Session Initiation Protocol (SIP) for PSTN Calls Extensions

Technical Documentation. Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.

Copyrights. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.

No Trade Secrets. Microsoft does not claim any trade secret rights in this documentation.

Patents. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.

License Programs. To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.

Trademarks. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.

Fictitious Names. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

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

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

Support. For questions and support, please contact dochelp@microsoft.com.
## Revision Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision History</th>
<th>Revision Class</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/4/2008</td>
<td>0.1</td>
<td>New</td>
<td>Initial version</td>
</tr>
<tr>
<td>4/25/2008</td>
<td>0.2</td>
<td>Minor</td>
<td>Updated based on feedback</td>
</tr>
<tr>
<td>6/27/2008</td>
<td>1.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>8/15/2008</td>
<td>1.01</td>
<td>Minor</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>9/12/2008</td>
<td>1.02</td>
<td>Minor</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>12/12/2008</td>
<td>2.0</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>2/13/2009</td>
<td>2.01</td>
<td>Minor</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>3/13/2009</td>
<td>2.02</td>
<td>Minor</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>7/13/2009</td>
<td>2.03</td>
<td>Major</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>8/28/2009</td>
<td>2.04</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>11/6/2009</td>
<td>2.05</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>2/19/2010</td>
<td>2.06</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>3/31/2010</td>
<td>2.07</td>
<td>Major</td>
<td>Updated and revised the technical content.</td>
</tr>
<tr>
<td>4/30/2010</td>
<td>2.08</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>6/7/2010</td>
<td>2.09</td>
<td>Editorial</td>
<td>Revised and edited the technical content.</td>
</tr>
<tr>
<td>6/29/2010</td>
<td>2.10</td>
<td>Editorial</td>
<td>Changed language and formatting in the technical content.</td>
</tr>
<tr>
<td>7/23/2010</td>
<td>2.10</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/27/2010</td>
<td>3.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>11/15/2010</td>
<td>3.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>12/17/2010</td>
<td>3.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>3/18/2011</td>
<td>3.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>6/10/2011</td>
<td>3.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>1/20/2012</td>
<td>4.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>4/11/2012</td>
<td>4.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>7/16/2012</td>
<td>4.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>10/8/2012</td>
<td>4.0.1</td>
<td>Editorial</td>
<td>Changed language and formatting in the technical content.</td>
</tr>
<tr>
<td>2/11/2013</td>
<td>4.0.1</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>Date</td>
<td>Revision History</td>
<td>Revision Class</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>7/30/2013</td>
<td>4.0.1</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>11/18/2013</td>
<td>4.0.1</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>2/10/2014</td>
<td>4.0.1</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>4/30/2014</td>
<td>4.1</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>7/31/2014</td>
<td>4.2</td>
<td>Minor</td>
<td>Clarified the meaning of the technical content.</td>
</tr>
<tr>
<td>10/30/2014</td>
<td>4.2</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>3/30/2015</td>
<td>5.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>9/4/2015</td>
<td>5.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>7/15/2016</td>
<td>5.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/14/2016</td>
<td>5.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>9/29/2016</td>
<td>5.0</td>
<td>None</td>
<td>No changes to the meaning, language, or formatting of the technical content.</td>
</tr>
<tr>
<td>4/27/2018</td>
<td>6.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>7/24/2018</td>
<td>7.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
<tr>
<td>8/28/2018</td>
<td>8.0</td>
<td>Major</td>
<td>Significantly changed the technical content.</td>
</tr>
</tbody>
</table>
# Table of Contents

## 1 Introduction

1.1 Glossary .................................................................................................................. 7
1.2 References .............................................................................................................. 9
   1.2.1 Normative References .................................................................................... 9
   1.2.2 Informative References .................................................................................. 9
1.3 Overview ................................................................................................................ 10
1.4 Relationship to Other Protocols ........................................................................ 11
1.5 Prerequisites/Preconditions ............................................................................... 11
1.6 Applicability Statement ..................................................................................... 11
1.7 Versioning and Capability Negotiation ............................................................ 11
1.8 Vendor-Extensible Fields .................................................................................... 12
1.9 Standards Assignments ...................................................................................... 12

## 2 Messages

2.1 Transport ............................................................................................................... 13
2.2 Message Syntax .................................................................................................. 13
   2.2.1 isGateway .................................................................................................... 13
   2.2.2 phone-context ............................................................................................. 13
   2.2.3 ms-call-source ............................................................................................ 14
   2.2.4 ms-early-media ........................................................................................... 14
   2.2.5 Anonymous Phone URI ............................................................................ 14
   2.2.6 ms-bypass ................................................................................................ 14
   2.2.7 ms-accepted-content-id ............................................................................ 14
   2.2.8 ms-trunking-peer ....................................................................................... 15
   2.2.9 ms-mediation-generated ....................................................................... 15

## 3 Protocol Details

3.1 isGateway Details ............................................................................................... 16
   3.1.1 Abstract Data Model .................................................................................. 16
   3.1.2 Timers ....................................................................................................... 16
   3.1.3 Initialization ............................................................................................... 16
   3.1.4 Higher-Layer Triggered Events ............................................................... 16
   3.1.5 Message Processing Events and Sequencing Rules ............................... 16
   3.1.6 Timer Events ............................................................................................ 16
   3.1.7 Other Local Events .................................................................................. 16
3.2 phone-context Details ....................................................................................... 16
   3.2.1 Abstract Data Model ................................................................................ 17
   3.2.2 Timers ....................................................................................................... 17
   3.2.3 Initialization ............................................................................................... 17
   3.2.4 Higher-Layer Triggered Events ............................................................... 17
   3.2.5 Message Processing Events and Sequencing Rules ............................... 18
   3.2.6 Timer Events ............................................................................................ 18
   3.2.7 Other Local Events .................................................................................. 18
3.3 ms-call-source Details ....................................................................................... 18
   3.3.1 Abstract Data Model ................................................................................ 18
   3.3.2 Timers ....................................................................................................... 18
   3.3.3 Initialization ............................................................................................... 18
   3.3.4 Higher-Layer Triggered Events ............................................................... 18
   3.3.5 Message Processing Events and Sequencing Rules ............................... 18
   3.3.6 Timer Events ............................................................................................ 19
   3.3.7 Other Local Events .................................................................................. 19
3.4 ms-early-media Details ..................................................................................... 19
   3.4.1 Abstract Data Model ................................................................................ 19
   3.4.2 Timers ....................................................................................................... 19
   3.4.3 Initialization ............................................................................................... 19
4.2.2.1  Step 1: INVITE Message Is Sent from the UAC ........................................... 30
4.2.2.2  Step 13: 200 Message Is Received by the UAC ........................................... 31

4.3  ms-call-source SIP Header ................................................................. 32

4.3.1  Inbound Call ................................................................................... 32
4.3.1.1  Step 2: INVITE Message Is Received by the UAC ................................. 32
4.3.1.2  Step 8: INVITE Message Is Received by the UAC ................................. 33
4.3.1.3  Step 9: 605 Message Is Sent from the UAC .......................................... 33
4.3.1.4  Step 12: 200 Message Is Sent from the UAC ........................................ 34

4.3.2  Outbound Call ................................................................................ 34

4.4  ms-early-media SIP Supported Header Option Tag .................................... 34

4.4.1  Inbound Call ................................................................................... 34
4.4.2  Outbound Call ................................................................................ 35
4.4.2.1  Step 1: INVITE Is Sent from the UAC ..................................................... 35
4.4.2.2  Step 7: 183 Message Is Received by the UAC ....................................... 36
4.4.2.3  Step 13: 200 Message Is Received by the UAC ..................................... 37

4.5  ms-bypass SIP Supported Header Option Tag .......................................... 38

4.5.1  Inbound Call ................................................................................... 38
4.5.1.1  Step 6: INVITE Message Is Received by the Protocol Client ................ 39
4.5.1.2  Step 17: 200 Message Is Sent by the Protocol Client ........................... 40

4.5.2  Outbound Call ................................................................................ 41
4.5.2.1  Step 1: INVITE Message Is Sent by the Protocol Client ...................... 42
4.5.2.2  Step 13: 200 OK Message Is Received by the Protocol Client ............. 44

4.6  ms-accepted-content-id SIP Header ....................................................... 45

4.6.1  Inbound Call ................................................................................... 45
4.6.1.1  Step 6: INVITE Message Is Received by the Protocol Client ................ 45
4.6.1.2  Step 17: 200 Message Is Sent by the Protocol Client ........................... 47

4.6.2  Outbound Call ................................................................................ 48
4.6.2.1  Step 1: INVITE Message Is Sent by the Protocol Client ...................... 48
4.6.2.2  Step 13: 200 Message Is Received by the Protocol Client ................... 51

4.7  ms-trunking-peer SIP Header ............................................................... 51

4.7.1  Inbound Call ................................................................................... 52
4.7.1.1  Step 6: INVITE Message Is Received by the Protocol Client .............. 52

4.7.2  Outbound Call ................................................................................ 53
4.7.2.1  Step 13: 200 Message Is Received by the Protocol Client .................... 54

4.8  ms-mediation-generated SIP Header ....................................................... 54

4.8.1  Outbound Call ................................................................................ 55
4.8.1.1  Step 5: 183 Message Is Received by the Protocol Client ...................... 55
4.8.1.2  Step 10: 180 Message Is Received by the Protocol Client ................. 56

5  Security .................................................................................................. 57

5.1  Security Considerations for Implementers ............................................. 57

5.2  Index of Security Parameters .............................................................. 57

6  Appendix A: Product Behavior ............................................................. 58

7  Change Tracking ................................................................................... 60

8  Index ..................................................................................................... 61
1 Introduction

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

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

1.1 Glossary

This document uses the following terms:

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

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

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

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

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

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

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

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

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

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

fully qualified domain name (FQDN): An unambiguous domain name that gives an absolute location in the Domain Name System's (DNS) hierarchy tree, as defined in [RFC1035] section 3.1 and [RFC2181] section 11.
gateway: A network edge device that bridges Microsoft Office Communications Server protocols with legacy telephony networks protocols.

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

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

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

offer: A message that is sent by an offerer.

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

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

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

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

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

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

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

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

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

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

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

user agent client (UAC): A logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server (UAS) for the processing of that transaction.
user agent server (UAS): A logical entity that generates a response to a Session Initiation Protocol (SIP) request. The response either accepts, rejects, or redirects the request. The role of the UAS lasts only for the duration of that transaction. If a process responds to a request, it acts as a UAS for that transaction. If it initiates a request later, it assumes the role of a user agent client (UAC) for that transaction.

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

1.2 References

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

1.2.1 Normative References

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

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


1.2.2 Informative References


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


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

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

![Figure 1: SIP transaction](image)

1.3 Overview

The extensions do the following:

- Enable a SIP user agent (SIP UA) to be aware that a remote SIP UA in a SIP **dialog** is a gateway, as described in section 2.2.1 and section 3.1. This information can be rendered to the user interface (UI) to provide a better user experience (UX).

- Enable a SIP **URI** to hold an address of a **dial string** that is given by a user, as described in section 2.2.2 and section 3.2.
▪ Enable a SIP UAS to detect a redundant call that is triggered as a result of a loop, as described in section 2.2.3 and section 3.3. A loop occurs when a call is forked to a PBX that forks the call back, using a new SIP dialog.

▪ Enable a SIP UA to indicate that it is willing to receive an SDP answer through a non-reliable 183 provisional response to an INVITE message, as described in section 2.2.4 and section 3.4. Note that the standard recommends sending an SDP answer for early media only through a reliable provisional response, as described in [RFC3262].

▪ Define an anonymous phone URI, as described in section 2.2.5 and section 3.5, as an alternative to the standard anonymous SIP URI, as described in [RFC3261]. Note that the standard anonymous SIP URI is not supported.

▪ Enable a SIP UA in the protocol network to indicate that it supports media bypass functionality, as described in section 2.2.6 and section 3.6. Media bypass has the media from the protocol network entity involved in a PSTN call going directly to the gateway used to interface with the PSTN for that call, without traversing any intermediate element in the protocol network.

▪ Enable a SIP UA in the protocol network to reference the appropriate Session Description Protocol (SDP) that was selected from a received offer when sending a SIP message with an answer to the offer, as described in section 2.2.7 and section 3.7.

▪ Identify the specific gateway used to interface with the PSTN for a PSTN call, as described in section 2.2.8 and section 3.8.

1.4 Relationship to Other Protocols

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

▪ SIP: Session Initiation Protocol, as described in [RFC3261].

▪ Session Initiation Protocol (SIP): Locating SIP Servers, as described in [RFC3263].

▪ the Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, as described in [RFC3325].

▪ the Session Initiation Protocol (SIP) Refer Method, as described in [RFC3515].

▪ the Session Initiation Protocol (SIP) "Replaces" Header, as described in [RFC3891].

▪ the Session Initiation Protocol (SIP) Referred-By Mechanism, as described in [RFC3892].

▪ an Offer/Answer Model with the Session Description Protocol (SDP), as described in [RFC3264].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

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

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

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.
2 Messages

2.1 Transport

This protocol relies on **SIP** transport.

2.2 Message Syntax

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

2.2.1 isGateway

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

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

contact-gw = "isGateway"
```

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

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

2.2.2 phone-context

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

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

- "dialstring"
- "enterprise"

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

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

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

In the previous line, **example.com** is the host part of the SIP URI. It is not affected by the **phone-context** parameter.
2.2.3 ms-call-source
The ABNF, as defined in [RFC5234], for the **ms-call-source** SIP header is as follows:

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

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

The syntax of this header is illustrated as follows:

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

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

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

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

2.2.5 Anonymous Phone URI
The anonymous phone **URI** is an alternative to the standard anonymous **SIP URI**, as specified in [RFC3261]. The user part of the SIP URI is set with the value "anonymous" and the parameter `user=phone` is added to the URI.

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

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

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

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

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

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

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

```
ms-accepted-content-id: <da6e05c91d6b4132afa14d8b528732e6>
```
2.2.8 ms-trunking-peer

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

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

The host, hostname, and quoted-string elements are specified in [RFC3261] section 25.

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

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

2.2.9 ms-mediation-generated

The ABNF, as defined in [RFC5234], for the ms-mediation-generated SIP header is as follows:

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

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

```plaintext
ms-mediation-generated: yes
```
3 Protocol Details

3.1 isGateway Details

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

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

Proxy Behavior
This parameter does not affect a SIP proxy.

3.1.1 Abstract Data Model
None.

3.1.2 Timers
None.

3.1.3 Initialization
None.

3.1.4 Higher-Layer Triggered Events
None.

3.1.5 Message Processing Events and Sequencing Rules
None.

3.1.6 Timer Events
None.

3.1.7 Other Local Events
None.

3.2 phone-context Details

UAC Behavior
A UAC that is about to send an INVITE message to an address of a dial string MUST use the following logic. If a UAC cannot resolve the dial string to a SIP URI with an E.164 number of a remote party, based on local provisioning, it MUST set the SIP URI of the Request URI header with a phone number and a phone-context of the phone number in the user part of the SIP URI, as specified in [RFC3966] section 5.1.5. The value of the phone-context SIP URI parameter holds the location
profile name of the user if the dial string could not be resolved or the resolution of the dial string is to a non-E.164 number. If a user profile name is not provisioned and the dial string is not an E.164 number, the user agent MUST set phone-context to the default predefined dialstring name.

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

A UAC SHOULD 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 be in either E.164 format or a private number with a phone-context that is set with the location profile of the UAC.

UAS Behavior

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

Proxy Behavior

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

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

A SIP proxy that receives an INVITE that contains a phone-context in the From URI SHOULD 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 apply the rules defined in the matched dial plan and add a P-Asserted-Identity (PAI) with the result of the translation. If the result of the translation is not an E.164 number, the proxy SHOULD 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.

[MS-OCPSTN] - v20180828
Session Initiation Protocol (SIP) for PSTN Calls Extensions
Copyright © 2018 Microsoft Corporation
Release: August 28, 2018
3.2.5 Message Processing Events and Sequencing Rules
None.

3.2.6 Timer Events
None.

3.2.7 Other Local Events
None.

3.3 ms-call-source Details

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

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

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

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

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

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

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

3.3.1 Abstract Data Model
None.

3.3.2 Timers
None.

3.3.3 Initialization
None.

3.3.4 Higher-Layer Triggered Events
None.
3.3.5 Message Processing Events and Sequencing Rules
None.

3.3.6 Timer Events
None.

3.3.7 Other Local Events
None.

3.4 ms-early-media Details

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

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

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

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

3.4.1 Abstract Data Model
None.

3.4.2 Timers
None.

3.4.3 Initialization
None.

3.4.4 Higher-Layer Triggered Events
None.

3.4.5 Message Processing Events and Sequencing Rules
None.
3.4.6 Timer Events
None.

3.4.7 Other Local Events
None.

3.5 Anonymous Phone URI Details

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

3.5.1 Abstract Data Model
None.

3.5.2 Timers
None.

3.5.3 Initialization
None.

3.5.4 Higher-Layer Triggered Events
None.

3.5.5 Message Processing Events and Sequencing Rules
None.

3.5.6 Timer Events
None.

3.5.7 Other Local Events
None.

3.6 ms-bypass Details

A user agent (UA) supporting media bypass SHOULD <8> include a Session Initiation Protocol (SIP) Supported header with the ms-bypass option tag whenever it advertises the options it supports. Media bypass has the media from the protocol network entity involved in a public switched telephone network (PSTN) call going directly to the gateway used to interface with the PSTN for that call, without traversing any intermediate element in the protocol network.
3.6.1 Abstract Data Model
None.

3.6.2 Timers
None.

3.6.3 Initialization
None.

3.6.4 Higher-Layer Triggered Events
None.

3.6.5 Message Processing Events and Sequencing Rules
None.

3.6.6 Timer Events
None.

3.6.7 Other Local Events
None.

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

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

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

Proxy Behavior
This parameter does not affect a SIP proxy.

3.7.1 Abstract Data Model
None.
3.7.2 Timers
None.

3.7.3 Initialization
None.

3.7.4 Higher-Layer Triggered Events
None.

3.7.5 Message Processing Events and Sequencing Rules
None.

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

None.

3.9 ms-mediation-generated Details

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

3.9.1 Abstract Data Model

None.

3.9.2 Timers

None.

3.9.3 Initialization

None.

3.9.4 Higher-Layer Triggered Events

None.

3.9.5 Message Processing Events and Sequencing Rules

None.

3.9.6 Timer Events

None.

3.9.7 Other Local Events

None.
4 Protocol Examples

4.1 isGateway SIP Contact Header Parameter

4.1.1 Inbound Call

Figure 2: Inbound call

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

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

4.1.1.1 Step 3: INVITE Message Is Received by the UAC

INVITE sip:10.56.66.167:1501;transport=tls;ms-opaque=56d3073f52;ms-received-cid=8000 SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role=rs-from;lr;ms-identity=C8yb10ausk5JrJ0eabpGevn17YoohtCTBsbEB30y33pwmR9xH_oTA1gAA;ms-route-sig=eaOM1vIX8i1JEtotgeV9nVQESDR_2qoR9xH_oTA1gAA>;tag=D78DE2B24FD98B88DCC879B2 Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=TRUE;ms-internal-info="daqI8a1fcNqkUHJyMoUxqQadrDTCWr9xH7_OEdQAA"
Authentication-Info: Kerberos
rsauth="602306092A864886F712011100F44F1125B31E1322F6E6665212D0DEDCA4", srand="A805D66", 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
4.1.1.2 Step 7: 200 Message Is Sent from the UAC

SIP/2.0 200 OK
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branch=TRUE;ms-internal-info="daqI8a1fcNQkUHDJyMoUxdQdrDTgwR9XH7_OEdQAA"

Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bK27555a4e;ms-received-port=2861;ms-received-cid=8900

Record-Route: <sip:server1.example.com:5061;transport=TLS;ms-role=rs-from;lr;ms-identity=C8yb10ausk5JrrJOeabpGevnl7YoohctFbsEB30y33pmWwR9xH_oTAlgAA;ms-route=sig=eaOm1vIX8i1jET obtgsV9nVQESDR_2qwR9xH_oTAlgAA;tag=D78DE2B2FF72EB24FDA98BB8DCC879B2

Contact: <sip:alice@server1.example.com;opaque=user:epid:reTyjuqAaVmcCIO4qlA4vwAA;gruu>

User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
P-Preferred-Identity: <sip:alice@server1.example.com>, <tel:+15555550103>

Proxy-Authentication: Kerberos qop="auth", realm="SIP Communications Service", opaque="C216B7E9", crand="ddee2a45", cnum="4A", targetname="sip:server1.example.com", response="602306092a864886f7120102020101100fffffff77de97a16f96939a9cc29ed8d735499"

Content-Type: application/sdp
4.1.2 Outbound Call

Figure 3: Outbound call

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

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

4.1.2.1 Step 1: INVITE Message Is Sent from the UAC

INVITE sip:+15555550103@server1.example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.66.167:1501
Max-Forwards: 70
From: <sip:alice@server1.example.com>;tag=85e83db3c6;epid=782abb8f70
To: <sip:+15555550103@server1.example.com;user=phone>
Call-ID: accd397afa9439d880f45cfc804bd66
CSeq: 1 INVITE
Contact: <sip:alice@server1.example.com;opaque=userid:reTyjguqA4vMcCIO4qLa4vwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
Ms-Conversation-ID: AchdT5LJvLJvKtNrrSjejQUAy0wMfoA==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
4.1.2.2 Step 13: 200 Message Is Received by the UAC

SIP/2.0 200 OK
Authentication-Info: Kerberos
rspauth="602306092A864886F7120102020101100FFFFFF0714800DE2F658803052D07C86052224",
srand="B997079B", snum="50", opc="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=782abb870
TO: <sip:+15555550103@server1.example.com;user=phone>;epid=571f84bb45;tag=a0f83282b
CSEQ: 1 INVITE
CALL-ID: acdc979afad9439d880f45cfce04bd66
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-role=rs-from;lr;ms-route-sig=eab5FYPD_LMiadWiQ5t6m72y4vocRve_oTAlgAA>
CONTACT: <sip:server1.example.com@server1.example.com;gruu;opaque=srvr:MediationServer:ANaNdceyEM
B-dKmlqX-wAAR;grid=439be8c54ef04ce0b2a8842286f86c53>;isGateway
CONTENT-LENGTH: 1412
SUPPORTED: gruu
SUPPORTED: replaces
CONTENT-TYPE: application/sdp; charset=utf-8
ALLOW: UPDATE
P-ASSERTED-IDENTITY: <sip:+15555550103@server1.example.com;user=phone>
SERVER: RTCC/3.0.0.0 MediationServer
ALLOW: Ack, Cancel, Bye,Invite,Refer
4.2  phone-context SIP URI Parameter

4.2.1  Inbound Call

![Diagram of phone-context SIP URI Parameter](image)

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

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

4.2.1.1  Step 3: INVITE Message Is Received by the UAC

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

```
INVITE sip:10.56.66.167:1501;transport=tls;ms-opaque=56d3073f52;ms-received-cid=8000
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role-rs-from;lr;ms-identity=C8yb10ausk5JrrJ0eabpGevn17YoohtcFBeEB30y33pmWwR9xH_oTA1gAA;ms-route-sig=ea0m1VX81jiETctqsV9nVQBE3DR_2qWRoXH_oTA1gAA>;tag=D75DEZB2FF72EB24FDA98B88DC879B2
Via: SIP/2.0/TLS 10.56.64.207:2861;branch=z9hG4bKD262F653.B047DC47;branched=TRUE;ms-internal-info="dagI8afcrQ7kUHD3yMoUxdQurDTCw9xh7_OEdQAA"
Authentication-Info: Kerberos
Max-Forwards: 69
Content-Length: 1606
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bK0D262F653.B047DC47;ms-received-cid=8900
From: <sip:+15555550103@server1.example.com;user=phone>;epi=571F84BB45;tag=ed77bad0f0
```

Figure 4: Inbound call

The preceding figure includes one message in each direction because other messages repeat the same values.
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-dKmjgQwAA;grid=9b192c6b829d4373adbB8e9ef4df03>;isGateway
Supported: replaces
Supported: gruu=10
User-Agent: RTCC/3.0.0.0 MediationServer
Content-Type: application/sdp; charset=utf-8

4.2.1.2 Step 7: 200 Message Is Sent from the UAC

SIP/2.0 200 OK
Via: SIP/2.0/TLS 10.56.64.202:5061;branch=z9hG4bKD262F853.B047DC47;branched=True;ms-internal-info="daqI8a1fcNQQHJDJyMoXkdQudzDTCwR9xH7_CEdQAA"
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=r-s;from;lr;ms-identity=C8ybi0auxk5Jrj0eabpGevn17YoochctFBsE3B3oy33pmWwR9xH_oTA1gAA;ms-route-sig=ea0m1vIX81JETotgsV9nVQESDR_2qeR9xH_oTA1gAA;tag=D78DE2B2FF7249888DCC879B2
Contact: <sip:alice@server1.example.com;opaque=epid:reTyjqAaVmcCIO4qlAwAA;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="ddee2a45", cnum="44", targetname="sip/server1.example.com", response="602306092a86488f7120102020101100fffffff77de9d7a16f9693a9cc29ed8d6735499"
Content-Type: application/sdp
4.2.2 Outbound Call

Figure 5: Outbound call

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

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

4.2.2.1 Step 1: INVITE Message Is Sent from the UAC

```
INVITE sip:72181;phone-context=dialstring@example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.64.148:4031
Max-Forwards: 70
From: <sip:test2@example.com>;tag=cefe741803;epid=7d725e08a1
To: <sip:72181;phone-context=dialstring@example.com;user=phone>
Call-ID: a6a53b0e8b7d40a3b445dc4d9249b6fe
CSeq: 1 INVITE
Contact: <sip:test2@example.com;opaque-user:epid:ONaA0AXIFCRDgr367kcHwAA;gruu>
User-Agent: UCCP/2.0.6362.36 OC/2.0.6362.36 (Client)
Ms-Conversation-ID: Achis3b6kqiLEhnZR/#DMH2N7CO9hg==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
```
4.2.2.2 Step 13: 200 Message Is Received by the UAC

SIP/2.0 200 OK
Authentication-Info: NTLM rsrpauth="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-conf-received-port=4031;ms-conf-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-sign=aababLHUMznhhFXTzutN9dwPQ-RmwQYZA_UIeyt1QAA>
CONTACT: <sip:SH13-LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGxJb1zwQfgAA;grid=f1f9379bd9334f65a1dfb77bed58905;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

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

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

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

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

INVITE sip:10.56.66.167:3080;transport=tls;ms-opaque=0e2b3bcc10;ms-received-cid=300
SIP/2.0
Record-Route: <sip:server1.example.com:5061;transport=tls;ms-role=rs-to;ms-role=rs-from;lr;ms-route=aa1PYPx-ublLaoi5Z/QqMHLGcU3lxkBBilLt2ZQAA>;tag=8951C70C798E10EA48EB96EAA4B379BC
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bK76F2CFD5.31901062;branched=TRUE;ms-internal-info="aaC8UGYE_vlAjq36gl1v1Ni15UxkBBihbkIPAAA"
Authentication-Info: NTLM rspauth="01000004441541C22E2F66F9C08F09", srand="4CB66F5", 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=7d2abb8f70
Call-ID: ee22d219e9f44411bbac7b304ddc1096
4.3.1.2 Step 8: INVITE Message Is Received by the UAC

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

```
CSeq: 1 INVITE
Contact: <sip:test2@example.com;opaque=user:epid:ONaA0AXIFCRDgr367kcHWAA;gruu>
User-Agent: UCCP/2.0.6362.36 OC/2.0.6362.36 (Client)
Ms-Conversation-ID: AchisczV2kxU07mT2ieBaNoX1H8g==
Supported: timer
Supported: ms-sender
ms-keep-alive: UAC;hop-hop=yes
Supported: ms-conf-invite
Content-Type: application/sdp
```

4.3.1.3 Step 9: 605 Message Is Sent from the UAC

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

```
SIP/2.0 605 Decline Everywhere
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=aaKlz4lwQeqhL-R5X7wN8hEhuJwK6MHw6hbkIPAAA
Via: SIP/2.0/TLS 10.198.92.126:4757;branch=729ab37d-c0f5-4ad7-b7e0-8f3dad99065
To: <sip:+15555550108@example.com;user=phone>;epid=782abb8f70;tag=b9bc5b444c
Call-ID: 729ab37d-c0f5-4ad7-b7e0-8f3dad99065
Contact: <sip:SH13-LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXHNJb1ZwQf gagA;grid=2cfb52f9df4b930adfa82dbfcd39e4>;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
```

---

[MS-OPCSTN] - v20180828
Session Initiation Protocol (SIP) for PSTN Calls Extensions
Copyright © 2018 Microsoft Corporation
Release: August 28, 2018
4.3.1.4 Step 12: 200 Message Is Sent from the UAC

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

SIP/2.0 200 OK
Via: SIP/2.0/TLS 172.29.106.3:5061;branch=z9hG4bK76F2CFD5.31901062;branched=TRUE;ms-internal-info="aaC8UGYE_v1Ajm36gJ31-v1MQi150xkBBhhbIPAAA"
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=782aab8f70;tag=281b612cd0
Call-ID: ee22d219e9f44441bbac7b304ddc1096
CSeq: 1 INVITE
Record-Route: <sip:server1.example.com:5061;transport-tls;ms-role-rt-from;lr;ms-identity=B5buGzywo49cKOaabbgxdAgaQRu_k9cZxy4Wi-659s6BBws2WZQAA;ms-route-sig=a3Oeh9351YMaV5Aytn4katb_zD-6MHw6L22WZQAA>;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"
  response="010000073006906642f6a9f9c08f09"
Content-Length: 0

4.3.2 Outbound Call

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

4.4 ms-early-media SIP Supported Header Option Tag

4.4.1 Inbound Call

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

Figure 7: Outbound call

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

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

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

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

```
INVITE sip:+15555550100@example.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 10.56.66.167:3137
Max-Forwards: 70
From: <sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
To: <sip:+15555550100@example.com;user=phone>
Call-ID: ca22890914c34bf8a7439df1e6834420
CSeq: 1 INVITE
Contact: <sip:test1@example.com;opaque-user:epid:reTyjuqAaVmcC104qlA4vwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Client)
Ms-Conversation-ID: Achit1olq5CCFcXhRKeZABfaZvWNw==
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 gop="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
c=IN IP4 10.56.66.167
m=audio 50016 RTP/AVP 114 111 112 115 4 8 0 97 101
k=base64:Bcw/3c0RQ/ndiix3QiLgO9s3z1ZhEcL32C85c74zuN3wpyIrxxl1eIA4kErwh
a=candidate:Hfb3G/XvuV5g7gXYyDw7jyyZ8aIUsFPeoQRKnK3g3vU 1 x4Ykt3u0C7f7mAWomKNMQ UDP 0.900 10.56.66.167 50016
a=candidate:Hfb3G/XvuV5g7gXYyDw7jyyZ8aIUsFPeoQRKnK3g3vU 2 x4Ykt3u0C7f7mAWomKNMQ UDP 0.900 10.56.66.167 50008
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:aAzhJhKx1bOgjuVWNf18C4f1K91E5SJib6VIaWPF|2^31|1:1
a=cryptoscale:2 AES_CM_128_HMAC_SHA1_80
inline:VqAkQVzuZMKH1uaXv1+8kjiJlRsinyngtcuh2AA5k|2^31|1:1
a=maxptime:200
a=rtpmap:114 x-mrsra/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-mrsra/8000
a=fmtp:115 bitrate=18000
a=rtpmap:116 AAL2~G726~32/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional

4.4.2.2 Step 7: 183 Message Is Received by the UAC

The following 183 Session Progress message includes an SDP answer.
4.4.2.3 Step 13: 200 Message Is Received by the UAC

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

SIP/2.0 200 OK
Authentication-Info: NTLM rsauth="010000003240756E24DFD336F7DB686", sname="C1DF9895", snnum="105", opaque="B25450B8", gop="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-clid=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: ca22890914c34bf8a7439dfe1834420
RECORD-ROUTE: <sip:server1.example.com:5061;transport=tls;ms-roles=rs-from;lr;ms-route-sig=aehlWZJyUQ9GVPvYX5CBQn55MnVHAdhileyt1QAA>
CONTACT: <sip:SH13-LCT.example.com@example.com;gruu;opaque=srvr:MediationServer:TIRig7bu5kGXhJb1ZwQfAgAA;grid=b6796217d6ea465cbe261a778c10d5c0>;isGateway
CONTENT-LENGTH: 740
SUPPORTED: replaces
SUPPORTED: replaces
P-ASSERTED-IDENTITY: <sip:+17036508897@example.com;user=phone>
SERVER: RTCC/3.0.0.0 MediationServer
ALLOW: Ack, Cancel, Bye, Invite, Refer
v=0
c=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=rtpmap:60532
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 1 Bx2Is+Wl/HJbdQKM3FIBk UDP 0.900 10.198.92.126 60625
a=candidate:ZHqwSbPvIZyDX24RjvIW4lryUx/QbdAiP7FyQ0yvTGo 2 Bx2Is+Wl/HJbdQKM3FIBk UDP 0.900 10.198.92.126 60532
a=encryption:rejected
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:97 RED/8000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a-ptime:20
4.5 ms-bypass SIP Supported Header Option Tag

4.5.1 Inbound Call

Figure 8: Inbound call
The messages in the following subsections illustrate the use of the ms-bypass option tag in a Supported header in messages that are sent from and received by a protocol client.

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

```
INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f6d3a;ms-received-cid=475300 SIP/2.0
Record-Route: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300:Ieh.gU65xDwq_j78KvdcC-dRhxH1EBSv890EcFECdsTe7Q4nM1ETOTo1_iwBgJHnKsZgY3njnAA:lr;ms-route=sig=dcrEzxvkq3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG>
SIP/2.0 Record-Route: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300:Ieh.gU65xDwq_j78KvdcC-dRhxH1EBSv890EcFECdsTe7Q4nM1ETOTo1_iwBgJHnKsZgY3njnAA:lr;ms-route=sig=dcrEzxvkq3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG>
SIP/2.0 Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-internal-info="cehce-xZqcsRs3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG";lr;ms-route=sig=dcrEzxvkq3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG>
Authentication-Info: TLS-DK gqop="auth", opaque="F755045D", srnd="CC465BFD", snnum="26", rsnpauth="d6179291f72761e057a67adb7288fd256c2b1ed4", 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=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-internal-info="cehce-xZqcsRs3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG";lr;ms-route=sig=dcrEzxvkq3A_ZSAwy8D4JlygqxDKKREgif1FT6noRjHnKsZUY7CfCaG>
Content-Type: multipart/alternative; boundary=9dvaKhfhPJxCOyObvB70o0f2xfqiXN3J
Allow: ACK
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Session-Expires: 1800
Min-SE: 90
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
P-Asserted-Identity: <sip:+4259876543@company1;user=phone>
```
```
4.5.1.2 Step 17: 200 Message Is Sent by the Protocol Client

SIP/2.0 200 OKVia: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms-info="cehce-xXzqcRs3A_ZSAwy8D4JLgyqxDKFNgfTVFt6on83jHnsZUY47CgAA"Via: SIP/2.0/TLS
4.5.2 Outbound Call

```
Client  
  1. INVITE
  2. 100
  3. 200 (for PRACK)
  4. 401
  5. 200 (for INVITE)
  6. 180
  7. 800
  8. PRACK
   
Gateway  
  9. PRACK
  10. 200 (for PRACK)
  11. 200 (for INVITE)
  12. 200 (for INVITE)
  13. ACK
  14. ACK
  15. ACK
```

```
v=0  o=0  i=0  n=0  s=session=IN IP4 192.168.1.114  c=IN IP4 192.168.1.114  t=0  m=audio 10228 RTP/AVP 0 8 101 a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:coO876idP3y3k7RbKz17QkTilb4n12zOqyZnUWwBzR|2^31|1:i=amptime:200a=rtpmap:0 PCMU/8000a-rtpmap:8 PCMA/8000a-rtpmap:4 G723/8000a-rtpmap:101 telephone-event/8000-a-fmtp:101 0-16=a-x-bypass
```
Figure 9: Outbound call

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

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

```
INVITE sip:+14258901234@company1;user=phone SIP/2.0
Via: SIP/2.0/TLS 192.168.1.114:4535
Max-Forwards: 70
From: <sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
To: <sip:+14258901234@company1;user=phone>
Call-ID: e57df11a45947f1a5b90da8d957b8ae
CSeq: 1 INVITE
Contact: <sip:user112@company1;opaque=user;epid:54dd5867e8>
User-Agent: Client 1.0
Ms-Conversation-ID: AcrCQkQ2CGV+fQQpS5OpwWuDL+KaYQ==
Supported: timer
Supported: hstinfo
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, 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="7550450", targetname="PROXY.company1", crand="738839d3", cnum="12",
response="2b5e54bd29a1493e078947725cee0dca06bf3"
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
m=audio 25486 RTP/AVP 114 119 19 125 7 118 117 116 115 103 102 101 100 99 98 97 96 95 94 93 92 91 90 89 88 87 86 85 84 83 82 81 80 79 78 77 76 75 74 73 72 71 70 69 68 67 66 65 64 63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48 47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
m=video 30009 RTP/AVP 115 114 113 112 111 110 109 108 107 106 105 104 103 102 101 100 99 98 97 96 95 94 93 92 91 90 89 88 87 86 85 84 83 82 81 80 79 78 77 76 75 74 73 72 71 70 69 68 67 66 65 64 63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48 47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
a=control:audio 1
a=control:video 0
a=rtcp;rid=192.168.1.114
a=rtpmap:114 a-law/8000
a=rtpmap:9 ulaw/8000
a=rtpmap:112 red/8000
a=rtpmap:111 speex/8000
a=rtpmap:0 a-law
a=rtpmap:8 ulaw
a=rtpmap:116 red
a=rtpmap:115 speex
a=rtpmap:4 a-law
a=rtpmap:97 ulaw
a=rtpmap:13 red
a=rtpmap:118 speex
a=rtpmap:101 a-law
a=fmtp:114 0
a=fmtp:9 0
a=fmtp:112 0
a=fmtp:111 0
a=fmtp:0 0
a=fmtp:8 0
a=fmtp:116 0
a=fmtp:115 0
a=fmtp:4 0
a=fmtp:97 0
a=fmtp:13 0
a=fmtp:118 0
a=fmtp:101 0
a=fmtp:2 28
```

```
a=candidate:DzxkqW6pd3wMmObq9itqTbhq6yl4DLm1I8ZRB13J6c 2 AUw+1gvF2Gl3nLiF4otDhg TCP 0.250
192.168.1.114 50007
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80
inline:0Y1qCCFx84w1krR39x9PDA2HuNdtAB+6ekKly5a|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:b28szcBsdH7eBr13Ahecn34gKrh8OeCYQP61MxwxBc|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:8LUckWcobd31OR16KGZL1f+My7wvwftcSNw7G79|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: <3d45467919eb4c81be0c4e19c730c655>
Content-Disposition: session; handling=optional
v=0
o-- 0 0 IN IP4 192.168.1.114
s=session
c=IN IP4 192.168.1.114
b=CT:99980
t=0 0
m=audio 28238 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101
a=ice-ufrag:ayqK
a=ice-pwd:ckRbkR22l38Phmgvzm5n
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 59842 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:0Y1qCCFx84w1krR39x9PDA2HuNdtAB+6ekKly5a|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:b28szcBsdH7eBr13Ahecn34gKrh8OeCYQP61MxwxBc|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:8LUckWcobd31OR16KGZL1f+My7wvwftcSNw7G79|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
**4.5.2.2 Step 13: 200 OK Message Is Received by the Protocol Client**

SIP/2.0 200 OK
Authentication-Info: TLS-DSK qop="auth", opaque="F755045D", srandom="1D9666D9", snum="17", rsapath="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=dcw0SbeehYaHu9dRxfcQNPNLa1GM-c5DzikYU7AfRG2hHcH3QtgY3jngAA
CONTACT: <sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68AvYpqVvFy0hQAA;grid=46236573d0ae4339d88726b2bf7f7ab>;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-trunk-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresher=uas
Min-SE: 90
v=0
o=Gateway 1303417666 1303417345 IN IP4 10.1.2.12
s=session
c=IN IP4 10.1.2.12
t=0 0
m=audio 6390 RTP/AVP 0 13 101
a=rtpmap:6391 a=sendrecv
a=x-bypass
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:bN1zDJ0LC8QYNvMIdohDkGkwD/rCastpGb5ObNo|2^31|244:1
a=encrypt:optional
a=x-bypaassid:9CD08A01-E998-456a-AC8A-0289305933

------=_NextPart_000_0003_01CAC1FF.366488E0==
4.6 ms-accepted-content-id SIP Header

4.6.1 Inbound Call

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

Figure 10: Inbound call
4.6.1.1 Step 6: INVITE Message Is Received by the Protocol Client

INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f63a;ms-received-cid=475300 SIP/2.0
Record-Route: <sip:PROXY.company1:5061;transport=tls;ms-opaque=acee5f63a;ms-received-cid=475300>
Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branch=TRUE;ms-internal-info="cehce-xZqgRsA_ZSAwy8D4JLgyxgDKREqfIVFt6noRjHnKsZUY47CgAA"
Authentication-Info: TLS gkop="auth", opaque="F755045D", snum="26", rsapath="d61792f1f27b61e057a67adb7288fd256c2b0e4d", targetname="PROXY.comapny1", realm="SIP Communications Service", version=4
Max-Forwards: 69
Content-Length: 3161
 Via: SIP/2.0/TLS 10.1.1.102:57350;branch=z9hG4bKe82f3;ms-received-cid=475900
From: <sip:+4259876543@company1;user=phone>;epid=CDCFEF8F18;tag=3d965223ea
To: <sip:+14251234567@company1;user=phone>;epid=54dd586768
CSeq: 35 INVITE
Call-ID: df601b2d-e42e-4677-b921-c9dbf4e5940
Contact: <sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMoYVfS0hQAA;grid=bd9c42fc618147d0af4d8f84f718910b>;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=9dvaKhfPlJxOCOyObvB7000f2xfqiXN3J
Allow: ACK
Content-Disposition: Session;handling=optional;ms-proxy-2007fallback
Session-Expires: 1800
Min-SE: 90
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
P-Asserted-Identity: <sip:+4259876543;user=phone>
History-Info: <sip:user112@company1>;index=1
Content-Type: application/sdp
Content-ID: <72e03bb9-6acc-453b-aee0-48671344d83>
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
a=audio 56568 RTP/AVP 0 8 115 13 118 97 101
crtpc:56569
a=candidate:WPBogU8Ncp21Gv4/zj/6WviEjTkj55FxhrdRkHiZcc 1 tKavBj1xayi4rc19atyg UDP 0.830 10.1.1.102 56568
a=candidate:WPBogU8Ncp21Gv4/zj/6WviEjTkj55FxhrdRkHiZcc 2 tKavBj1xayi4rc19atyg UDP 0.830 10.1.1.102 56568
a=candidate:bgLnsm3DP4aSPQloj2Ak1UYeGDPsdlRRetvScj5izM 1 5VdtqyZIrMIPith0TX5Mcg TCP 0.150 10.3.0.7 59954
a=candidate:bgLnsm3DP4aSPQloj2Ak1UYeGDPsdlRRetvScj5izM 2 5VdtqyZIrMIPith0TX5Mcg TCP 0.150 10.3.0.7 59954
a=candidate:hdj5XrOXJw/ib/pE8R3lzSmwFi3ttrUtRt4pmcfbSY 1 RDbzrPzUksHqIX1Kaqv0bFA UDP 0.450 10.3.0.7 55690
a=candidate:hdj5XrOXJw/ib/pE8R3lzSmwFi3ttrUtRt4pmcfbSY 2 RDbzrPzUksHqIX1Kaqv0bFA UDP 0.450 10.3.0.7 57652
4.6.1.2 Step 17: 200 Message Is Sent by the Protocol Client

SIP/2.0 200 OK Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC7A4B7C3D3;branched=TRUE;ms=internal info="cehce_xXzqcRs3A_ZSAwy8D4JLgyqxDKREg_fIVFt6noRjHnKsZUY47CgAA" 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;tag=c608fec21a Call-ID: df601b2de42e4677-b921-c9df2e5980Cneg: 35 INVITERecord-Route: <sip:PROXY.company1:5061;transport=tls/propagate-state:F:C1.R475300:teh.gU65xDVwq_j78KvdcC-

47 / 63
4.6.2 Outbound Call

The messages in the following subsections illustrate the use of the ms-accepted-content-id Session Initiation Protocol (SIP) header in messages that are sent from and received by a protocol client.
4.6.2.1 Step 1: INVITE Message Is Sent by the Protocol Client

INVITE sip:+14258901234@company1;user=phone SIP/2.0
Via: SIP/2.0/TLS 192.168.1.114:4535
Max-Forwards: 70
From: <sip:user112@company1>;tag=ed04066c4a;epid=54dd5867e8
To: <sip:+14258901234@company1;user=phone>
Call-ID: e571df11a45947f1a5b90da8d957b8ae
CSeq: 1 INVITE
Contact: <sip:user112@company1;opaque=user:epid:jVxLXK19112yFm93r_ArNgAA;gruu>
User-Agent: Client 1.0
Ms-Conversation-ID: AcrCqkQ2CGV+fQQpS5OpwDL+KaYQ==
Supported: timer
Supported: hlistinfo
Supported: ms-safe-transfer
Supported: ms-cancel
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 gop="auth", realm="SIP Communications Service",
opaque="77550450", targetname="PROXY.company1", crand="7388939d", cnm="12",
response="2b5e54b5d29a1493e07894772e5ce0c0a06df3" 
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= jpegerin
c= IN IP4 192.168.1.114
b=CT:9998
n=0
m=audio 25486 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 100
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFITVLXwlt+YRAoobGxY4A 4 0/jKJd6e54nbJ5afchXniA UDP 0.830 192.168.1.114 25486
a=candidate:XhpPtyjMgVxDIhWFgBIMhdLFITVLXwlt+YRAoobGxY4A 2 0/jKJd6e54nbJ5afchXniA UDP 0.830 192.168.1.114 25486
a=candidate:+oWYSe96Han9j7GRgjAfAf471mvm2GeooLhFH816sNIM 1 wiGTb6bq53yn1/Keu8TGSg TCP 0.190 10.3.0.7 57587
a=candidate:+oWYSe96Han9j7GRgjAfAf471mvm2GeooLhFH816sNIM 2 wiGTb6bq53yn1/Keu8TGSg TCP 0.190 10.3.0.7 57587
a=candidate:+LqcUB1cwTUe3j3u1ihJq7UTE5SYTrNNWvpIzn7S41ho 1 X3SSHBYGZsFgLK8Z7sd5VNQ UDP 0.490 10.3.0.7 51247
a=candidate:+LqcUB1cwTUe3j3u1ihJq7UTE5SYTrNNWvpIzn7S41ho 2 X3SSHBYGZsFgLK8Z7sd5VNQ UDP 0.490 10.3.0.7 50976
a=candidate:DzvkqW6pd3wMmO99qtQ1bhQ6yI4DLm182Rb13J6c 1 AUW+1gVF2GlLnnLiF4otDhg TCP 0.250 192.168.1.114 50007
a=candidate:DzvkqW6pd3wMmO99qtQ1bhQ6yI4DLm182Rb13J6c 2 AUW+1gVF2GlLnnLiF4otDhg TCP 0.250 192.168.1.114 50007
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80 inline:OYqCCFx84WfkrR3XpFAPdK2hNdTAB+6ekK1y5a|2^31|1:1
a=encrypt:2 AES_CM_128_HMAC_SHA1_80 inline:b28SzCCBSdh7eBrl3AhhecN34qKh80eCYQq61MwWBC|2^31|1:1
a=encrypt:3 AES_CM_128_HMAC_SHA1_80 inline:8L0ckWboddb310Ri6KgZfLIF+My7ywCwftcSNW7G79|2^31

-----NextPart_000_0003_01CAC1FF.366488E0

Content-Type: multipart/alternative;boundary="-----NextPart_000_0003_01CAC1FF.366488E0"
Content-Length: 3052


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: <3d45476919eb4c81be0cde19c730c655>
Content-Disposition: session; handling=optional

v=0
o-- 0 0 IN IP4 192.168.1.114
s=session
c=IN IP4 192.168.1.114
b=CT:99980
t=0 0
m=audio 28238 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101
a=ice-ufrag:ayqK
a=ice-pwd: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 6566159 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:2 2 TCP-PASS 6566158 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+6ekK1y5a|2^31|1:1
a=cryptoscale:2 AES_CM_128_HMAC_SHA1_80 inline:b28SzCBSdH7eBr13AhecN34gK680eCYGG61MwxbC|2^31|1:1
a=cryptoscale: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=fmtp:115 bitrate=11800
a=rtpmap:4 G723/8000
a=rtpmap:97 RED/8000
a=rtpmap:13 CN/8000

------_NextPart_000_0003_01CAC1FF.40D0153C.366488E0

Content-Type: application/sdp
Content-Transfer-Encoding: 7bit
Content-ID: <7175476919eb4c81be0cde19c730c655>
Content-Disposition: session; handling=optional

v=0
o-- 0 0 IN IP4 192.168.1.114
s=session
c=IN IP4 192.168.1.114
b=CT:99980
t=0 0
m=audio 28238 RTP/AVP 114 9 112 111 0 8 116 115 4 97 13 118 101
a=ice-ufrag:ayqK
a=ice-pwd: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 6566159 10.3.0.7 59752 typ relay raddr 192.168.1.114 rport 50031
a=candidate:2 2 TCP-PASS 6566158 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+6ekK1y5a|2^31|1:1
a=cryptoscale:2 AES_CM_128_HMAC_SHA1_80 inline:b28SzCBSdH7eBr13AhecN34gK680eCYGG61MwxbC|2^31|1:1
a=cryptoscale: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
4.6.2.2 Step 13: 200 Message Is Received by the Protocol Client

SIP/2.0 200 OK
Authentication-Info: TLS-DK qop="auth", opaque="F755045D", rsnauth="3595c8ac2e6229b2eb9738ac707dc8c3e54f65f0", 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: e571df11a45947b3f1a5b90da8d957b8ae
RECORD-ROUTE: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300;lr;ms-route-sig=dcw0SbeehYaHu9dRxfcQNPNLaiGMc5DziyYU7AfKG2hHch3QtgY3jngAA>
CONTACT: <sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMnYVfYs0hQAA;grid=46236573d0ae4a339d83726b2bf7f7ab>;isGateway
CONTENT-LENGTH: 422
SUPPORTED: replaces
SUPPORTED: ms-safe-transfer
SUPPORTED: ms-bypass
SUPPORTED: ms-dialog-route-set-update
SUPPORTED: gruu-10
SUPPORTED: timer
SUPPORTED: 100rel
CONTENT-TYPE: application/gw-sdp
ALLOW: ACK
P-ASSERTED-IDENTITY: <sip:+14258901234@company1;user=phone>
SERVER: Mediation Server
Ms-Accepted-Content-ID: <3d45476919eb4c81be0c4e19c730c655>
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresher=uas
Min-SE: 90
v=0
o=Gateway 1303417666 1303417345 IN IP4 10.1.2.12
s=session
c=IN IP4 10.1.2.12
t=0 0
m=audio 6390 RTP/SAVP 0 13 101
a=IN IP4 10.1.2.12
a=rtpmap:6391
a=x-bypass
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:bN1zDJ0LC8QYNvMIdohDtGkWD/rCastpGz50bNo[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

---_NextPart_000_0003_01CAC1FF.366488E0--
4.7 ms-trunking-peer SIP Header

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

4.7.1 Inbound Call

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

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

```
INVITE sip:192.168.1.114:4535;transport=tls;ms-opaque=acee5f6d3a;ms-received-cid=475300 SIP/2.0
Record-Route: <sip:PROXY.company1:5061;transport=tls;opaque=state:F:Ci.R475300:1eh.gu65xDvwaJ38KvdcC-dRxh71EsAvboEcfEcdswTe7QM4niMeToTOI_1bWgjHnKSzgy3jngAA;1r;ms-route=sig=dcrEvqyqg3iKg2ApNy1bCyydC6hC7NNwE-5pC7xqjJF3xkXfhnKSzgy3jngAA;tag=45F7A969AB33112CFB987794D7F56D40 Via: SIP/2.0/TLS 10.1.1.54:5061;branch=z9hG4bK1C7C8A0E.19AB9CC74B7C3D3;branched=TRUE;ms-internal-info="cehce-xXzqRsa.5ZSawy8D4LgyxgDK1Egf1VfT6noRjHnKsZUY47CgAA"
Authentication-Info: TLS=DSK qop="auth", opaque="F755045D", srnd="CC46B5FD", snum="26", rspsig="d17929f177261e057a67adb7288fd256c214e4d", 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=79h4bke82f3c;ms-received-cid=475900 From: <sip:4259876543;phone-context=Location1@company1;user=phone>;epid=CDCFE8F18 To: <sip:+14251234567@company1;user=phone>;epid=54dd5867e8 CSeq: 35 INVITE Call-ID: df601b2d-e42e-4677-b921-c9dbfe25940 Contact: <sip:ms5.company1@company1;gruu;opaque=srvr:MediationServer:XzRY6u68aVipMoYVfYs0hQAA;grid=b942fc618147d0af4d8f84f718910b>;isGateway Supported: replaces Supported: ms-safe-transfer Supported: ms-bypass Supported: ms-dialog-route-set-update Supported: timer Supported: 100rel User-Agent: Mediation Server Content-Type: multipart/alternative; boundary=9dvaKhfhPJzCOyObvB70o0f2xfgiXN3J Allow: ACK ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="Gateway 1.0" Session-Expires: 1800 Min-SE: 90 Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE P-Asserted-Identity: <sip:+4259876543@company1;user=phone> History-Info: <sip:14251234567@company1;index=1> --9dvaKhfPjzrCOyobvB70o0f2xfgiXN3J Content-Type: application/sdp Content-ID: <72e03bb9-6acc-453b-a609-b867134d83> 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 8 115 113 118 97 101
```
4.7.2 Outbound Call

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

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

SIP/2.0 200 OK
Authentication-Info: TLS-DSK gqop="auth", opaque="f755045D", srand="1D9666D9", snum="17", rsparuth="3359c8ae2e6229b2eb9738ac707cd8c3e54f65f0", 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:Cl.R475300;lr;ms-route=sig=CfmmzS9cRv9h3Zy7j3hJLXZ7yY7M;src=srvr:MediationServer;grid=46236573d0ae4a339d83726b2bf7f7ab>;lsGateway
CONTENT-LENGTH: 422
SUPPORTED: replaces
SUPPORTED: ms-safe-transfer
SUPPORTED: ms-bypass
SUPPORTED: ms-dialog-route-set-update
SUPPORTED: gruu-10
SUPPORTED: timer
SUPPORTED: 100rel
CONTENT-TYPE: application/gw-sdp
ALLOW: ACK
P=ASSERTED-IDENTITY: <sip:+14258901234@company1;user=phone>
SERVER: Mediation Server
Ms-Accepted-Content-ID: <3d45476919eb4c81be0c4e19c730c655>
ms-trunking-peer: gateway.company1.com;trunk=trunk1;User-Agent="GateWay 1.0"
Allow: CANCEL,BYE,INVITE,REFER,NOTIFY,PRACK,UPDATE
Session-Expires: 1800;refresh=rsp
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
 cname=IN IP4 10.1.2.12
 a=rtpmap:39116 PCMU/8000
 a=rtpmap:39118 telephone-event/8000
 a=fmtp:39116 0-15
 a=ptime:20
 a=x-mediasettings:signalboostunsupported

4.8 ms-mediation-generated SIP Header

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

![Outbound Call Diagram]

Figure 12: Outbound Call

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

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

```
SIP/2.0 183 Session Progress
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
```
4.8.1.2 Step 10: 180 Message Is Received by the Protocol Client

SIP/2.0 180 Ringing
Authentication-Info: NTLM rspsauth="010000000000000000010008AC67ADF27DB686", srand="DF9D53C4", snum="103", opaque="B25450B8", qop="auth", targetname="server1.example.com", realm="SIP Communications Service"
Via: SIP/2.0/TLS 10.56.66.167:3137;ms-received-port=3137;ms-received-cid=100
FROM: "test1"<sip:test1@example.com>;tag=2b95504d65;epid=782abb8f70
TO: <sip:+15555550100@example.com;user=phone>;epid=6477F45221;tag=b5bb1243e3
CSEQ: 1 INVITE
CALL-ID: ca22890914c34bf8a7439dfe1e834420
CONTENT-LENGTH: 0
5  Security

5.1  Security Considerations for Implementers
None.

5.2  Index of Security Parameters
None.
6 Appendix A: Product Behavior

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

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

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

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

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

<2> Section 3.2: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<3> Section 3.2: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<4> Section 3.2: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<5> Section 3.2: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<6> Section 3.2: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.

<7> Section 3.5: Office Communications Server 2007, Office Communicator 2007: This behavior is not supported.
<8> **Section 3.6**: Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<9> **Section 3.7**: Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<10> **Section 3.8**: Office Communications Server 2007, Office Communicator 2007, Office Communications Server 2007 R2, Office Communicator 2007 R2: This behavior is not supported.

<11> **Section 3.9**: This behavior is not supported in Office Communicator 2007, Office Communicator 2007 R2, Lync 2010, Office Communications Server 2007, Office Communications Server 2007 R2, or Lync Server 2010.
7 Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements.
- A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Revision class</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Appendix A: Product Behavior</td>
<td>Updated list of supported products.</td>
<td>major</td>
</tr>
</tbody>
</table>
8 Index

A

Abstract data model
- anonymous phone URI 20
- isGateway parameter 16
- ms-accepted-content-id header 21
- ms-bypass option tag 21
- ms-call-source header 18
- ms-early-media option tag 19
- ms-mediation-generated header 23
- ms-trunking-peer header 22
- phone-context parameter 17

Anonymous phone URI 20
- abstract data model 20
- higher-layer triggered events 20
- initialization 20
- local events 20
- message processing 20
- timer events 20
- timers 20

Anonymous Phone URI message 14

C

Capability negotiation 11

Change tracking 60

Contact header
- isGateway parameter 16

E

Examples 24
- isGateway SIP contact header parameter 24
- ms-accepted-content-id SIP header 45
- ms-bypass option tag
  - inbound call 38
  - outbound call 41
- ms-bypass SIP supported header option tag 38
- ms-call-source SIP header 32
- ms-early-media SIP supported header option tag 34
- ms-mediation-generated SIP header 54
- ms-trunking-peer SIP header 51
- phone-context SIP URI parameter 28

Supported header
- ms-bypass option tag
  - inbound call 38
  - outbound call 41

F

Fields - vendor-extensible 12

G

Glossary 7

H

Higher-layer triggered events

I

Implementer - security considerations 57

Inbound call examples
- isGateway SIP contact header parameter
  - 200 message sent from UAC 25
  - INVITE message received by UAC 24
- ms-accepted-content-id SIP header
  - 200 message sent by protocol client 47
  - INVITE message received by protocol client 45
- ms-bypass SIP supported header option tag
  - 200 message sent by protocol client 40
  - INVITE message received by protocol client 39
- ms-call-source SIP header
  - 200 message sent from UAC 34
  - 605 message sent from UAC 33
  - INVITE message received by UAC - step 2 32
  - INVITE message received by UAC - step 8 33
- ms-trunking-peer SIP header
  - INVITE message received by protocol client 52
- phone-context SIP URI parameter
  - 200 message sent from UAC 29
  - INVITE message received by UAC 28

Index of security parameters 57

Informative references 9

Initialization
- anonymous phone URI 20
- isGateway parameter 16
- ms-accepted-content-id 22
- ms-bypass option tag 21
- ms-call-source header 18
- ms-early-media option tag 19
- ms-mediation-generated header (section 3.9.3 23, section 6.58)
- ms-trunking-peer 22
- phone-context parameter 17

Introduction 7

isGateway 16
- abstract data model 16
- higher-layer triggered events 16
- initialization 16
- local events 16
- message processing 16
- timer events 16
- timers 16

isGateway message 13

isGateway SIP contact header parameter example 24
- inbound call 24
  - 200 message sent from UAC 25
  - INVITE message received by UAC 24
  - outbound call 26

---

[MS-OPCTN] - v20180828
Session Initiation Protocol (SIP) for PSTN Calls Extensions
Copyright © 2018 Microsoft Corporation
Release: August 28, 2018
Local events

- anonymous phone URI
- isGateway parameter
- ms-accepted-content-id header
- ms-bypass option tag
- ms-call-source header
- ms-early-media option tag
- ms-trunking-peer option tag
- phone-context parameter

Message processing

- anonymous phone URI
- isGateway parameter
- ms-accepted-content-id header
- ms-bypass option tag
- ms-call-source header
- ms-early-media option tag
- ms-mediation-generated header
- ms-trunking-peer header
- phone-context parameter

Message syntax

Messages

Anonymous Phone URI
- isGateway
- ms-accepted-content-id
- ms-bypass
- ms-call-source
- ms-early-media
- ms-mediation-generated
- ms-trunking-peer
- phone-context
- transport
- ms-accepted-content-id
- abstract data model
- higher-layer triggered events
- initialization
- local events
- message processing
- timers
- ms-accepted-content-id message
- ms-accepted-content-id SIP header example
- inbound call
- 200 message sent by protocol client
- INVITE message received by protocol client
- outbound call
- 200 message received by protocol client
- INVITE message sent by protocol client
- ms-call-source
- (section 3.3, section 3.4)
- abstract data model
- higher-layer triggered events
- initialization
- local events
- message processing
- timer events
- timers
- ms-call-source message
- ms-call-source SIP header example
- inbound call
- 605 message sent from UAC
- 200 message sent from UAC
- INVITE message received by UAC – step 2
- INVITE message received by UAC – step 8
- outbound call
- ms-early-media
- abstract data model
- higher-layer triggered events
- initialization
- local events
- message processing
- timer events
- timers
- ms-early-media message
- ms-early-media SIP supported header option tag example
- inbound call
- 183 message received by UAC
- 200 message received by UAC
- INVITE sent from UAC
- ms-mediation-generated
- abstract data model
- higher-layer triggered events
- initialization
- (section 3.9.3, section 6)
- message processing
- other local events
- timer events
- timers
- ms-mediation-generated message
- ms-mediation-generated SIP header example
- outbound call
- 180 message received by protocol client
- 183 message received by protocol client
- ms-trunking-peer
- abstract data model
- higher-layer triggered events
- initialization
- local events
- message processing
- timer events
- timers
- ms-trunking-peer message