IP Office Public SIP Trunks Overview and Specification

Release 9.0
Issue 01.AB
November 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose

specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Description

This document contains an overview of IP Office SIP trunk features and provides a listing of supported SIP trunk specifications.

Intended audience

This document is intended for sales, sales engineers, and other personnel who need to describe the capabilities of IP Office SIP trunks.

Chapter 2: Overview

A growing number of service providers now offer PSTN access to small and medium businesses via public SIP trunk connections, either to extend their reach beyond their typical copper based network coverage areas, or so that multiple services (voice and internet access) can be bundled into a single network connection. Although detailed public SIP trunk service offerings vary depending on the exact nature of the offer from the specific service provider, SIP trunks can potentially provide several advantages compared to traditional analog or digital trunks. These advantages include:

- cost savings resulting from reduced long distance charges, more efficient allocation of trunks, and operational savings associated with managing a consolidated network
- simplified dialing plans and number portability
- geographic transparency for local accessibility creating a virtual presence for incoming calls
- trunk diversity and redundancy
- multi-media ready to roll out future SIP enabled applications
- fewer hardware interfaces to purchase and manage, reducing cost and complexity
- faster and easier provisioning

IP Office delivers functionality that enhances its ability to be deployed in multi-vendor SIP-based VoIP networks. While this functionality is primarily based on the evolving SIP standards, there is no guarantee that all vendors, interpret and implement the standards in the same way. To help the SIP service provider, Avaya operates a comprehensive SIP Compliance Testing Program referred to as GSSCP. This program validates the operation of the IP Office solution with the service provider's SIP trunk offering. For more information about GSSCP, see the web page https://avaya.my.salesforce.com/apex/sp_ViewDetailPage?c=a3d30000000L5klAAC&Id=a3j30000000L7mAAAS.

IP Office 9.0 SIP trunk enhancements

IP Office SIP trunk capabilities improve configuration flexibility and deliver a broad feature set to support various service provider implementation scenarios.

Direct Media over SIP trunks on IP Office 500 v2

With direct media, all IP endpoints can send Real-time Transport Protocol (RTP) directly to each other rather than having all the media flow through the IP Office, using up VCM and relay resources. During call set up, each endpoint is told the RTP address of the other that it is connected to, rather than being allocated a port on the IP Office. This reduces network and VCM utilization for more optimized implementations. This feature extends the direct media capability to the IP 500 v2 platform.

In order to enable Allow Direct Media on a SIP Line, the Fax Transport cannot be T.38 or T.38 fallback because IP Office needs to stay in the media path in order to detect the fax tones. This

means that with a single ITSP, it is not possible to support both Direct Media and T.38 at the same time.

Enabling **Allow Direct Media** also does not mean that in every case it will be possible. If the **DTMF Transport** setting of the SIP Line and the IP endpoint are not compatible, then a direct media connection will not generally be established. If the SIP Line uses RFC2833 for DTMF, and a call is made using an H.323 set which does not support RFC2833, then the connection will not be direct unless **Force direct media with Phones** is also enabled. In this case, if there are any key presses indicated from the set, the media will be 'shuffled in' so that the IP Office is in the media path and can inject the RFC2833 telephone event indications into the media stream. After fifteen seconds of no key presses, the media is 'shuffled out' to make it direct again.

For outgoing calls even with **Allow Direct Media** enabled, the initial INVITE contains the media address of a port on the IP Office, not the address of the originating set. As soon as the call is answered, another INVITE is sent to establish direct media. This allows for ease of providing early media changes even before media is reliably negotiated, in the case of transfers or forwards.

SIP Trunks alarms

IP Office can generate an SNMP Trap when there are no free channels available to handle a call on a SIP Trunk. This allows external applications to monitor the performance of IP Office and determine whether it is sufficiently provisioned.

Super G3 fax

IP Office enables SIP Trunks to detect tones generated by Super G3 fax machines and configure the DSP channel with the appropriate codec and ECAN settings. It provides inter-operability with service providers that support higher data rate fax machines. Super G3 fax capabilities are not supported on Linux servers.

For an incoming local fax, IP Office can detect:

- ANS
- CED
- ANS with phase reversal
- ANSam(ANS with amplitude modulation)
- ANSam with phase reversal (typical response from SG3 faxes)

IP Office also detects all their corresponding signals from the network for an outgoing fax:

- NetANS
- NetCED
- NetANS with phase reversal
- NetANSam
- NetANSam with phase reversal

For each of these, IP Office will reconfigure the DSP accordingly, renegotiate to T38, and reconfigure the silence suppression and ECAN accordingly or renegotiate/continue on G711.

SIP response mapping to ISDN (Q.850) cause values

For SIP calls, this feature sends and receives Reason headers with Q.850 content. This header is included in specific SIP response messages as specified in RFC3398. The Q.850 content includes an ISDN cause value and text. The cause received in the Reason header is used in the disconnect message for the ISDN line and the cause received from ISDN determines the SIP error message and is included in the Reason header.

RFC2833 Default payload configuration option

You can configure the default RFC2833 payload used when initiating SIP calls. Some devices and networks cannot negotiate the dynamic payload type for RFC2833 and insist on a value different from the IP Office default of 101. For an incoming call IP Office accepts the offered DTMF payload.

Some supported endpoints, such as 1120e SIP phones and Flare for Windows, do not follow this setting as they are not configured through IP Office Manager directly.

Session refresh

Session refresh provides IP Office Manager the ability to initiate the use of SIP Session Timers on SIP and Session Manager (SM) trunks, whether the other end also requires or supports it or not. Sessions are refreshed by sending a periodic INVITE or UPDATE message and checking for the response. In previous releases, SIP calls between IP Office Manager endpoints did not make use of this mechanism to detect the loss of SIP sessions caused by failure in the network path or remote endpoint. This can result in resources not being freed appropriately.

Chapter 3: SIP messaging

SIP trunk prerequisites

Before any calls can be made, the system must have sufficient SIP trunk licenses for the maximum number of simultaneous SIP trunk calls expected.

On Server Edition systems, the **System | Telephony | Telephony | Maximum SIP Sessions** value must match the total number of SIP set and trunk calls that can occur at the same time.

Outgoing call message details

Related topics:

Destination URI on page 13
From field content on page 14
To field content on page 14
Contact field content on page 15
P-Asserted Identity field content on page 15
Typical outgoing call scenarios on page 16

Destination URI

The destination URI in an INVITE message has the general format of an e-mail address. Specific rules have been defined for expressing telephone numbers in this format. These rules are defined in RFC 2806 and RFC 3261 (section 19.1.6). A sample URI for a call on a SIP trunk is:

```
sip: 12125551234@ITSP_Domain SIP/2.0
```

The **ITSP_Domain** in the following headers is taken from the **SIP Line | ITSP Domain Name** field. If that is empty, the IP Address of the IP Office LAN interface is used or the public address of that interface if topology discovery is used.

From field content

If the call is originated from an IP Office endpoint, the settings on the **SIP line | SIP URI** tab determine whether the information should be taken from the trunk's SIP credentials, or from the **User | SIP** tab.

- If the channel's Local URI is set to ***** then the extension number of the set will be used for the User part of the identity.

  ```
  From: "SipDisplayNameAlice" <sip: 311@ITSP_Domain>;tag=8a9fed65b
  ```

- If the channel's Local URI is set to 'Use Internal Data' then the **User | SIP | SIP Name** will be used for the User part of the identity, and the ITSP Domain for the host part.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@ITSP_Domain>;tag=8a9fed65b
  ```

- If the SIP Name field also contains a domain (indicated by the presence of @) then that domain will be used.

  ```
  From: "SipDisplayNameAlice" <sip: SipName@USER_Domain>;tag=8a9fed65b
  ```

- If Call-ID is blocked either by short code or if the **User | SIP | Anonymous** checkbox is checked then the From: header will be anonymous, unless the **SIP Line | Send From in Clear** checkbox is checked.

  ```
  From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=8a9fed65b
  ```

- If the channel's **Local URI** is set to **Use Credentials …** then there must first be at least one set of SIP Credentials defined, and that account selected in the channel's **Registration** dropdown selection box. The corresponding field from the **SIP Line | SIP Credentials** tab will be used for the User part of the identity.

  ```
  From: "Line17Cred2" <sip:Line17Cred2@ITSP_Domain>;tag=8a9fed65b
  ```

- The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

  ```
  Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
  ```

To field content

Since the identity of the called party is not known at the time of the initial INVITE, the **To:** field shows only the information necessary to route the call, which is the dialed digits after any short code and ARS manipulation, prefix manipulation, and removal of any end-of-dial digits (**#** in North America).

```
To: <sip: 12125551234@ITSP_Domain>
```

Contact field content

The contact identity is populated similarly to the **From:** header. If Call-Id blocking is invoked: via **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox then the **Contact:** field becomes semi-anonymous:

```
Contact: <sip:anonymous@135.55.86.70:5060;transport=udp
```

P-Asserted Identity field content

Without Call-Id blocking, this field essentially mirrors the **From:** field.

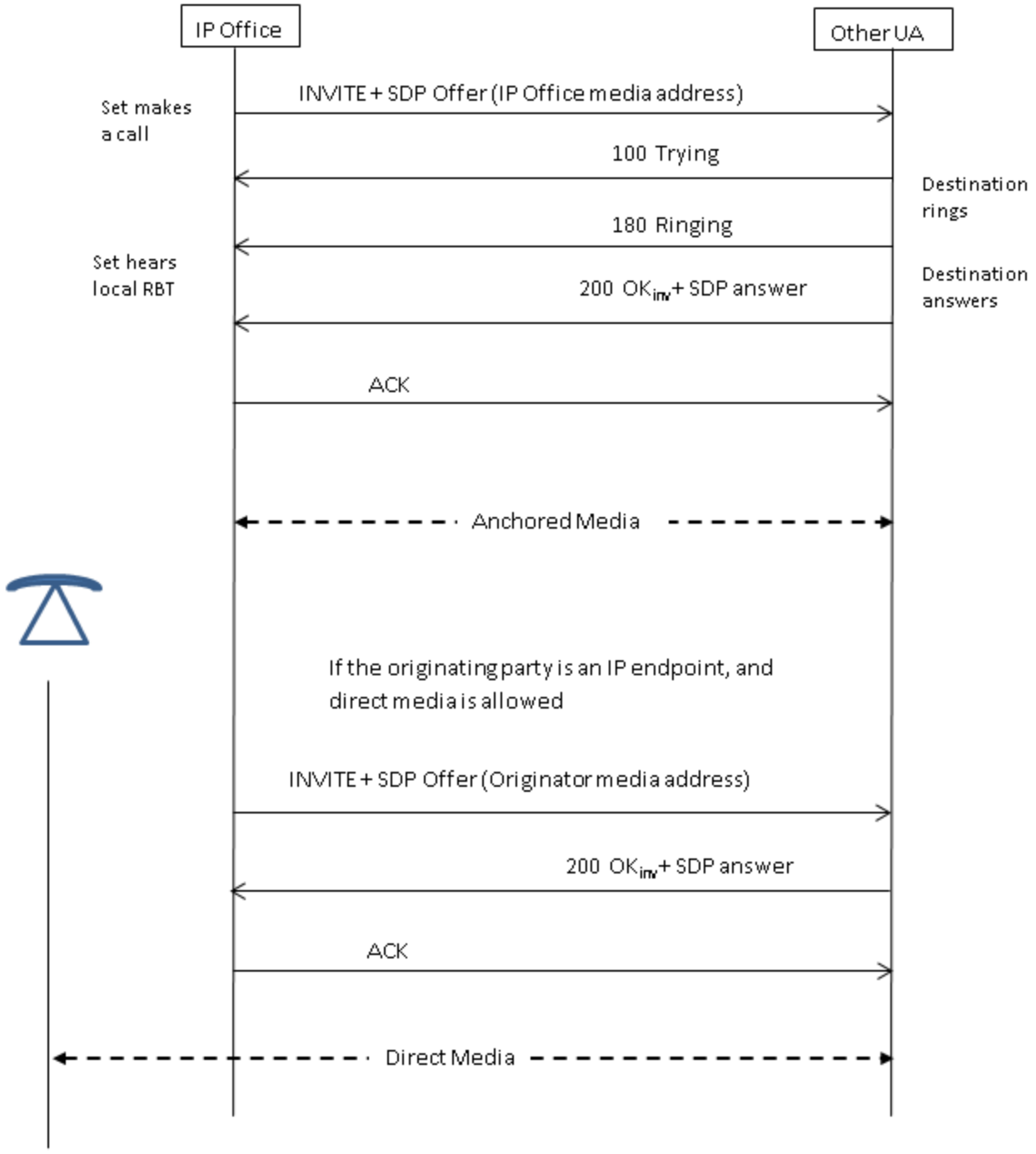
P-Asserted-Identity: " SipDisplayName " <sip: SipName@ITSP_Domain>

Call-Id blocking: using **W** in a short code, or by checking the **User | SIP | Anonymous** checkbox results in the **P-Asserted** field being the only header that carries the calling party information, and so is unchanged from the non-blocked case above.

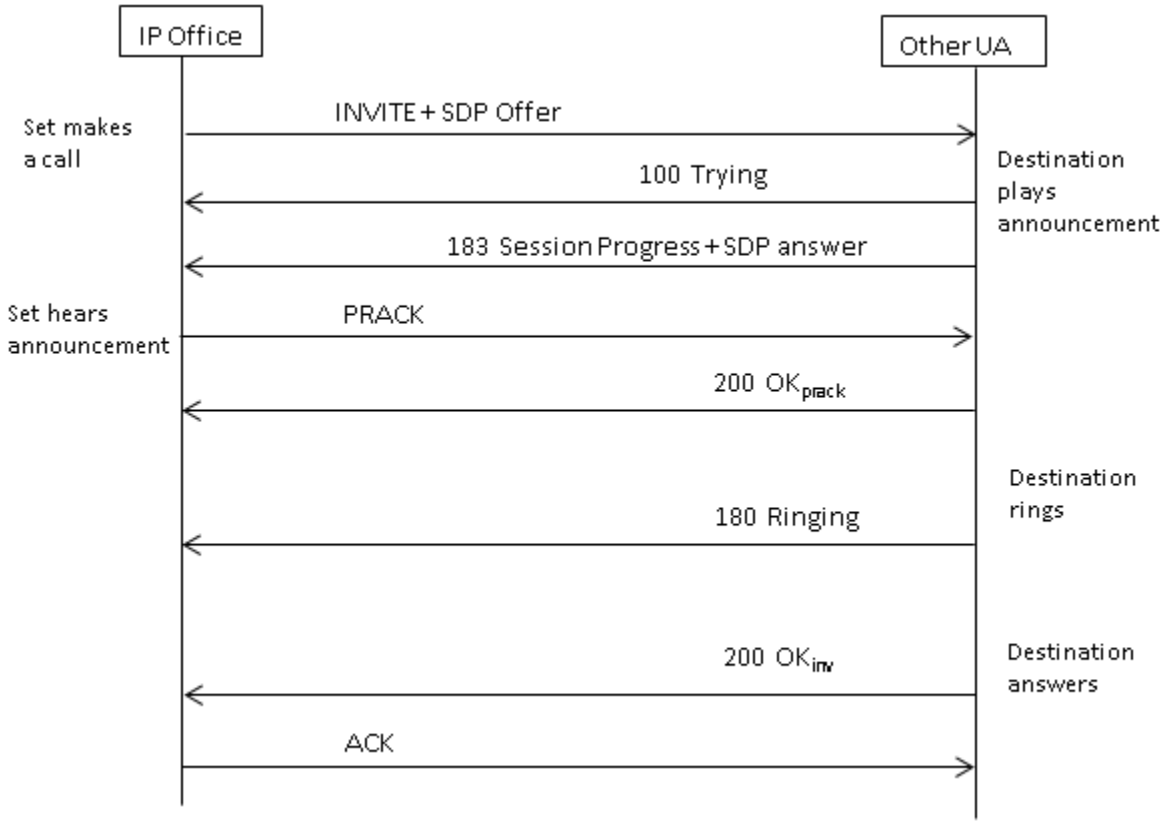
```
P-Asserted-Identity: " SipDisplayName" <sip:SipName@ITSP_Domain>
```

Typical outgoing call scenarios

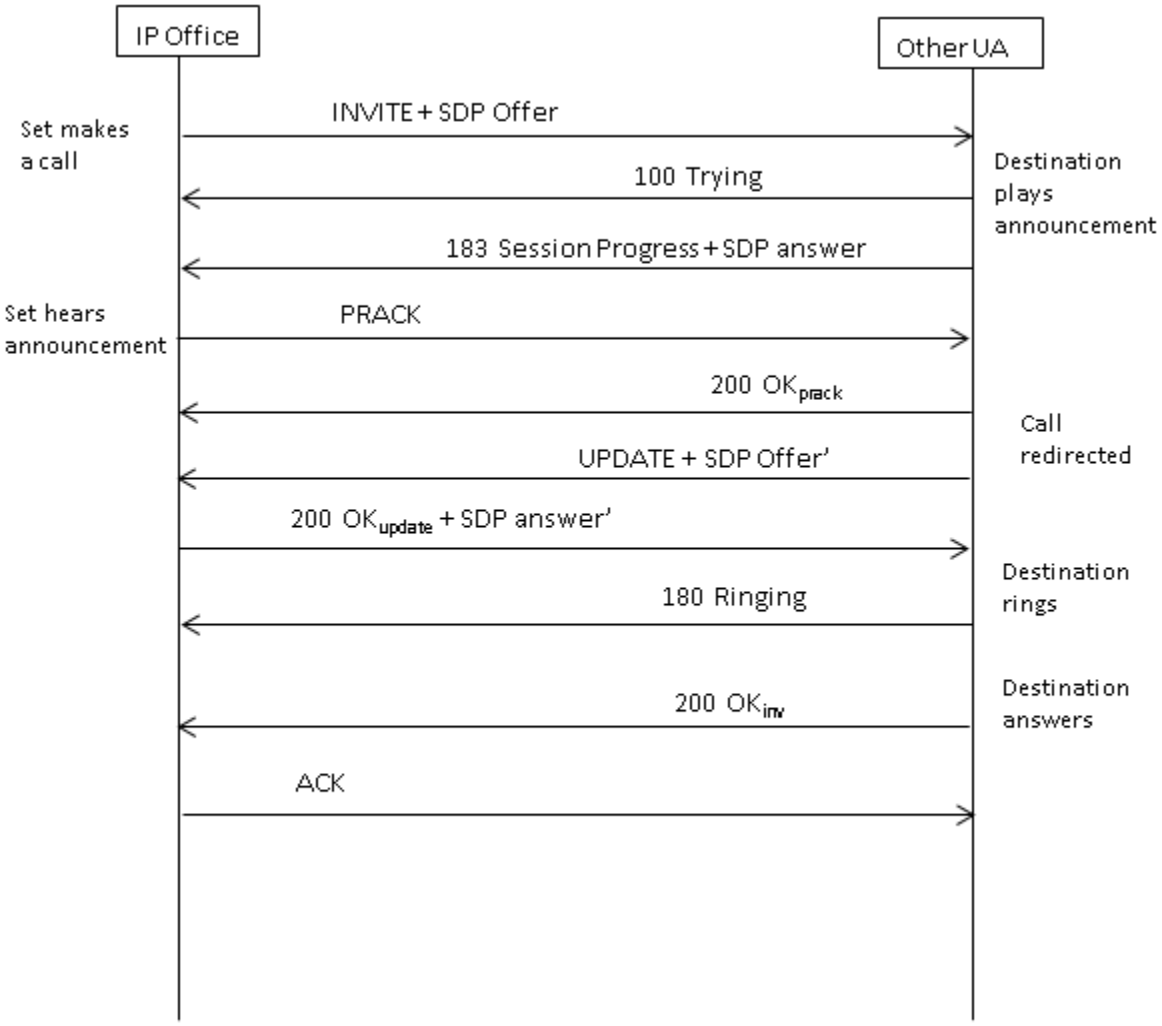
INVITE with SDP, local ringback



INVITE with SDP, early media



INVITE with SDP, early media re-directed by destination



Incoming call message details

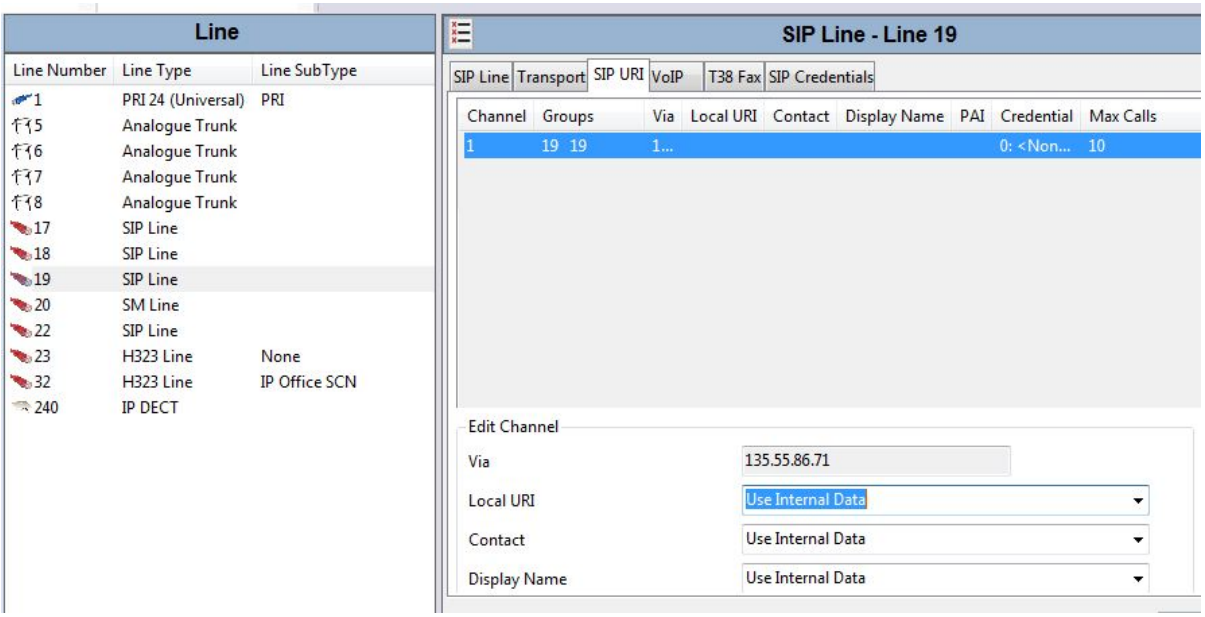
Related topics:

[Incoming call routing](#) on page 19
[Media path connection](#) on page 20
[Typical incoming call scenarios](#) on page 20

Incoming call routing

When a SIP INVITE is received by IP Office, its origin is compared to the known IP addresses of the SIP lines configured. If a match is not found, then the INVITE is presented internally to the set interface to determine if it matches any of the registered terminals. SIP messages from unknown endpoints are discarded, and solicit no response from IP Office.

SIP lines have incoming and outgoing groups associated with them, which are configured on the **SIP line | SIP URI** tab. In the example below, the incoming and outgoing groups are both 19, and the **Local URI** specifies **Use Internal Data**. With this **Local URI** setting, to route a call to a user, the **User | SIP | SIP Name** field is used to match against the incoming digits.



The incoming group indicates the identity of an **Incoming Call Route**, which is used to match the incoming digits in the Request-URI to a target. That target could be a set, a hunt group, another trunk, or an ARS entry.

Due to this grouping, calls incoming to several different trunks or trunk types can use the same **Incoming Call Route**, but in order for this to work,the **Local URI** must be manually set to **<*>**.

Incoming Call Routes are identified by the **Line Group ID** or optionally, an **Incoming Number** may be specified to match against in the received digits. Then a **Destination** specified, which may be a specific target, or may contain only a **<.>** to indicate that the digits are to be matched against known system targets.

Media path connection

IP Office does not provide in-band ringback to incoming SIP trunk calls. This is different from what is done for H.323. The only scenario in which an incoming SIP trunk call will hear in-band ringback occurs when the call terminates on an analog trunk. With analog trunks, the media path is cut through immediately because IP Office has no way of determining the state (ringing, busy, answered) of the trunk.

IP Office connects “early” media before the call is answered by sending a 183 Session Progress response only if the following two conditions are met:

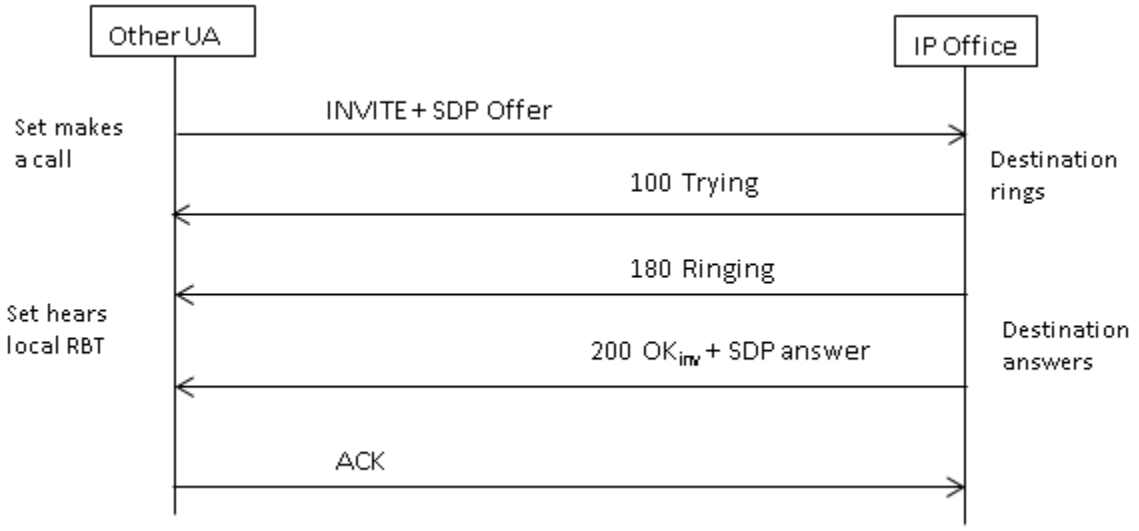
- A PROGRESS (in-band tone indication OR 183 Session Progress with SDP) message is received from the destination (this can only happen in a SIP-to-PRI or SIP-to-SIP tandem scenario).
- The INVITE message contains SDP.

IP Office does not attempt to connect early media on PROGRESS when there is no SDP in the initial INVITE, since this is unlikely to succeed. The reason there is no SDP in INVITE is probably that the originating system does not know the originator’s media address yet. A typical scenario where this is the case occurs when the call on the originating system comes from an H.323 SlowStart trunk.

Typical incoming call scenarios

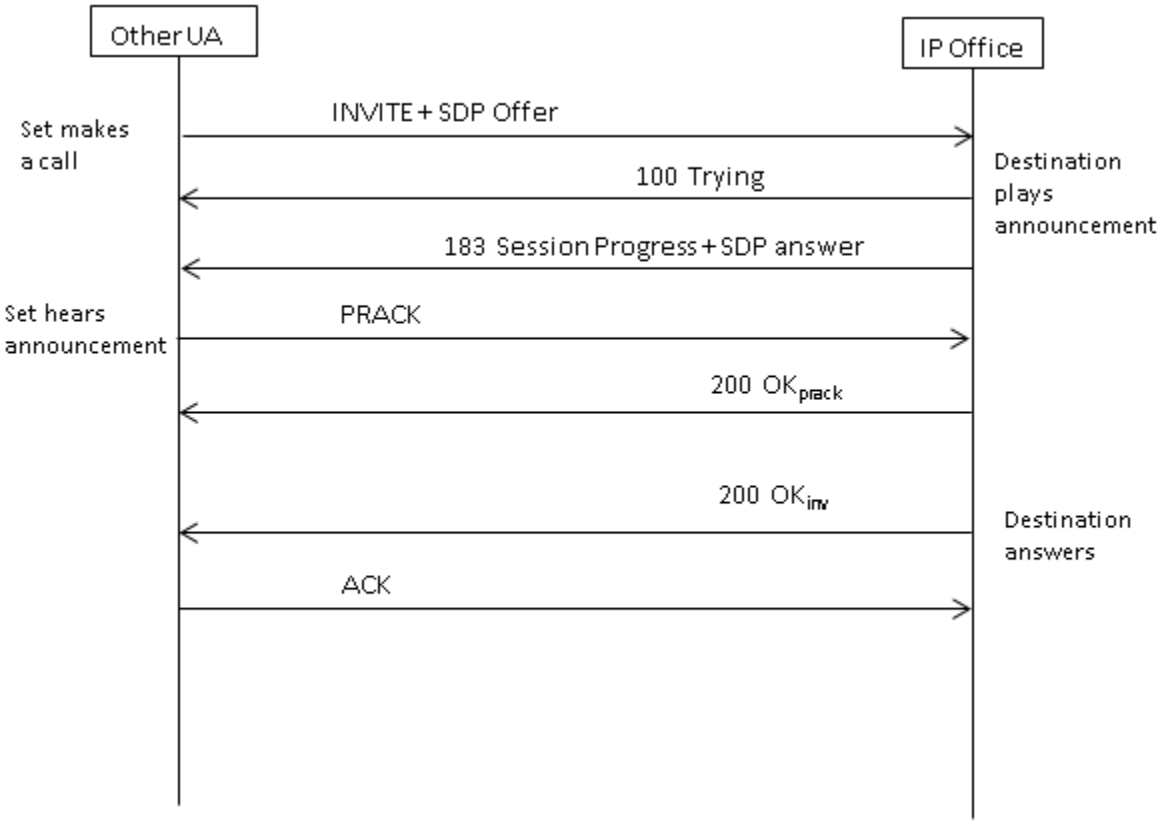
INVITE with SDP, local ringback

If the destination is an analog trunk, the 180 Ringing will be replaced with a 183 Progress with SDP followed immediately by a “fake” answer in order that the media will be connected right away so that the originator hears whatever in-band tones are present on the analog trunk (ringback or busy). If the target is a set that is unconditionally call forwarded over an analog trunk, then there will be a 180 Ringing without SDP, followed immediately by the “fake” answer.



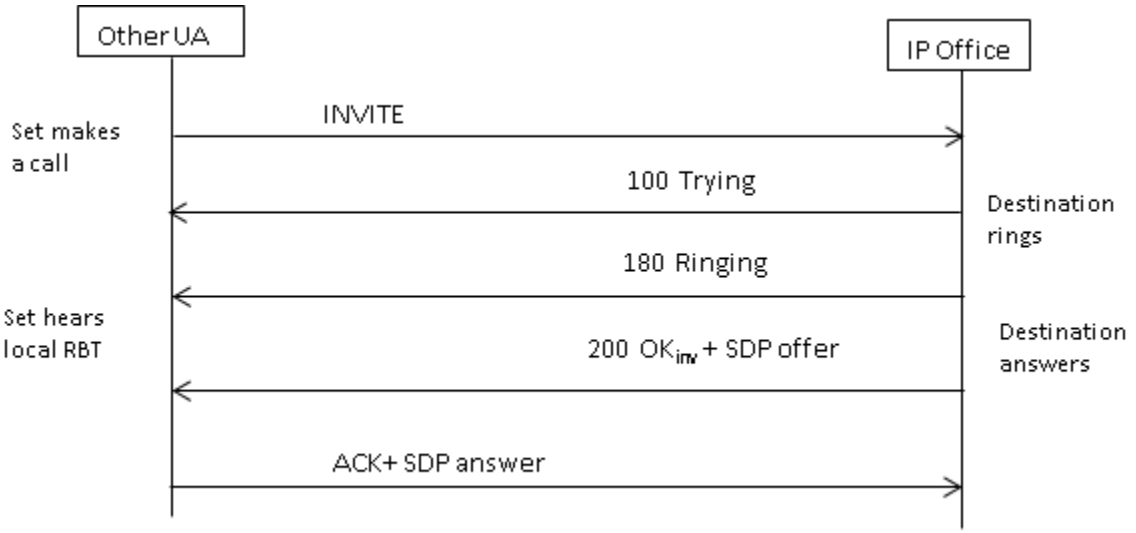
INVITE with SDP, early media

If the SIP Trunk receives a FAR_PROGRESS (in-band) message from its peer in the core (e.g. from a tandem PRI or SIP trunk), it sends a 183 Session Progress message with SDP to the far end. IP Office will connect the media on receipt of 180 or 183 with SDP.



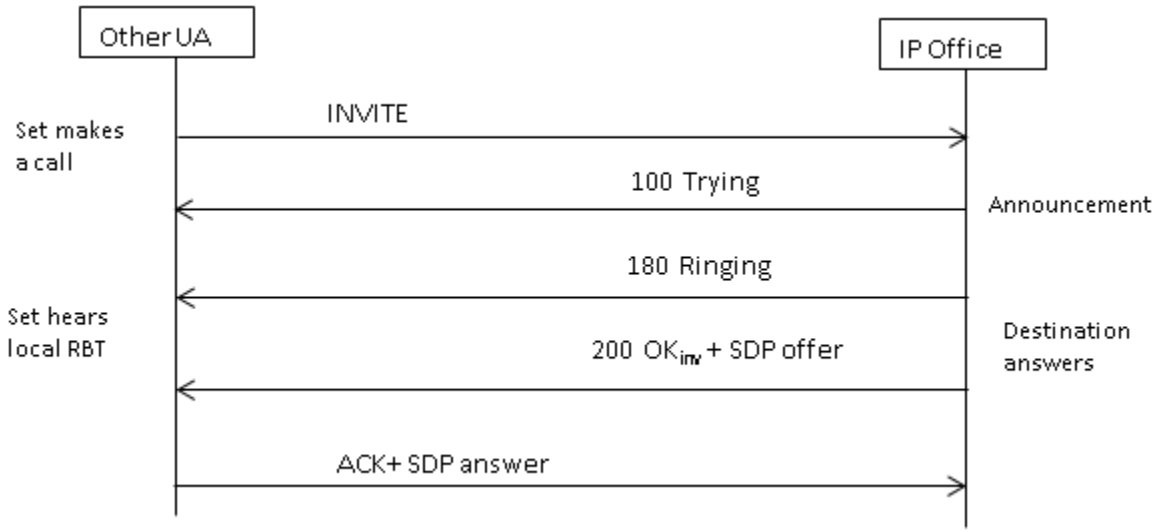
INVITE without SDP, local ring back

IP Office does not attempt to send early media in this scenario.



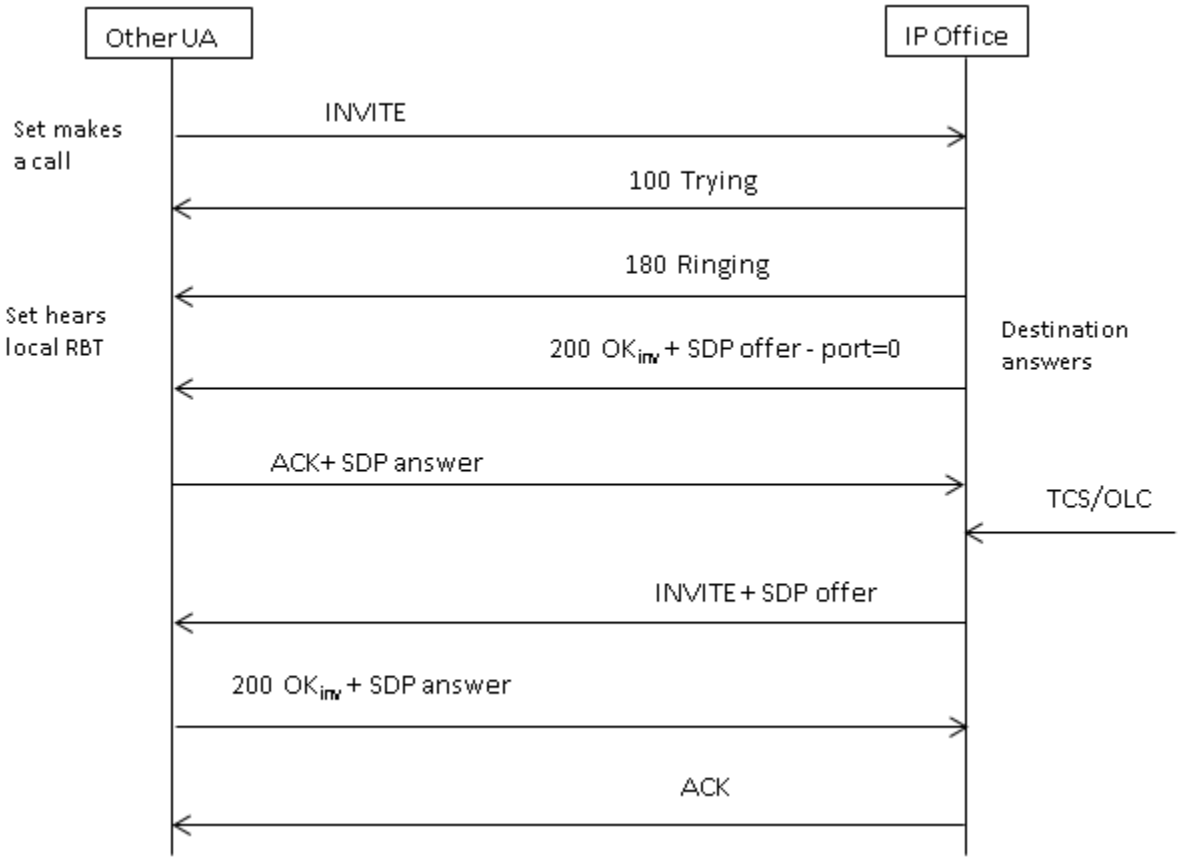
INVITE without SDP, early media

In this scenario, the far end attempts to connect media before the call is answered. IP Office does not provide early media when receiving an empty INVITE, but rather 180 Ringing instead. There is no requirement to provide an SDP in the 180 Ringing provisional response, as that response is not sent reliably using the PRACK mechanism.



INVITE without SDP, call terminates on H.323 endpoint

If the destination of the call is an H.323 trunk, the destination media address is not known when the call is answered. Therefore, the SDP offer in 200 OK will contain a null port number (and IP address). Once the logical channels are opened on the H.323 side, IP Office sends a re-INVITE using the real media address.



Codec selection

Codec selection is based on the Offer/Answer model specified in RFC 3264. The endpoint that issues the offer includes the list of codecs that it supports. IP Office offers the codecs set on the **SIP line | VoIP** tab, not those that are set on the extension.

The other endpoint sends an answer that should normally contain a single codec. If there are multiple codecs in the answer, IP Office only considers the first codec. If the SIP Line is

configured to do Codec Lockdown (Re-Invite Supported is a prerequisite) then it will send another INVITE with the single chosen codec.

DTMF transmission

DTMF over RTP (RFC 2833) can be used in IP Office. Asymmetric dynamic payload negotiation is supported when it is necessary to bridge multiple SIP endpoints that do not support payload negotiation. The value used for an initial offer is configured on the **System | Codecs** tab. The default value is 101. Upon receipt of an offer with an RFC2833 payload type, IP Office will automatically use the proposed value rather than its own configured value. This helps to support networks that do not negotiate payload types.

There are cases in which direct media is desirable between SIP trunks and endpoints that do not support RFC2833. To allow for this, if key presses are indicated from the set, the IP Office will ‘shuffle’ the media in. This connects its own media engine to the endpoint and to the SIP trunk, and injects the digits in-band using the negotiated dynamic payload. After fifteen seconds of no key presses, the media will be shuffled back out to re-establish a direct connection again.

Fax over SIP

T.38 Fax over SIP is supported on the IP500 v2 platform deployed as standalone or as an expansion gateway. G.711 fax is also supported, and is supported on Linux servers. For networks that do or do not support T.38, IP Office allows both G3 and Super G3 fax machines to interoperate.

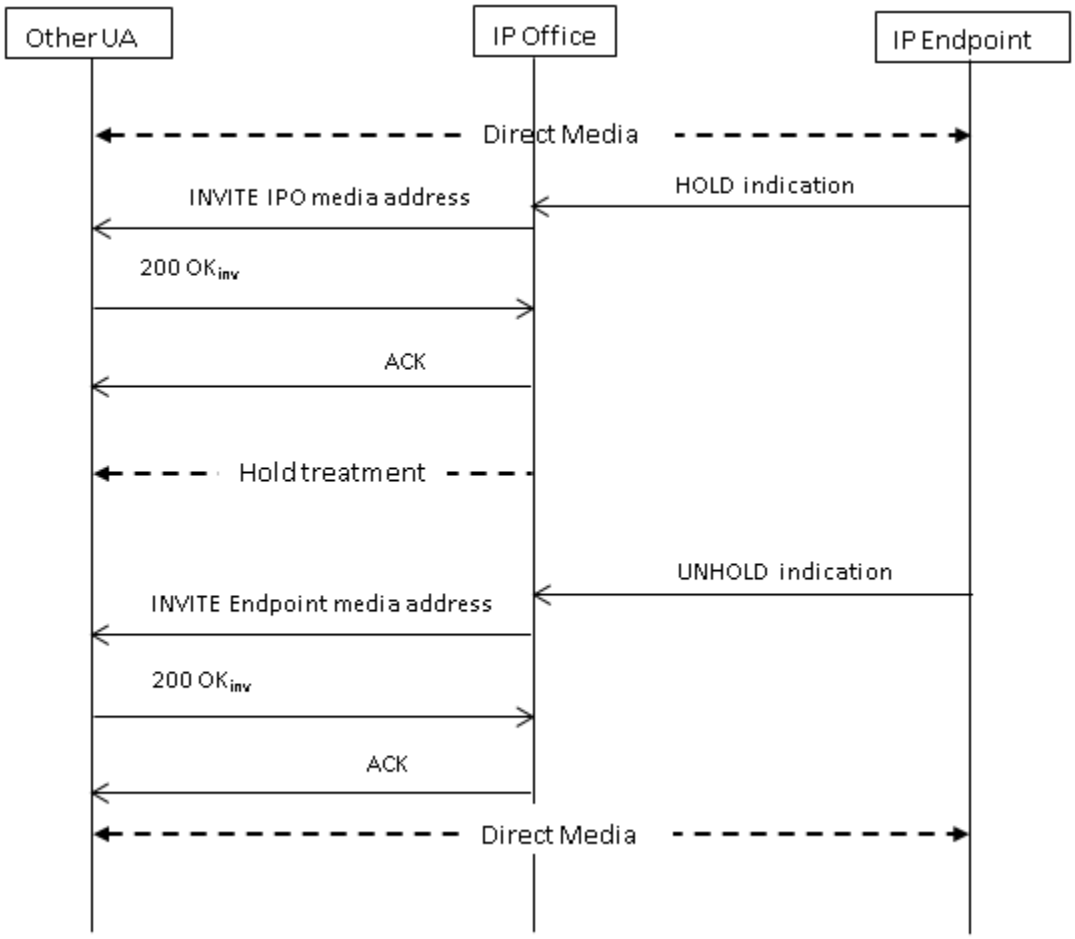
There are configuration parameters that control the behavior in different networks. If T.38 is supported in a network, then it may make sense to select T.38 as the Fax Transport preference in order to make use the inherent quality provided by the redundancy mechanisms. On the other hand, if all of the fax machines in the network are Super G3 capable, there may be a need to take advantage of the increased speed that this encoding provides. Since T.38 is not capable of encoding Super G3, G.711 may be a better choice for the Fax Transport. In either case, IP Office will accept codec change requests from the far SIP endpoint to switch to T.38 or to G.711.

T.38 Fax Transport and Direct Media are mutually exclusive on a given SIP Line. IP Office keeps itself in the media path so that it can detect fax tones to make the switch to T.38.

Hold scenarios

Hold originated by IP Office

When an IP Office DS set or non-IP trunk puts a SIP trunk on hold, there is no indication to the network. The voice path is merely switched in the TDM domain to the appropriate hold treatment source, be it tones, silence or music. For IP sets and trunks, be they H.323 or SIP, if the call uses direct media, there will be a re-INVITE sent to redirect the media source from the set or trunk endpoint to a port on the IP Office in order to connect hold treatment. When the call is then unheld, another INVITE will go out to connect the set with the far end.



Hold originated by far end

The far end of a SIP trunk can put the IP Office on hold by sending it re-INVITE with an SDP Offer containing:

- A **sendonly** attribute. IP Office replies with an SDP Answer containing the **recvonly**attribute.
- An "**inactive**" attribute. IP Office replies with **inactive**.
- A zero media connection address (c=0.0.0.0). IP Office replies with **inactive**.

Unhold

A held call is unheld by means of an SDP Offer with the **sendrecv** attribute (or no direction attribute, since **sendrecv** is assumed if not specified).

Unhold from mutual hold

Either end can un-hold the other end, i.e., allow it to transmit again, by sending a new Offer with the **sendrecv** or **recvonly**attribute. The other end replies with **sendonly** if the call is still on hold at its end.

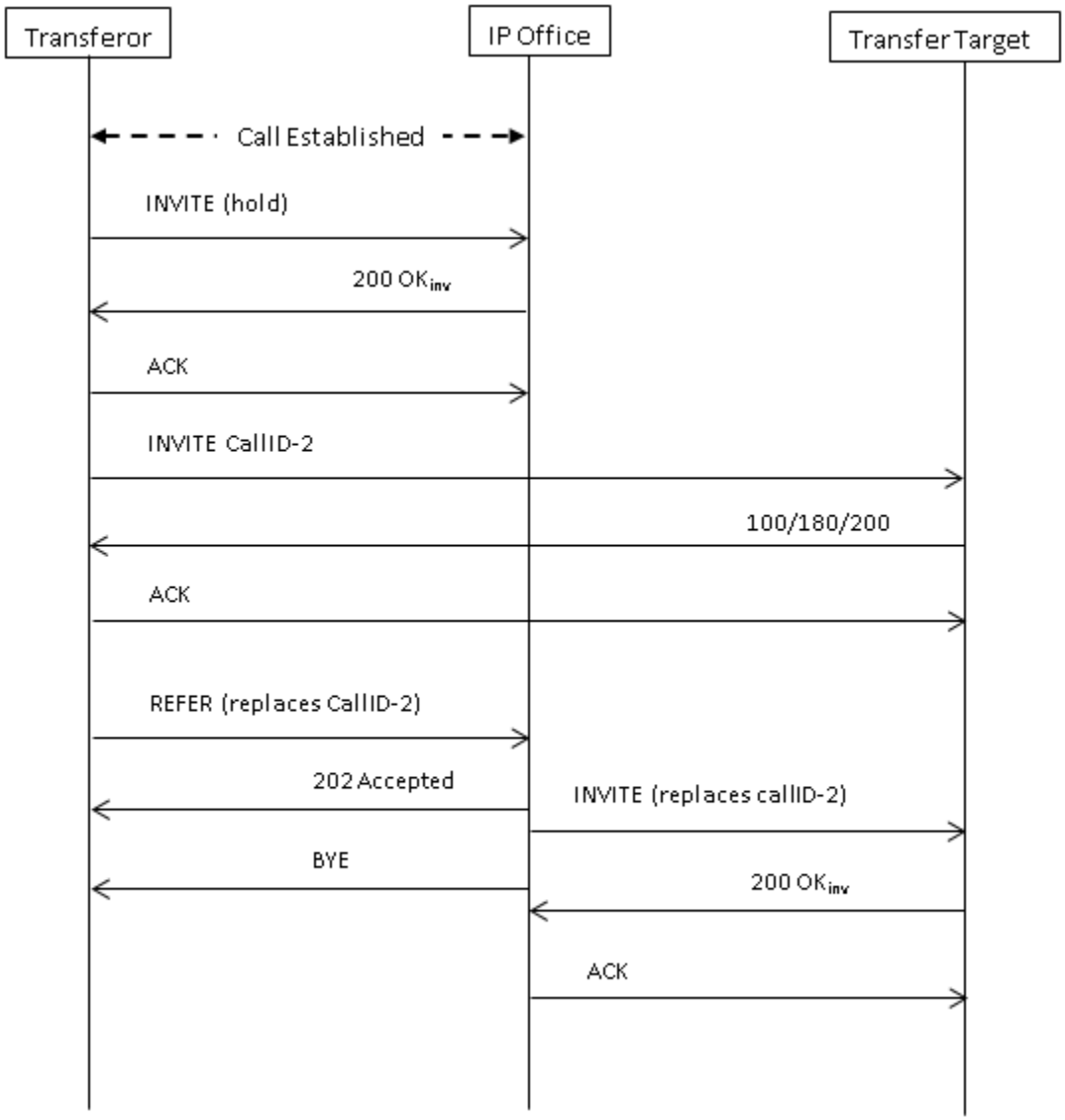
SIP REFER

After a SIP call has been established between two parties (the "Primary call), the SIP REFER method is used by the **TransferOR** end of the call to transfer the **TransferEE** end to a **Transfer Target**. The REFER message provides the Transfer Target's contact information in the Refer-To header. This causes the TransferEE to establish the Secondary call to the Transfer Target, thus completing the transfer.

For public SIP trunks, IP Office supports only consultative call transfer using REFER. Consultative transfer is also known as Attended. With consultative transfer, the TransferOR puts the Primary call on hold and establishes a **Consult** call to another party. After the consultation, the TransferOR completes the transfer, causing the TransferEE to connect to the Transfer Target, thereby replacing the Transfer Target's call with the TransferOR.

REFER can be configured to accept incoming, reject incoming, or decide based on the presence of REFER in the **Allow:** header in responses to OPTIONS messages. Similarly, there is the same configuration for outgoing REFER.

Although the TransferOR and TransferEE must be SIP endpoints, the Transfer Target may be a TDM, PRI, H.323 or SIP terminal on the same IP Office, or an endpoint reachable over the same SIP line as the REFER request is received from.


Transferor
IP Office
Transfer Target
Call Established
INVITE (hold)
200 OKinv
ACK
INVITE CallID-2
100/180/200
ACK
REFER (replaces CallID-2)
202 Accepted
INVITE (replaces callID-2)
BYE
200 OKinv
ACK

Chapter 4: IP Office SIP trunk specifications

This section outlines the SIP trunk capabilities supported by IP Office.

RFCs

- ITU-T T.38 Annex D, Procedures for real-time Group 3 facsimile communication over IP networks
- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications
- RFC 2327 - SDP: Session Description Protocol
- RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication
- RFC 2833/RFC 4733 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2976 - The SIP INFO Method
- RFC 3087 - Control of Service Context using SIP Request-URI
- RFC 3261 - Session Initiation Protocol
- RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3515 – The Session Initiation Protocol (SIP) Refer method
- RFC 3550 - RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3665 - Session Initiation Protocol Basic Call Flow Examples
- RFC 3666 - Session Initiation Protocol PSTN Call Flows
- RFC 3725 - Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3824 - Using E.164 numbers with the Session Initiation Protocol (SIP)
- RFC 3842 - A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol
- RFC 3891 - The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 4028 - Session Timers in the Session Initiation Protocol (SIP)
- RFC 4566 - SDP: Session Description Protocol
- RFC 5359 - Session Initiation Protocol Service Examples

- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted
- RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3398 - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping
- RFC 3407 - Session Description Protocol (SDP) Simple Capability
- RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 5379 - Guidelines for Using the Privacy Mechanism for SIP
- RFC 5806 - Diversion Indication in SIP
- RFC 5876 - Updates to Asserted Identity in the Session Initiation Protocol (SIP)
- RFC 6337 - Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
- RFC 6432 - Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses

Transport protocols

- UDP
- TCP
- RTP
- RTCP

Request methods

- INVITE
- ACK
- BYE
- CANCEL
- INFO
- REFER
- REGISTER
- SUBSCRIBE
- NOTIFY
- PRACK
- OPTIONS
- UPDATE
- PUBLISH
- MESSAGE
- PING

Response methods

- 100 Trying
- 180 Ringing
- 181 Call Is Being Forwarded
- 182 Call Queued
- 183 Session progress
- 200 OK
- 202 ACCEPTED
- 3XX
- 4XX
- 5XX
- 6XX

Headers

- Accept
- Alert-Info
- Allow
- Allow-Event
- Authorization
- Call-ID
- Contact
- Content-Length
- Content-Type
- CSeq
- Diversion
- From
- History-Info
- Max-Forwards
- P-Asserted-Identity
- P-Early-Media
- P-Preferred-Identity
- Privacy
- Proxy-Authenticate
- Proxy-Authorization
- Proxy-Require
- Require
- Remote-Party-ID
- Server
- Session-Timers
- Supported
- To
- User-Agent
- Via
- WWW-Authenticate

Index