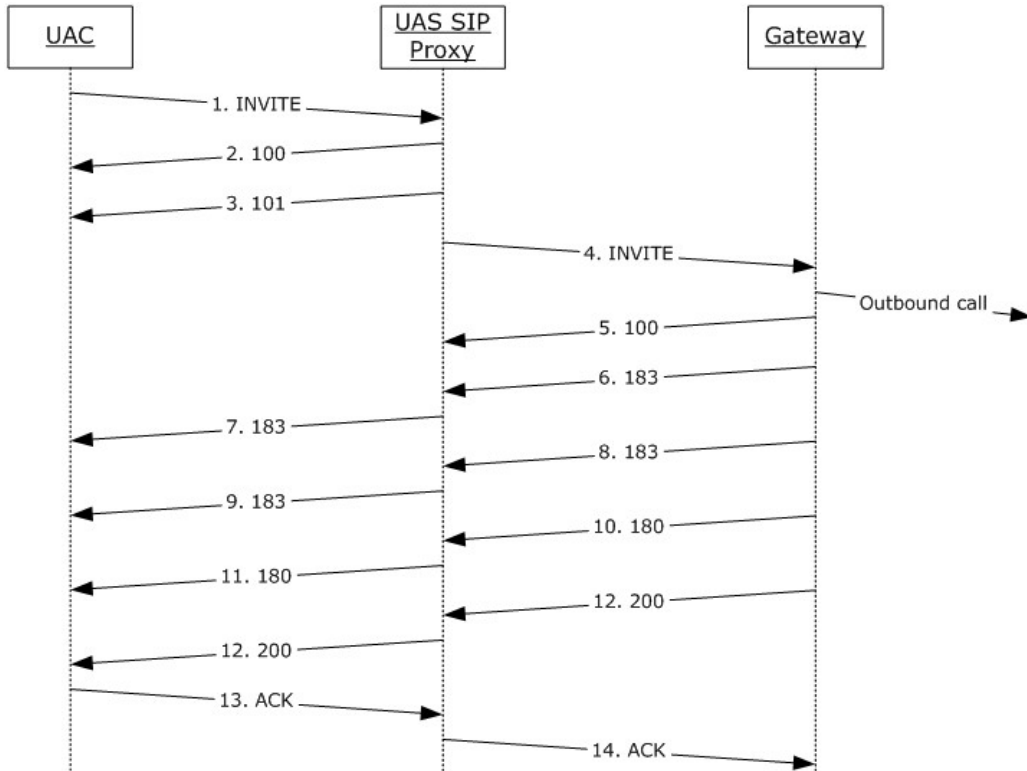


Figure 3: Outbound Call

This illustration 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 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 12: 200 Message is Received by UAC

```
SIP/2.0 200 OK
Authentication-Info: Kerberos
rspauth="602306092A864886F71201020201011100FFFFFFFF0714800DE2F658803052D07C86052224",
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=srvr:MediationServer:ANaNrdcy8EmB-
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 SIPURI Parameter

4.2.1 Inbound Call

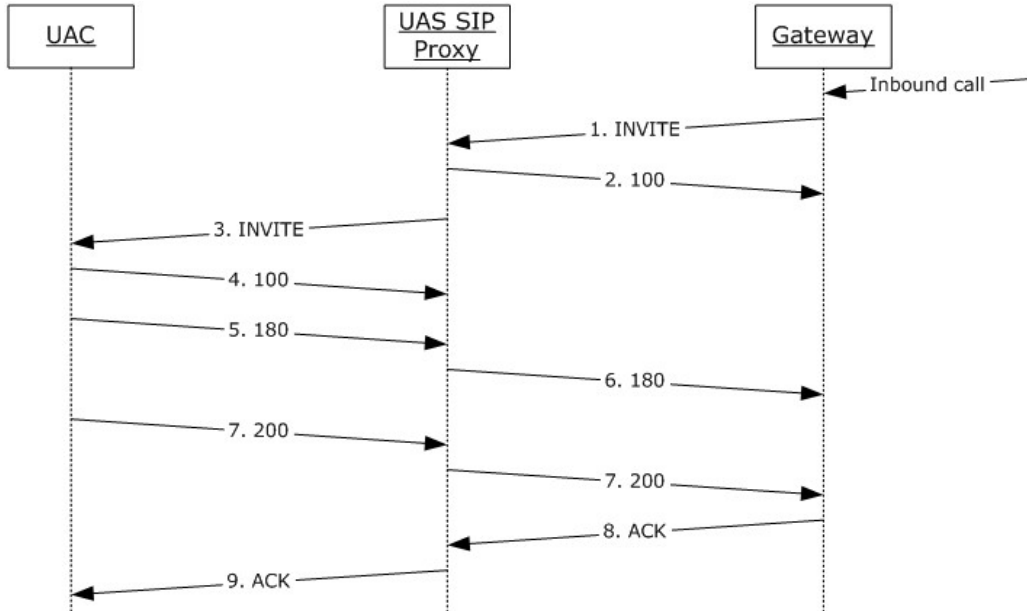


Figure 4: Inbound Call

This illustration 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 UAC

A UAS proxy replaces the **Request URI** with the **phone-context** 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="daqI8alfcNQkUHDJyMoUxdQudrDTCwR9xH7_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:+15555550103@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:ANaNrncy8EmB-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 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=C8ybl0ausk5JrrJOeabpGevnl7YoohtFBsEB30y33pmWwR9xH_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="602306092a864886f71201020201011100ffffffff77de9d7a16f9693a9cc29ed8d6735499"
Content-Type: application/sdp

4.2.2 Outbound Call

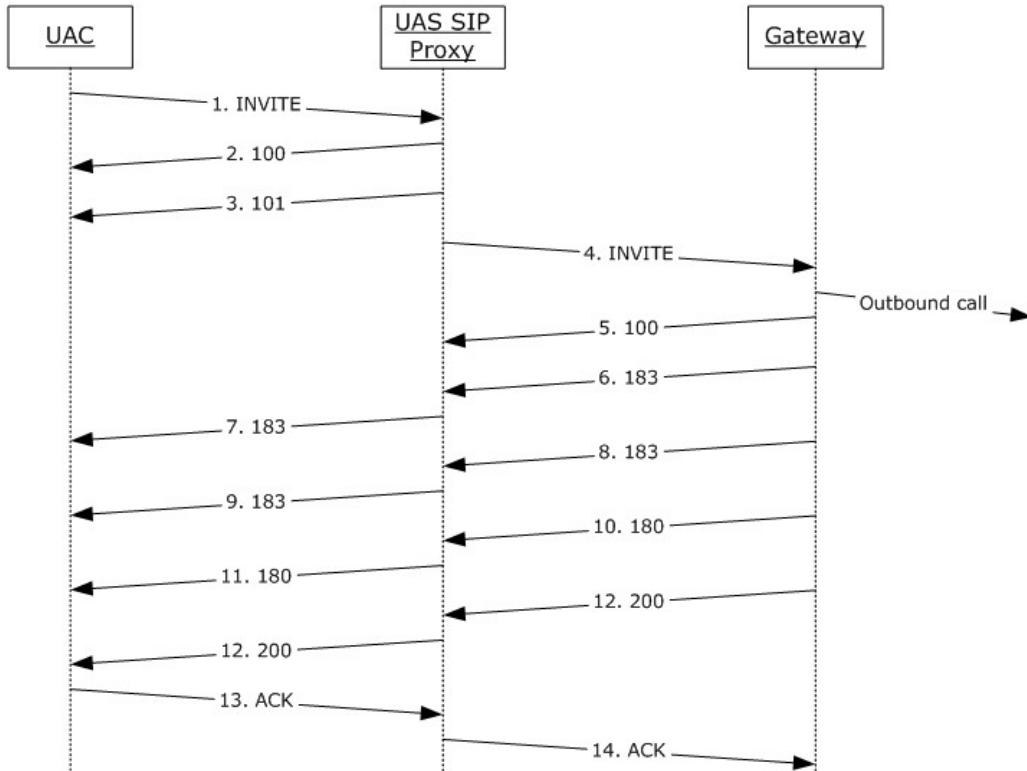


Figure 5: Outbound Call

This illustration 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 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/+DMH2N7C09hg==
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 12: 200 Message is Received by 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;grid=f1
f9379bd9334f65aaldfb77bed58905>;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

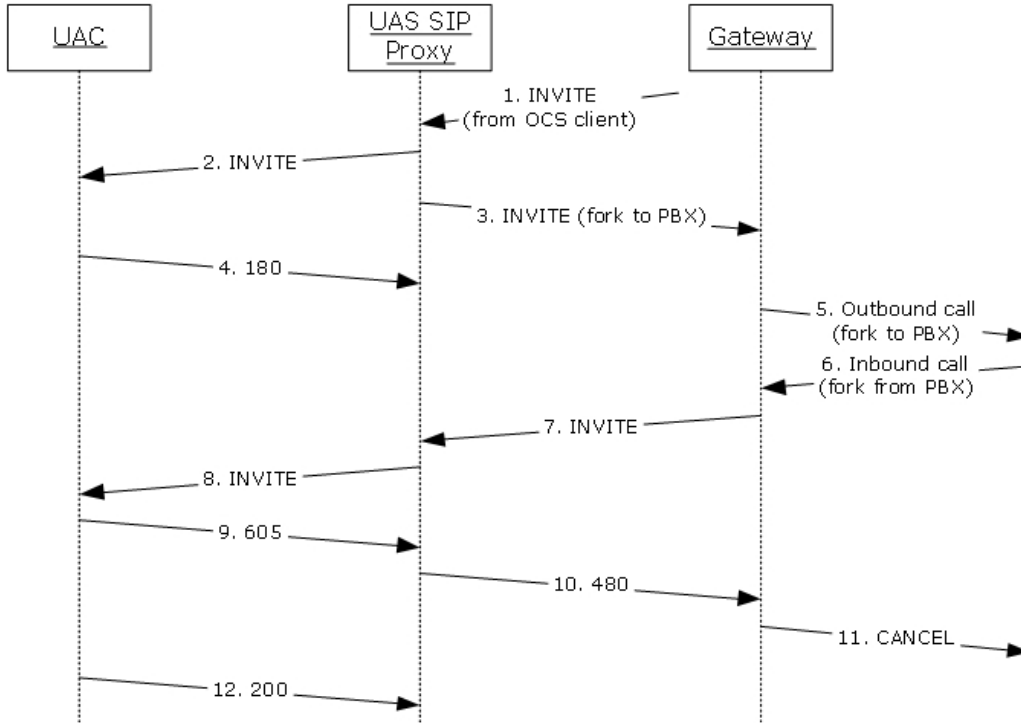


Figure 6: Inbound Call

This illustration 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 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_vlAjm36glJl-vlNQi15UxkBBihbkIPAAA"
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 UAC

This call originates from the 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=aa30eh935IYJmaV5AyTn4katb_Zd-6MHw6Lt2WZQAA>;tag=8951C70C798E10EA48EB96EAA4B379BC
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bKD300E89E.BA307C3A;branched=TRUE;ms-internal-info="aaK1z4lwQeqhL-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:+15555550108@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;grid=2c fb52f9fd4b4930a6f0a82dbfcd39e4>;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 UAC

This INVITE is rejected with a 605 Decline because it originated as a result of a loop in the 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="aaK1z4lwQeqhL-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:+15555550108@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 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_vlAjm36glJl-vlNQi15UxkBBihbkIPAAA"
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-ubLAoi5ZiOqMHLGcU3l0xkBBiLt2WZQAA>;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 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

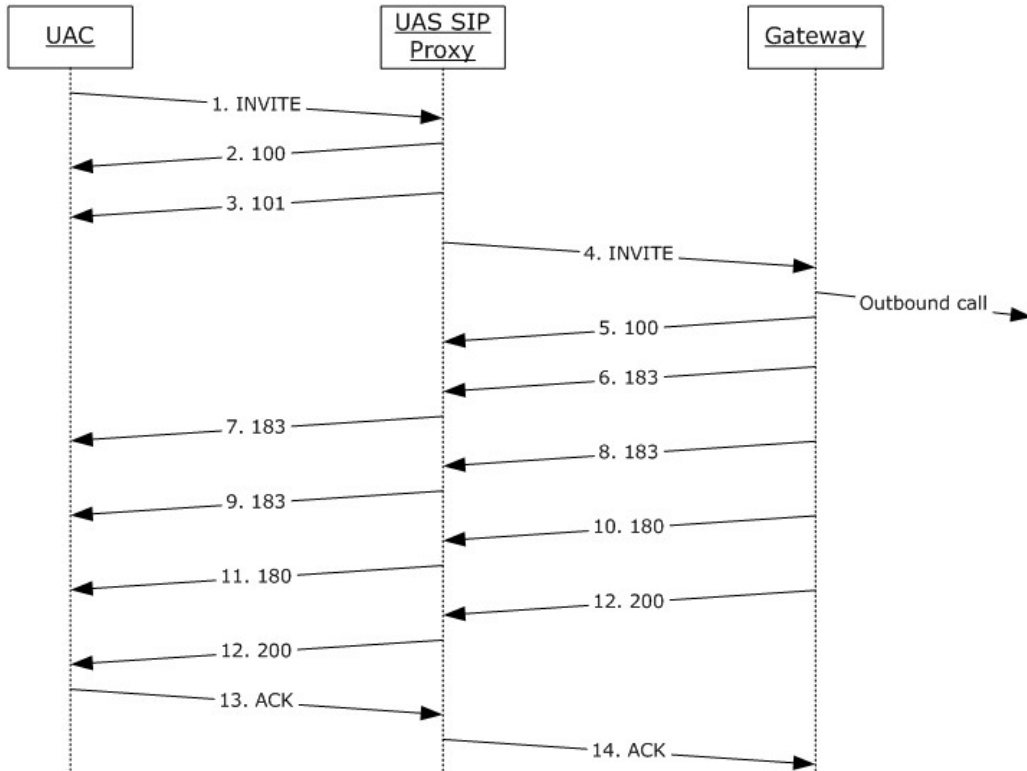


Figure 7: Outbound Call

This illustration 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 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: Achit1o1q5CCFcXhrKeZABfaZzvWNw==
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:aAzhJhKx1bOgjuVWNfI8C4f1K9lE5SJt6vFTAWP|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:VqAkQvuZOMKH1uaXvi+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 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 12: 200 Message is Received by 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: ca22890914c34bf8a7439dfele834420
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-route-
sig=aaelhWZJsyQvUcPVgXY5rCBgN5MnVHAhdiIeytlQAA>
CONTACT: <sip:SH13-
LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXhNJb1ZwQfgAA;grid=b6
796217d6ea465cbe261a778c10d5c0>;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

This section follows the behavior described in footnote [<10>](#).

4.5.1 Inbound Call

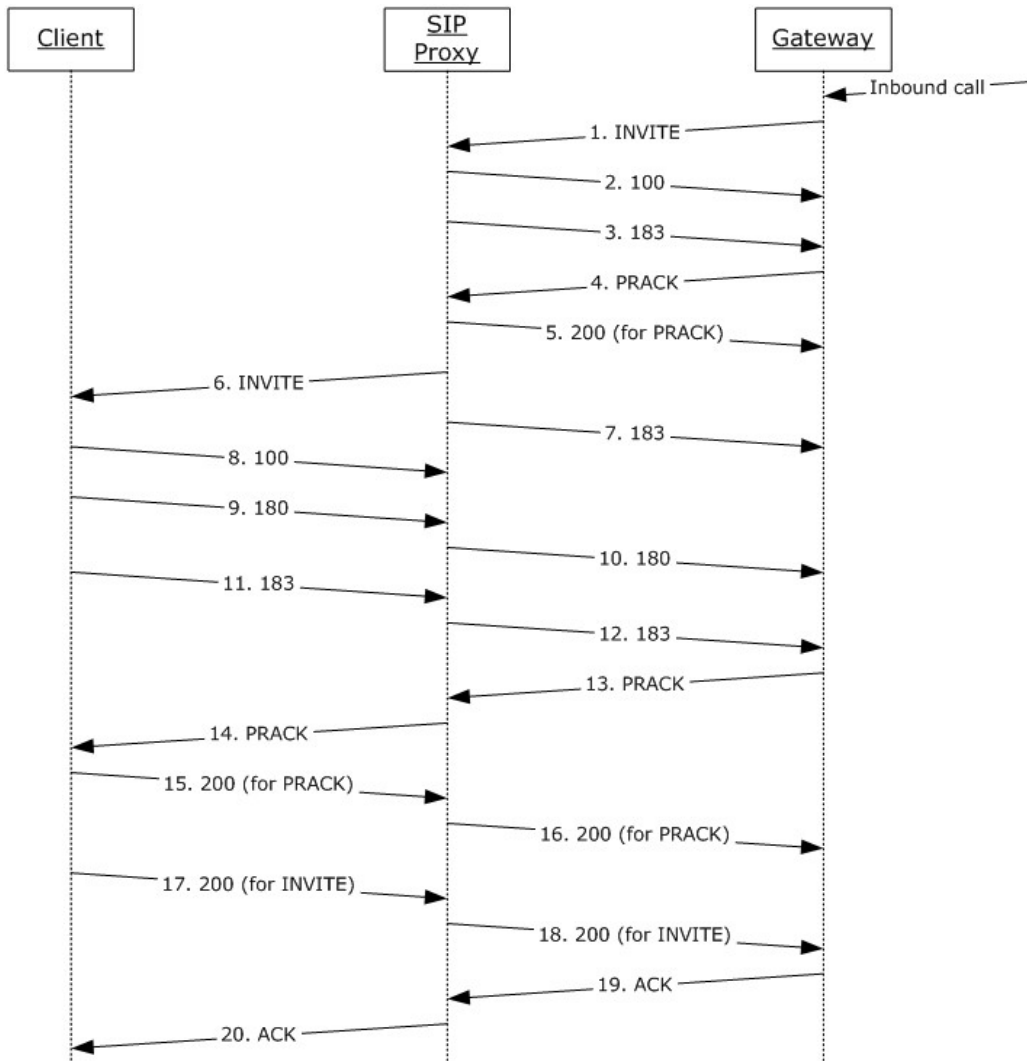


Figure 8: Inbound Call

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 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-
dRxH7lEBsv8oECfECdswTe7QW4niMEtoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzxxkq3iKgc2ApWyiXbCYC7NNwE-
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;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/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 55690
a=candidate:hdj57XrOXJwib/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 57652
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLWlFQ 1 8yhh8eM+T1Z9w0CbEkzWfA TCP 0.250
10.1.1.102 207 52082
a=candidate:JqHr0VQ3SBcleDZ+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:f6VloCUyKIzjLEBRg46FFt7BenyVzlLNek3EJ6T3|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtM1tvdv|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:1000000t=0 0m=audio 50352 RTP/AVP 0 8 115 13 118 97 101c=IN IP4
10.1.1.102a=rtcp:50353a=ice-ufrag:LxLAa=ice-pwd:3470M/yHdvxSWmMghs+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:f6VloCUyKIzjLEBRg46FFt7BenyVzlLNek3EJ6T3|2^31|1:1a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtM1tvdv|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=optionalv=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 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=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.gU65xODvWq_j78KvdcC-
dRxH7LEBsv8oECfECdswTe7QW4niMEtoToi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzvxkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40Contact:
<sip:user112@company1;opaque=user:epid:jVxLXK19112yFm93r_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: 362v=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:coOkWf6dIPsrYkRXi7QkjHb4n1ZwOQyZn0wWwBZR|2^3|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

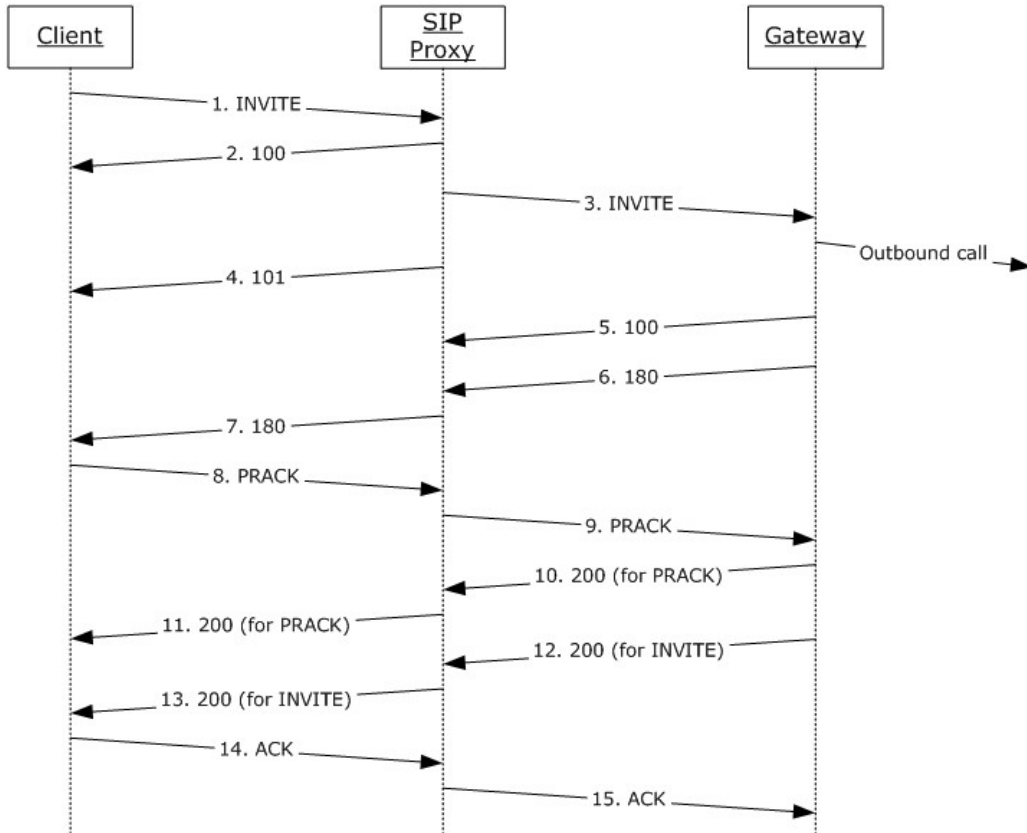


Figure 9: Outbound Call

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 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-byassid: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:ayqK
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: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-byassid:9CD08A01-E998-456a-AC8A-D028930E5933

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

4.5.2.2 Step 13: 200 OK Message is Received by 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=dcw0SbeehYaHu9dRxfqcNPNLaiGM-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;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/rCastpGbz5ObNo|2^31|244:1
```

```

a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
aptime:20
a=x-mediasettings:signalboostunsupported

```

4.6 ms-accepted-content-id: SIP Header

This section follows the behavior described in footnote [<11>](#).

4.6.1 Inbound Call

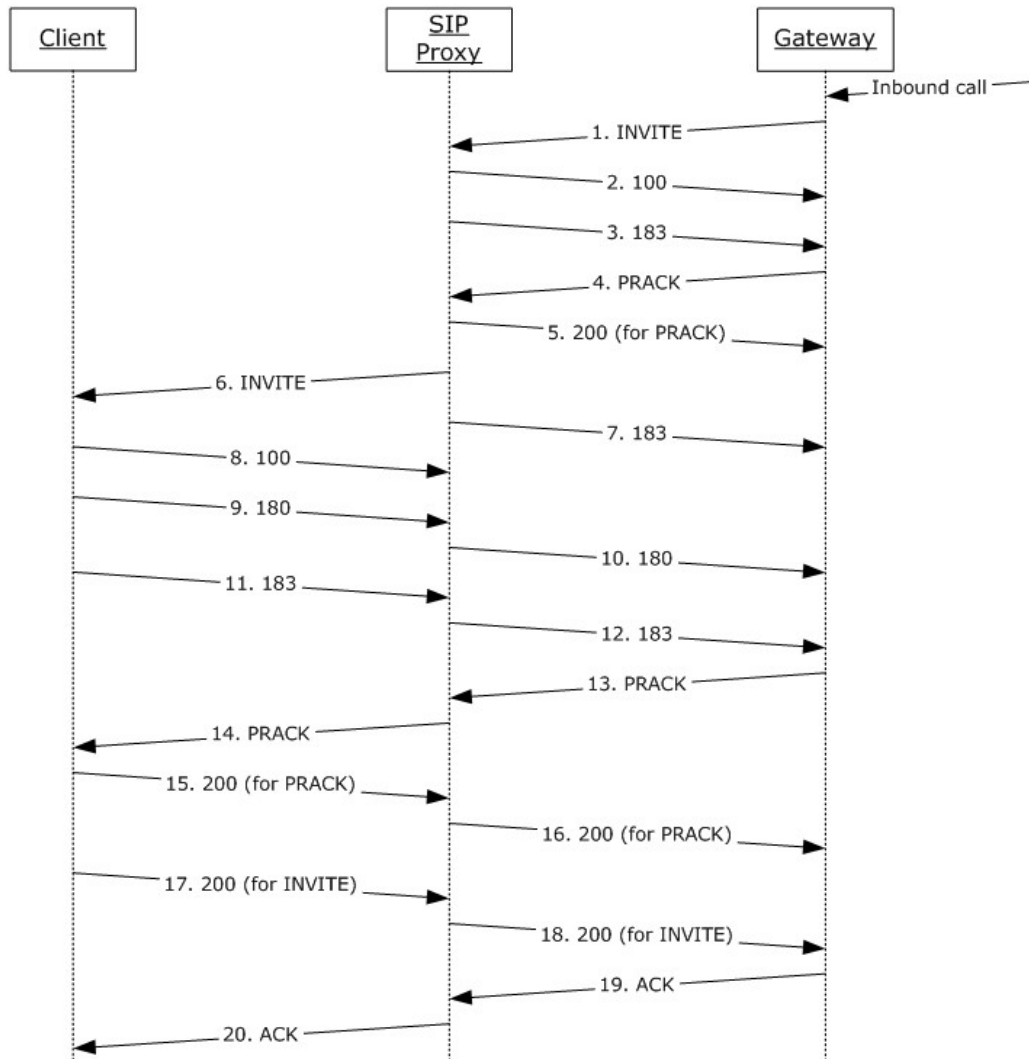


Figure 10: Inbound Call

The following messages illustrate the use of the **ms-accepted-content-id** 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 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-
dRxH7LEBsv8oECfECdswTe7QW4niMEtoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzxvkq3iKgc2ApWyIXbCYC7NNwE-
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;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 0tKavBjIaxiy4rc19atywg UDP 0.830
10.1.1.102 56568
```

```

a=candidate:wPBogiU8Nlp21GV4/zj/6WviEjTkj55FxrdrkHiZcc 2 0tKavBj1axiy4rc19atywg UDP 0.830
10.1.1.102 56569
a=candidate:bgLnsM3DP4aSPQloj2Ak1IUyGDPsldLRetvScj5izM 1 5VdtqvYZImPIpTh0Tx5Mcg TCP 0.150
10.3.0.7 59954
a=candidate:bgLnsM3DP4aSPQloj2Ak1IUyGDPsldLRetvScj5izM 2 5VdtqvYZImPIpTh0Tx5Mcg TCP 0.150
10.3.0.7 59954
a=candidate:hdj57XrOXJwib/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 55690
a=candidate:hdj57XrOXJwib/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 57652
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLwLFQ 1 8yhh8eM+T1Z9w0CbEkzWfA TCP 0.250
10.1.1.102 207 52082
a=candidate:JqHr0VQ3SBcleDZ+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+5hOmtM1tvdv|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:1000000t=0 0m=audio 50352 RTP/AVP 0 8 115 13 118 97 101c=IN IP4
10.1.1.102a=rtcp:50353a=ice-ufrag: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:f6V1oCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtM1tvdv|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=optionalv=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-

```

4.6.1.2 Step 17: 200 Message is Sent by 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=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.gU65xODvwq_j78KvdcC-
dRxH7LEBsv8oECfECdswTe7QW4niMEtoTOi_iwBgjHnKsZgY3jngAA;lr;ms-route-
sig=dcrEzvxvkq3iKgc2ApWyiXbCYC7NNwE-
pYCMYxgjFJ3kxfHnKsZgY3jngAA>;tag=45F7A969AE33112CB9877940D7F56D40Contact:
<sip:user112@company1;opaque=user:epid:jVxLXK19112yFm93r_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: 362v=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:coOkWf6dIPsrYkRXi7QkjHb4n1ZwOQyZn0wWwBZR|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

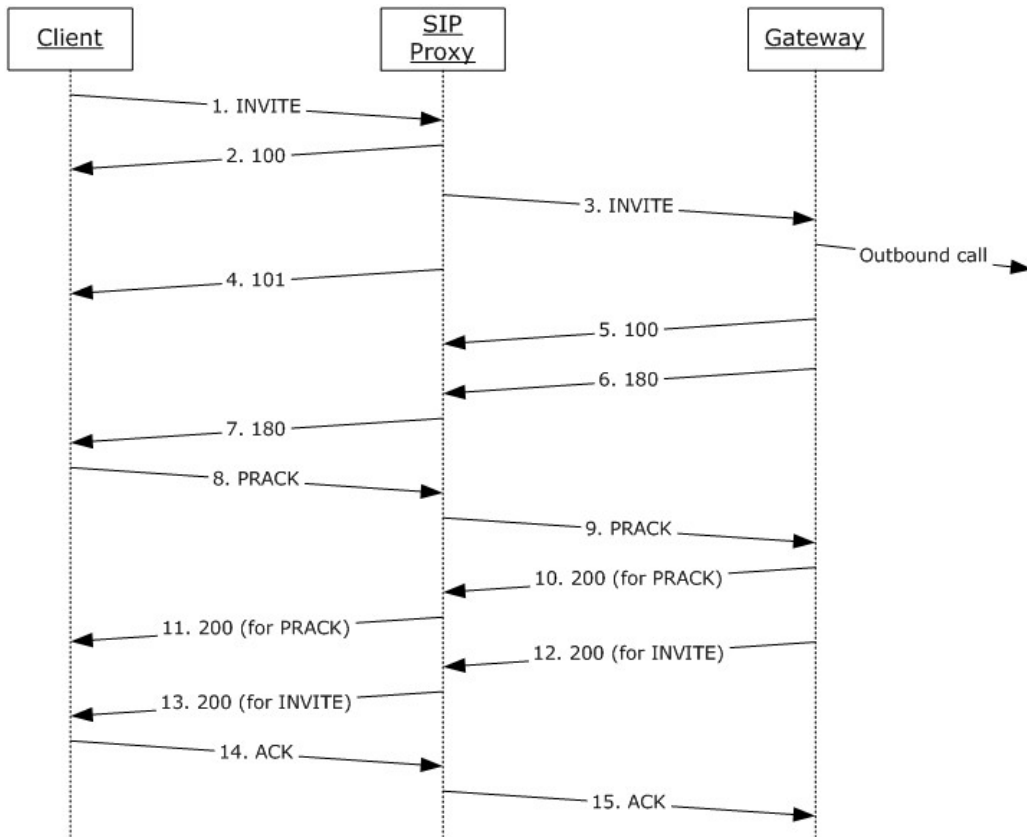


Figure 11: Outbound Call

The messages in the following subsections illustrate the use of the **ms-accepted-content-id** 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 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:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeooLhFH8L6sN1M 1 wiGTb6hg53yn1/Keu8TGSg TCP 0.190
10.3.0.7 57587
a=candidate:+oWYSe96Hnd9j7GRgjAf47ImvcM2GeooLhFH8L6sN1M 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:OY1qCCFx84fwIkrR39XpDA2HuNdtAB+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-frag:ayqK
a=ice-pwd:ckRbkR221v38PhlmgvzmVe5n
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--

```

4.6.2.2 Step 13: 200 Message is Received by 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;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/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

This section follows the behavior described in footnote [<12>](#).

4.7.1 Inbound Call

The messages in the following subsections illustrate the use of the **ms-trunking-peer** SIP header in messages that are sent from and received by a protocol client. 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 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-
dRxH7LEBsv8oECfECdswTe7QW4niMEtoTOi_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="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-diallog-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;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 0tKavBjlaxiy4rc19atywg UDP 0.830
10.1.1.102 56568
a=candidate:wPBogiU8Nlp21GV4/zj/6WviEjTkj55FxhrdRkHiZcc 2 0tKavBjlaxiy4rc19atywg 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/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 1 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 55690
a=candidate:hdj57XrOXJwib/pE8R3lzSwmfWi3trrUtRt4pmcfb5Y 2 RDbzrPzUksHqIX1Aqv0bFA UDP 0.450
10.3.0.7 57652
a=candidate:JqHr0VQ3SBcleDZ+TPZ4wktouOoWH1fag30kyuLwLFQ 1 8yhh8eM+T1Z9w0CbEkzWfA TCP 0.250
10.1.1.102 207 52082
a=candidate:JqHr0VQ3SBcleDZ+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+5hOmtM1tvdv|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:tbZ34R5hvhfBSvLMD0/uiQ7AWOCJD5Hj+Q58HQm|2^31
a=rtmpmap:0 PCMU/8000
a=rtmpmap:8 PCMA/8000
a=rtmpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtmpmap:13 CN/8000
a=rtmpmap:118 CN/16000a=rtmpmap:97 RED/8000a=rtmpmap: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:1000000t=0 0m=audio 50352 RTP/AVP 0 8 115 13 118 97 101c=IN IP4
10.1.1.102a=rtcp:50353a=ice-ufrag: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:f6VloCUyKIzjLEBRg46FFt7BenyVz1LNEk3EJ6T3|2^31|1:1a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:P46SfAzfbRN3d06tBm787I3Pv/3j+5hOmtM1tvdv|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=optionalv=0o=Gateway 94331345 94331031 IN IP4 10.1.2.12s=sessionc=IN IP4
10.1.2.12t=0 Om=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-

```

4.7.2 Outbound Call

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

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 released service packs:

- Microsoft® Office Communications Server 2007
- Microsoft® Office Communicator 2007
- Microsoft® Office Communications Server 2007 R2
- Microsoft® Office Communicator 2007 R2
- Microsoft® Lync™ 2010
- Microsoft® Lync™ Server 2010

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product 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 3.2:](#) Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

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

[<7> Section 3.6:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported. For all other products, a UA supporting media bypass is required to include a SIP Supported header with the ms-bypass option tag whenever it advertises the options it supports.

[<8> Section 3.7:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

[<9> Section 3.8:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

[<10> Section 4.5:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

[<11> Section 4.6:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

[<12> Section 4.7:](#) Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

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](#) 18
Contact header
 [isGateway parameter](#) 14
[isGateway](#) 14
[ms-accepted-content-id header](#) 20
[ms-bypass option tag](#) 19
[ms-call-source header](#) 17
[ms-early-media option tag](#) 17
[ms-trunking-peer header](#) 20
[phone-context parameter](#) 15
SIP URI
 [phone-context parameter](#) 15
Supported header
 [ms-bypass option tag](#) 19
 [ms-early-media option tag](#) 17
[Anonymous phone URI](#) 18
[abstract data model](#) 18
[higher-layer triggered events](#) 18
[initialization](#) 18
[local events](#) 19
[message processing](#) 18
[sequencing rules](#) 18
[timer events](#) 19
[timers](#) 18
[Applicability](#) 10

C

[Capability negotiation](#) 10
[Change tracking](#) 58
Contact header
 [isGateway parameter](#) 14
 abstract data model ([section 3.1.1](#) 14, [section 3.1.1](#) 14)
 example
 inbound call
 [200 sent from UAC](#) 23
 [INVITE received by UAC](#) 22
 [outbound call](#) 24
 [200 received by UAC](#) 25
 [INVITE sent from UAC](#) 24
 [higher-layer triggered events](#) 14
 [initialization](#) 14
 [local events](#) 14
 [message processing](#) 14
 [messages](#) 12
 [sequencing rules](#) 14
 [timer events](#) 14
 [timers](#) 14

D

Data model - abstract
[anonymous phone URI](#) 18
Contact header
 [isGateway parameter](#) 14

[isGateway](#) 14
[ms-accepted-content-id header](#) 20
[ms-bypass option tag](#) 19
[ms-call-source header](#) 17
[ms-early-media option tag](#) 17
[ms-trunking-peer header](#) 20
[phone-context parameter](#) 15
SIP URI
 [phone-context parameter](#) 15
Supported header
 [ms-bypass option tag](#) 19
 [ms-early-media option tag](#) 17

E

Examples
isGateway Contact header parameter
 [inbound call](#) 22
 [200 sent from UAC](#) 23
 [INVITE received by UAC](#) 22
 [outbound call](#) 24
 [200 received by UAC](#) 25
 [INVITE sent from UAC](#) 24
[ms-accepted-content-id header](#) 44
 [inbound call](#) 44
 [200 sent from UAC](#) 46
 [INVITE received by UAC](#) 45
 [outbound call](#) 47
 [200 received by UAC](#) 50
 [INVITE sent from UAC](#) 48
[ms-bypass option tag](#) 36
 [inbound call](#) 37
 [200 sent from UAC](#) 39
 [INVITE received by UAC](#) 37
 [outbound call](#) 40
 [200 received by UAC](#) 43
 [INVITE sent by UAC](#) 40
ms-call-source header
 [inbound call](#) 30
 [200 sent from UAC](#) 32
 [605 sent from UAC](#) 31
 INVITE received by UAC ([section 4.3.1.1](#) 30,
 [section 4.3.1.2](#) 31)
 [outbound call](#) 32
ms-early-media option tag
 [inbound call](#) 32
 [outbound call](#) 33
 [183 received by UAC](#) 34
 [200 received by UAC](#) 35
 [INVITE sent from UAC](#) 33
[ms-trunking-peer header](#) 51
 [inbound call](#) 51
 [INVITE received by UAC](#) 51
 [outbound call](#) 53
 [200 received by UAC](#) 53
phone-context SIP URI parameter
 [inbound call](#) 26
 [INVITE received by UAC](#) 26
 [message sent from UAC](#) 27

- [outbound call](#) 28
 - [200 received by UAC](#) 29
 - [INVITE sent from UAC](#) 28
- Supported header
 - [ms-bypass option tag](#) 36
 - [inbound call](#) 37
 - [200 sent from UAC](#) 39
 - [INVITE received by UAC](#) 37
 - [outbound call](#) 40
 - [200 received by UAC](#) 43
 - [INVITE sent by UAC](#) 40
- ms-early-media option tag
 - [inbound call](#) 32
 - [outbound call](#) 33
 - [183 received by UAC](#) 34
 - [200 received by UAC](#) 35
 - [INVITE sent from UAC](#) 33

F

- [Fields - vendor-extensible](#) 11

G

- [Glossary](#) 6

H

- Higher-layer triggered events
 - [anonymous phone URI](#) 18
- Contact header
 - [isGateway parameter](#) 14
- [isGateway](#) 14
- [ms-accepted-content-id header](#) 20
- [ms-bypass option tag](#) 19
- [ms-call-source header](#) 17
- [ms-early-media option tag](#) 18
- [ms-trunking-peer header](#) 20
- [phone-context parameter](#) 16
- SIP URI
 - [phone-context parameter](#) 16
- Supported header
 - [ms-bypass option tag](#) 19
 - [ms-early-media option tag](#) 18

I

- [Implementer - security considerations](#) 55
- [Index of security parameters](#) 55
- [Informative references](#) 7
- Initialization
 - [anonymous phone URI](#) 18
- Contact header
 - [isGateway parameter](#) 14
- [isGateway](#) 14
- [ms-accepted-content-id](#) 20
- [ms-bypass option tag](#) 19
- [ms-call-source header](#) 17
- [ms-early-media option tag](#) 18
- [ms-trunking-peer](#) 20
- [phone-context parameter](#) 16
- SIP URI

- [phone-context parameter](#) 16
- Supported header
 - [ms-bypass option tag](#) 19
 - [ms-early-media option tag](#) 18

J

- [isGateway: SIP Contact Header Parameter message](#) 12

K

- Local events
 - [anonymous phone URI](#) 19
- Contact header
 - [isGateway parameter](#) 14
- [isGateway](#) 14
- [ms-accepted-content-id header](#) 20
- [ms-bypass option tag](#) 19
- [ms-call-source header](#) 17
- [ms-early-media option tag](#) 18
- [ms-trunking-peer header](#) 21
- [phone-context parameter](#) 16
- SIP URI
 - [phone-context parameter](#) 16
- Supported header
 - [ms-bypass option tag](#) 19
 - [ms-early-media option tag](#) 18

L

- Message processing
 - [anonymous phone URI](#) 18
- Contact header
 - [isGateway parameter](#) 14
- [isGateway](#) 14
- [ms-accepted-content-id header](#) 20
- [ms-bypass option tag](#) 19
- [ms-call-source header](#) 17
- [ms-early-media option tag](#) 18
- [ms-trunking-peer header](#) 21
- [phone-context parameter](#) 16
- SIP URI
 - [phone-context parameter](#) 16
- Supported header
 - [ms-bypass option tag](#) 19
 - [ms-early-media option tag](#) 18

M

- [Messages](#) 12

- [isGateway: SIP Contact Header Parameter](#) 12
- [ms-accepted-content-id: SIP Header](#) 13
- [ms-bypass: SIP Supported Header Option Tag](#) 13
- [ms-call-source: SIP Header](#) 12
- [ms-early-media: SIP Supported Header Option Tag](#) 12
- [ms-trunking-peer: SIP Header](#) 13
- [phone-context: SIP URI Parameter](#) 12
- [transport](#) 12
- ms-accepted-content-id ([section 2.2.6](#) 13, [section 3.7](#) 19)
 - [abstract data model](#) 20
 - [example](#) 44
 - [higher-layer triggered events](#) 20
 - [initialization](#) 20
 - [local events](#) 20
 - [message processing](#) 20
 - [sequencing rules](#) 20
 - [timer events](#) 20
 - [timers](#) 20
- ms-accepted-content-id: SIP Header message 13
- ms-bypass ([section 2.2.5](#) 13, [section 3.6](#) 19)
 - [abstract data model](#) 19
 - [example](#) 36
 - [inbound call](#) 37
 - [200 sent from UAC](#) 39
 - [INVITE received by UAC](#) 37
 - [outbound call](#) 40
 - [200 received by UAC](#) 43
 - [INVITE sent by UAC](#) 40
 - [higher-layer triggered events](#) 19
 - [initialization](#) 19
 - [local events](#) 19
 - [message processing](#) 19
 - [sequencing rules](#) 19
 - [timer events](#) 19
 - [timers](#) 19
- ms-bypass: SIP Supported Header Option Tag message 13
- ms-call-source ([section 2.2.3](#) 12, [section 3.3](#) 16)
 - [abstract data model](#) 17
 - example
 - [inbound call](#) 30
 - [200 sent from UAC](#) 32
 - [605 sent from UAC](#) 31
 - INVITE received by UAC ([section 4.3.1.1](#) 30, [section 4.3.1.2](#) 31)
 - [outbound call](#) 32
 - [higher-layer triggered events](#) 17
 - [initialization](#) 17
 - [local events](#) 17
 - [message processing](#) 17
 - [sequencing rules](#) 17
 - [timer events](#) 17
 - [timers](#) 17
- ms-call-source: SIP Header message 12
- ms-early-media 17
 - [abstract data model](#) 17
 - example
 - [inbound call](#) 32
 - [outbound call](#) 33
 - [183 received by UAC](#) 34
 - [200 received by UAC](#) 35
 - [INVITE sent from UAC](#) 33
 - [higher-layer triggered events](#) 18
 - [initialization](#) 18
 - [local events](#) 18
 - [message processing](#) 18
 - [sequencing rules](#) 18
 - [timer events](#) 18
 - [timers](#) 18
- ms-early-media: SIP Supported Header Option Tag message 12
- ms-trunking peer
 - [sequencing rules](#) 21
- ms-trunking-peer ([section 2.2.7](#) 13, [section 3.8](#) 20)
 - [abstract data model](#) 20
 - [example](#) 51
 - [inbound call](#) 51
 - [outbound call](#) 53
 - [higher-layer triggered events](#) 20
 - [initialization](#) 20
 - [local events](#) 21
 - [message processing](#) 21
 - [timer events](#) 21
 - [timers](#) 20
- ms-trunking-peer: SIP Header message 13

N

- [Normative references](#) 7

O

- [Overview \(synopsis\)](#) 8

P

- [Parameters - security index](#) 55
- [phone-context](#) 14
 - [abstract data model](#) 15
 - example
 - [inbound call](#) 26
 - [INVITE received by UAC](#) 26
 - [message sent from UAC](#) 27
 - [outbound call](#) 28
 - [200 received by UAC](#) 29
 - [INVITE sent from UAC](#) 28
 - [higher-layer triggered events](#) 16
 - [initialization](#) 16
 - [local events](#) 16
 - [message processing](#) 16
 - [sequencing rules](#) 16
 - [timer events](#) 16
 - [timers](#) 16
- [phone-context: SIP URI Parameter message](#) 12
- [Preconditions](#) 10
- [Prerequisites](#) 10
- [Product behavior](#) 56

R

- References

[informative](#) 7
[normative](#) 7
[Relationship to other protocols](#) 10

S

Security
[implementer considerations](#) 55
[parameter index](#) 55

Sequencing rules
[anonymous phone URI](#) 18
Contact header
[isGateway parameter](#) 14
[isGateway](#) 14
[ms-accepted-content-id header](#) 20
[ms-bypass option tag](#) 19
[ms-call-source header](#) 17
[ms-early-media option tag](#) 18
[ms-trunking-peer header](#) 21
[phone-context parameter](#) 16

SIP URI
[phone-context parameter](#) 16

Supported header
[ms-bypass option tag](#) 19
[ms-early-media option tag](#) 18

SIP headers

Contact
isGateway parameter ([section 2.2.1](#) 12, [section 3.1](#) 14)
ms-accepted-content-id ([section 2.2.6](#) 13, [section 3.7](#) 19)
ms-call-source ([section 2.2.3](#) 12, [section 3.3](#) 16)
ms-trunking-peer ([section 2.2.7](#) 13, [section 3.8](#) 20)

Supported
[ms-bypass option tag](#) 13
ms-early-media option tag ([section 2.2.4](#) 12, [section 3.4](#) 17)

SIP URI
[phone-context parameter](#) 14
[abstract data model](#) 15
example
[inbound call](#) 26
[INVITE received by UAC](#) 26
[message sent from UAC](#) 27
[outbound call](#) 28
[200 received by UAC](#) 29
[INVITE sent from UAC](#) 28
[higher-layer triggered events](#) 16
[initialization](#) 16
[local events](#) 16
[message processing](#) 16
[messages](#) 12
[sequencing rules](#) 16
[timer events](#) 16
[timers](#) 16

[Standards assignments](#) 11

Supported header
[ms-bypass option tag](#) 19
[abstract data model](#) 19
[example](#) 36
[inbound call](#) 37

[200 sent from UAC](#) 39
[INVITE received by UAC](#) 37
[outbound call](#) 40
[200 received by UAC](#) 43
[INVITE sent by UAC](#) 40
[higher-layer triggered events](#) 19
[initialization](#) 19
[local events](#) 19
[message processing](#) 19
[messages](#) 13
[sequencing rules](#) 19
[timer events](#) 19
[timers](#) 19

[ms-early-media option tag](#) 17
[abstract data model](#) 17
example
[inbound call](#) 32
[outbound call](#) 33
[183 received by UAC](#) 34
[200 received by UAC](#) 35
[INVITE sent from UAC](#) 33
[higher-layer triggered events](#) 18
[initialization](#) 18
[local events](#) 18
[message processing](#) 18
[messages](#) 12
[sequencing rules](#) 18
[timer events](#) 18
[timers](#) 18

T

Timer events
[anonymous phone URI](#) 19
Contact header
[isGateway parameter](#) 14
[isGateway](#) 14
[ms-accepted-content-id header](#) 20
[ms-bypass option tag](#) 19
[ms-call-source header](#) 17
[ms-early-media option tag](#) 18
[ms-trunking-peer header](#) 21
[phone-context parameter](#) 16

SIP URI
[phone-context parameter](#) 16

Supported header
[ms-bypass option tag](#) 19
[ms-early-media option tag](#) 18

Timers
[anonymous phone URI](#) 18
Contact header
[isGateway parameter](#) 14
[isGateway](#) 14
[ms-accepted-content-id header](#) 20
[ms-bypass option tag](#) 19
[ms-call-source header](#) 17
[ms-early-media option tag](#) 18
[ms-trunking-peer header](#) 20
[phone-context](#) 16

SIP URI
[phone-context parameter](#) 16

Supported header

- [ms-bypass option tag](#) 19
 - [ms-early-media option tag](#) 18
- [Tracking changes](#) 58
- [Transport](#) 12
- Triggered events
 - [anonymous phone URI](#) 18
 - Contact header
 - [isGateway parameter](#) 14
 - [isGateway](#) 14
 - [ms-accepted-content-id header](#) 20
 - [ms-bypass tag option tag](#) 19
 - [ms-call-source header](#) 17
 - [ms-early-media tag option tag](#) 18
 - [ms-trunking-peer header](#) 20
 - [phone-context parameter](#) 16
- SIP URI
 - [phone-context parameter](#) 16
- Supported header
 - [ms-bypass tag option tag](#) 19
 - [ms-early-media tag option tag](#) 18

V

- [Vendor-extensible fields](#) 11
- [Versioning](#) 10