Network Working Group
Internet Draft
Intended status: Informational
Expires: February 2012

J. Haluska
Telcordia
R. Ahern
AT&T Customer Information Services
Marty Cruze
CenturyLink
C. Blackwell
Verizon
August 15, 2011

Considerations for Information Services and Operator Services Using SIP

draft-haluska-sipping-directory-assistance-11.txt

Status of this Memo

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft will expire on February 15, 2009.

Copyright Notice

Abstract

Information Services are services whereby information is provided in response to user requests, and may include involvement of a human or automated agent. A popular existing Information Service is Directory Assistance (DA). Moving ahead, Information Services providers envision exciting multimedia services that support simultaneous voice and data interactions with full operator backup at any time during the call. Information Services providers are planning to migrate to SIP based platforms, which will enable such advanced services, while continuing to support traditional DA services.

Operator Services are traditional PSTN services which often involve providing human or automated assistance to a caller, and often require the specialized capabilities traditionally provided by an operator services switch. Market and/or regulatory factors in some jurisdictions dictate that some subset of Operator Services continue to be provided going forward.

This document aims to identify how Operator and Information Services can be implemented using existing or currently proposed SIP mechanisms, to identity existing protocol gaps, and to provide a set of Best Current Practices to facilitate interoperability. For Operator Services, the intention is to describe how current operator services can continue to be provided to PSTN based subscribers via a SIP based operator services architecture. It also looks at how current operator services might be provided to SIP based subscribers

via such an architecture, but does not consider the larger question of the need for or usefulness or suitability of each of these services for SIP based subscribers.

This document addresses the needs of current Operator and Information Services providers; as such, the intended audience includes vendors of equipment and services to such providers.

Table of Contents

1. Introduction

Information Services are services whereby information is provided in response to user requests. This may include involvement of a human or automated agent. Information Services may include call completion to a requested telephone number and other extensions provided on behalf of the owner of the information, such as assistance with purchases. The users normally access the Information Services by dialing an appropriate dialing sequence and verbally requesting an operator or automated system for the information. Examples of such dialing sequences for directory assistance currently include "411" or "1-NPA-555-1212" in North America, or "118xxx" in many European countries. Dialing sequences for operator services in North America often include "0" either by itself or as a prefix. In Europe the

dialing sequence varies by country, but may include "00", or "100" plus additional digits depending on the service being requested. The users may also request information through other access methods, such as chat (IM), email, Web (HTTP) or SMS initiated requests. The Information may be delivered to the user via any mode, such as verbal announcements, chat (IM), email, Web (HTTP), MMS, or SMS.

A popular existing Information Service is Directory Assistance (DA). DA is a well known service in today's PSTN, and is generally identified with "411" or "NPA-555-1212" type services in North America. Today's DA services provide a user with telephone number associated with a name and locality provided by the user, can complete the call for the user, and can send SMS with the listing to the user's wireless phone. Other Information Services provide the user with a wide range of information, such as movie listings and the weather.

Moving ahead, Information Services providers envision exciting multimedia services that support simultaneous voice and data interactions with full operator backup at any time during the call. For instance, a directions Information Service may announce and display directions to the requested listing, with the option for the caller to request transfer to an operator with the latest call context information.

Operator Services are traditional PSTN services which often involve providing human or automated assistance to a caller, and often require the specialized capabilities traditionally provided by an operator services switch. Market and/or regulatory factors in some jurisdictions dictate that some subset of Operator Services continue to be provided going forward. Some examples of such services include collect calls, third party billed calls, and busy line verification.

Operator and Information Services providers are planning to migrate to SIP based platforms, which will enable such advanced services, while continuing to support traditional DA services.

Implementing Operator and Information Services with SIP will require the exchange of certain information, and possibly the use of specialized capabilities which are not normally required for other types of calls. This document aims to identify such information, and stimulate discussion about how this information could be exchanged. Existing mechanisms will be used where appropriate, and currently existing proposals will be favored over new extensions.

Some of the services discussed in this document are based on Operator Services offered in North America. Also, many of the

signaling issues described are based on North American PSTN signaling. However, the ideas in this document are not intended to be exclusive to North America, and are intended to be useful in other environments as well.

For Operator Services, the intention is to describe how current operator services can continue to be provided to PSTN based subscribers via a SIP based operator services architecture. It also looks at how current operator services might be provided to SIP based subscribers via such an architecture, but does not consider the larger question of the need for or usefulness or suitability of each of these services in such an environment. Specifically, many of the constraints and assumptions regarding access to wireline services via a copper loop, under which services such as Busy Line Verification, Interrupt, and services where the operator controls the "line" make sense, do not have natural parallels in a SIP based environment. Some of these services are treated here for completeness.

A basic architecture utilizing an application server as the primary controller, performing third party call control to route incoming calls among media servers, operator workstations, etc. is described. Interface to the PSTN is described using PSTN gateways which interwork between ISUP or MF signaling and SIP.

Operator services in the North American PSTN often utilize MF trunks. As there is currently no specific specification for MF/SIP interworking, we assume that the PSTN gateway performs an internal MF to ISUP translation.

The use of existing SIP mechanisms is described where possible. Some of the main mechanisms described include third party call control, the REFER method with several extensions (e.g. Replaces), the Join header, Netann, and some of the ongoing work in the MEDIACTRL working group.

It is assumed that appropriate business relationships are in place between involved providers, and that the providers involved have trust relationships as described in [RFC3325]. In other words, this document does not assume general operation on the open internet, but rather between sets of providers with appropriate business and trust relationships. Individual providers may decide to provide handling for other requests, but this is beyond the scope of this document.

2. Protocol Gaps

As indicated above, one of the purposes of this document is to identify gaps in existing protocols, with respect to implementing Directory Assistance and Operator Services in SIP. Several gaps have been identified, and these are listed in this section of the document for convenience to the reader. These include:

- Charge Number
- Coin Deposit Tones
- Carrier Information: ISUP TNS, CIP, and CSI parameters, and "cic", "dai" tel URI parameters

3. Terminology

This section defines terms that will be used to discuss Information and Operator Services.

"0-" ("zero minus") Dialing - Invocation of Operator Services by dialing "0" with no further digits.

"0+" ("Zero Plus") Dialing - Invocation of Operator Services by dialing "0" followed by a phone number.

Application Server (AS) - An Application Server is a server providing value added services. It controls SIP sessions on behalf of the services supported by the service provider’s network.

Back End Automation - Back End Automation refers to automation of the function that provides listing information to the caller. This includes playing a verbal announcement with the listing information, and may also include prompting the user for additional service requests (e.g., call completion service).

Branding - Branding is a service where customized announcements are provided to the caller to identify the service provider. For example, if the service is provided to a Home Provider’s subscribers by a third party provider, branded service might include a message thanking them for using that Home Provider. Thus the user experience is that the service is provided by their Home Provider rather than some third party. Branding can be influenced by a number of factors, including but not limited to the identity of the caller’s Home Provider, or of other providers involved in the call.

Call Completion - Call Completion is a service where a call is initiated by the provider on behalf of the user. For example, in the DA service, once the DA provider has identified the requested listing, it may offer to complete the call for the caller, usually for some additional fee. This relieves the user from having to remember the number and then dial it.

DA Provider - The DA provider is the provider of DA services to end users. Since DA services are a subset of IS services, a DA provider is also an IS provider, and the definition of IS provider holds true for DA provider, except that the scope of services is limited to DA services.

Front End Automation - Front End Automation refers to automation of the initial customer contact, whereby a branded announcement may be played, a prompt is played to the user, and the user's spoken request is recorded. Speech recognition and querying for the listing information are performed as part of front end automation.

Home Provider - The service provider who is responsible for providing voice services to the calling customer. This is the service provider that has the business relationship with the calling customer. The identity of the home provider influences call processing treatment, such as branding and operator queue selection.

Home Subscriber Server (HSS) - The Home Subscriber Server is an IMS network element similar to a Home Location Register. It is a database containing information about the subscriber, user equipment, filter criteria for call processing triggers, etc.

Information Services (IS) Provider - The IS provider is the provider of Information Services to end users. The Information Services provider provides retail services directly to end users, and provides wholesale services to other service providers.

Intermediate Provider - In the context of this document, an Intermediate Provider is a provider which has agreements with home providers to handle OIS requests, and with OISPs which actually provide the requested services. Note that some home providers will have direct relationships with OISPs, rather than using an Intermediate Provider. Intermediate Providers are the targets of SIP requests from home providers since they are involved when a home provider does not have a direct relationship with an OISP. Intermediate Providers perform retargeting of received SIP requests toward the OISP. Intermediate providers make service level decisions, such as receiving requests for a service (such as DA calls) from other networks, deciding which provider will actually

provide the service, and forwarding the request to that provider, retargeting the Request-URI as necessary.

Layer 3 connectivity - This refers to IP connectivity, for example as provided by an Internet Service Provider or Managed IP service provider. If one entity has Layer 3 connectivity to another entity, then it can route packets to that entity. This does not imply anything about any physical path between the entities. Nor does it imply any application layer connectivity between the entities.

Media Server - A Media Server is a general-purpose platform for executing real-time media processing tasks. Examples of typical functions performed by media servers include playing announcements, collecting speech and/or DTMF digits, and performing conferencing functions.

Operator and Information Services Provider (OISP) - In this document, this term refers to an Information Services Provider, Directory Assistance Provider, or Operator Services Provider, depending on the context. This term is used for brevity. We are also defining this to be an adjective, thus "OISP services" is a convenient, intuitive way to say "Operator and Information Services".

Operator Services - Traditional PSTN services which often involve providing human or automated assistance to a caller, and often require the specialized capabilities traditionally provided by an operator services switch. Some examples of such services include collect calls, third party billed calls, and busy line verification.

Retail OIS service - A retail OIS service is one which is provided to a user by the user’s Home Provider.

SIP Layer connectivity - When two SIP service providers interconnect for the purpose of exchanging SIP sessions or calls, they are said to have SIP layer connectivity to one another.

Time Division Multiplexed (TDM) Local Exchange Carriers (LECs) - ATDM LEC provides local exchange service to end users utilizing TDM-based switching systems.

Transit Provider - In the context of this document, a transit provider simply "moves calls", and has no concept of OIS services. It may perform SIP rerouting of the request, but does not perform SIP retargeting. Such a provider is used when a provider cannot directly route calls to another provider. For example, an Intermediate Provider might use a Transit Provider if for some

reason (e.g. error condition) it cannot route a call directly to an OISP. This is in contrast to an Intermediate Provider (see definition earlier in this section).

Whisper - During front end automation, the OIS-MS will record and may time compress the caller's perhaps meandering speech into what is known as the "Whisper". This is intended to be played into a human operator's ear, should the call be referred to an operator, to avoid the operator from having to prompt the caller again. The whisper is obtained during the front end automation, and saved as an audio file.

Wholesale OIS service -A Wholesale OIS Service is one which is provided to a user by a Service Provider other than the user's Home Provider.

Zero Minus ("0-") Dialing - Invocation of Operator Services by dialing "0" with no further digits.

Zero Plus ("0+") Dialing - Invocation of Operator Services by dialing "0" followed by a phone number.

4. High Level Requirements

In addition to all-IP scenarios, it must be possible to support interworking with existing PSTN and wireless based providers, via both SS7 and MF interconnections.

It must be possible to support collection of usage information. This includes both online and offline usage information. It must be possible to perform usage collection for all actions associated with a particular call, and further to be able to correlate actions across multiple provider elements and across providers.

It must be possible to support multiple Operator and Information Services Providers (OISPs) per originating provider. The choice as to which OISP to be used could be on a per subscriber basis, or on other criteria.

It must be possible to support multiple OISP providers per call. For example, one provider might be used for front end automation, and another used for operator assistance.

It must be possible to provide an automated announcement to the user, and prompt the user for the type of query and query information.

It must be possible to pass a "whisper" to the operator workstation.

It must be possible to connect the user to a human operator.

It must be possible to provide an automated announcement of the requested information.

It must be possible to prompt the user for call completion.

It must be possible to perform call completion.

It must be possible to support the case where OIS services are provided by the caller's Home Provider. This scenario is known in the OIS industry as the Retail scenario. In this case, the caller's Home Provider is also an OISP, and provides OIS service to its own subscribers. This is illustrated in the following figure:

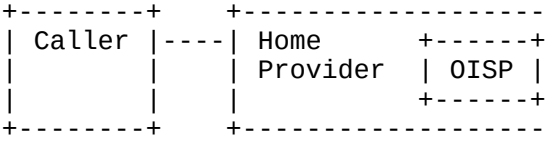


Figure 1 Services Provider by Home Provider

It must be possible to support the case where OIS services are provided by a direct third party provider. In this scenario, the OISP is a third party service provider, and there is direct SIP layer connectivity as well as business relationships between the calling user's provider and the OISP. This is illustrated in the following figure:

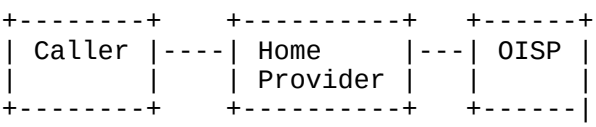


Figure 2 Services Provider by a Direct Third Party Provider

It must be possible to support the case where services are provided by an indirect third party provider. In this scenario, the OISP is a third party provider, but the caller's Home Provider does not have direct SIP connectivity to the OISP. Further, it's possible that it has no business relationship with the OISP. The caller's provider routes the call to a provider with whom it does have a relationship, referred to in this document as an "intermediate provider", and this intermediate provider in turn routes either to the OISP, with which it has a relationship, or there could be multiple intermediate providers. This is illustrated in the following figure:

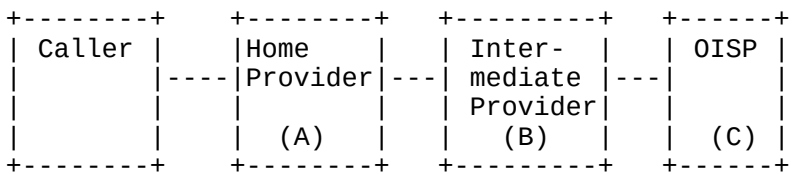


Figure 3 Services Provided by an Indirect Third Party Provider

It must be possible to support the case where transit providers are included between any other providers involved in the call. The transit provider only "moves calls" between other providers, and is involved in no other way with OIS services. I.e., it simply forwards the call towards the destination, without making any service level decisions, in contrast to an Intermediate provider as described previously. This is illustrated in the following figure:

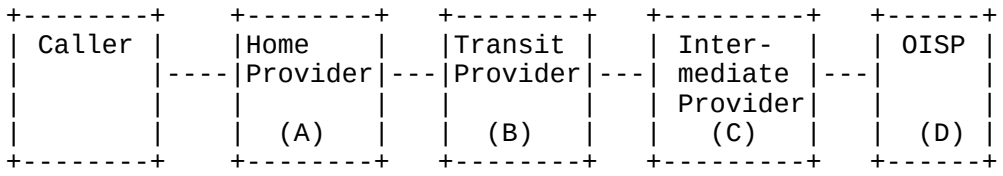


Figure 4 Involvement of a Transit Provider

It must be possible to support both Information Services as well as Operator Services. Examples of Operator services include Operator Intercept, Busy Line Verification, Call Restrictions, etc.

4.1. Potential Future Requirements

The following are potential future requirements.

Operation via the general internet, not specific to any particular SDO's architecture, and not depending on any protocol extensions specific to those architectures, should be supported.

It must be possible to support non voice initiated Information Services requests. Possible examples include chat (IM), email, Web (HTTP) or SMS initiated requests. In the case that the subscriber makes a purchase via some online auction service, that subscriber can via IM or email request the assistance of an operator.

It must be possible to provide an application interface to other types of systems. An example could be a web based API, so that once some online search engine has located some business listing, the services of the Information Services provider could be invoked by the user from the web page.

It must be possible to support IPTV interactive services. As multiple services such as IM and telephony are integrated with IPTV, it must be possible to initiate Information Services requests in this context as well.

5. Information Services

Information Services (IS) are services whereby information is provided in response to user requests. This may include involvement of a human or automated agent. Usually, the user accesses the Information Service by placing a voice call to the automated Information Service and verbally requests the information, such as phone number, movie listings, weather, etc. Frequently, a live operator is attached to recognize the user's verbal request. Sometimes, the user can utilize other access methods, such as SMS, IM, or HTTP-initiated requests. These additional methods are not currently covered in this document.

Information Services are often provided on a wholesale basis to Home Providers, and include features such as branded announcements.

Directory Assistance (DA) is a specific type of Information Service whereby end users request a telephone number for an entity.

Purchase services and Concierge services facilitate the Information Services operator providing assistance to the caller after the listing has been announced and perhaps call completion performed. The call is routed to an Information Services operator who interacts with the customer, offering to help make a purchase. Concierge service is similar; the Information Services operator offers to make e.g. restaurant reservations for the caller.

The following represents a list of representative steps taken during the course of a typical DA request and identifies a set of required high level capabilities.

1. Initial recognition of an OIS call. At some point, the call needs to be identified as an OIS call, and appropriate routing or other logic must be invoked in order to fulfill the request. This could be based on any number of criteria, including but not limited to analysis of the "address information" - e.g. the digits or Request-URI emitted by the caller's UA. This could occur at any number of places - e.g. in the caller's UA, in a proxy in the home provider, or in some downstream element.

2. Identification of the requested service. There are many possible OIS services, and the number of these is only expected to increase as providers respond to customer needs. At some point during call processing it is necessary to identify exactly which service is desired. For example "directory assistance with call completion" is a service where after the listing information is provided to the caller, the option is provided for the call to be placed automatically, so the customer need not hang up, remember the digits, and dial the number. Another example is "directory assistance only", where call completion is not offered. There are multiple factors which could affect the service which is to be offered, and the logic deciding this could be located anywhere along the path to the OIS provider. Some of the information required to make such decisions could include:

- The digits dialed by the caller.
- The Request-URI emitted by the caller's UA.
- The identity of the calling party, for instance the calling party number.
- The charge number associated with the caller's account.
- The identity of the calling party's home provider.

- The identity of the provider which directly hands off the call to the OISP.
- The identity of other provider which the request might traverse
- The Originating Station Type, in case the call was originated in the PSTN.
- Trunk group information, in case the call was originated in the PSTN.
- Capabilities and characteristics of the caller’s user equipment.

3. Routing of the OIS call. The call must be routed towards an entity which can provide the requested service. Each entity or network handling the call routes it based on the logic located in that provider, and the information currently available. For instance, the home provider may know very little about OIS services, having farmed that service out to another provider. Consequently it might simply route all such calls towards the OIS provider, which decides which service is to be offered.

4. Authentication. When one provider passes a call to another provider, there is a need for the providers involved to be sure of each other’s identity. This might be through explicit security mechanisms such as mutual TLS or security gateways using IPSec tunnel mode, it might be through reliance on a closed set of trusted interconnected providers, or some other policy set by the providers involved.

5. Receipt of the OIS call. The OIS provider needs to be able to receive such calls.

6. Querying upstream providers for information. The OISP, or an intermediate provider may require information from an upstream provider. For instance, the capabilities and characteristics of the caller’s equipment may be needed in order to influence call processing.

7. Selection of automated voice platform. When it has been determined that the call must be routed to an automated voice platform, there are a number of factors to be taken into account to determine an appropriate, available platform for the call. It must

be possible to determine an appropriate, available automated voice platform to which the call should be routed.

8. Connection of caller to automated voice platform. The OISP must be able to connect the caller to an appropriate automated voice platform.

9. Provision of branded announcements. The OISP must be capable of providing custom announcements to the caller based on a number of criteria. For example, it might greet the caller, thanking them for using their Home Provider's service. Though the service is actually provided by the OISP, business arrangements would dictate such branded announcements.

10. Query the caller. The OISP must be capable of playing a voice request to the customer asking them for the listing. For example "Name and city, please."

11. Recording a spoken request. The OISP must be capable of recording the caller's spoken request. This both for speech recognition, and also for playing back the "whisper" to a human operator should one be required, to prevent having to ask the customer to repeat the request.

12. Speech recognition. The OISP must be able to pass the caller's spoken request to speech recognition system, suitable for querying a listing database.

13. Listing database query. The OISP must be capable of querying one or more listings databases using the request.

14. Decide to use human operator if listing query fails. If the listing query fails, or the speech recognition fails, the OISP must be able to decide to send the call to a human operator.

15. Selection of appropriate operator. When it has been determined that the call must be routed to a human operator, there are a number of factors to be taken into account to determine the appropriate operator for the call. It must be possible to determine an available, appropriate human operator to which the call should be routed.

16. Routing of call to operator workstation. Once the appropriate operator has been identified, the call must be routed to that operator's workstation.

17. Whisper. Once the operator answers the call, the previously recorded request should be played to the operator as a "whisper", prior to connecting the caller to the operator.

18. Connection of caller to operator. Once the operator has heard the whisper, the caller can be connected to the human operator. The operator queries the caller for the request, and initiates a query to the listing database.

19. Playing listing information. Once the listing information is returned from the database, the caller must be connected to a media resource which speaks the listing information to the caller.

20. Prompting for call completion. If the identified service includes call completion, the caller should be prompted for this service, for example by pressing some DTMF key. In such a case, the AS would instruct the MS to prompt the user, and collect any DTMF stimulus from the user. The MS would do so, and would report back to the AS whether the DTMF stimulus was received.

21. Call completion. If the caller requests call completion, the call should be automatically initiated for the caller.

6. Operator Services

Operator Services are traditional PSTN services which often involve providing human or automated assistance to a caller, and often require the specialized capabilities traditionally provided by an operator services switch. Market and/or regulatory factors in some jurisdictions dictate that some subset of Operator Services continue to be provided going forward.

This document assumes an architecture with SIP based OISPs, SIP based home providers, and SIP based end users. Since it is necessary to maintain backward compatibility with traditional TDM based providers and end users, these are also considered. It may not be necessary, desirable, or technically feasible to support every existing Operator Service using SIP, or to support both SIP and TDM based end users for all Operator Services. This is the subject of ongoing investigation, and the current iteration of this document assumes that both SIP and TDM based home providers and end users are in scope for these services, unless specifically indicated to the contrary. A future revision may update this assumption based on the findings of the investigation.

With respect to Operator Services, this iteration of this document intends to provide an introduction to and descriptions of some of these services, as well as provide some high level requirements. It is intended that the subsequent iteration will build upon this, providing more detailed requirements, suggested SIP mechanisms, and more call flows.

Operator Services are typically provided by the requesting party's OISP. In some cases, such as Busy Line Verification, the target or called party's OISP may be involved as well.

Next, several traditional Operator Services will be described. As indicated above, the current iteration of this document is silent regarding which of these may or may not be candidates for implementation with SIP, or towards SIP end users. Note that unless specifically indicated, most of these services are traditionally provided by the caller's OISP.

Operator Assistance. This allows the caller to perform either "zero minus" or "zero plus" dialing to be connected to a human or automated system for assistance with the call.

Collect calls. This allows the caller to request that the called party accept the charges for the call. Typically an OISP utilizes a human operator or automated system to provide this service.

Rate Quotes. This allows the caller to request a quote for the cost or rate for specific calls.

Third party billed calls. This allows the caller to request that a third party (different than the calling or called party) be contacted and requested to accept charges for the call (although in some limited cases, contacting the third party is not necessary).

Busy Line Verification and Interrupt. This allows a caller to have the OISP determine whether a target line is in use, and if so, to "barge in" to the conversation and request whether the target party is willing to accept a call from the caller. This service is initially handled by the caller's OISP, which then contacts the target party's OISP, which is able to perform the verification and interrupt on the target party.

Coin Calls. Operator services systems must be able to control TDM-based network controlled coin stations (payphones). This includes monitoring of coin deposit tones (to verify payment) sent from the coin station, as well as sending supervision (control) signals to the coin station. Network controlled coin stations are connected to

TDM based end offices via specialized phone lines which support the required signaling. These end offices, in turn, connect to TDM based OISPs using specialized trunks capable of conveying the coin signaling. The OISP monitors and controls the coin station via these trunks. "Smart" coin stations perform coin detection locally and do not require network control, and are not discussed here. This service is provided by the OISP associated with the coin station.

Emergency Calls. Sometimes a caller dials "0" instead of the standard emergency dialstring, resulting in placement of an emergency call to the OISP. The OISP must properly route such a call toward the PSAP. This service is provided by the caller’s OISP.

Calling Card Billing Service. This enables a calling party to bill a call to a calling card number.

Commercial Credit Card Billing Service. This enables a calling party to bill a call to a commercial credit card.

Directory Assistance (DA). In some contexts, DA is considered as an Operator Service. Within the context of this document, we consider DA as an Information Service, which is related to but distinct from Operator Services.

The following sections describe an initial set of basic high level capabilities required for supporting Operator Services. The capabilities for Information Services generally apply for Operator Services as well. This work is currently under study, and a complete set of required capabilities is expected to be identified in the near future. Similarly to the required capabilities for Information Services, the use of existing SIP mechanisms will be investigated for providing these capabilities.

6.1. Inter Provider Capabilities

Ability to accept requests from other providers. This is the ability to accept incoming OIS requests from other providers, including home providers, intermediate providers, and transit providers.

Ability to terminate calls to other providers. This applies to call completion services, as well as other services such as third party billing.

6.2. Inter OISP Capabilities

These are capabilities between OISPs.

Inward connection. This is a call from one OISP to another, e.g. so that the originating OISP may request services from the terminating OISP. One example of this is Busy Line Verification, where the caller calls their own OISP, and this OISP places an "inward" call to the target party's OISP, which would have the capability to perform the verification of the target party.

Transfer between OISPs. In this case, one OISP transfers the call to another OISP, to be handled by that OISP, so that the first OISP is no longer in the signaling path.

Moving connection from one OISP to another. An example of this case is where one OISP farms out a specific service to another OISP. The first OISP performs initial handling of the call, to determine the desired service. The call is sent to a different OISP with which the first has a relationship. The first OISP remains in the signaling path, and when the provided service is complete, the first OISP determines what if any additional processing may be necessary. This is similar to a third party call control type arrangement.

6.3. Intra OISP Capabilities

Note that some of the following capabilities may be required for inter OISP scenarios as well; this is the subject of ongoing analysis and is not covered in the current iteration of this document.

Placing a caller on hold, possibly with announcements. This is used in many services, including Information Services.

Exchanging information between Application Server and Operator Workstations/Automated Platforms. This capability is required whenever an operator workstation or automated platform is used. Because an Operator Workstation interacts with a human user, it is expected that additional information, beyond that which an automated system would exchange with an application server, will be required. Further, several modes of application server control are currently under investigation. The first is where the workstation or automated platform is more or less autonomous, and is capable of initiating calls and directly impacting call processing. The other is more of a master-slave relationship, where the AS is in complete control. The

master-slave model requires that more information be exchanged with the AS than does the autonomous model. Other models may be possible.

Queuing and call distribution. Resources including human operators and automated platforms need to be tracked and managed, and the appropriate resource of the appropriate type needs to be selected on a per invocation basis. What is needed is that for a particular call, that a set of criteria be provided and the best match resource be selected. This is the job of the ACD server. Some means is needed to communicate the selection criteria for human operators and automated platforms to the ACD server.

Operator Registration and Location. Human operators may not be interchangeable, and have specific attributes such as skillsets which can be used to identify the best human operator to service a particular call. Operators log in at workstations at the beginning of a shift, and log out during breaks and at the end of a shift. It is important to associate each available operator with the workstation at which they are logged in, so that requests can be sent to the appropriate human operator. This is needed because the selection process described above identifies a particular human operator; it is then necessary to identify the workstation at which that operator can be reached.

Bridging and removal of operator or automated system. Many operator services require that either a human operator or automated system be "bridged" onto a call, and to be removed at some point.

6.4. Capabilities Required for Specific Services

Connection Hold and Ringback. This capability involves having the OISP "hold" the connection, such that the originating caller remains connected, even if they attempt to hang up. This is mainly used in relation to emergency services. Ringback is the ability for the OISP to call back the calling party after they have hung up. This too is often used in conjunction with emergency calls. Note that these are only discussed in this document in the context of controlling a PSTN based endpoint, as this capability does not carry over directly to SIP based endpoints.

Coin Station Control. This is the ability of the OISP to determine the coinage deposited into a TDM based network controlled coin station (as opposed to an "intelligent" coin station which performs such functions locally). This involves interpretation of the coin control signals sent via specialized trunks from the end office to

which the TDM based coin station is connected via a specialized phone line. Additionally, the need to signal toward the coin station needs to be supported as well, for example to instruct the station to return coins to the caller. This capability is intended to interact with the specialized coin trunk.

Network Service Recall. After a call resulting from Operator Services is completed, the caller may signal the desire to return back to the OISP, without placing another call. In the traditional PSTN, this is typically accomplished by the user signaling a hook flash or other distinctive stimulus.

Verification and Interrupt. This is used in the Busy Line Verification and Interrupt service, and allows the OISP to determine if the target number is in use, to listen to a scrambled representation of the conversation, and to interrupt the target party's conversation to ask if they would accept a call from the caller.

Transfer of emergency services call to selective router. Sometimes a caller places an emergency call using a dial string which invokes operator assistance (such as "0" in North America), rather than an emergency call dial string. In such cases, the OISP must be able to pass the emergency call to the appropriate PSAP. Handling of these types of calls is outside the scope of this document. Standards for emergency calling with SIP are still in development.

7. OISP Internal Architecture

This section describes an initial view of the elements internal to the OISP architecture.

The following types of elements may be present within the OISP infrastructure:

Automatic Call Distributor (ACD) server - The ACD provides queuing and call distribution functions for human operators. Specifically, it is the component that tracks the availability of the human operators and selects an available operator utilizing complex algorithms based on operator skills, type of call, type of request, calling party information, etc. Similar functionality is required with respect to automated platforms. The ACD server is modeled as an Application Server. Two different models of ACD include a "query" model, where the ACD accepts a request and returns a response (such as a SIP redirection response) identifying the selected resource,

and an "inline" model, where the ACD server accepts a request and inserts itself into the signaling path, making its selection and sending requests to that resource. There is currently work in the MEDIACTL working group regarding Media Resource Brokers (MRBs) which may be relevant to this.

The ACD server may also contain functionality for tracking and maintaining statistics about resource utilization; this is sometimes referred to as force management.

Customer Profile Database - The Customer Profile Database is a per subscriber database maintained by an OISP about its customers. Some of this information might be statically provisioned, other information such as customer preferences or session information might be populated dynamically as a result of customer interactions.

Messaging Gateways - Messaging Gateways provide access and data via E-mail, SMS, MMS, WAP.

Operator and Information Services Application Server (OIS-AS) - The OIS-AS contains AS functions specifically for directory assistance and information services as well as other Operator Services. This may coordinate multiple call legs, connecting the caller in sequence to one or more OIS-MS and/or operator workstations according to the logic contained within. The OIS-AS may need to communicate with elements of other providers, for instance to query information about the capabilities and characteristics of the caller’s equipment, or to access another provider’s operator resources.

Operator and Information Services Media Server (OIS-MS) - The OIS-MS provides the media resources for playing announcements, performing voice recognition, performing listing database queries, generating whisper from the user’s verbal request, etc.

Operator Workstations - Operator Workstations provide an interface to the human operator. They may receive the customer’s recorded request (e.g. name and city of requested listing), information from listing or other databases, and also terminate a multimedia session with the customer. Operator workstations are specialized SIP endpoints, and may be modeled in various ways, such as UAs or media servers.

PSTN Gateways - OISPs need to interface with the PSTN. Thus, gateways are needed to interface between the OISP and both signaling and bearer. The bearer is handled by trunk gateways, which interface RTP streams on the OISP side to TDM trunks on the PSTN side. The signaling may be handled by signaling gateways which interface SS7

on the PSTN side and SIP on the OISP side. Currently in North America, inband signaling on MF trunks is common for interfacing to OISPs, and trunk gateways need to be able to interpret and report as well as generate the appropriate MF signaling.

Service Databases - Service Databases store service specific information (e.g. listing information such as name, address, and phone number, etc.) These may be located in the OISP's network and/or in other networks, and more than one may be used.

SIP Proxy - One or more SIP proxies may be present in the OISP network, to facilitate SIP communications with other providers as well as to perform call processing functions between OISP components.

The following figure shows a simplified view of an OISP internal architecture. The lines show logical connectivity; elements communicate via the proxy. A single OIS-AS is shown, along with up to "k" OIS-MS and up to "m" Operator Work Stations, and an ACD server. Communications between elements are assumed to traverse a proxy, which has been omitted from the figure for brevity.

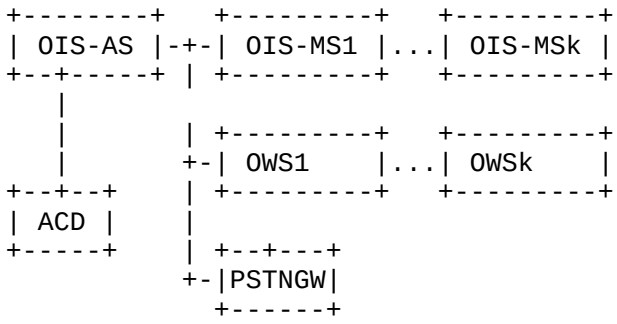


Figure 5 Simplified view of OISP Internal Architecture

8. General Approach

This section describes one possible way to implement DA using SIP. Other ways may be possible.

The general approach involves having the OIS-AS host most of the processing logic, and to control the call in general. The OIS-AS implements a third party call control (3PCC) functionality, as

described in [RFC3725]. It terminates the signaling dialog from the caller, and originates dialogs towards other components as necessary. There may be multiple sequential sessions set up during the course of a DA call.

For example, the OIS-AS would initiate a new dialog towards a MS for front-end automation. When it gets the 200 OK from the MS with SDP, it passes that SDP back toward the caller. When the front end automation has completed, the OIS-MS sends a BYE containing message bodies conveying the success of the operation (i.e., was it able to obtain the listing) as well as any data related to the operation. In case of success, the body might carry the listing information, or a URI pointing to it. In case of failure, it might carry a URI pointing to the whisper file.

In case of failure, the OIS-AS would determine that the call needs to be routed to a human operator. The OIS-AS first needs to identify a suitable operator to handle this request. The ACD server has this responsibility, and could be implemented as a redirect server facing the OIS-AS, redirecting towards the best suited available operator. Facing the operator workstations, the ACD server could be implemented as a presence server, maintaining availability of each operator, as well as the associated information for each (e.g. languages, skill level, cost, etc).

The OIS-AS would then send an INVITE toward the identified operator workstation. This INVITE includes the caller’s SDP as well as a URI pointing to the whisper file. The workstation could play the whisper to the operator as the call is answered. The operator workstation’s SDP would be passed back to the caller via a re-INVITE or UPDATE request.

If the operator is successful in locating the desired listing, the workstation would send a BYE containing message bodies with an indication of success, and either the listing information of a pointer to the same.

The OIS-AS would then initiate a call leg towards an OIS-MS for back end automation. The INVITE would include the same body with the listing information that was sent by the operator workstation. The OIS-MS returns its SDP, which the OIS-AS would propagate back over the originating leg via a re-INVITE or UPDATE request. The back end automation process includes audibly playing out the listing information, and possibly offering call completion service. The OIS-MS sends a BYE with a message body indicating whether call completion is desired.

If call completion is desired, the OIS-AS sends a REFER back over the originating call leg to the caller, and clears the call.

These examples describe simple voice scenarios. Other media types may be possible. For example, it may be desirable to send the listing information via text message to the caller's terminal, or to show a video clip. Such features require knowledge of the calling terminal's capabilities and characteristics. The mechanism described in [RFC3840] Indicating User Agent Capabilities in the Session Initiation Protocol (SIP) can be used for this. The capabilities might have been signaled in the initial INVITE request. Otherwise, the OIS-AS can query for capabilities using an OPTIONS request. Additionally, some non SIP mechanism might be used, such as querying a database (e.g. IMS HSS) in the caller's network.

References to a whisper file can be passed using the mechanism described in [RFC4483].

Other information signaled via message bodies includes the success or failure status of operations (such as identifying the requested listing), or other data (such as the listing information).

Context information may be maintained on a per call basis. It could include such information as the caller's preferred language, etc. A URI pointing to the context information could be passed between elements in the OISP infrastructure.

Note that the IETF MEDIACTRL working group is currently developing mechanisms for control of SIP based MSs by ASs; this work may be applicable for OIS as well.

9. Signaling Mechanisms

This section discusses the signaling mechanisms required to provide OIS services.

9.1. PSTN Protocol Interworking

Operator Services will need to interoperate with the existing PSTN. This includes both receiving incoming call requests from the PSTN as well as initiating calls towards the PSTN. There are several issues which are specific to PSTN interworking.

Current Operator Services systems use both SS7 ISUP and MF signaling. PSTN gateways interwork between the PSTN signaling and

SIP signaling, and between the PSTN's circuit switched bearer channels and RTP. [RFC3398] defines ISUP-SIP interworking procedures. ATIS, which is responsible for defining North American specific telecommunications standards, provides North American procedures in [T1679]. There is currently no standard for MF-SIP interworking; rather, ATIS standards assume a gateway model whereby MF signaling is logically mapped to ISUP, then ISUP-SIP interworking procedures are applied.

ISUP interworking involves two mechanisms; parameter mapping and encapsulation. Some concepts exist natively in both PSTN and SIP signaling, and thus both PSTN signaling and SIP define protocol mechanisms for conveying such information. Mapping between these is specified in interworking standards such as [RFC3398] and [T1679].

Other ISUP parameters have no direct equivalent in SIP, but are needed in SIP headers so that proxies and other SIP entities can route calls; extensions have defined SIP headers and parameters for this purpose. In order to convey those parameters which have no mapping to SIP headers, encapsulation of ISUP messages is used, whereby the ISUP message content is encoded in a MIME body which is carried in SIP messages. [T1679] specifies that the entire ISUP message be encapsulated in a MIME body of type "application/ISUP", as registered with IANA and defined in [RFC3204]. [NSS] defines a MIME type "application/NSS"; this standard specifies that the only parameters which do not have mappings to SIP be included in the NSS body, along with identification of the ISUP version and ISUP message type, rather than encapsulating the entire ISUP message. [T1679] is the ATIS standard for North American networks.

Thus, PSTN gateways send SIP messages containing SIP headers and parameters mapped from ISUP parameters where specified, and carrying an "application/ISUP" MIME body containing an entire encapsulated ISUP messages.

It should be noted that when MF PSTN signaling is used, the use of encapsulated ISUP involves logically mapping the MF signaling to the corresponding ISUP information elements, generation of the corresponding ISUP message, and MIME encapsulation of this generated ISUP message in the corresponding SIP message.

9.2. Conveying Application Specific Information

Some information carried by PSTN signaling, such as the ISUP Called Party Number is required for routing calls. Other information, such

as Charge Number, is for use by applications such as operator services, and is not needed for routing the call.

With SIP, information needed for routing requests, or which otherwise needs to be available to proxies, should be present in message headers. Note that proxies may add headers and modify header content.

Message bodies can be carried in SIP requests and responses. Such bodies are generated by and consumed by endpoints, and are expected to be passed transparently by proxies. Additional headers such as Content-type and Content-disposition describe the MIME type of the message body as well as how the receiving endpoint is to handle unsupported MIME types. Messages can contain more than one body, as described in [RFC2045].

Moreover, much of the information delivered to an operator services system is expected to be provided by trusted equipment in the caller's home provider, rather than by the caller's user equipment.

Architectures such as IMS include application servers which have the ability to act as Back to Back User Agents (B2BUAs). Whereas proxies cannot insert message bodies, B2BUAs can in fact do so, because they act as SIP endpoints.

Not all information passed in PSTN signaling can be conveyed natively in SIP, but operator services systems expect this information. One option for doing this is to have an application server in the caller's home provider, acting as a B2BUA, populate a MIME body in the INVITE sent to the operator services provider, for consumption by an OIS AS. There is at the time of this writing no agreement on a MIME type to use for this purpose.

Some ISUP information for which SIP mappings are not currently defined is also expected to be relevant for calls initiated using SIP. Charge Number is business related information, and is expected to apply regardless of whether a caller is using a SIP or PSTN device. The same is true for Originating Line Information. Again, the use of a MIME body is potential option. Mechanisms for some of this information in SIP header fields and parameters are described in several Internet-Drafts at the time of this writing, and are described in this document where applicable.

9.3. Calling Party's Identity

In many cases, downstream providers may need to know the calling party's identity. This might be needed to influence call processing,

or for usage collection purposes. Also, the calling party's identity in the form of a SIP URI might be needed so that the identity of the home provider can be determined.

The calling party's equipment populates the From header in SIP messages. This is not trusted. There are several methods for providing "network-asserted identities", which under the appropriate conditions can be trusted.

The SIP Identity mechanism defined in [RFC4474] provides a standardized, architecture agnostic SIP mechanism for cryptographically assuring the user's identity. However, this mechanism has seen little deployment.

The P-Asserted-Identity header [RFC3325] is a private extension to SIP that enables a network of trusted SIP servers to assert the identity of authenticated users. This is the prevalent mechanism currently used in service provider environments.

Note that some networks may allow their users to hide their identity. In the current North American PSTN, for such cases the caller id information is often transported through the network, marked with a privacy indication such that it will not be presented to the called party. In SIP, the Privacy header field defined in [RFC3323] is used.

Bilateral agreements between VOIP providers determine whether providers are within the same "trust domain" as defined in [RFC3324], and what information, including network-asserted identities, may be exchanged between providers. Depending on such agreements, it is possible that the caller identity information is obscured or completely absent. As indicated in [RFC3325], "Masking identity information at the originating user agent will prevent certain services, e.g., call trace, from working in the Public Switched Telephone Network (PSTN) or being performed at intermediaries not privy to the authenticated identity of the user."

When an OIS provider is not privy based on bilateral agreement to network asserted identity information from the calling network when the caller has requested privacy, it may be unable to implement any call processing logic based on such information.

If the OISP desires to reject anonymous calls, [RFC5079] defines a new SIP response code 433 (Anonymity Disallowed) for this purpose.

The following shows an example of an INVITE message contain a P-Asserted-Identity header.

```
INVITE sip:da@provider-c.example SIP/2.0
Via: SIP/2.0/UDP proxy-b.provider-b.example.com:5060
;branch=y9hG4bK74bf9
Via: SIP/2.0/UDP proxy-a.provider-a.example.com:5060
;branch=x9hG4bK74bf9
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234@provider-a.example.com>
P-Asserted-Identity: "732758123" <sip:73237581234@provider-
a.example.com>
Content-Type: application/sdp
Content-Length: ...
[SDP not shown]
```

9.4. Provider Identification

As discussed, in some deployment scenarios, the OISP makes use of the identities of other providers involved in the call. This section discusses how those identities can be conveyed using SIP.

9.4.1. Home Provider

In many cases, the OISP needs to identify the caller’s Home Provider. This may be needed for branding purposes as well as to potentially influence treatment in other ways.

The basic mechanism for determining the home provider is to derive it from the right hand side (RHS) of the network asserted identity.

In SIP, identities are expressed as URIs. These can be SIP (or SIPS) URIs, or "tel" URIs.

[RFC3261] defines the SIP URI, which is used for identifying SIP resources. The RHS can be expressed as a DNS domain name or as an IPv4 or IPv6 address. The hostname format is most suitable for providing an identity to reach the calling party. For instance the mechanisms defined in [RFC3263] for locating SIP servers depends on the use of domain names for the various types of DNS lookups such as NAPTR, SRV, and A.

If a provider decides to provide network asserted identities expressed as SIP URIs using IP addresses instead of hostnames, it forfeits the use of such standardized mechanisms for reaching its users. It also becomes difficult to derive the home provider identity from the network asserted identity.

[RFC3966] defines the "tel" URI, which is used for describing resources identified by phone numbers. The "tel" URI format does not include a domain. Thus, if the network asserted identity includes only a "tel" URI, no direct information about the home provider is provided.

The SIP Identity mechanism is intended for use with SIP URIs. The PAI mechanism can use either a SIP URI, a "tel" URI, or both.

This document depends on the home provider providing a network asserted identity containing a hostname. This includes the SIP identity where the SIP URI contains a hostname, or a PAI header containing at least a SIP URI with a hostname.

Very simply, the RHS of the hostname in the SIP URI is extracted and used as the basis to influence call processing. In cases where the caller’s identity is not available, as discussed in the "Calling Party’s Identity" section, then the home provider’s identity is consequently also not available, and call processing logic based on such information (such as branding) cannot take place.

9.4.2. Intermediate Provider

In some cases, the OISP may need to know the identity of an intermediate provider which the call has traversed. Recall that for our purposes, we define "intermediate provider" as having a business relationship with both the home provider (to handle OIS requests) and with an OISP (which will actually provide the requested service.) This may be needed to influence treatment.

The use of the SIP History-Info mechanism defined in [RFC4244], can be used for this. As the call moves from one provider to the next and is retargeted, corresponding entries are added to the SIP History-Info header. If the domain name format is used for the retargeted entities, then the History-Info header now includes a list of traversed SIP domains or providers, which can be consulted by the OISP.

According to [RFC4244], entries should be added to the History-Info header whenever the Request-URI is modified. Cases may exist where the call is sent to another provider but the URI is not modified. In such cases, the provider is not captured by the History-Info header.

The following figure illustrates the use of the History-Info header for this purpose.

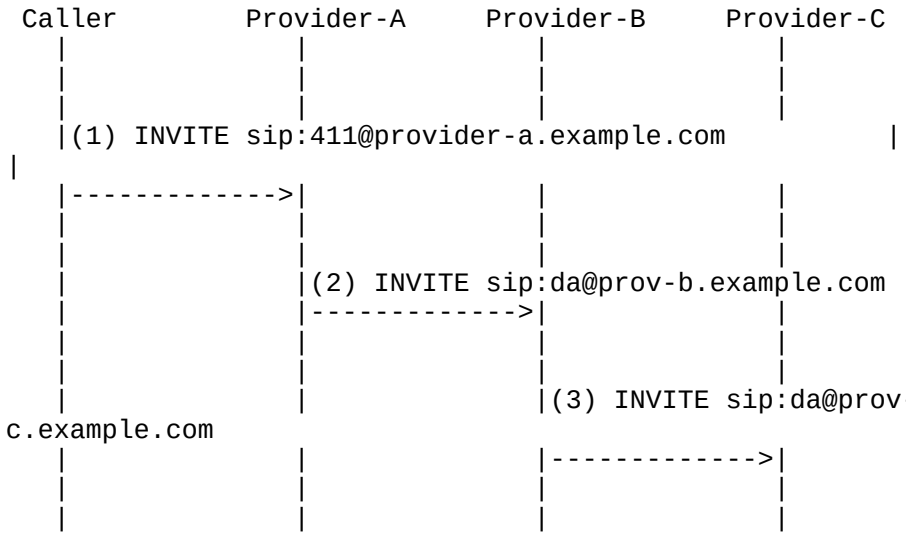


Figure 6 Use of History-Info header to identity traversed providers

1. The user dials "411", and the resulting INVITE to its home proxy is for "sip: 411@provider-a.example.com". No History-Info header is included yet.

```
INVITE sip:411@provider-a.example.com SIP/2.0
(other message content omitted)
```

2. The home proxy retargets this to "sip:da@prov-b.example.com", and adds a History-Info header which includes the targeted-from URI:

```
INVITE sip:DA@prov-b.example.com SIP/2.0
History-Info: sip:411@provider-a.example.com; index=1
(other message content omitted)
```

3. Proxy-B retargets this to "SIP: da@prov-c.example.com", and appends another entry to the History-Info header:

```
INVITE sip:DA@prov-c.example.com SIP/2.0
History-Info: sip:411@provider-a.example.com; index=1,
<sip:da@prov-b.example.com>; index=1.1
(other message content omitted)
```

When this request arrives a Proxy-C in Provider C (OISP), it conveys the following:

- The Request-URI (SIP: da@prov-c.example.com) indicates this as a DA call
- The History-Info header conveys the history of the request:
- It started as a SIP URI for "sip:411@provider-a.example.com"
- It was then targeted to provider B
- It is now targeted to provider C

Please note that if a transit provider were encountered, the transit provider would simply route the request toward Provider C, and would not perform retargeting. It would not modify the Request-URI nor the SIP History-Info header contents.

9.5. Originating Line Information/ANI II Value

In the current PSTN in North America, OIS providers have the ability to tailor treatment based on the type of originating station. For instance, calls from prison phones are restricted from accessing DA services. Example values include POTS, coin, hospital, prison/inmate, cellular, etc. In the PSTN in North America, this information is signaled for SS7 calls using the Originating Line Information (OLI) information element, and in MF calls using the ANI II digits. To support interworking with the PSTN, it must be possible to convey the Originating Line Information value. The

ability to convey this information natively with SIP is currently lacking.

It is also desirable to characterize certain types of originating SIP based callers using these same values, e.g. prison, police, etc.

[TS24229] defines the "oli" parameter for conveying Originating Line Information in SIP using a tel URI parameter, is aimed at telecommunications service provider applications, and has been adopted by 3GPP, making it the preferred approach. This document defines the parameter to convey the 2-digit numeric OLI value. This is in contrast to the "cpc" parameter defined in [draft-mahy-iptel-cpc], which specified a limited subset of string based values. This mechanism would be applicable for both PSTN interworking and also for SIP originated calls.

The "isup-oli" parameter is sometimes used to convey OLI information for PSTN interworking, but it is not defined in any standards document.

For PSTN interworking, the current version of [T1679] does not specify a SIP mapping for the OLI parameter. Thus, that document specifies that it be carried in an encapsulated ISUP message in a MIME body. This mechanism would be applicable to PSTN interworking but not for SIP originated calls.

9.6. Trunk Group Identifier

The incoming trunk group number provides information which could be used to influence call processing, thus this information is needed. Trunks are point to point circuits and as such, their remote termination point is unambiguously known. As such, knowledge of the incoming trunk group conveys the identity of the provider offering the call.

For PSTN interworking, the incoming trunk group identifier is a key piece of information and must be known. Thus, at a PSTN to IP interworking point, the trunk group information must be kept and signaled forward. This holds for OISP’s accepting incoming calls from the PSTN as well as upstream providers accepting calls from the PSTN.

[RFC4904], "Representing trunk groups in tel/sip Uniform Resource Identifiers (URIs)" defines a way to signal incoming and/or outgoing trunk group information as a parameter in SIP URIs and tel URIs.

To represent incoming trunk groups, the trunk group parameter is included in the Contact header of the SIP message. The "trunk-context" parameter should also be included, to ensure that the trunk group is unambiguously identified, since trunk group numbers are not globally unique.

At the time of this writing, [T1679], which specifies PSTN interworking for North American networks, does not include this mechanism, possibly because it predates [RFC4904]. However, gateways should include this information for operator services.

The following example shows an INVITE containing a trunk group identification in the Contact header:

```
INVITE sip:da@provider-c.example.com SIP/2.0
Via: SIP/2.0/UDP proxy-b.provider-b.example.com:5060
;branch=y9hG4bK74bf9
Via: SIP/2.0/UDP proxy-a.provider-a.example.com:5060
;branch=x9hG4bK74bf9
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234;tgrp=101; trunk-context=gateway-
a.provider-b.example.com@ provider-b.example.com;user=phone>
P-Asserted-Identity: "7327581234" <sip:73237581234@provider-
a.example.com>
Content-Type: application/sdp
Content-Length: ...
```

This example identifies trunk group 101, with the trunk-context identifying gateway-a.provider-b.com. Together these unambiguously identify the incoming trunk group. Both of these parameters are tel URI parameters and thus appear on the left hand side of the "@" sign. The domain of the SIP URI formed from this tel URI is provider-b.example.com, and the "user=phone" parameter is a SIP URI parameter.

9.7. Identification of PSTN Originated Calls

Since calls arriving via PSTN trunks may require different processing from those received from SIP endpoints, it must be possible to distinguish between these types of calls. For PSTN originated calls, the Contact header identifies the gateway, and also the presence of the "tgrp" parameter in that header indicatesthat the call was received via a PSTN trunk. Obviously the presence of an encapsulated ISUP message also identifies the call as such.

In some cases, the identity of the home PSTN provider of the caller may be known (e.g., the call arrived via a dedicated trunk group from a PSTN end office). In such cases, the gateway may populate the host portion of the SIP URI in a P-Asserted-Identity header field with a value of local significance within the OISP identifying that PSTN home provider. Conveyance of such information beyond the OISP is outside the scope of this document.

Note that some implementations may make use of the trunk group parameters in a non standard or proprietary manner, including them when the call did not originate from the PSTN. Thus, the mere presence of these parameters does not guarantee that the call originated in the PSTN. Rather, the value of the trunk-context parameter must also be taken into account, and the OISP must recognize this as identifying a PSTN trunk group.

9.8. Dialed Digits

Currently in the North American PSTN, the OIS provider may take into account the digits dialed by the user. In that scenario the dialed digits are frequently forwarded to the OIS provider.

Using SIP, the dialed digits would typically be sent by the user’s equipment in the form of a SIP URI in the Request-URI of a SIP INVITE. In this case, the Request-URI would be in a form such as "sip:411@provider-a.example.com".

The use of tel URIs instead of SIP URIs in the Request-URI is also theoretically possible. In this case, the URI might be formatted as "tel:411;phone-context=+1",where in this case the "+1" identifies the country code "1" for North America, or "tel:411;phone-context=+1-732", identifying a more specific context. However, the use of tel URIs in the Request-URI is not common in current service provider deployments.

It is possible that retargeting could take place, in which case the dialed digits would be lost.

The SIP History-Info mechanism defined in [RFC4244] provides a mechanism for solving exactly this type of problem. It defines a new optional SIP header, History-Info, to provide a standard mechanism for capturing the request history information. Whenever a node which supports this mechanism modifies the Request-URI of a request, it captures this in the History-Info header.

The following example shows an INVITE containing a History-Info header, which conveys the original dialed digits, after having been retargeted.

```
INVITE sip:DA@prov-b.example.com SIP/2.0
(other message content omitted)
History-Info: sip:411@provider-a.example.com; index=1,
<sip:da@prov-b.example.com>; index=1.1
```

Please see the section titled "Arbitrary Involved Provider" for an example of a flow where the History-Info mechanism delivers the dialed digits to the OISP when retargeting has occurred.

9.9. Retargeting to Identify the Desired Service

It is necessary to identify the service being requested. Such services might include directory assistance with or without call completion. The logic to determine this might reside in one or more points in the network. Additionally, the identification of the service might be refined as the request traverses potentially multiple networks, depending on the availability of additional information.

It is proposed here to retarget the Request-URI of the SIP request to specify the desired service. While the initial Request-URI might specify "SIP:411@provider-a.example.com", a downstream element might invoke service logic and determine that this call should be sent to OISP C’s network for directory assistance with call completion, and change the Request-URI to "SIP:da-with-call-completion@oisp-c.example.com".

A similar approach is taken for identifying resources in [RFC4240].

[CSI], a work in progress, discusses explicit service identifiers for using in IMS [IMS] based networks.

9.10. Charge Number

In the current PSTN in North America, a Charge Number is signaled with call originations. The Charge Number identifies the customer or account with which the caller is associated. In many cases it is the same as the Calling Party Number, while in others it is different - e.g. the main number for a business which has many individual calling numbers. This might be needed for usage collection, but it also could influence call processing, especially when a particular type of service applies for any caller associated with a particular charge number.

There is currently no IETF standardized mechanism to convey the Charge Number in SIP. The need to convey equivalent information for SIP based callers is also under investigation.

[PCI] proposes a "P-Charge-Info" SIP header for carrying charge information for a call. It is intended to facilitate carrying information equivalent to OLI for SIP originated calls. It is also intended to support PSTN interworking by carrying the ISUP Charge Number value.

For PSTN interworking, [T1679] does not specify a SIP mapping for the Charge Number parameter. Thus, it is carried in an encapsulated ISUP message in a MIME body. The P-Charge-Info header, if standardized, would be useful in this role.

For SIP originated calls, there is no currently standardized way to carry this information. The P-Charge-Info header, if standardized, would be useful in this role.

9.11. Access Prefix

In the current PSTN in North America, operator services calls are often originated by dialing a prefix such as "0". In ISUP signaling, the "0" is not carried in the Called Party Number parameter. Rather, it is stripped, and the ISUP Operator Services Information (OSI) parameter carries an indication of the original access prefix.

For SIP originations, there are several options. First, the dialed digits, including any prefix, can be included in the Request-URI. Alternatively, an AS in the caller's home provider can retarget the request based on the digits, such that new Request-URI identifies the requested service. The original dialed digits can be carried in the retargeted-from Request-URI in a History-Info header. For example, a Request-URI containing a zero plus 10 digits might be retargeted at an AS to sip:operator-assistance@provider-b.example.com. Though not currently standardized, these options can also be used for PSTN interworking. I.e., the GW could choose to prepend a prefix to the digits in the Request-URI based on the received Operator Services Information parameter. Additionally, the GW could support building a Request-URI which specifies the requested service, based on analysis of the incoming ISUP signaling.

For PSTN originations, the Request-URI can be formed as described above for SIP originations. Additionally, this information is also conveyed via the Operator Services Information parameter in the encapsulated ISUP.

9.12. Signaling of Carrier Information

In North America, the handling of PSTN calls utilizing Interexchange Carrier (IXC) networks are subject to specific regulatory requirements, resulting in specific signaling requirements which may differ from those in other regions. Reflecting this is the definition of ANSI ISUP parameters not defined in the ITU-T as well as specific usage for certain ISUP parameters. Interworking between ISUP and SIP signaling for such scenarios is documented in several specifications, but there are issues with these specifications. This section identifies the ISUP parameters involved in IXC signaling in North America, and provides an overview of some of the issues with current interworking specifications. Subsequent sections will specifically address each parameter. The relevant ANSI ISUP parameters include the Transit Network Selection (TNS) parameter, the Carrier Identification Parameter (CIP), and the Carrier Selection Information (CSI) parameter.

The ISUP Transit Network Selection (TNS) parameter is used to route calls to a specific carrier. In North American networks, it is used on several different interfaces to request that a call be routed to a particular carrier. TNS is also used in ITU-T ISUP.

Specialized switches called Access Tandems (ATs) provide IXC networks with access to Local Exchange Carrier (LEC) switches. When

a LEC switch originates an IXC call through an AT, it uses the TNS to inform the AT of the IXC to which the call is to be routed.

Based on business arrangements, IXCs may also provide access to other IXCs. Thus a LEC switch may need to route a call using IXC B, but might have connectivity to only IXC A. The LEC switch could, depending on arrangements, send the call to IXC A, with the TNS parameter specifying IXC B. This requests IXC A to hand the call to IXC B.

Also in North America, carrier selection procedures allow a caller to presubscribe to a particular IXC, and further to casually dial on a per call basis yet a different IXC to be used. Based on business arrangements, the carrier which will actually carry the call may be different from the presubscribed or dialed carrier. In ANSI ISUP, the Carrier Identification Parameter (CIP) is used to convey the dialed or presubscribed carrier, and accordingly the value of the CIP parameter may differ from that of any included TNS parameter. The definition of a separate parameter for this in ANSI ISUP underscores the need to separately identify the dialed or presubscribed carrier from the carrier which actually routes the call.

Both [RFC3398] and [T1679] discuss interworking between the "cic" tel URI parameter and the ISUP TNS and/or CIP parameters. This document points out that there are issues with both these specifications, but does not attempt to resolve those issues here.

[RFC3398] provides guidance on mapping between the "cic" tel URI parameter and the corresponding ISUP parameter. It essentially states that "cic" maps to TNS except for North American networks, where ANSI ISUP is used, where it maps to CIP, also allowing for application of local policy.

Some information not discussed in [RFC3398] includes the fact that for North American networks it is not an either/or choice between inclusion of TNS and CIP, that both ISUP parameters may be present, that their values may differ, the nature of the relationship between these parameters, or what to do in the ISUP to SIP direction when both TNS and CIP are present. Also, for a given "cic" parameter received by the gateway, and depending on the outgoing PSTN interface type, a TNS value may also need to be determined and populated in the outgoing IAM, in addition to the CIP parameter.

[T1679] specifies a mapping between the ISUP TNS parameter and the "cic" parameter in the Request-URI for North American networks. In doing so, it precludes the use of the "cic" parameter to convey the

identity of the dialed or presubscribed carrier for PSTN interworking scenarios, as is suggested in [RFC4694], [DAI], and [RFC3398] for North American networks. Also, when the "cic" parameter is used to convey TNS for PSTN interworking scenarios, then if the "cic" parameter were also to be used to convey the dialed or presubscribed carrier for SIP originated calls, there is a potential for ambiguity regarding the meaning of a received "cic" parameter.

The Carrier Selection Information (CSI) ISUP parameter indicates how the IXC identified in the CIP parameter was selected. For example, it may be the caller's presubscribed carrier, or may have been casually dialed, etc. The "dai" tel URI parameter described in [DAI] is intended to convey this information in SIP.

The signaling of carrier selection information for non interworked, all-SIP calls in North American networks is for further study.

9.13. Transit Network Selection

As indicated above, the TNS identifies the IXC to which a call is to be routed. Note that it does not identify the network in which the call will actually terminate. The TNS is used in cases where it is necessary to specify the specific IXC through which the call should be routed. One example is when a call is handed off via an AT which provides access to multiple IXCs, in this case it is necessary to identify the desired IXC to the AT. Another example is when business arrangements dictate that the call be handed off to one IXC, which hands the call off to yet another specified IXC. For example, a call may be handed to IXC A with the TNS identifying IXC B; in this case the TNS instructs IXC A to hand off the call to Carrier B.

The domain of a SIP URI in the Request-URI of a SIP INVITE can be seen to fill a role analogous to that of the TNS. If one provider needs to route a call to a specific provider, it would populate the domain in the Request-URI with the domain of that specific provider. When the call reaches that specific provider, it is typically (though not always) sent to a different provider to terminate the call. The analog to the example in the previous paragraph would be for a SIP provider to hand an INVITE to SIP Provider A with the domain in the Request-URI identifying SIP Provider B. As in the previous example, the signaling would reflect business arrangements.

One potential mechanism for interworking for North America between the ISUP TNS and SIP is to map between TNS and a SIP domain

representing the provider identified in the TNS. Mappings between TNS values and corresponding SIP domains would need to be pre-established and maintained at gateways implementing this mechanism. When such a gateway receives an ISUP IAM containing a TNS parameter, it would populate the domain of the Request-URI of the corresponding SIP INVITE with the appropriate domain mapped from the received TNS value. Conversely, when a gateway implementing this mechanism receives a SIP INVITE, the domain of the SIP URI would be consulted by the gateway and potentially mapped to any included TNS value. Note that the inclusion of a TNS value is dependent upon local policy, which may be determined from several factors including the provisioned characteristics of the trunk group via which the call is routed.

Note that this mechanism precludes the use of tel URIs in the Request-URI for calls involving IXCs; such URIs, including their parameters, would need to be converted to SIP URIs as described in [RFC3966].

For SIP originated calls, the domain of the Request-URI is already used to identify the provider to which the request should be routed, thus there is no need to for additional SIP signaling to express such information.

9.14. Carrier Identification

In the current PSTN in North America, callers can specify the IXC they want to use for a particular long distance call. Otherwise, their presubscribed IXC is used. In either case the carrier identification code (CIC) of the chosen carrier is signaled. In ANSI ISUP this is signaled in the Carrier Information Parameter (CIP). Per [RFC3398], for interworking from ANSI ISUP to SIP, the CIP is mapped to the "cic" tel URI parameter, and vice versa. Note that in North America, the CIP, which identifies the selected carrier, may have a different value than the TNS, and is not used for routing purposes.

For SIP originated calls, the "cic" parameter can also be used to identify the selected carrier, as described in [RFC4694]. Note however that [RFC4694] describes a usage of "cic" where it is used for routing, which is more consistent with ITU-T ISUP than with ANSI ISUP, where it is not used for routing. As a result, some of the procedures in that document would require modification to be applicable to North American deployments.

9.15. Carrier Selection Information

The ISUP Carrier Selection Information (CSI) parameter describes how the selected IXC was chosen; e.g. presubscribed, dialed, etc. One example of the utility of this information comes from Operator services calls that include call completion, whereby a call is initiated on behalf of the caller. In order to know which IXC to use, and how that IXC was chosen, the operator services provider needs to receive the CIP and Carrier Selection Information. In ANSI ISUP this describes the carrier identified in the CIP; while in ITU-T ISUP it describes the carrier identified in the TNS. Thus in both cases it describes the selection of the carrier identified in the "cic" tel URI parameter of the Request-URI.

When interworking from ISUP to SIP, this information is included in the encapsulated ISUP. The "dai" parameter proposed in [DAI] can also be used to be carry this information. The "dai" parameter can also be used for SIP originated calls. Thus, the dai information would be associated with the carrier identified in the ANSI CIP or the ITU-T TNS. That is, in the ANSI model, it is associated with the carrier information that is delivered to the interested application(s) rather than the information that is used for routing.

9.16. Passing Whisper

During front end automation, the OIS-MS will record and may time compress the caller’s perhaps meandering speech into what is known as the "whisper". This is intended to be played into a human operator’s ear, should the call be referred to an operator, to avoid the operator from having to prompt the caller again. The whisper is obtained during the front end automation, and saved to an audio file.

If the call needs to be transferred to a human operator, the whisper will need to be played to the operator at the same time or slightly prior to connecting the caller to the operator. Thus, the operator workstation needs to be able to access the whisper file.

When the OIS-MS performs front end automation, it generates the whisper and saves it as an audio file. The location, storage type, and format are out of the scope of this document. What is needed is a way for the OIS-

AS, so it could potentially be used for later processing, such as passing to a human operator.

Due to size constraints, it may not be feasible or desirable to pass the actual audio file containing the whisper. This document will discuss the most general case of passing a pointer, in the form of a URI, to the audio content. What follows is a description of one possible way to implement this. The work of the recently formed IETF MEDIACTRL working group may provide alternatives.

Since the whisper is an output of the front end automation process, it makes sense to return this upon completion of that process. The most reasonable time to do this is when the OIS-MS sends the BYE.

Any SIP request, including BYE, can contain a message body. [RFC4483] defines an extension to the URL MIME External-Body Access-Type to satisfy the content indirection requirements for SIP. These extensions are aimed at allowing any MIME part in a SIP message to be referred to indirectly via a URI.

This is illustrated in the following figure. Note that the proxy has been omitted for clarity, as have some messages not crucial to illustrating the use of this mechanism. All SIP signaling traverses the proxy.

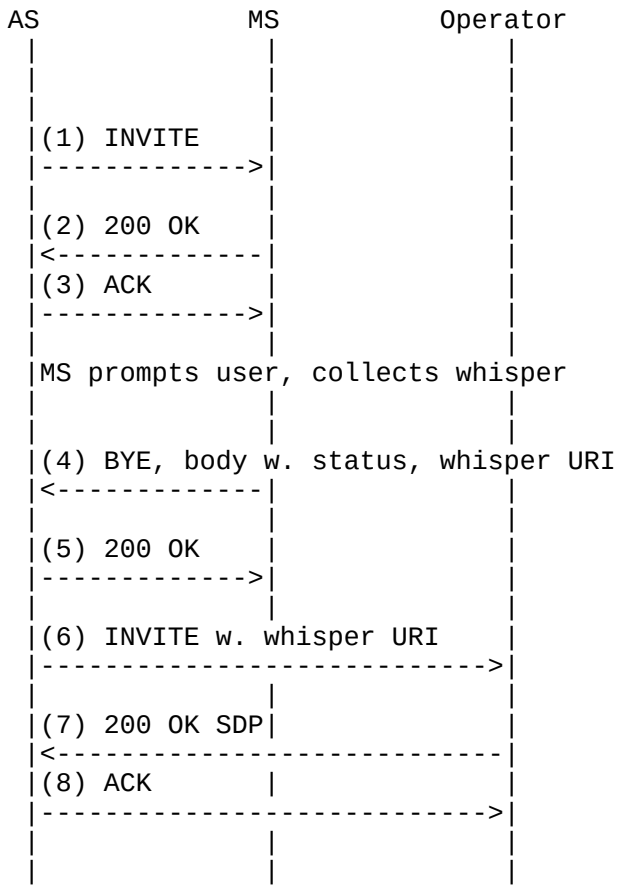


Figure 7 Call flow illustrating passing of whisper

1. INVITE AS->MS
INVITE sip:da@ms-1.oisp-c.example.com SIP/2.0
[remainder of message omitted]

2. 200 OK MS->AS
SIP/2.0 200 OK
[remainder of message omitted]

```
4. BYE MS->AS
BYE sip:as-1@as-1.oisp-c.example.com SIP/2.0
[non relevant portions of message omitted]
Content-Type: message/external-body; access-type="URL";
    URL="http://ms1.oisp-c.example.com/whisper/20070206092700-
0001.wav"
    expiration="Tues, 06 Feb 2007 09:30:00 GMT";
<CRLF>
Content-Type: audio/x-wav
Content-Disposition: render
<CRLF>



5. 200 OK AS->MS
SIP/2.0 200 OK
[remainder of message omitted]


6. INVITE AS->Operator Workstation
INVITE sip:operator@operator-123.oisp-c.example.com SIP/2.0
[non relevant portions of message omitted]
Content-Type: message/external-body; access-type="URL";
    URL="http://ms1.oisp-c.example.com/whisper/20070206092700-
0001.wav"
    expiration="Tues, 06 Feb 2007 09:30:00 GMT";
<CRLF>
Content-Type: audio/x-wav
Content-Disposition: render
<CRLF>


7. 200 OK Operator->AS
SIP/2.0 200 OK
[remainder of message omitted]
```

Note that this same mechanism also supports the case where front end automation is performed by one provider, and another provider provides the operator assistance. In this type of scenario, provisions need to made such that the second provider can access the resources referenced by the URI.

9.17. Calling Equipment Capabilities and Characteristics

It may be necessary for the OIS provider to learn the capabilities and characteristics of the caller's equipment. This would be useful when the OIS provider wishes to provide content to the caller other than that which was used on the call to the OISP. For example, the OIS provider might wish to send listing information via text message, or play a video clip about a particular venue about which he has requested information.

[RFC3840] Indicating User Agent Capabilities in the Session Initiation Protocol (SIP), defines mechanisms by which a UA can convey its capabilities and characteristics to other user agents and to the registrar for its domain. This information is conveyed as parameters of the Contact header field.

This information might be included in the incoming INVITE to the OISP, if the caller's UA supports this mechanism and is configured to do so. Otherwise, the OISP could query the caller's UA by sending a SIP OPTIONS request, and the UA, if it supports this mechanism, would include its capability feature tags in the response to the OISP.

The following is an example of an INVITE containing capability feature tags, as it arrives at the OISP. In this case, the UA supports audio, video, and text. Other included tags provide additional information.

```
INVITE sip:da@provider-c.example.com SIP/2.0
Via: SIP/2.0/UDP proxy-b.provider-b.example.com:5060
;branch=y9hG4bK74bf9
Via: SIP/2.0/UDP proxy-a.provider-a.example.com:5060
;branch=x9hG4bK74bf9
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234@provider-a.example.com>;audio;video;text
     ;actor="principle";automata;mobility="fixed"
     ;methods="INVITE,BYE,OPTIONS,ACK,CANCEL"
P-Asserted-Identity: "7327581234" <sip:73237581234@provider-
a.example.com>
P-Asserted-Identity: tel:+7327581234
Content-Type: application/sdp
Content-Length: ...
[SDP not shown]
```

If the OISP wishes to query the UA, it can send an OPTIONS request to the UA, and the UA, if it supports this mechanism, would include the feature capability tags in the Contact header, as show above, in the 200 OK response.

9.18. Media Server Returning Data to the Application Server

The OIS-AS needs to know the outcome of the operations performed by the OIS-MS, e.g. success/failure of front end automation, etc. Some mechanism is needed to convey this information. This could be conveyed using non SIP mechanisms.

Any SIP message, including BYE, can carry message bodies. The simplest way for a OIS-MS to return data to an OIS-AS is to encapsulate the data in a MIME body. This requires agreement between both sides on the format and semantics of these bodies.

Another approach is to use the content indirection mechanism to point to the data, however this may be rather cumbersome if only a small amount of data is to be returned.

Some OIS service may make use of VoiceXML, whereby the OIS-AS invokes VoiceXML scripts on the OIS-MS, and the OIS-MS returns data to the OIS-AS. [RFC5552] describes a SIP interface to VoiceXML media services, which is commonly employed between

application servers and media servers offering VoiceXML processing capabilities. This may be found useful for OIS services.

The topic of application server control of media services is currently under study, and is the subject of the IETF MEDIACTRL working group's efforts.

This information can also be conveyed using non SIP mechanisms. Describing such mechanisms is out of the scope of this document.

9.19. Control of Cut Through Direction for PSTN Interworking

For PSTN interworking scenarios, it may be desirable to explicitly control the "duplex" of the PSTN circuit; whether it be a two way connection or one way in the forward direction. The rules about SDP offer/answer indicate that as soon as an entity sends an SDP offer, it should be prepared to receive media for that session.

However, in practice some deployments may require that a 18x response containing SDP be sent in the backward direction before "blocking gates" are opened to allow media in the reverse direction.

SDP provides a "mode" attribute with values such as "a=sendonly", "a=recvonly", "a=sendrecv" for explicit control of the directionality. This mode attribute can be included in the SDP sent toward the PSTN GW in order to signal what duplex and directionality is desired. If it's desired to have a talk path only in the backward direction, such that audio is sent toward the caller but not in the opposite direction, then SDP with "a=sendonly" can be sent to the GW. When it's desired to have both-way cut through, an updated SDP can be sent with "a=sendrecv". This should affect not only the duplex of the voice path but also the related PSTN signaling sent by the GW towards the PSTN switch. For example, with ISUP, the GW should send an ACM with the User Network Interaction bit set in the Optional Backward Call Indication. Existing standards on PSTN interworking do not address this aspect of gateway behaviour.

Further, some service provider networks may implement media authorization policies that require the use of the P-Early-Media SIP header field as defined in [RFC5009]. In such networks, or when interoperating with such networks, the response sent toward the PSTN GW as described above should also include the P-Early-Media header field with the "em-param" value set to "sendrecv".

9.20. With Holding of Final Responses

Currently in the PSTN, for operator services, signaling of Answer, whether this be an ISUP ANM or MF Answer Supervision, is often with held, leaving the call in an alerting state while the caller interacts with the operator services system. The motivation for this is that in the PSTN, billing normally starts when answer is signaled. For some calls answer may never be signaled; in others it may be signaled for instance when a call completion call is answered.

The equivalent of answer indication in SIP is the 200 OK final response. It is not an intrinsic property of SIP based systems that billing must start upon 200 OK. In cases where it’s desired to emulate the PSTN behaviour, the 200 OK can be with held. When this is done, normal SIP procedures need to be followed to prevent the session from timing out. For example, the UAS can periodically retransmit non-100 provisional responses as described in Section 13.3.1.1 of [RFC3261].

10. Example Call Flow - Directory Assistance

10.1. Basic Flow

The following call flow provides examples of how a DA service could be implemented using the mechanisms described in this document. It is intended to illustrate the intended use of the proposed signaling mechanism. Some messages not crucial to this may be omitted for clarity.

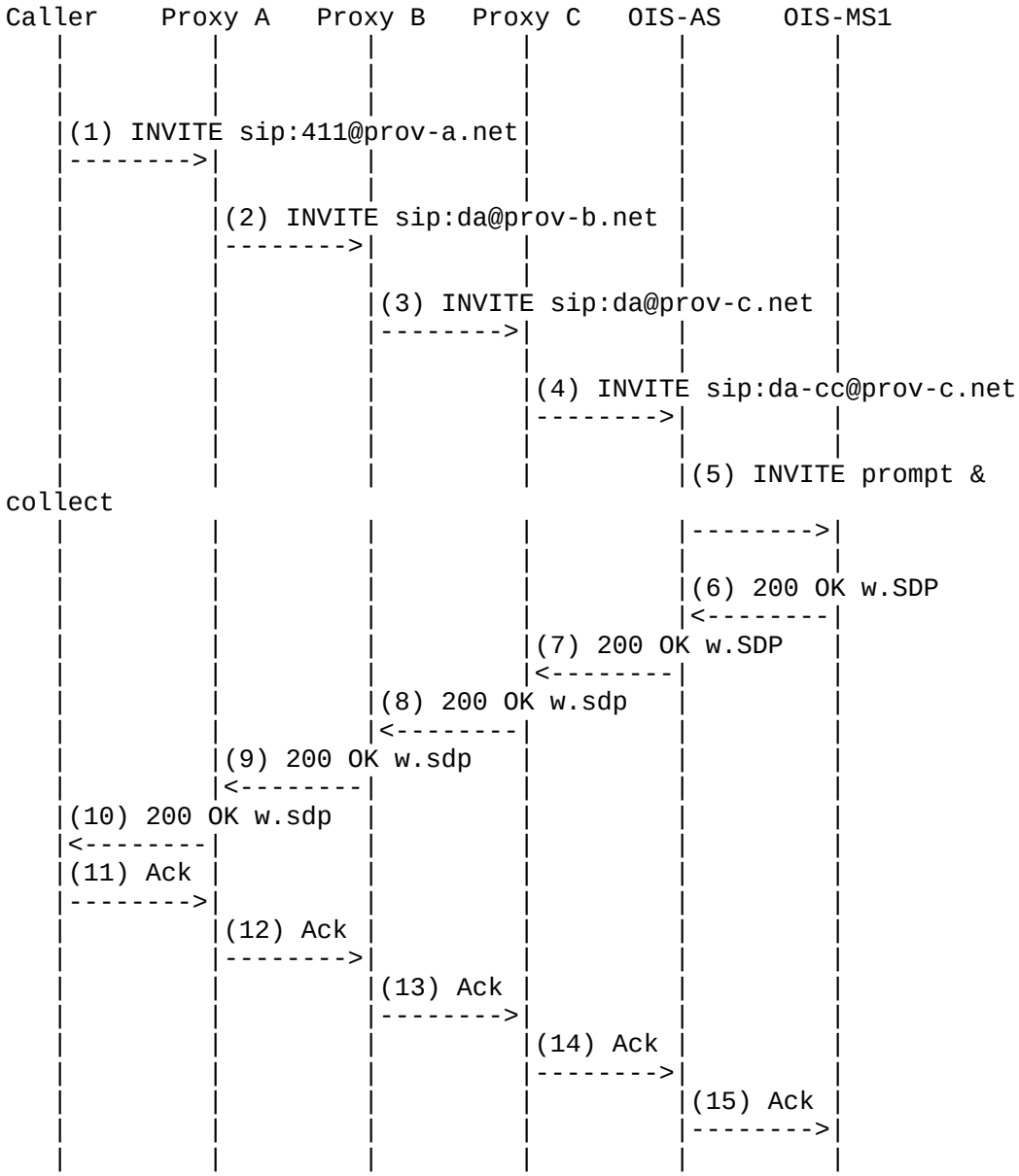


Figure 8 DA Call flow, part 1

For brevity, only relevant SIP headers will be shown. The following test refers to Figure 8.

The user, homed in provider A, initiates a request for an OIS service, for instance by dialing "411". The user's UA sends a SIP INVITE. It might contain a "tel" URI.

1. INVITE UE -> Home Proxy

```
INVITE sip: 411@provider-a.example.com SIP/2.0
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234@provider-a.example.com>
Content-Type: application/sdp
Content-Length: ...
```

The home provider knows nothing of OISP services, for instance it might be a rather small scale provider. It is essentially set up to forward all calls of this type to Provider B. It translates the Request-URI to a SIP URI and sends the call on to provider B. Because of this retargeting, it adds a History-Info header to capture the dialed digits.

The caller's identity is verified in a manner consistent with this provider's policies, and the proxy adds two P-Asserted-Identity headers: one with a SIP URI, and another with a "tel" URI.

2. INVITE proxy-a -> proxy-b

```
INVITE sip:411@provider-b.example.com SIP/2.0
Via: SIP/2.0/UDP proxy-a.provider-a.example.com:5060
;branch=x9hG4bK74bf9
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234@provider-a.example.com>
P-Asserted-Identity: "7327581234" <sip:73237581234@provider-
a.example.com>
P-Asserted-Identity: tel:+7327581234
History-Info: sip:411@provider-a.example.com; index=1
Content-Type: application/sdp
Content-Length: ...
```

Proxy-b in provider-b's network receives the request. This is a larger network, and it has business relationships with several OIS providers, as well as with several providers which serve subscribers. This provider has logic which requires it to query the Home Provider's network to find some information related to the caller. This is not likely to be a SIP related function, and is thus out of scope for this document. The logic executes, taking the result of this query into account. It is determined that the call is for directory assistance, and that the call should be routed to provider C for handling.

So, proxy-b retargets the Request-URI to reflect this, and routes the call to provider C (the OISP). It adds another entry to the History-Info header to capture this retargeting.

3. INVITE proxy-b -> proxy-c

```
INVITE sip:da@provider-c.example.com SIP/2.0
Via: SIP/2.0/UDP proxy-b.provider-b.example.com:5060
;branch=y9hG4bK74bf9
Via: SIP/2.0/UDP proxy-a.provider-a.example.com:5060
;branch=x9hG4bK74bf9
Via: SIP/2.0/UDP client.provider-a.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:7327581234@provider-a.example.com>;tag=1234567
To: sip:411@provider-a.example.com
Contact: <sip:7327581234@provider-a.example.com>
P-Asserted-Identity: "732758123" <sip:73237581234@provider-
a.example.com>
P-Asserted-Identity: tel:+7327581234
History-Info: sip:411@provider-a.example.com; index=1,
<sip:da@provider-a.example.com>; index=1.1
Content-Type: application/sdp
Content-Length: ...
```

Proxy-c in provider C’s network receives the request. The source of the request is authenticated via mechanisms not described here. It needs to know how to bill this call, and thus needs to know which provider it came from. It looks at the topmost Via header, and sees that the call came from provider B.

It examines the History-Info header, and is able to identify the dialed digits. It can also determine from the SIP URI which domains have been traversed, as long as each has retargeted and appended an entry in the header.

The proxy determines that the call needs to go the OIS-AS for handling, so it retargets if necessary and forwards the INVITE.

The OIS-AS performs 3PCC. It determines that the call needs a branded announcement based on the identity of the home provider, which it derives from the P-Asserted-Identity header. It initiates a new call leg toward OIS-MS1 for front end automation. Per [RFC4240], the "dialog" portion of the Request-URI indicates the "prompt & collect" service. The URI identifies the VoiceXML script to be executed. The SDP is the caller’s SDP.

5. INVITE OIS-AS -> MS1

```
INVITE sip:dialog@ois-as.prov-c.example.com; \
       voicexml=http://vxmlserver.example.net/cgi-bin/script.vxml \
SIP/2.0
Via: SIP/2.0/UDP ois-as.prov-c.example.com:5060
;branch=z9hG4bK74bf9
From: <sip:ois-as@ois-as.prov-c.com>;tag=1234567
To: sip:dialog@ois-as.prov-c.example.com; \
       voicexml=http://vxmlserver.example.net/cgi-bin/script.vxml
Contact: <sip:ois-as@ois-as.prov-c.example.com>
Content-Type: application/sdp
Content-Length: ...
```

The OIS-MS responds with a 200 OK, with its own SDP. The OIS-AS now sends a 200 OK response back toward the caller, with the MS’s SDP. Note that the OIS-AS could first have sent non final response back toward the user.

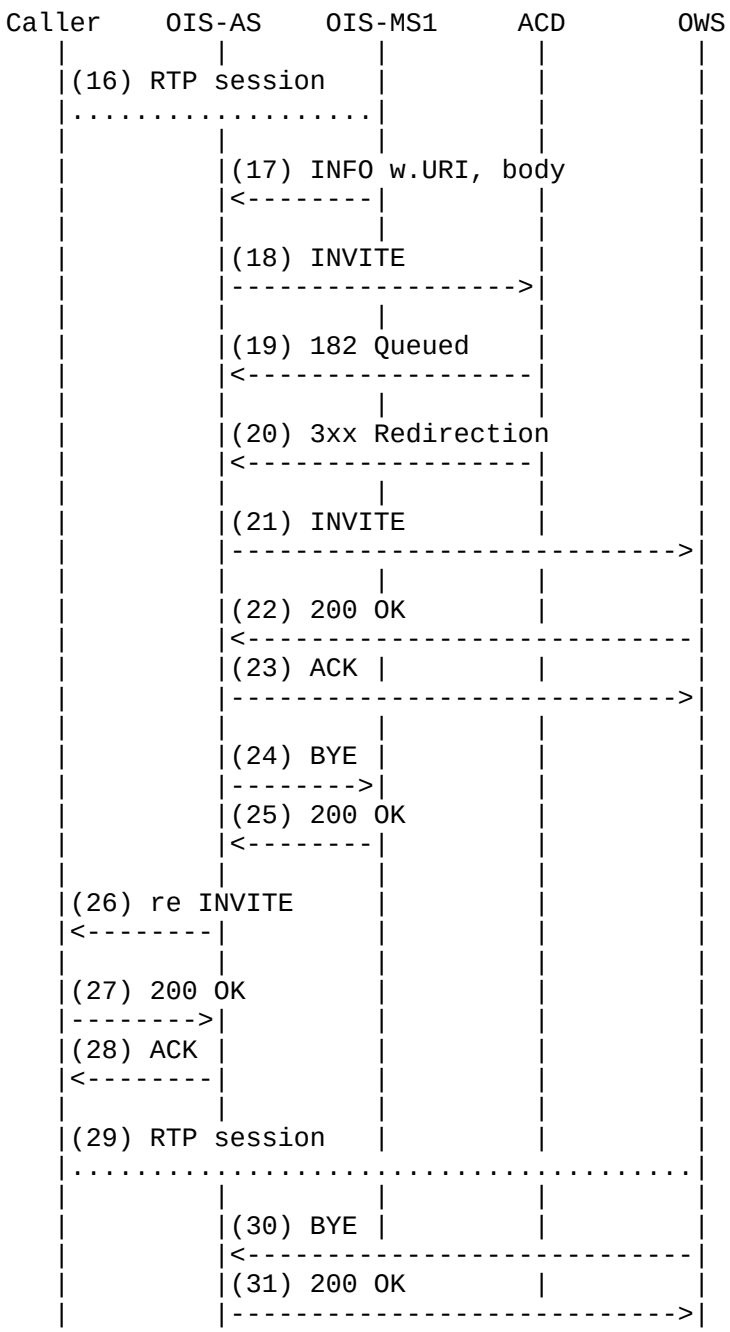

Caller
OIS-AS
OIS-MS1
ACD
OWS
(16) RTP session
(17) INFO w.URI, body
(18) INVITE
(19) 182 Queued
(20) 3xx Redirection
(21) INVITE
(22) 200 OK
(23) ACK
(24) BYE
(25) 200 OK
(26) re INVITE
(27) 200 OK
(28) ACK
(29) RTP session
(30) BYE
(31) 200 OK

Figure 9 DA Call flow, part 2

The following text refers to Figure 9.

The user is now connected (16) to the MS, which plays a branded announcement, and prompts for the listing information. When the user speaks his request, the MS processes the audio to obtain a "whisper" file, or condensed version of the request. In this example, the MS is unable to successfully perform the query, so it sends an indication of this to the AS. In this example, the indication is sent using an as yet unspecified protocol message carried in a message body in a SIP INFO message, which also carries a URI which points to the whisper file. Other mechanisms, including non SIP mechanisms, could also be used to this end (this is the subject of further study). The AS allows the caller to remain connected to the MS while it sets up a call to an operator workstation (OWS), allowing for the possibility to play custom announcements to the caller.

The OIS-AS decides based on the failure indication that it needs to route the call to a human operator. It sends an INVITE (18) to the ACD server. This INVITE carries information about the required characteristics, such as language and skill set, of the operator which should be selected for this call. The means by which this information is carried has yet to be defined. One possible way an ACD could be implemented is as a presence server, such that it keeps track of the availability of all the operators. The Media Resource Broker being discussed in the IETF MEDIACTRL working group also represents an approach to ACD.

If the call needs to be queued due to lack of an immediately available resource, the ACD may send a 812 Queued response (19). In this example, the ACD server is implemented as a redirect server - it sends a 3XX response (20) which identifies the operator the OIS-AS should contact. Alternately, the ACD server could have proxied the request to the operator.

The OIS-AS now sends an INVITE (21) containing the URI to the whisper, as well as the caller’s SDP, to the indicated operator workstation. The operator workstation sends a 200 OK (22) with its SDP, which the OIS-AS sends toward the caller in a re-INVITE (26). Only when the workstation has sent a final response to the INVITE, the AS sends a BYE (24) to the MS.

The caller is now connected to the operator (29), and the operator helps the caller with the listing. The operator workstation launches a query, and a response is received. The operator signals a BYE (30) toward the OIS-AS, which may contain the listing information in a message body, a pointer (URI) to the listing information, or it may pass this information to the OIS-AS using some other, non SIP mechanism.

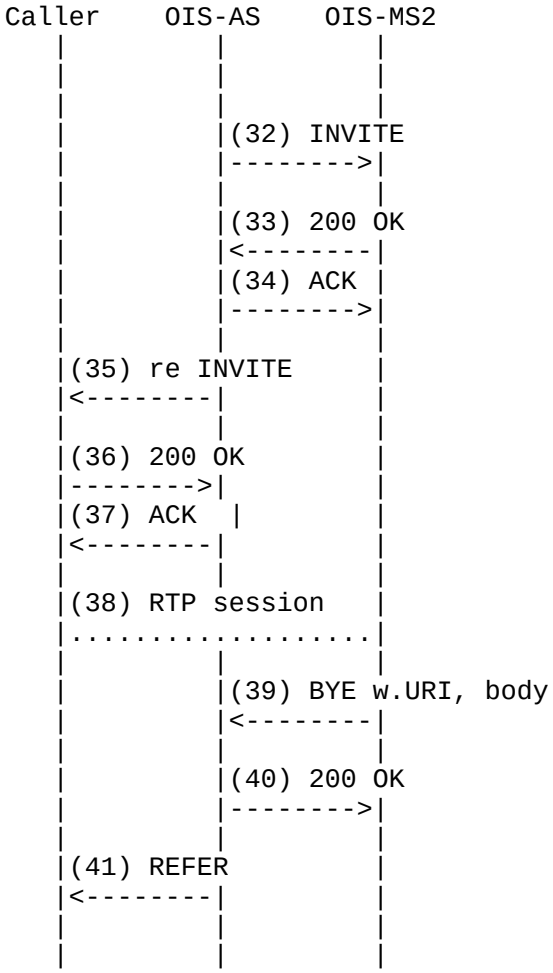


Figure 10 DA Call flow, part 3

The following text refers to Figure 10.

The OIS-AS sends an INVITE (32) to another OIS-MS, MS2, for back end automation. (Note that though MS2 is shown as a separate element, the functionality it provides may or may not require a separate element.) When it receives MS2's SDP in the 200 OK (33), it sends a re-INVITE (35) toward the user to update the SDP. At this point an audio session is in place between the caller and the back end automation MS (38). The MS plays the listing information, and offers call completion service. The caller accepts, so OIS-MS2 sends a BYE (39) with a message body containing the result of the call completion offer. Since call completion was requested, the OIS-AS sends a REFER (41) to the caller, to cause it to place a call to the listed party. The OIS-AS may or may not care about subsequent NOTIFYs from the caller, and drops out of the call.

10.2. OISP Drops Out at Call Completion Setup

The OISP may want to support different call flow options with respect to call completion. Reasons for this may include the desire to free up resources quickly, provide additional functionality, etc. When the OISP wants to provide the listing information and free resources as soon as possible, a simple flow based on REFER can be used, as illustrated below.

In this flow, the caller is already connected to an OISP resource such as an MS, and requests call completion. In (2), the OISP sends a REFER to initiate the call completion call. The caller's UA indicates acceptance of the REFER by sending a 202 Accepted (3). It then sends a NOTIFY indicating that it is attempting to contact the indicated resource, by sending an INVITE (10). When the AS receives this notification, it understands that the caller is attempting the call completion call, so it drops the call by sending BYE in (6)and (8). The various notifications sent by the caller to the OISP can be used to monitor progress of the call, or may simply be ignored from an application standpoints (from a protocol standpoint they must be acknowledged).

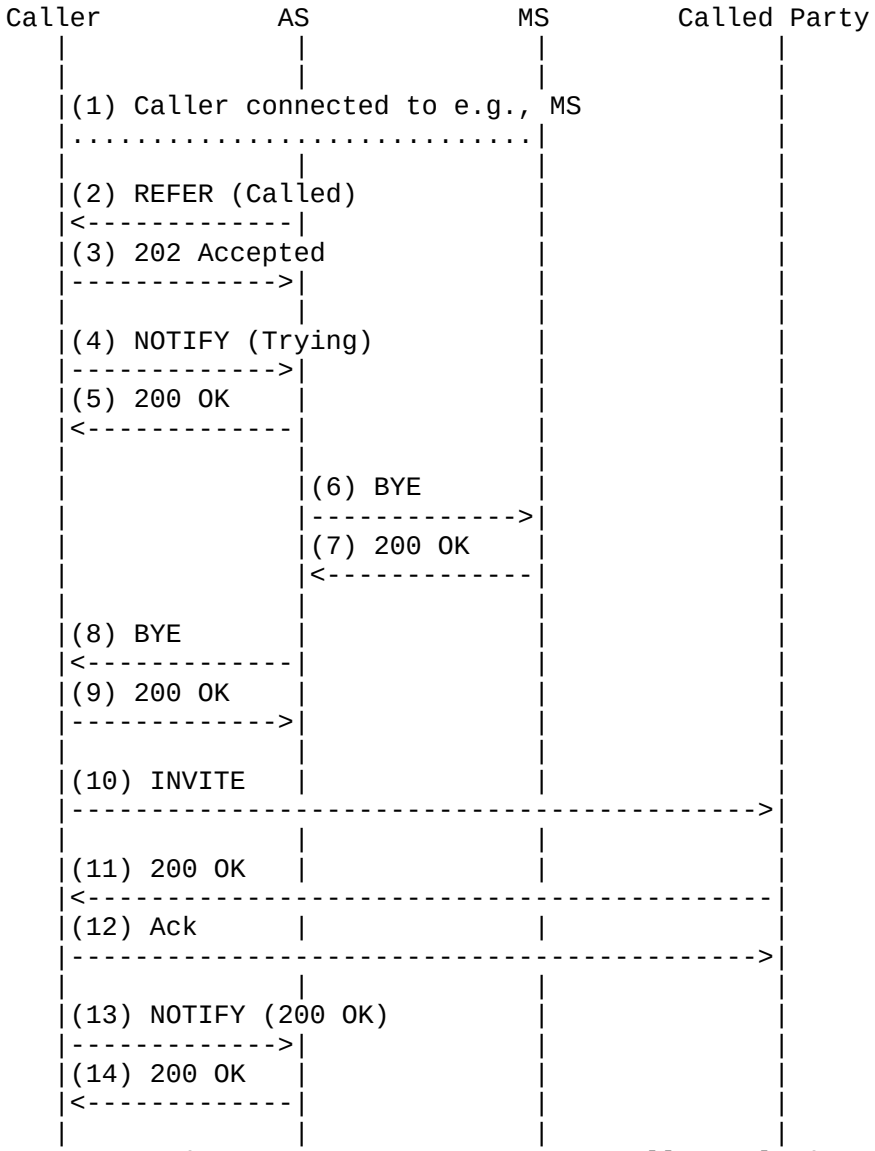
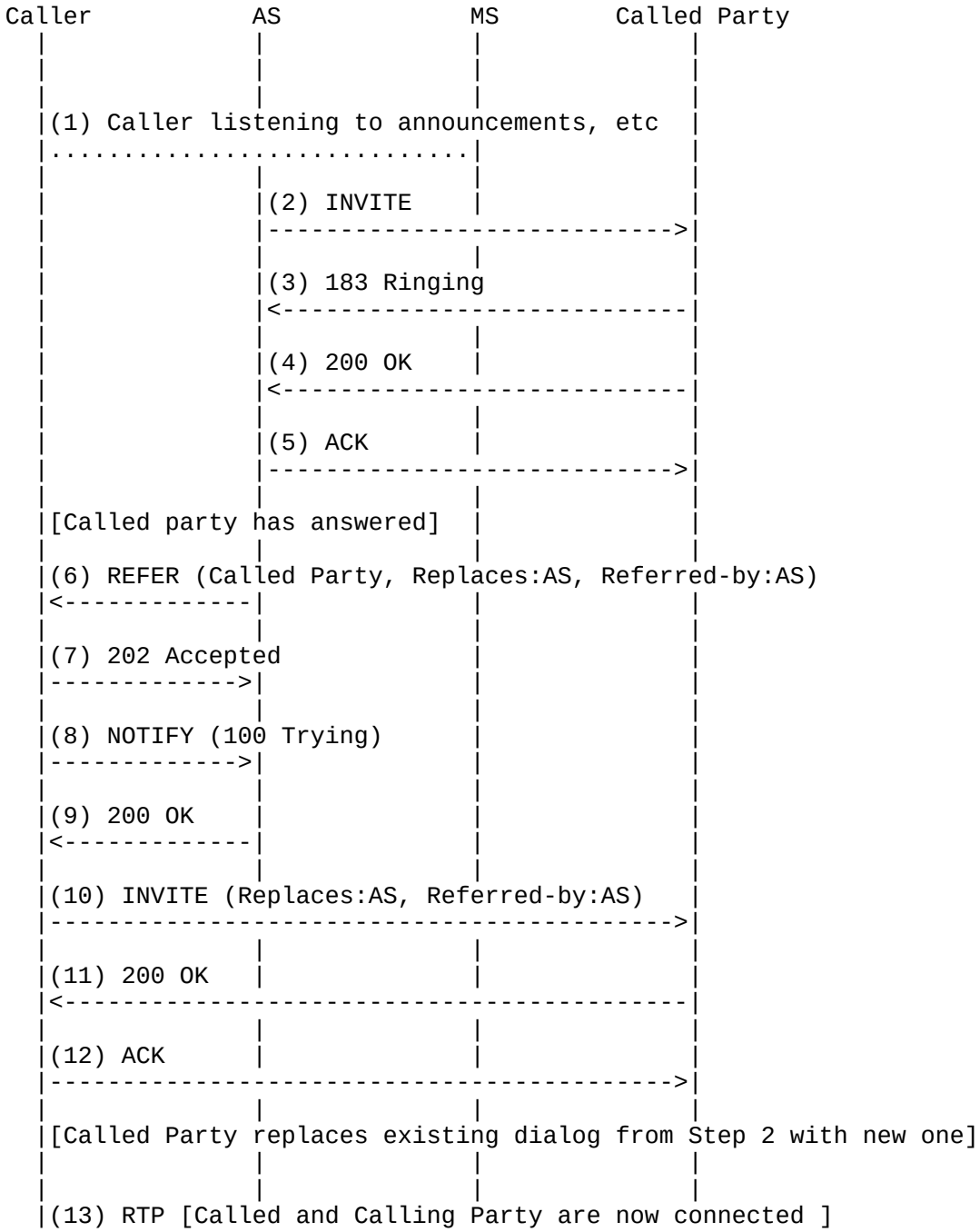


Figure 11 OISP Drops Out at Call Completion Setup

10.3. OISP Drops Out After Call Completion Call is Answered

The OISP may need to remain in the signaling path until the call completion call is answered. One way to implement this is to use the REFER method with the Replaces header, as described in [RFC3891]. In this case, once the call completion call is answered (5), the OISP's AS sends a REFER (6) toward the caller with a Replaces header identifying the current dialog between the AS and called party, and Referred-by header identifying the AS. This causes an INVITE (10) to be sent toward the called party, also with Replaces and Referred-by headers. As described in [RFC3891], this causes a new session to be set up with the called party, replacing the existing sessions. As part of this, the original session is torn down (16). Thus, the OISP's resources are removed from the call.


Caller
AS
MS
Called Party
(1) Caller listening to announcements, etc
(2) INVITE
(3) 183 Ringing
(4) 200 OK
(5) ACK
[Called party has answered]
(6) REFER (Called Party, Replaces:AS, Referred-by:AS)
(7) 202 Accepted
(8) NOTIFY (100 Trying)
(9) 200 OK
(10) INVITE (Replaces:AS, Referred-by:AS)
(11) 200 OK
(12) ACK
[Called Party replaces existing dialog from Step 2 with new one]
(13) RTP [Called and Calling Party are now connected]

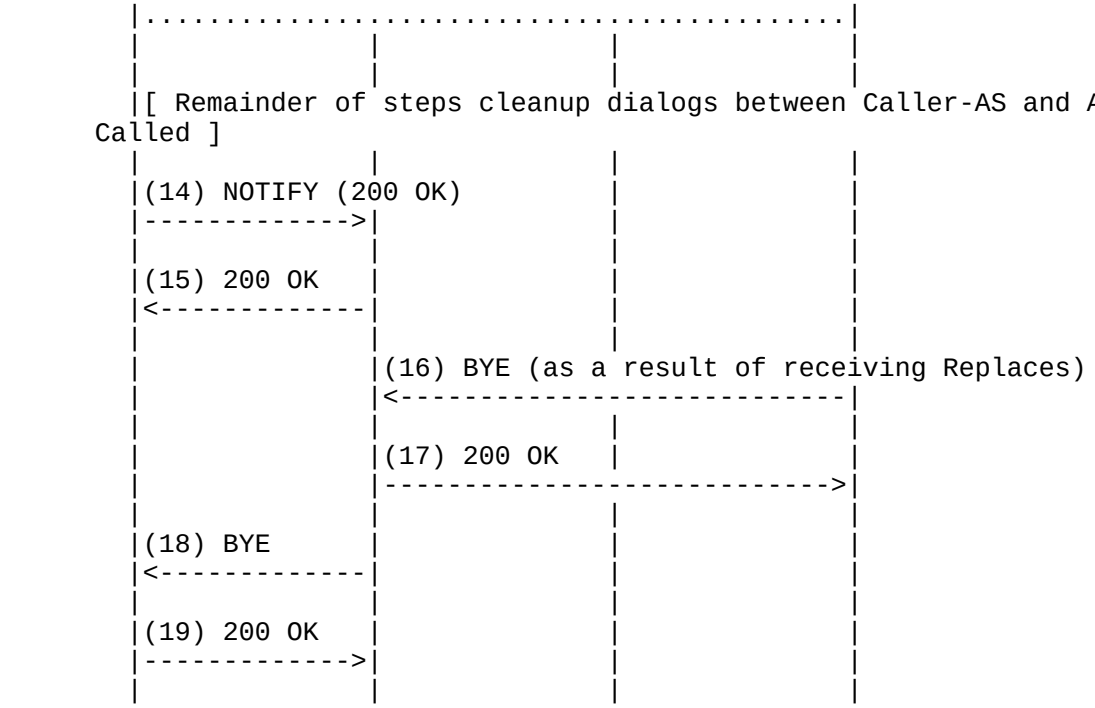
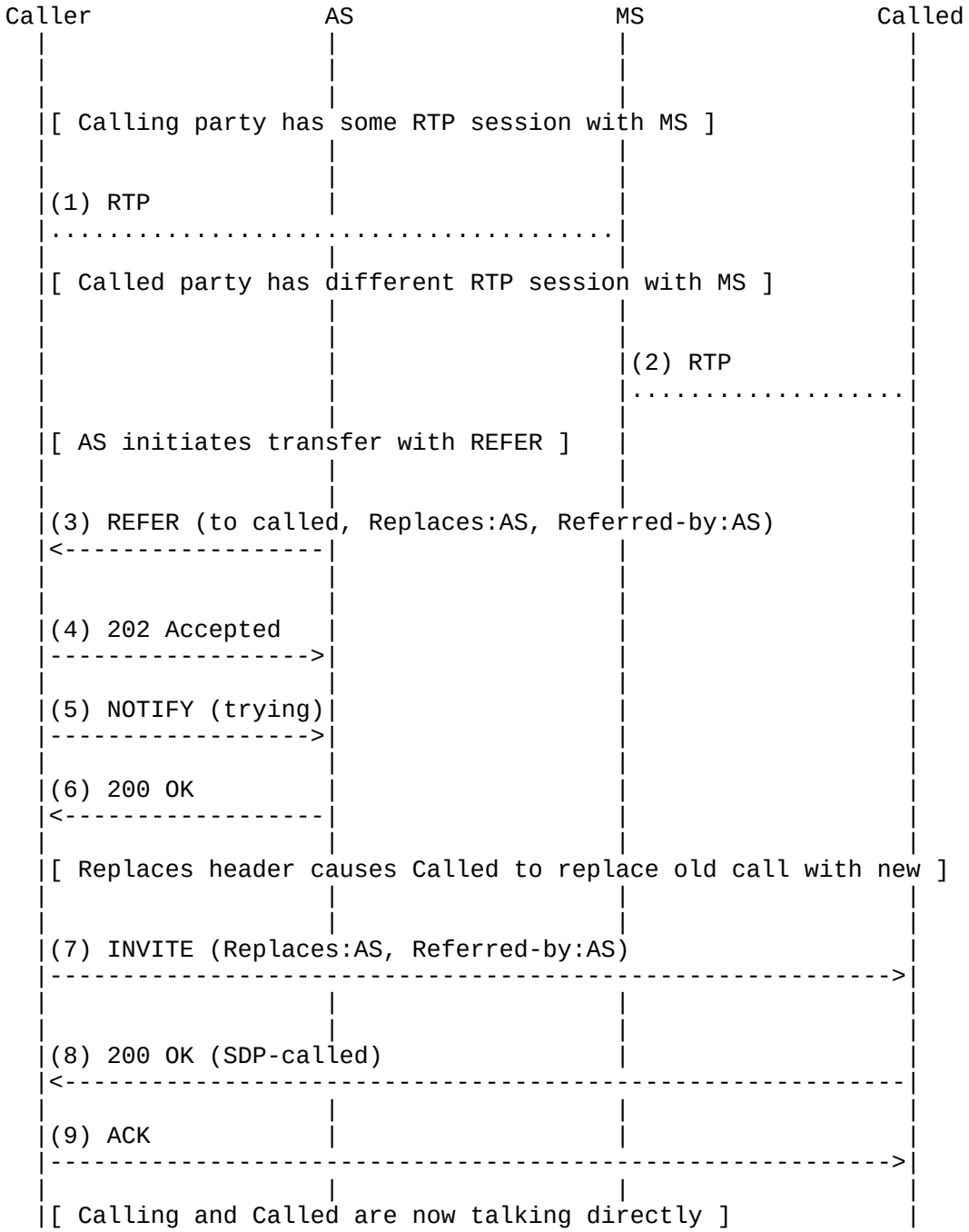


Figure 12 OISP Drops After Call Completion is Answered

10.4. OISP Drops Out After Interaction with Called Party

In this scenario, the OISP needs to interact with the called party, then desired to remove its resources from the call. Collect calls are one example where this might be used. This also uses REFER with Replaces. The OISP places a call to the called party, and interactions between OISP resources (automated or human) occur. The OISP then sends a REFER with Replaces and Referred-by to the calling party, which then sends an INVITE as described for the previous scenario.

In this scenario, the OISP has one media session (1) with the caller and another (2) with the called party. After interactions have been completed, the OISP initiates the transfer by sending a REFER (3) with Replaces and Referred-by headers. This causes the caller's UA to send a corresponding INVITE (7) containing those headers. As with the previous scenario, this causes initiation of a new session replacing the existing session, as well as teardown (10) of the existing session.


Caller
AS
MS
Called
[Calling party has some RTP session with MS]
(1) RTP
[Called party has different RTP session with MS]
(2) RTP
[AS initiates transfer with REFER]
(3) REFER (to called, Replaces:AS, Referred-by:AS)
(4) 202 Accepted
(5) NOTIFY (trying)
(6) 200 OK
[Replaces header causes Called to replace old call with new]
(7) INVITE (Replaces:AS, Referred-by:AS)
(8) 200 OK (SDP-called)
(9) ACK
[Calling and Called are now talking directly]

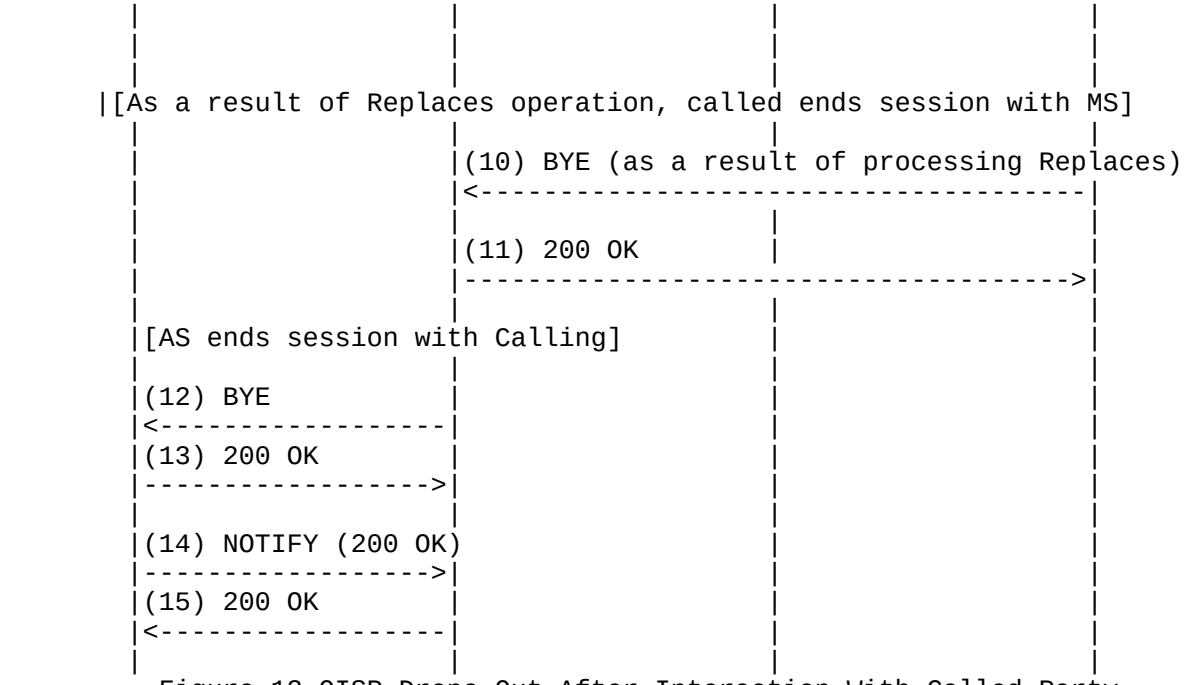
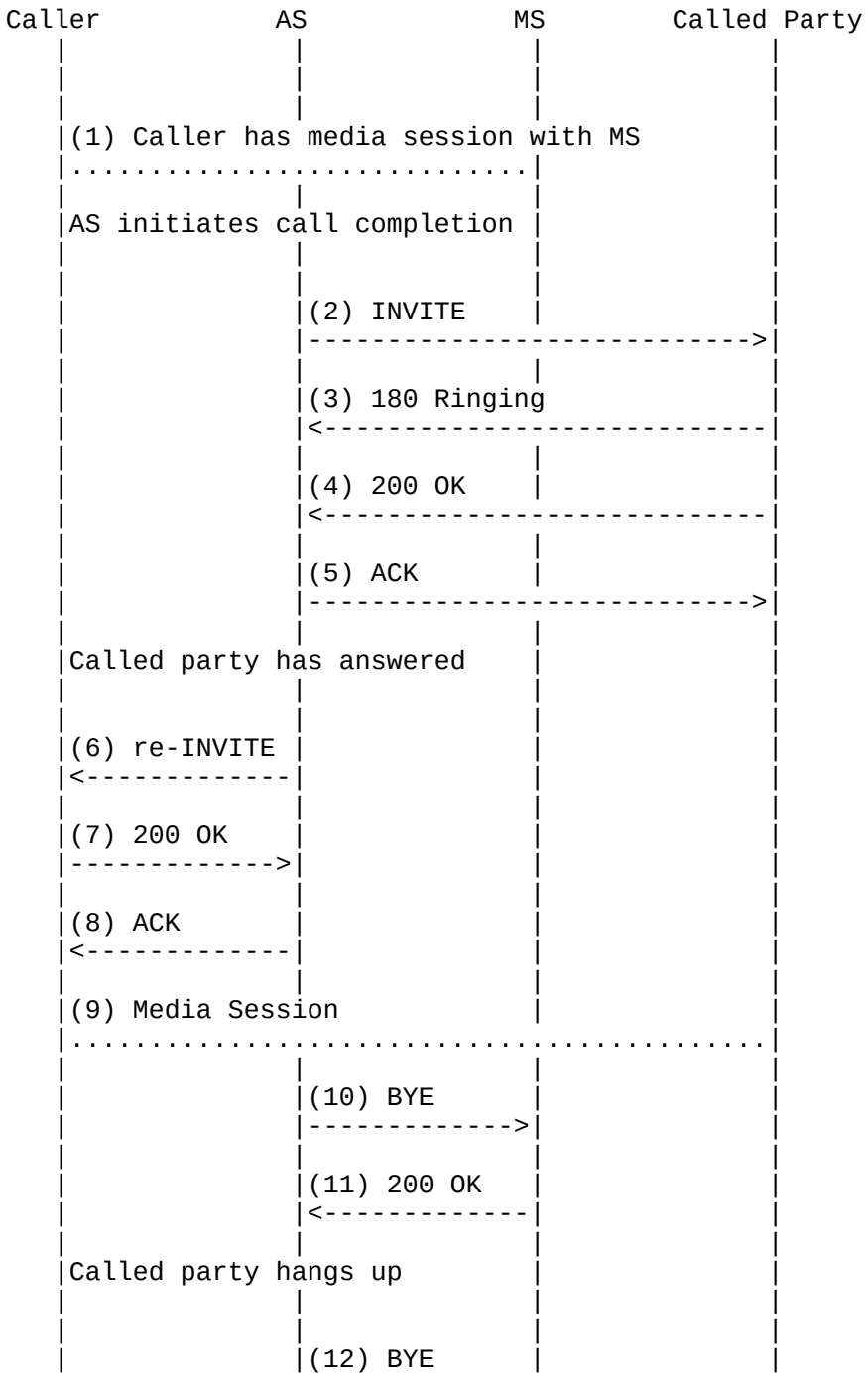


Figure 13 OISP Drops Out After Interaction With Called Party

10.5. OISP Remains in Path

In some cases, the OISP desires to maintain its elements in the signaling path and possibly in the media path as well for the duration of the call completion call. One possible reason for doing this is so that the caller can request to be returned to the OISP for additional services after the call has completed.

The figure below begins with the caller already connected to OISP resources. The AS initiates call completion in steps 2 through 5 by sending an INVITE toward the called party. The AS then sends a re-INVITE toward the caller to update the SDP, and step 9 shows the media session established between the caller and the called party, and in step 10 clears the previous session with the MS. When the called party hangs up in step 12, the AS responds. In step 14, the AS has the opportunity to redirect the caller to a MS or other resource to offer additional services, but in this case simply clears the dialog with the caller.


Caller
AS
MS
Called Party
(1) Caller has media session with MS
AS initiates call completion
(2) INVITE
(3) 180 Ringing
(4) 200 OK
(5) ACK
Called party has answered
(6) re-INVITE
(7) 200 OK
(8) ACK
(9) Media Session
(10) BYE
(11) 200 OK
Called party hangs up
(12) BYE

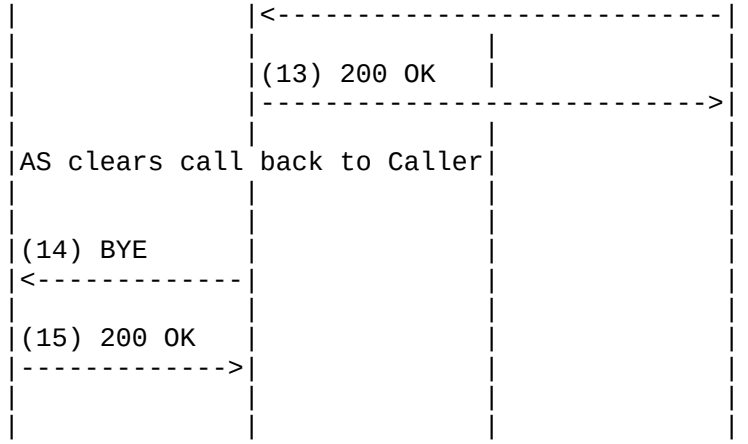


Figure 14 OISP Remains in Signaling Path

10.6. Return of Call to OISP

In some cases, it is desirable that the caller be able to request, typically via keypad stimulus such as the octothorpe or pound sign, to be returned to the OISP operator (human or automated). One way this can be accomplished is for the OISP to use KPML [RFC4730] to subscribe to the desired keypress. The flow presented here assumes that the calling UA, or an intermediary acting on its behalf, supports this event package, and is able to detect the desired keypress. Examples of such intermediaries include back to back user agents (B2BUAs) and Session Border Controllers (SBCs). Another option is for the OISP to insert some element such as a MS into the media stream, which is capable of detecting and notifying the desired keypress.

In (1) the caller has already been connected to called party via the AS. In (2), the AS subscribes to KPML events from the caller's UA. Note that in some environments, this could be intercepted and acted upon by intermediaries such as B2BUAs or SBCs. As long as this does not interfere with notification, this is transparent to the OISP. When the caller presses the specified keypress to request return to the OISP, a NOTIFY (6) is sent to the AS. At this time, the OISP can perform whatever actions are necessary, such as perhaps sending a re-INVITE or UPDATE to move the media session to an OISP resource.

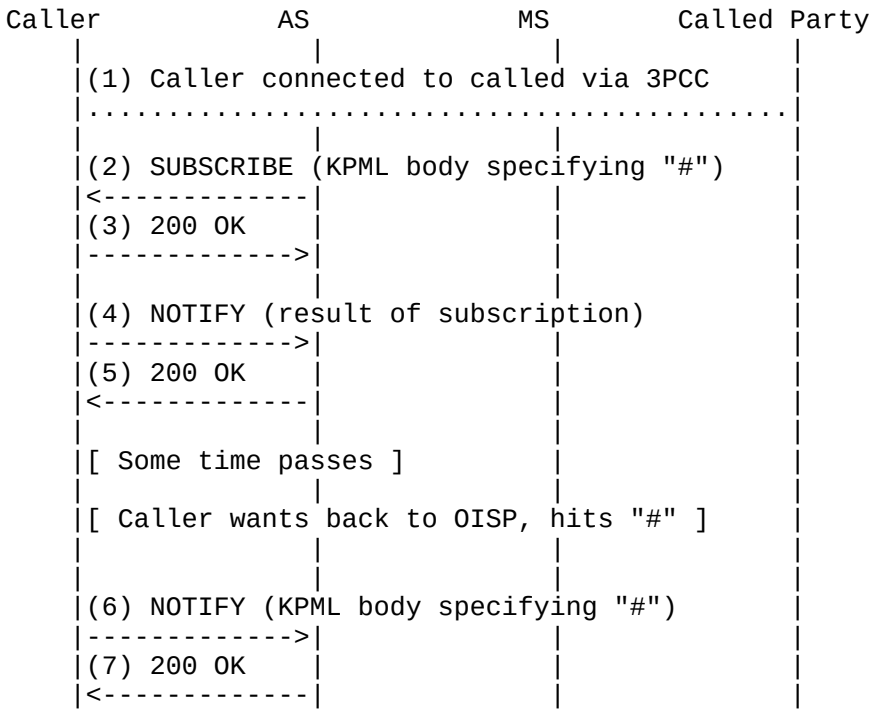
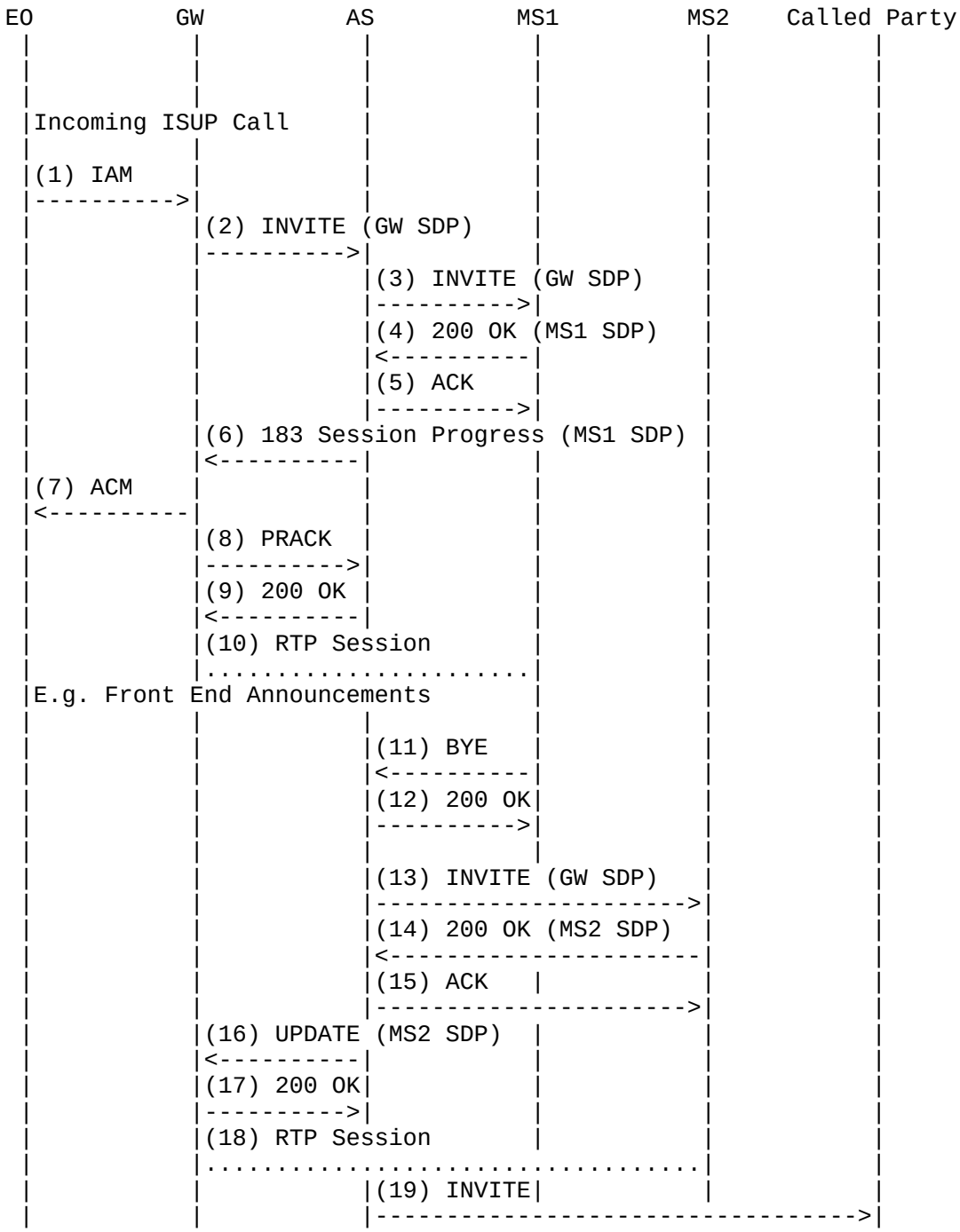


Figure 15 Return of Call to OISP

10.7. PSTN Origination

The following example shows a call from a PSTN caller. In this case, the incoming IAM is translated at the PSTN gateway to a SIP INIVTE. Though not specifically shown, the INVITE contains the IAM encapsulated in a MIME body, and any ISUP parameters are mapped to SIP headers and/or parameters as described in [T1679]; additionally the mechanisms described in this document are also applied, such as encoding of the trunk group information in the Contact header per [RFC4904].

Note that the 183 Session Progress in step (6) contains the SDP of the media server. As described in Section 9.19 "Control of Cut Through Direction for PSTN Interworking", this may be required in some deployments before media in the reverse direction is allowed by blocking gates.


EO
GW
AS
MS1
MS2
Called Party
Incoming ISUP Call
(1) IAM
(2) INVITE (GW SDP)
(3) INVITE (GW SDP)
(4) 200 OK (MS1 SDP)
(5) ACK
(6) 183 Session Progress (MS1 SDP)
(7) ACM
(8) PRACK
(9) 200 OK
(10) RTP Session
E.g. Front End Announcements
(11) BYE
(12) 200 OK
(13) INVITE (GW SDP)
(14) 200 OK (MS2 SDP)
(15) ACK
(16) UPDATE (MS2 SDP)
(17) 200 OK
(18) RTP Session
(19) INVITE

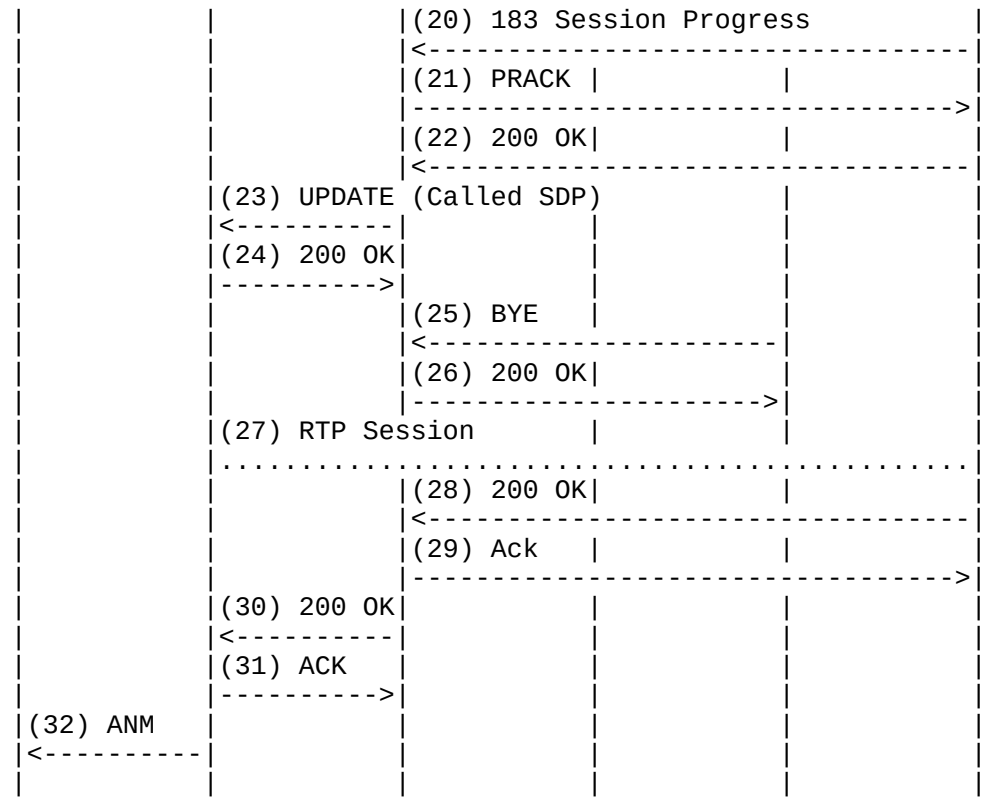
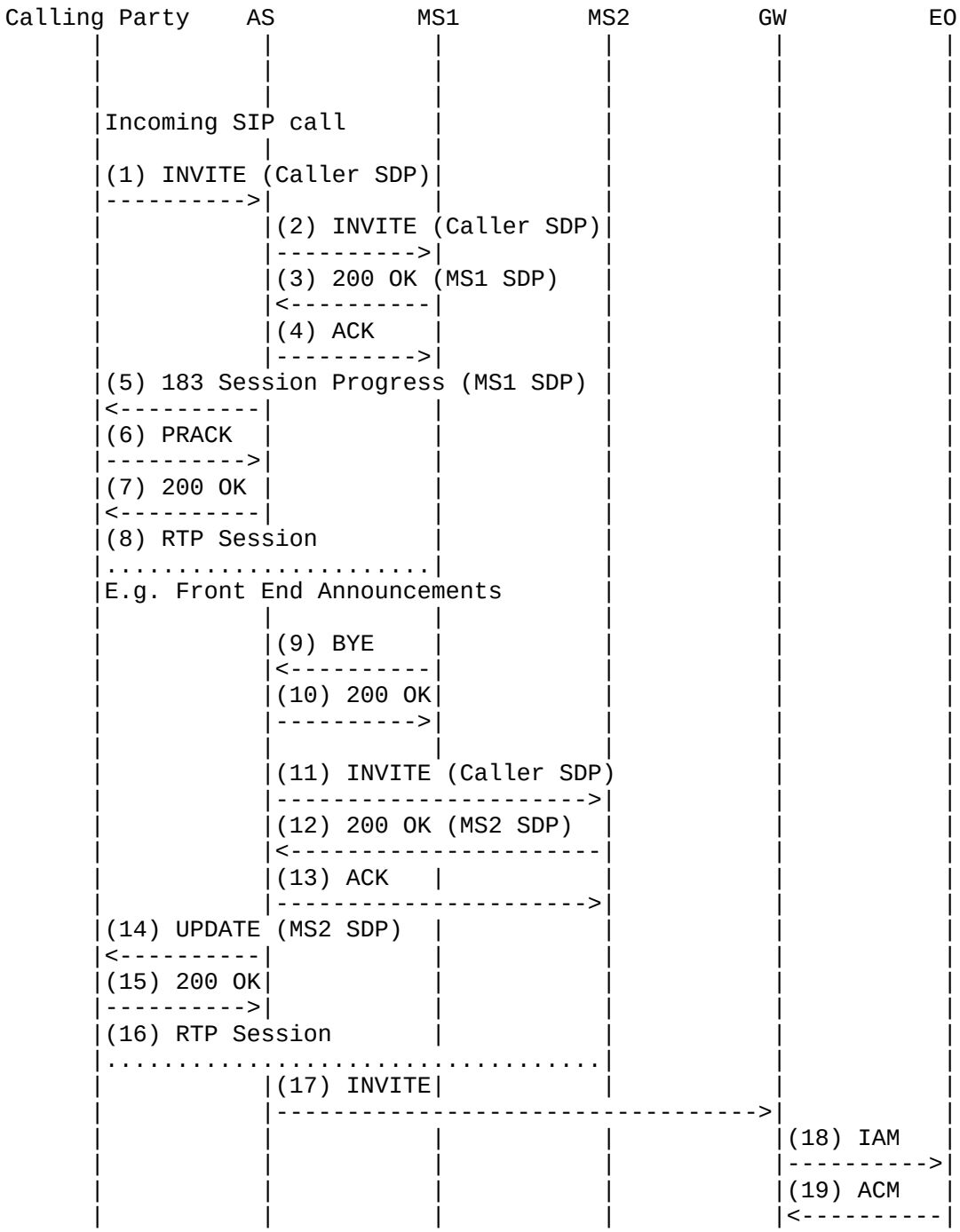


Figure 16 PSTN Origination

10.8. PSTN Termination

The following example shows a call which results in call completion to a destination on the PSTN. In Step 17 the AS sends an INVITE toward the PSTN gateway which results in an IAM being sent which initiates the PSTN call leg.


Calling Party
AS
MS1
MS2
GW
EO
Incoming SIP call
(1) INVITE (Caller SDP)
(2) INVITE (Caller SDP)
(3) 200 OK (MS1 SDP)
(4) ACK
(5) 183 Session Progress (MS1 SDP)
(6) PRACK
(7) 200 OK
(8) RTP Session
E.g. Front End Announcements
(9) BYE
(10) 200 OK
(11) INVITE (Caller SDP)
(12) 200 OK (MS2 SDP)
(13) ACK
(14) UPDATE (MS2 SDP)
(15) 200 OK
(16) RTP Session
(17) INVITE
(18) IAM
(19) ACM

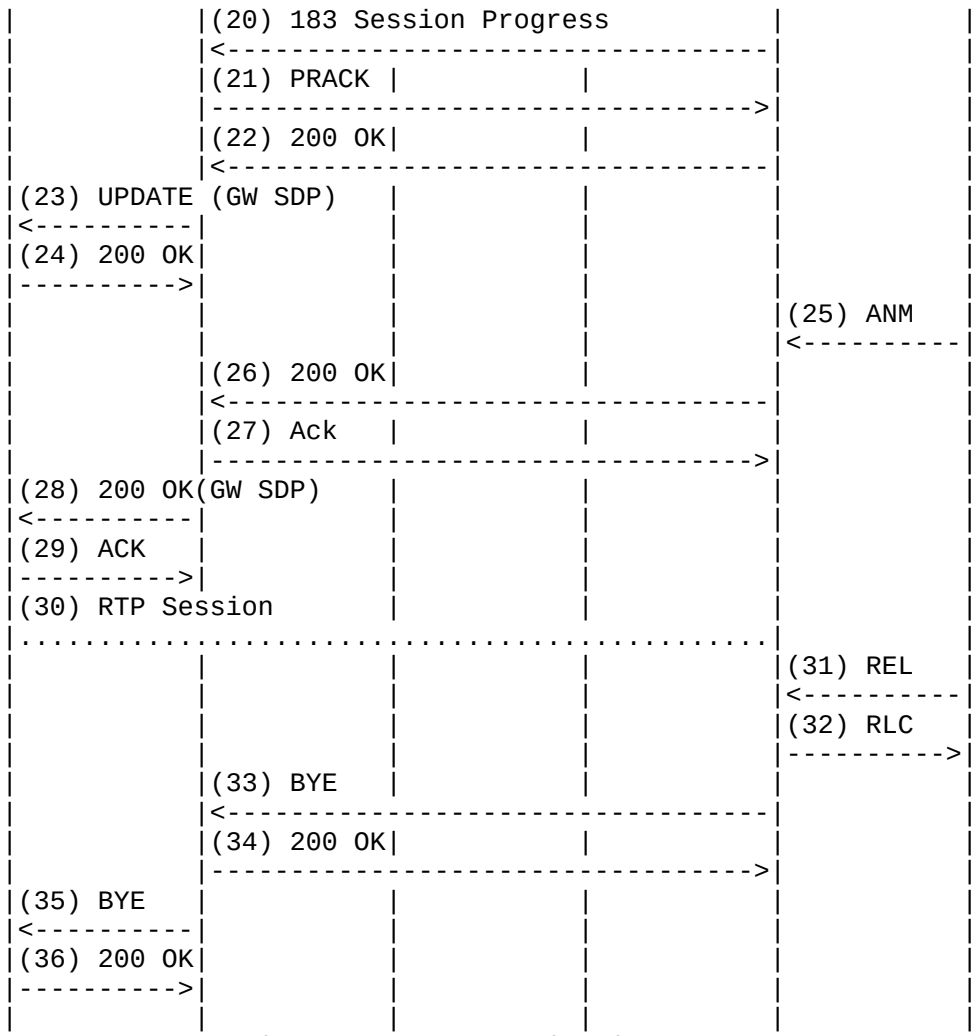
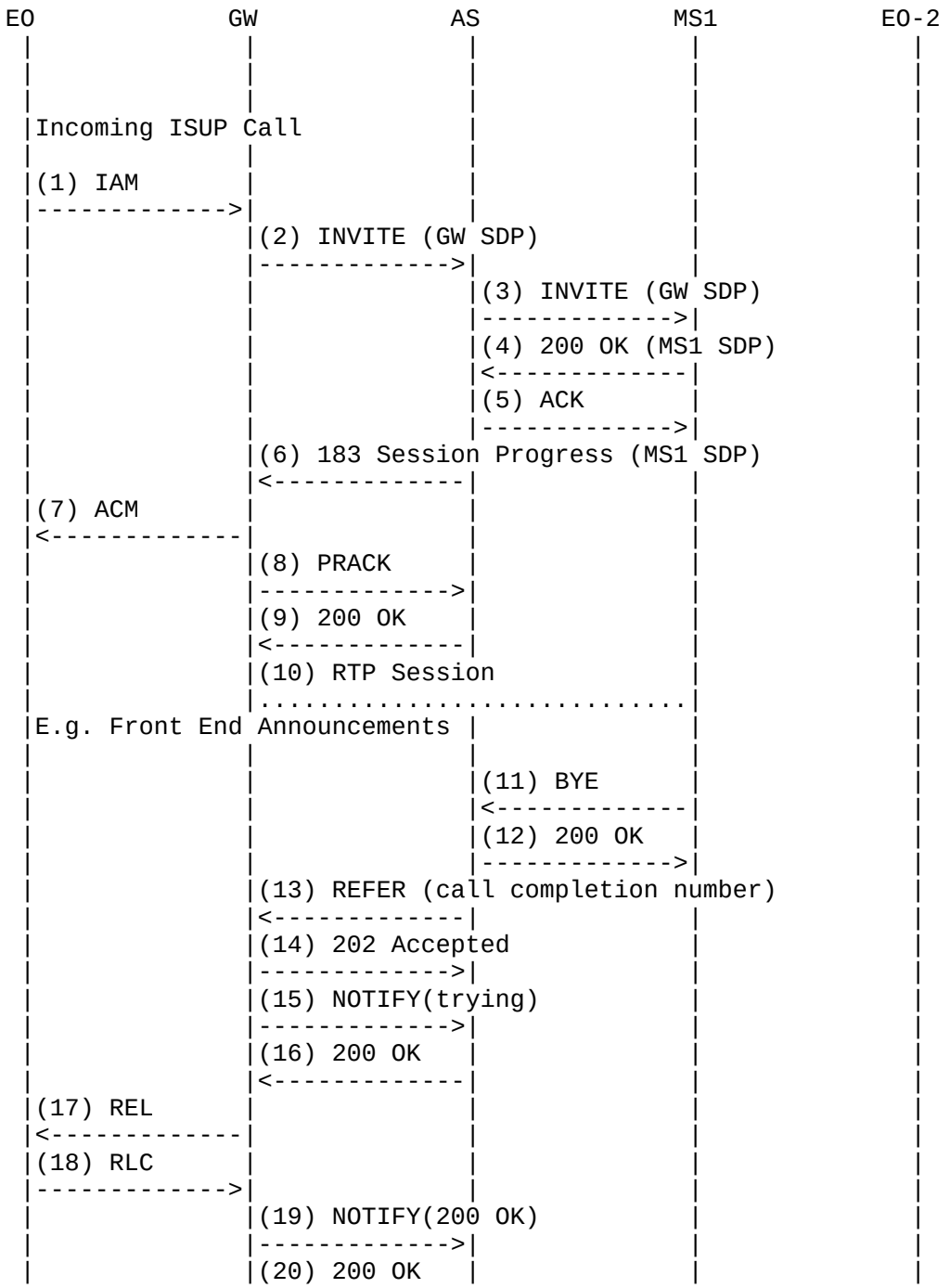


Figure 17 PSTN Termination

10.9. Call Completion By Releasing Call Back to PSTN

This example shows how when a call is received from the PSTN, call completion can be achieved by releasing the call back to the PSTN to have a PSTN switch initiate the call completion call. This allows call completion to occur in the PSTN, and completely drops the call from the OISP. The PSTN feature which supports this is called Release To Pivot; other implementations may also exist. The

gateway’s connection to the PSTN needs to be specifically provisioned to support this feature. There is currently no standard describing the invocation of this feature using SIP; nor does this document intend to do this. Rather, it intends to illustrate one way in which it might be done. This flow appears as the equivalent of a blind transfer with the PSTN gateway as the originator; the key thing is that the PSTN gateway needs to understand this as a request for Release to Pivot or equivalent PSTN feature.


EO
GW
AS
MS1
EO-2
Incoming ISUP Call
(1) IAM
(2) INVITE (GW SDP)
(3) INVITE (GW SDP)
(4) 200 OK (MS1 SDP)
(5) ACK
(6) 183 Session Progress (MS1 SDP)
(7) ACM
(8) PRACK
(9) 200 OK
(10) RTP Session
E.g. Front End Announcements
(11) BYE
(12) 200 OK
(13) REFER (call completion number)
(14) 202 Accepted
(15) NOTIFY(trying)
(16) 200 OK
(17) REL
(18) RLC
(19) NOTIFY(200 OK)
(20) 200 OK

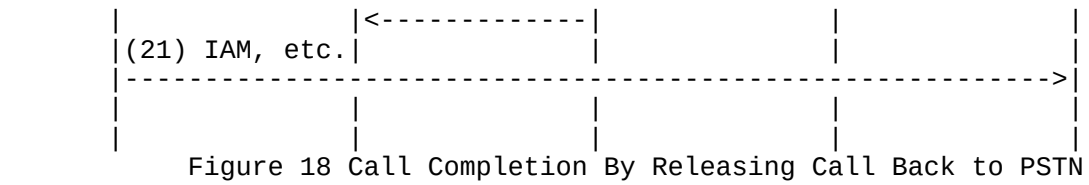


Figure 18 Call Completion By Releasing Call Back to PSTN

11. Operator Services Example Call Flows

The following call flows provide examples of how specific operator services could be implemented using the mechanisms described in this document. The purpose is to illustrate one way to implement these services using the proposed signaling mechanisms.

11.1. Network Controlled Coin Calls

This flow depicts a SIP based OISP handling calls from a network controlled coin station. The OISP needs to determine the coinage deposited by the station. Note that "smart" coin stations do not require interaction with the OISP. This discussion only addresses control of TDM based network controlled coin stations.

The configuration is as follows. Network controlled coin stations are connected to TDM based end offices (EOs) using special access lines, the characteristics of which are not important to this discussion. The EO exchanges signaling with the station over this access line, but does not perform the coin control. Operator Services switches historically provide the control for these types of calls, and the EO connects to the Operator Switch via special coin control trunks. The EO translates between coin access and coin trunk signaling.

The signaling includes coin station control and coin deposit indications. The OISP sends coin station control signaling to the coin station to instruct it to collect coins, return coins, etc. The coin deposit signaling is sent by the coin station toward the OISP, and indicates the coinage inserted by the user.

Coin station control signaling includes signals such as coin collect, coin return, operator ringback, etc. The way in which these signals are conveyed depends on the type of coin trunk being used. For SS7 ISUP coin trunks, these are conveyed using the Service Activation (SAP) ISUP parameter. For MF trunks using multiwink coin signaling, these signals are conveyed using a series MF hook state transition events known as "winks". For MF trunks using Expanded

Inband Signaling (EIS), these signals are conveyed as tone bursts in conjunction with a wink. The relevant MF signaling is described in [GR506].

When the AS communicates with the GW using encapsulated ISUP, such as for SS7 ISUP trunks and cases where the gateway internally converts between MF and encapsulated ISUP, then the AS can convey coin control signaling to the GW using encapsulated ISUP that includes the appropriate Service Activation Parameter (SAP) value. This encapsulated ISUP is carried within the SIP signaling sent to the GW.

For multiwink signaling, the AS could connect the GW to an MS and instruct the MS to play the appropriate signals using an existing mechanism such as netann, VXML, etc. As mentioned above, the multiwink signals are MF hook transition events. [RFC5244] defines a mechanism for signaling the ABCD states used to represent MF hook states within an RTP stream. The MS would generate the appropriate "telephone-event" RTP payload format packets defined in RFC 5244 in response to requests from the AS. In order to be able to render these events on the TDM side, the GW would need to implement reception of RFC 5244 packets.

For EIS signaling, an MS could be used as above, generating the appropriate tones and hook transitions in response to requests from the AS. The hook transition events as above could be accomplished using RFC 5244. The audio tones could be transmitted using an audio codec such as G.711. Alternatively, RFC 4733 "tone" RTP payload format packets as described in Section 4 of that document could be used. Finally, new RFC 4733 codepoints have been registered with IANA for these tones, so the can be conveyed using the "telephone-event" RTP payload format.

Coin deposit signaling is sent as tone bursts on the trunk from the coin station towards the OISP, regardless of whether ISUP or MF signaling is used on the trunk. The tones could be detected by the GW, or they could be detected by a MS that has been connected by the AS. In either case, some mechanism is needed in order for the AS to request detection and for the MS to report detection of these tones. KPML [RFC4730] and VXML both natively support the reporting of DTMF tones, but there is currently no standardized way to represent the tone bursts representing the deposit of coins. The possibility arises to represent the coin deposit tones in KPML or VXML by mapping them to some set of service provider specified DTMF digits.

The following examples illustrates the use of encapsulated ISUP to convey the coin control signaling, and detection of coin deposit signals at the GW, with the GW reporting coin deposits using KPML. As identified above, other alternatives are possible.

In the following flow, the EO is the end office service the coin station, the PSTN GW is the GW terminating the voice trunks and signaling from the EO, the AS is the OIS AS, the MS is a media server in the OIS provider, and the called party is self explanatory.

In step 1, the coin station (not shown) has signaled a call request to the EO, which in turn selects a coin trunk toward the OISP PSTN GW, and initiates the corresponding signaling. In steps 2 through 4, the PSTN GW sends an INVITE to the AS, which accepts the call.

In steps 5 through 7, the AS sends a SIP INFO message containing encapsulated ISUP, which contains an ISUP SAP parameter with the Feature Code Indicator (FCI) indicating "Network Service Attached", which is an instruction to the coin station that an Operator Services System has been connected. The GW sends the corresponding PSTN signaling back toward the coin station.

In steps 8 through 10, the AS using the same procedures sends encapsulated ISUP with a SAP parameter with the FCI indicating "Coin Collect" which instructs the coin station to collect and report on coin deposits.

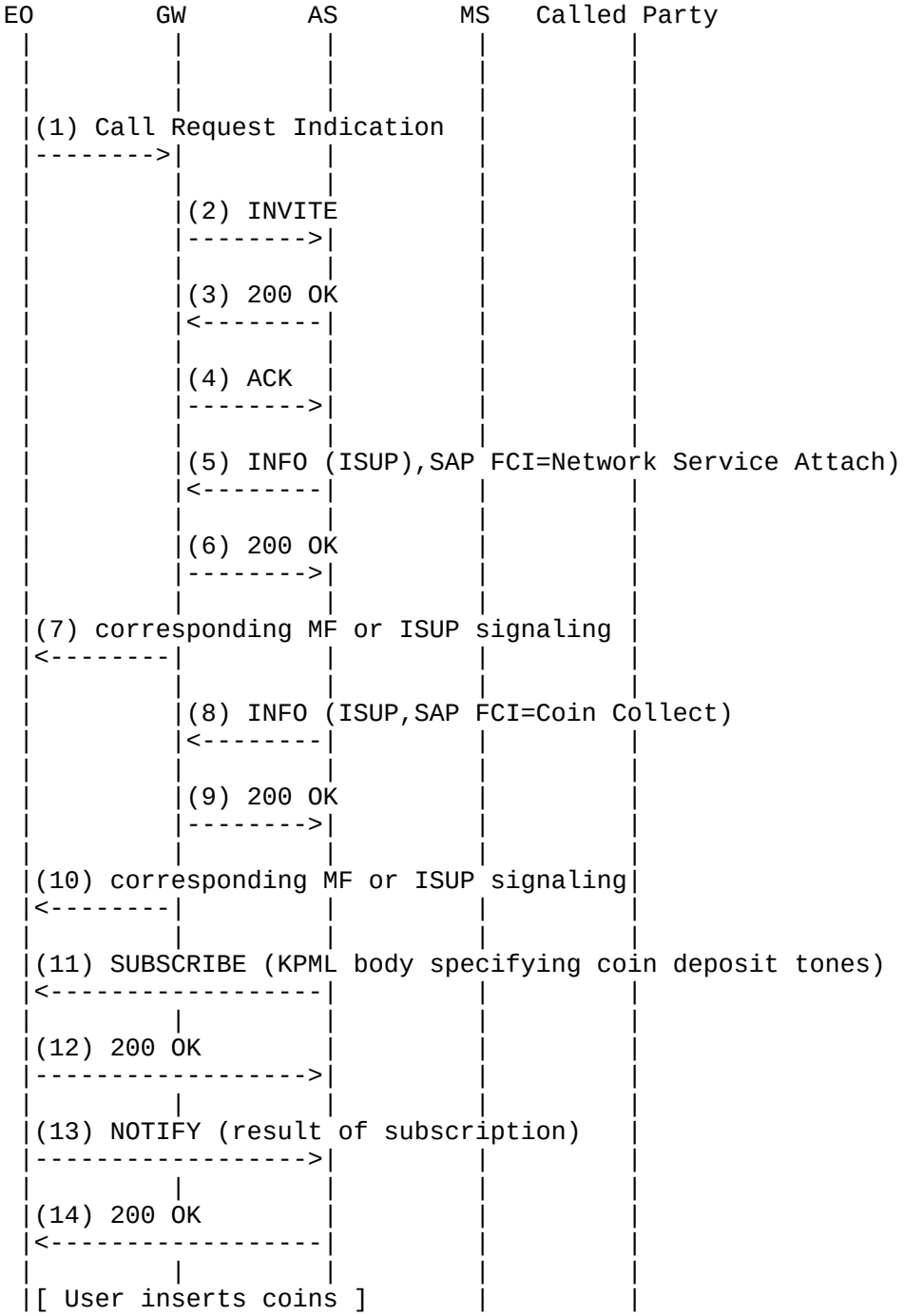
The coin deposits will be signaled as tones over the trunk, so the AS in steps 11 through 14 subscribes to these events at the GW. This example assumes an extension to KPML to support these tones, but the mechanism is the same even if a new event package were defined.

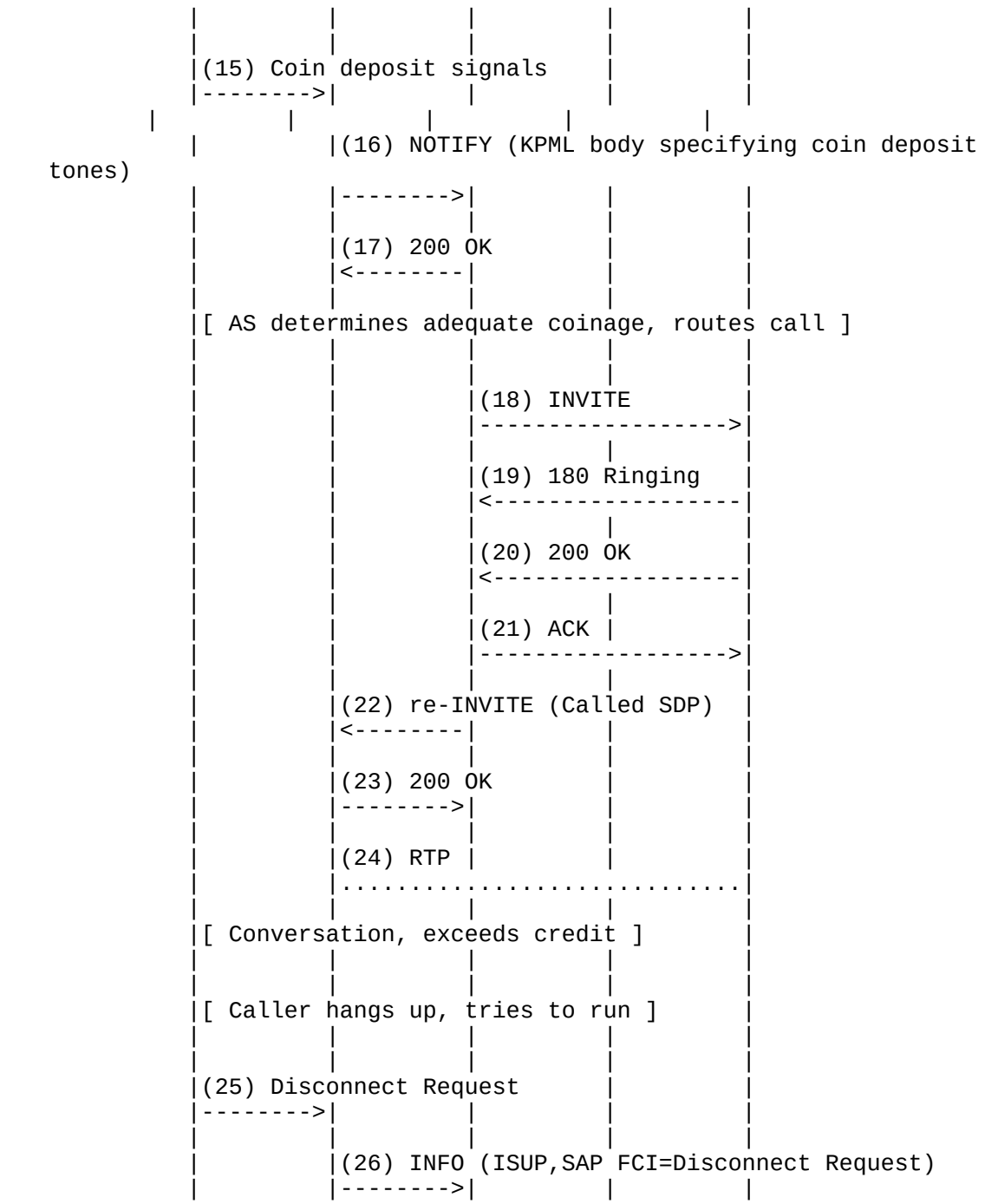
In 15, the user deposits coins into the station, and these events are signaled by the EO to the GW. In step 16, the GW sends SIP NOTIFY messages to the AS for each such event.

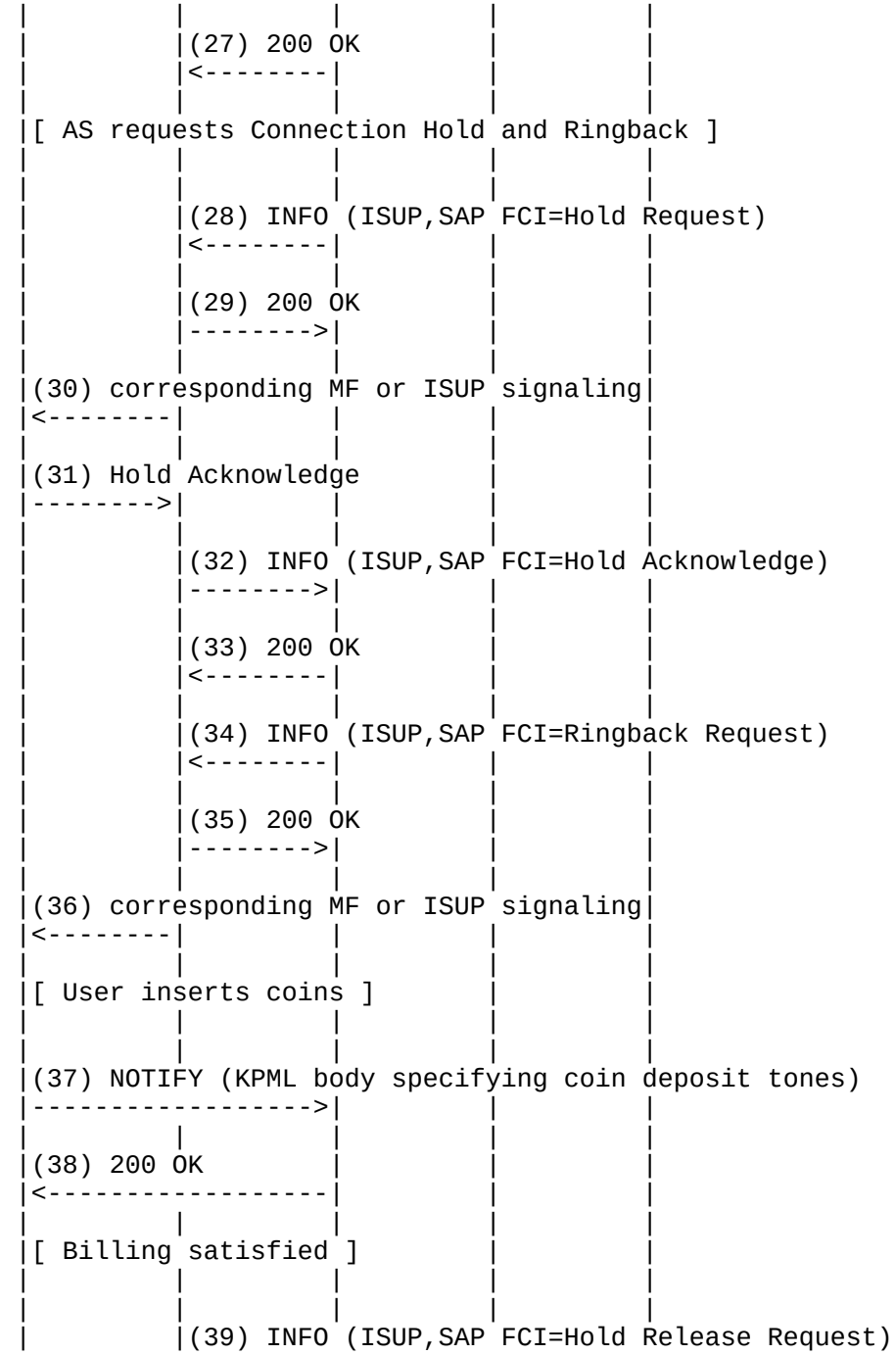
When the AS determines that adequate payment has been collected, it routes the call, as depicted in steps 18 through 24.

In this example, the caller exceeds his credit, and hangs up the phone. This is represented by steps 25 through 27.

Using similar signaling, the OISP sends an Operator Hold and Ringback request toward the station, to "keep the line open" and to ring the station so that the user can be prompted to pay the exceeded credit. This is represented in steps 28 through 36. In this case, the honest user inserts the required coins, and this is signaled to the OISP in steps 39 through 41. From steps 42 on, the line is "released".


EO
GW
AS
MS
Called Party
(1) Call Request Indication
(2) INVITE
(3) 200 OK
(4) ACK
(5) INFO (ISUP),SAP FCI=Network Service Attach)
(6) 200 OK
(7) corresponding MF or ISUP signaling
(8) INFO (ISUP,SAP FCI=Coin Collect)
(9) 200 OK
(10) corresponding MF or ISUP signaling
(11) SUBSCRIBE (KPML body specifying coin deposit tones)
(12) 200 OK
(13) NOTIFY (result of subscription)
(14) 200 OK
[User inserts coins]


(15) Coin deposit signals
(16) NOTIFY (KPML body specifying coin deposit tones)
(17) 200 OK
[AS determines adequate coinage, routes call]
(18) INVITE
(19) 180 Ringing
(20) 200 OK
(21) ACK
(22) re-INVITE (Called SDP)
(23) 200 OK
(24) RTP
[Conversation, exceeds credit]
[Caller hangs up, tries to run]
(25) Disconnect Request
(26) INFO (ISUP,SAP FCI=Disconnect Request)


(27) 200 OK
[AS requests Connection Hold and Ringback]
(28) INFO (ISUP,SAP FCI=Hold Request)
(29) 200 OK
(30) corresponding MF or ISUP signaling
(31) Hold Acknowledge
(32) INFO (ISUP,SAP FCI=Hold Acknowledge)
(33) 200 OK
(34) INFO (ISUP,SAP FCI=Ringback Request)
(35) 200 OK
(36) corresponding MF or ISUP signaling
[User inserts coins]
(37) NOTIFY (KPML body specifying coin deposit tones)
(38) 200 OK
[Billing satisfied]
(39) INFO (ISUP,SAP FCI=Hold Release Request)

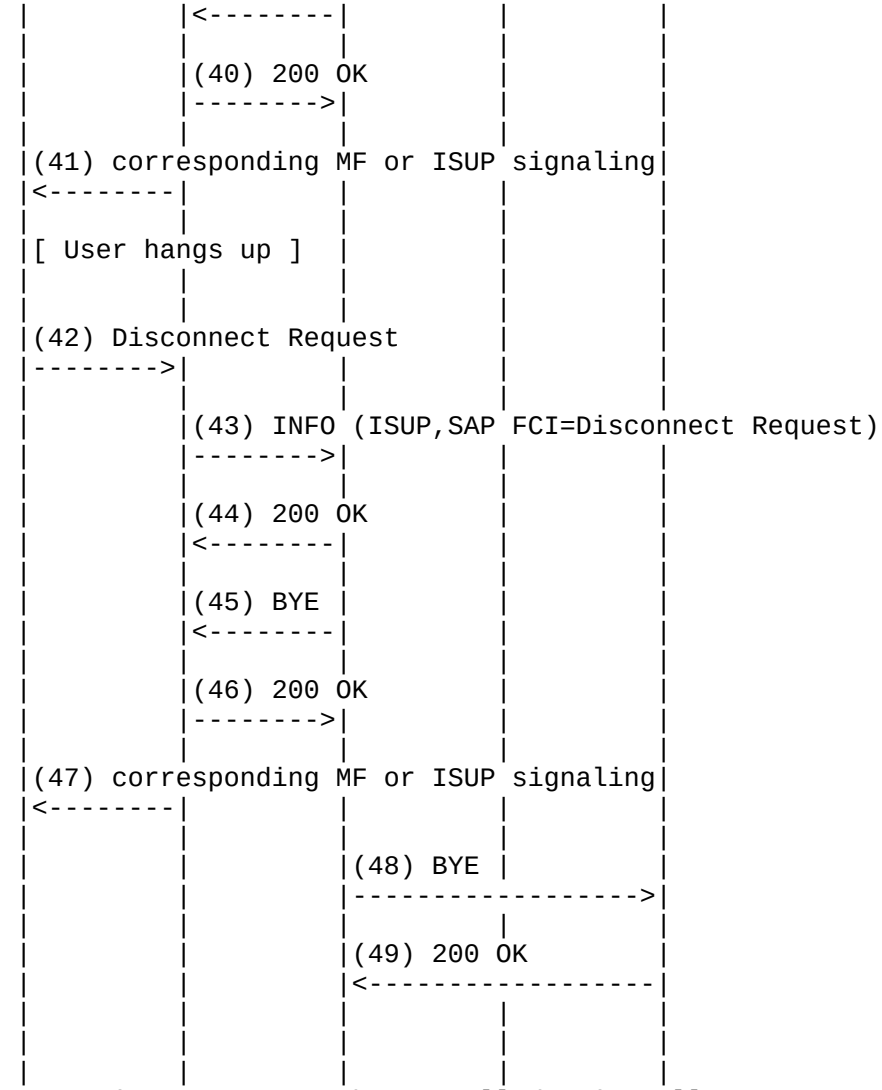


Figure 19 Network Controlled Coin Call

11.2. Busy Line Verification and Interrupt

An existing PTSN service is Busy Line Verification and Interrupt. In the Busy Line Verification (BLV) Service, a customer obtains

operator assistance to determine if a called line is in use. In Operator Interrupt Service, the operator provides a BLV Service and, if requested by the caller, interrupts a conversation in progress and relays a message. If the interrupted party is willing to hang up, the call can be reoriginated by the caller to the called party. At the caller's request, the connection between the caller and the called party can be reinitiated and handled by the operator as a Call Completion Service.

11.2.1. PSTN Target

Currently, BLV/I is handled by the Operator Services System placing calls via special BLV/I trunk toward the target. Use of this type of trunk results in the Operator Services System being able to monitor a scrambled version of the target's conversation, and being able to barge in to speak to the target. In this document, the focus of BLV/I toward a PSTN target is on having the OIS components such as OWS and AS be able to communicate with the EO via BLV/I trunks. For IP targets, SIP capabilities are used.

The following figure depicts a BLV/I call to a PSTN target. In steps (1) through (8) the caller is routed to an AS which performs 3PCC to connect this caller to an operator workstation.

The operator determines the user's request, and initiates (9) a call toward the target via a BLV/I trunk. Ensuring that the call is routed via the correct type of trunk can be handled the same using SIP as in the PSTN; that is, by prepending specified routing digits to the target number. The operator is bridged by the EO onto the target's line, during which time no voice is sent toward the caller. A one way connection can be explicitly signaled, or the operator workstation can simply not send RTP at this time. The operator workstation or GW implements a scrambler so that only the presence or absence of speech can be determined, and the operator then reports to the caller on the status. If there is speech, then the operator reports that the line is busy, and may offer to interrupt the caller.

If this is desired, the operator removes the scrambler, and indicates to the target of the caller's desire to call them, and drops off. The operator informs the caller of the result, and drops the caller, who may then re attempt the call. The option where the OISP offers the call as a call completion service is not shown here, but this poses no unique requirements with respect to call completion.

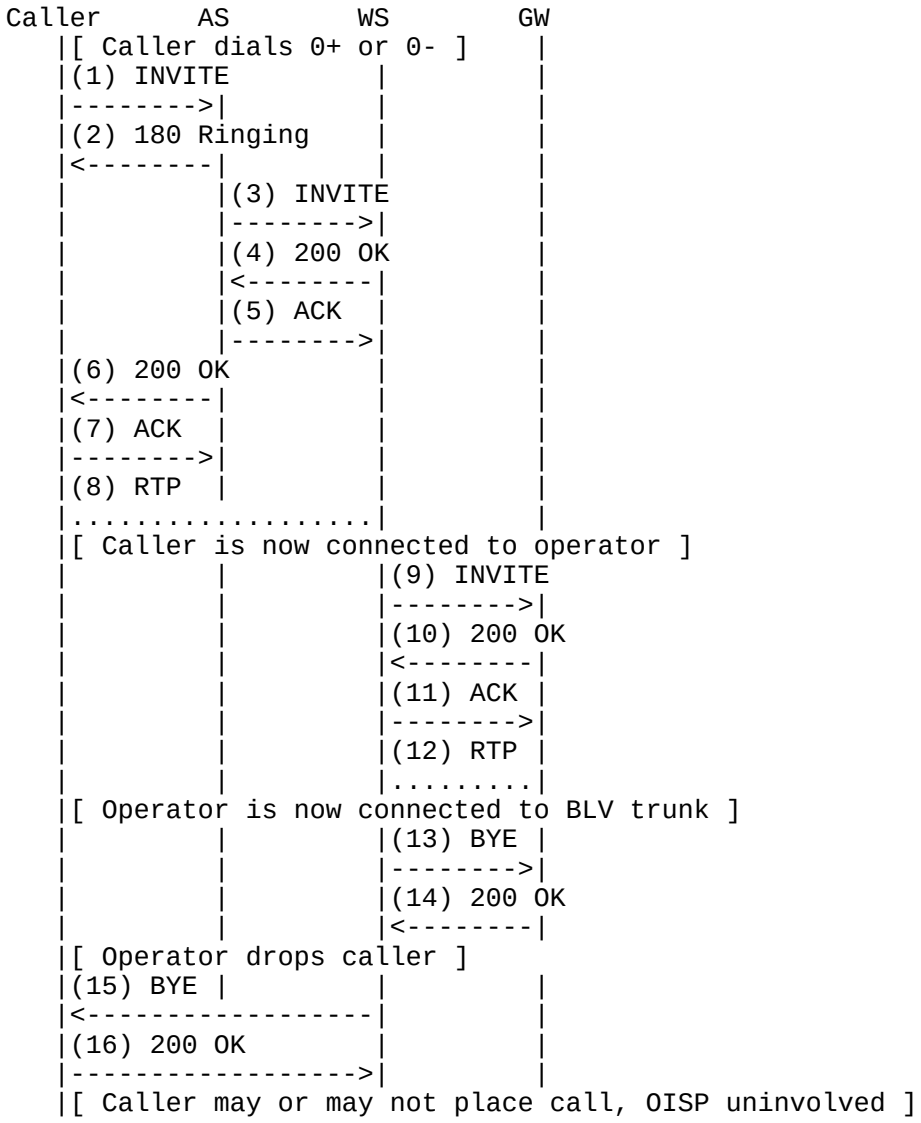


Figure 20 BLV/I to PSTN Target

11.2.2. SIP Target

The following depicts a BLV/I call to a SIP target. Note that this is included mainly for completeness. The characteristics of POTS based subscribers support such a service, but many of those characteristics may not be applicable to SIP based endpoints. POTS access can carry only a single call at a time; as a packet switched technology SIP does not share this inherent restriction. There is typically a strong association between a physical POTS line and the address (phone number) used to reach it, while a SIP address of record is a logical address which can be registered with various endpoints, even simultaneously. Also, attempts towards such a set of devices can be tried in sequence or in parallel; thus the same concept of "busy" does not carry directly from POTS access to SIP. The ambiguity of "busy" may also have impacts on the "interrupt" aspect of this service.

The approach detailed here is based on that described in the PacketCable Residential SIP Telephony Feature Specification, [RST]. The main aspects of this approach include using the Event dialog package [RFC4235] to determine whether the device has an active call, and using the Join header in order to bridge onto the current conversation for monitoring and interrupting the user. Additional aspects include the operator workstation performing the scrambling function, and the use of a preconfigured network asserted workstation identity from which the user device must accept and process the BLV/I related requests.

Steps 1 through 8 represent an incoming call to the OISP being connected to an operator workstation. The operator interacts with the caller and determines the BLV/I request.

In steps 9 through 12, the operator workstation subscribes to the Dialog event package at the target party’s UA, and receives a NOTIFY identifying any active dialogs.

In 13 through 16, the workstation sends an INVITE with a Join header [RFC3911] to bridge onto the active call. The INVITE includes a P-Asserted-Identity value corresponding to the value prearranged between the OISP and the target’s home provider. The user devices are configured to accept SUBSCRIBEs for Dialog event package and INVITEs with the Join header when the P-Asserted-Identity contains this value. Thus, the user device accepts the Join header. Initially, the workstation acts in a receive only mode, and further, implements an audio scrambler such that speech is distinguishable as such, but is non intelligible. Thus the operator can determine whether the person at the target device is in active conversation.

During this time, the workstation does not exchange media with the caller, who may be put on hold (not show here).

The operator can then report the status to the caller, and offer the Interrupt service. If accepted, the scrambling function is removed from the voice path between operator and target, and the operator "barges in" on the conversation, informs the target party of the caller’s request, and asks whether the target would like to accept the call. The operator can then drop the session with the target and inform the caller about the target’s response. There is of course no guarantee of the target’s or caller’s subsequent actions.

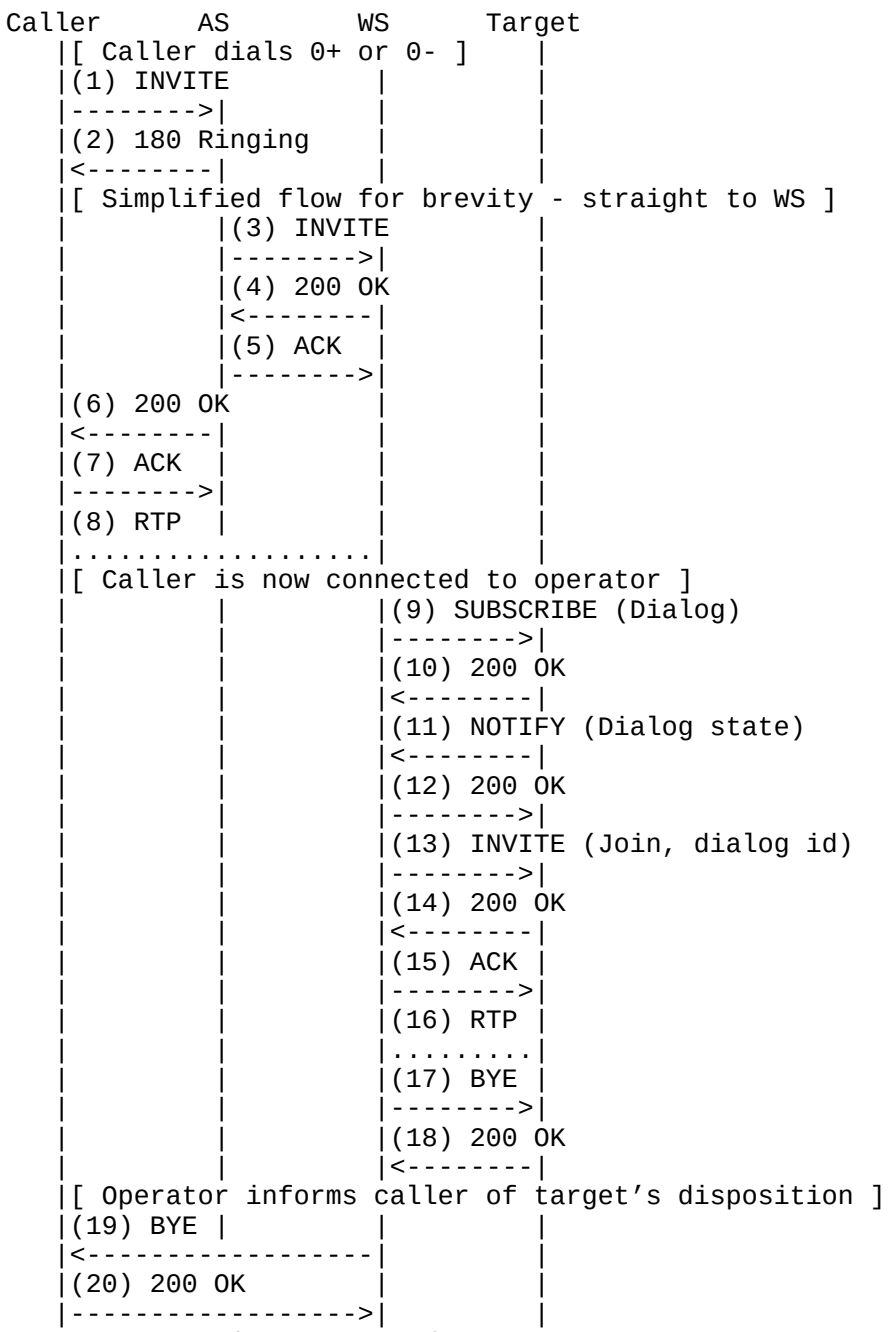


Figure 21 BLV/I to SIP Target

11.3. Inward Calls

Typically, operator services are provided by the OISP serving a user's originating provider. In some cases, another OISP must be involved. One example is BLV/I, where an OISP can only invoke BLV/I for targets served by providers that the OISP serves. In the case of a caller desiring to invoke BLV/I to a target served by a different provider, the caller's request would be routed to the same OISP as usual. That OISP would identify the OISP serving the target, and initiate an "inward" call to an operator in that OISP, and request that operator to perform the BLV/I. For this feature, the initiating OISP acts as the caller to the OISP serving the target. Currently, Inward calls are originated by operators at operator workstations, and terminated to operators at operator workstations.

Inward calls need to be distinguishable from calls from subscribers that are routed to operators. Further, inward calls should be accepted only from other OISPs, never from subscribers, and only from those OISPs with appropriate business relationships.

The request should be screened based on the identity of originator. Since the From header can easily be spoofed, a network-asserted identity should be used for this. Within trust domains that use the P-Asserted-Identity [RFC3325] header as a network asserted identity, this header should be used for this purpose. Alternatively, the SIP Identity mechanism [RFC4474] can be used in domains where this is used for network asserted identity. Rather than maintain lists of every possible URI for which Inward requests are allowed, the decision could be based on the domain in the SIP URI. Requests from domains corresponding only to OISPs which are authorized to make Inward requests would be accepted.

In the current North American PSTN, the digits dialed by the operator placing Inward call can be used to identify the type of service being requested, so that the destination OISP can properly handle the request. These digits are known as Operator Special Dialed Code (OSDC) digits. Thus, the Request-URI should include the OSDC digits, and the AS should populate the Request-URI as a SIP URI which includes the SIP domain of the destination OISP as well as the OSDC code.

For Inward calls to PSTN based OISPs, the call should be placed via a PSTN gateway, and should appear to the destination OISP the same as any other Inward call.

11.4. Intercept

Intercept service provides the capability for a customer to be informed that a working number is no longer in service or why a working number is no longer in service. Basically, it provides announcements to the caller, which may be fixed or dynamic. Currently in the North American PSTN, Intercept may be handled by individual end offices, or may be sent to Operator Services Systems, which have specialized resources for handling such requests. When a call reaches a PSTN switch for a number which requires Intercept treatment, that switch, known as the "intercepted switch", initiates an Intercept request for that "intercepted number". The request to an OISP specifies the intercepted number, and an "intercept type", which provides an indication of the general reason for intercept. Often, the OISP needs to consult an "intercept database" to determine specific processing for a particular intercepted number.

Currently, with MF, dedicated Intercept trunk groups are typically used, so the call is implicitly identified as such. The ANI digits identify the intercepted number, and the II digits identify the intercept type. For ISUP, dedicated trunk groups may or may not be used, but the SAP parameter identifies the intercept type, and the Called Party Number parameter identifies the intercepted number. In both cases, the key information conveyed include identification of the request as intercept, intercept type, and intercepted number.

11.4.1. Intercept Request Via SIP

Intercept requests to a SIP based OISP need to convey the same information currently conveyed. Such requests can be treated as a call forwarded to an Intercept service. Thus, the Request-URI should identify the request as Intercept, as well as conveying the intercept type. The currently defined values for intercept type include regular, blank, and trouble. Prepending these with "intercept-" in the left hand side of the Request-URI unambiguously identifies the request as intercept and conveys the intercept type. Treating this as a redirection, the SIP History-Info header can be used to convey the intercepted number. An example of such an INVITE (relevant fields only) follows:

```
INVITE sip:intercept-trouble@oisp-c.example.com SIP/2.0
From: <sip:7327581111@provider-a.example.com>;tag=1234567
To: <sip:7327582222@provider-b.example.com>
History-Info: <sip:7327582222@provider-b.example.com>; index=1
Content-Type: application/sdp
Content-Length: ...
```

Upon receiving such a request, the AS would typically perform any required processing, including database lookups, and generate a request to a MS to play the specified announcement. The conventions described in [RFC4240] can be used for this.

An example high level message flow follows:

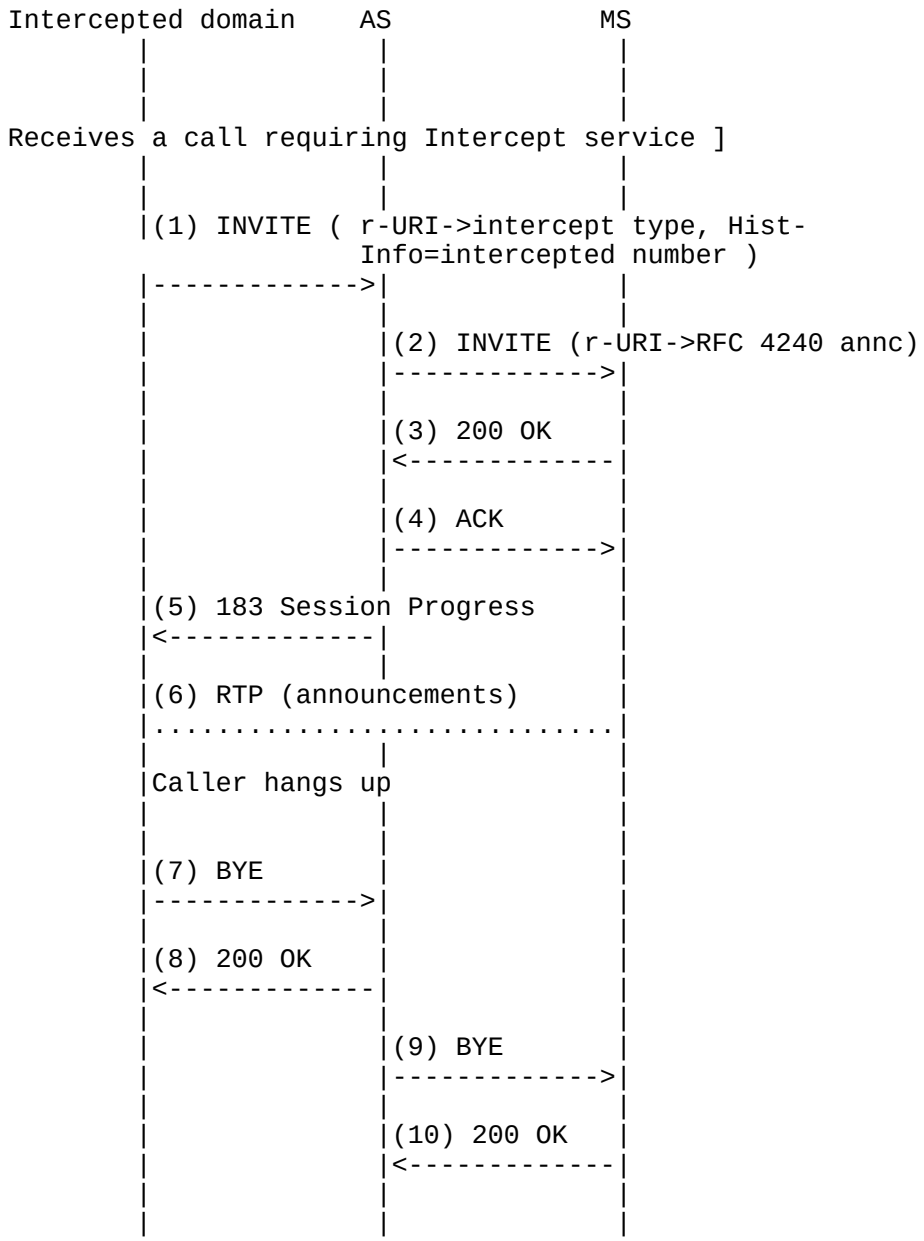
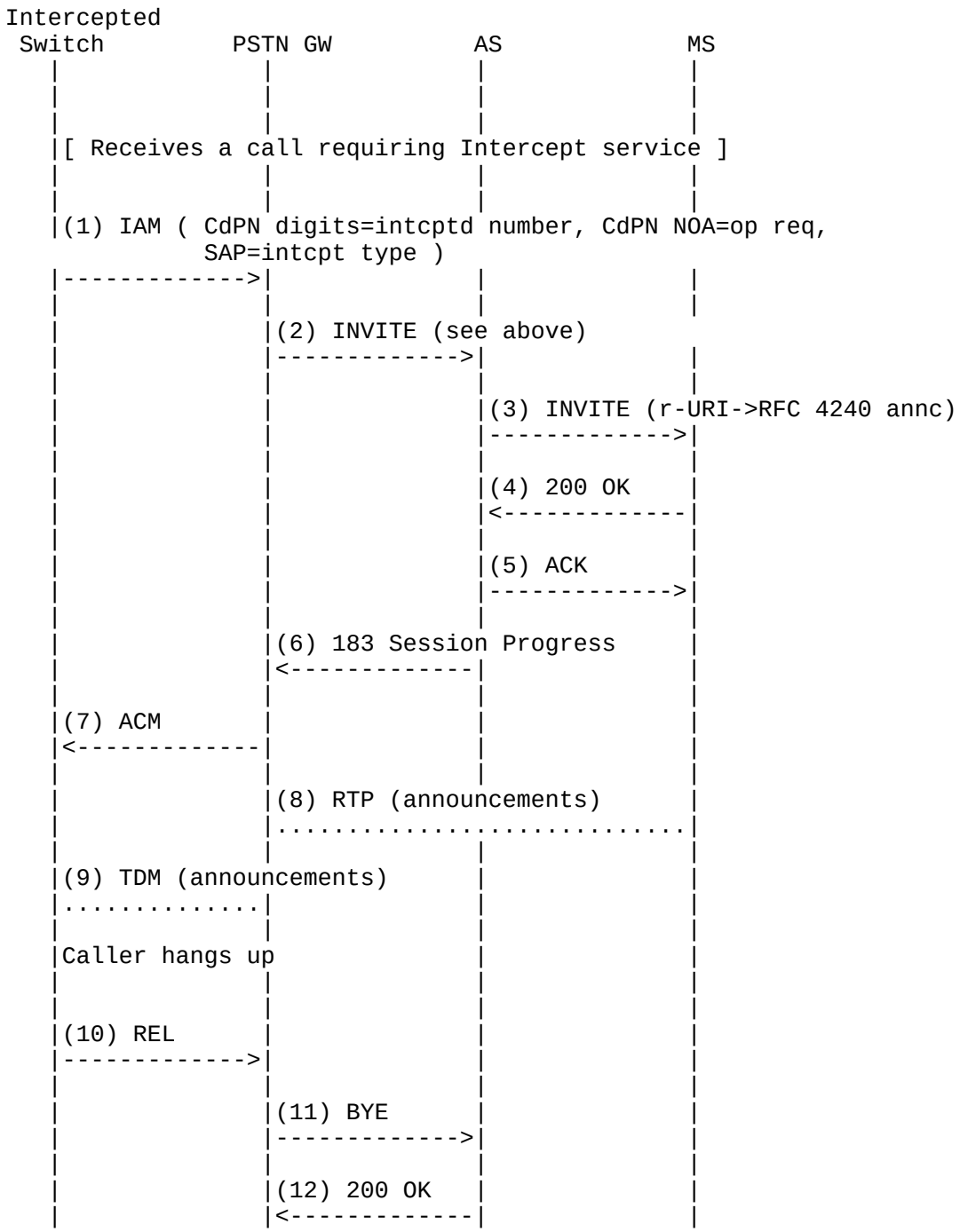


Figure 22 Intercept Request Via SIP

11.4.2. Intercept Request Via PSTN

When intercept requests are received from PSTN interfaces, the PSTN gateway needs to translate the incoming signaling to SIP. The preferred approach is to have the PSTN gateway construct an INVITE request of the form described above for requests received via SIP. This method requires additional functionality on the part of the gateway, but the AS only needs to recognize one type of INVITE request for Intercept.

Alternatively, the gateway could construct an INVITE containing encapsulated ISUP, in which the Called Party Number and SAP fields are most significant. Also, the Request-URI should contain the Called Party Number. With this method, the PSTN gateway treats the INVITE the same as other INVITEs, but requires the AS to recognize this as an Intercept request by examining the encapsulated ISUP body contents.


Intercepted Switch
PSTN GW
AS
MS
[Receives a call requiring Intercept service]
(1) IAM (CdPN digits=intcptd number, CdPN NOA=op req, SAP=intcpt type)
(2) INVITE (see above)
(3) INVITE (r-URI->RFC 4240 annc)
(4) 200 OK
(5) ACK
(6) 183 Session Progress
(7) ACM
(8) RTP (announcements)
(9) TDM (announcements)
Caller hangs up
(10) REL
(11) BYE
(12) 200 OK

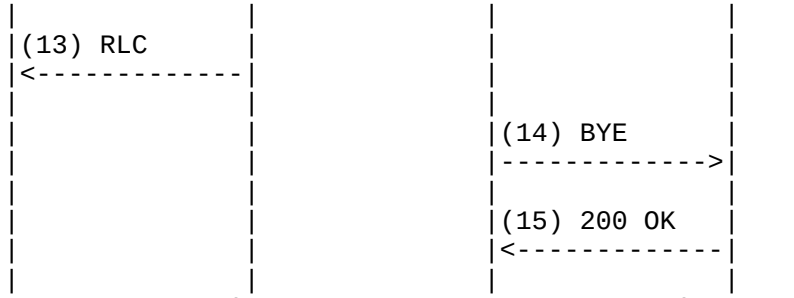
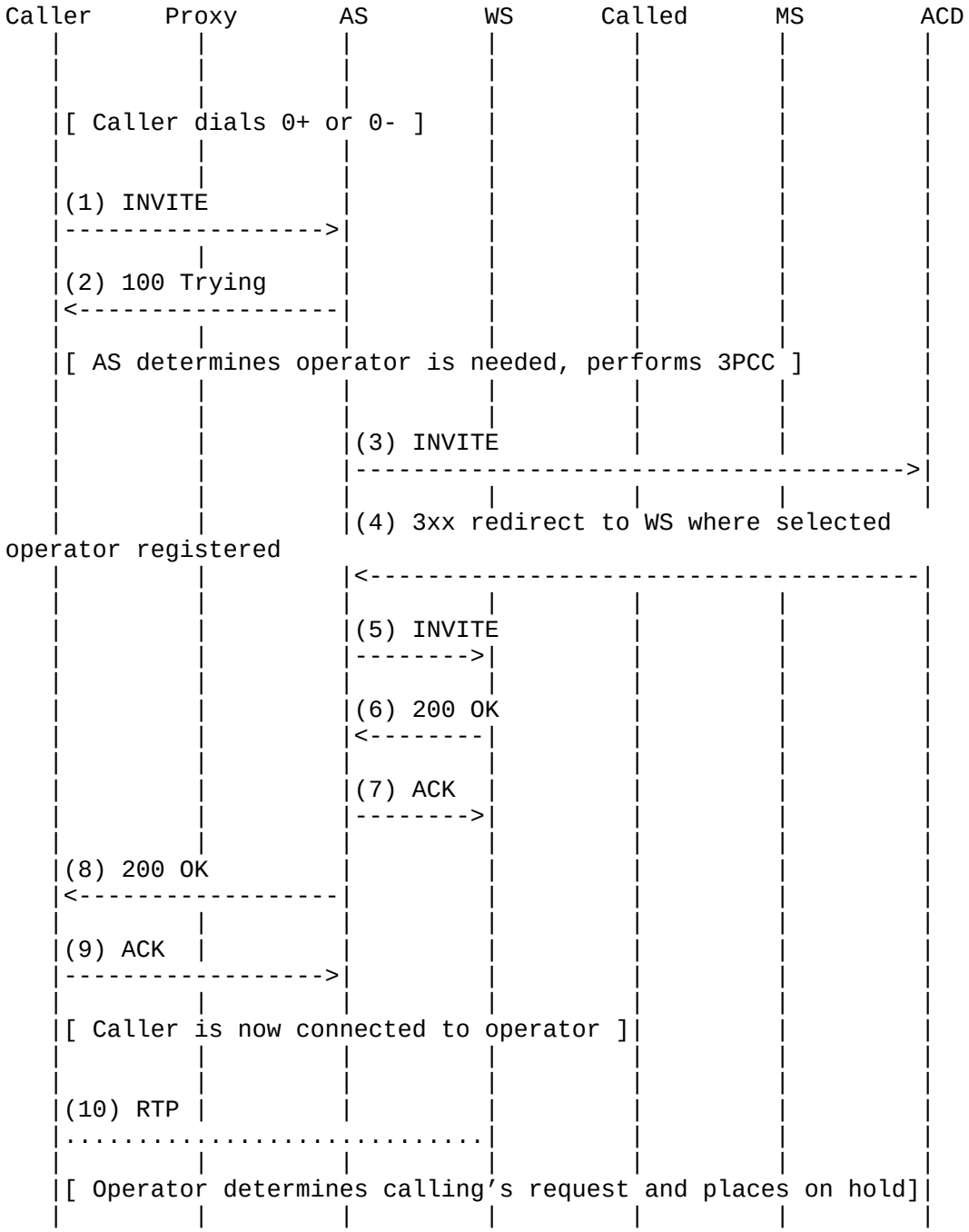
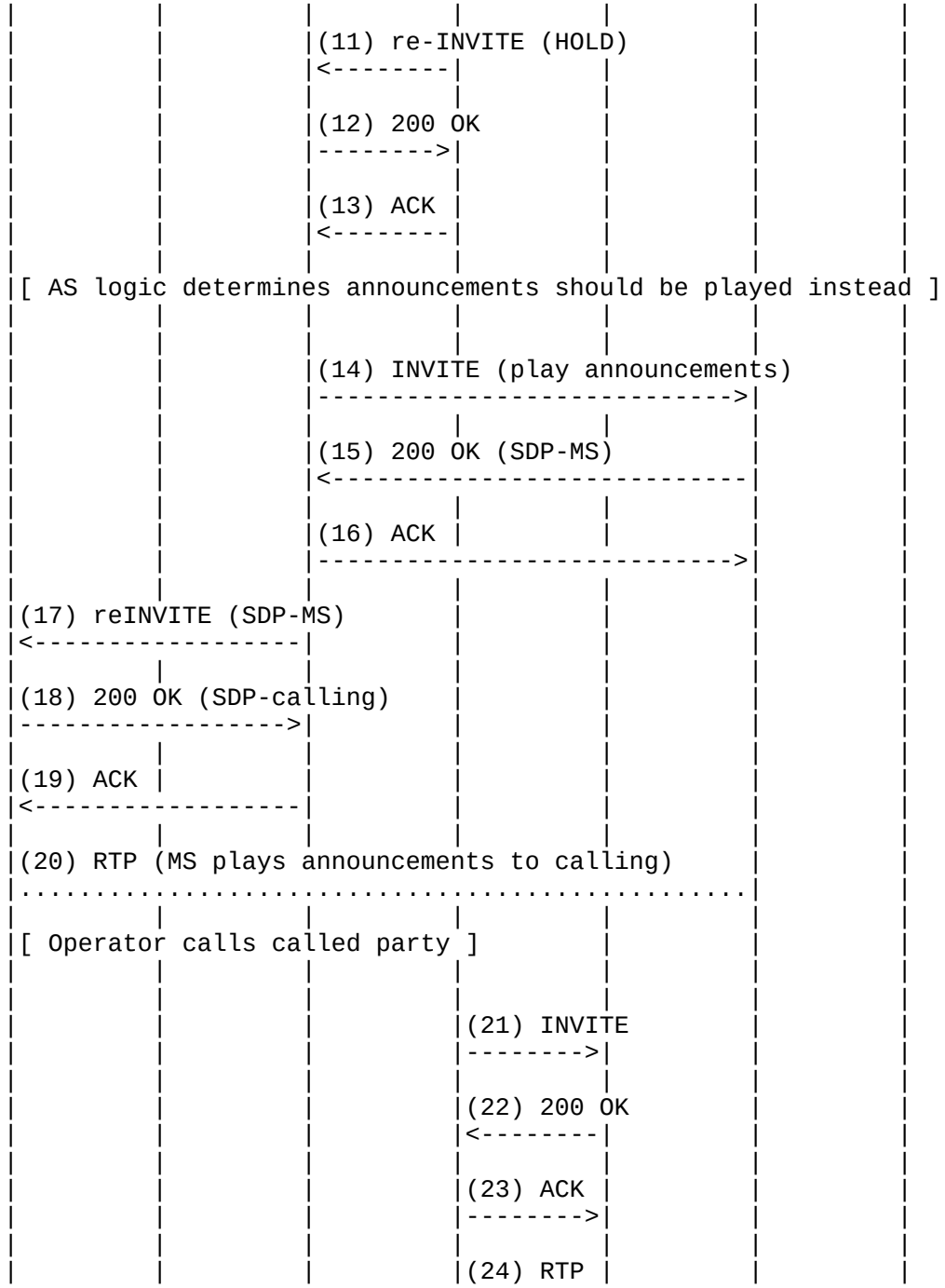


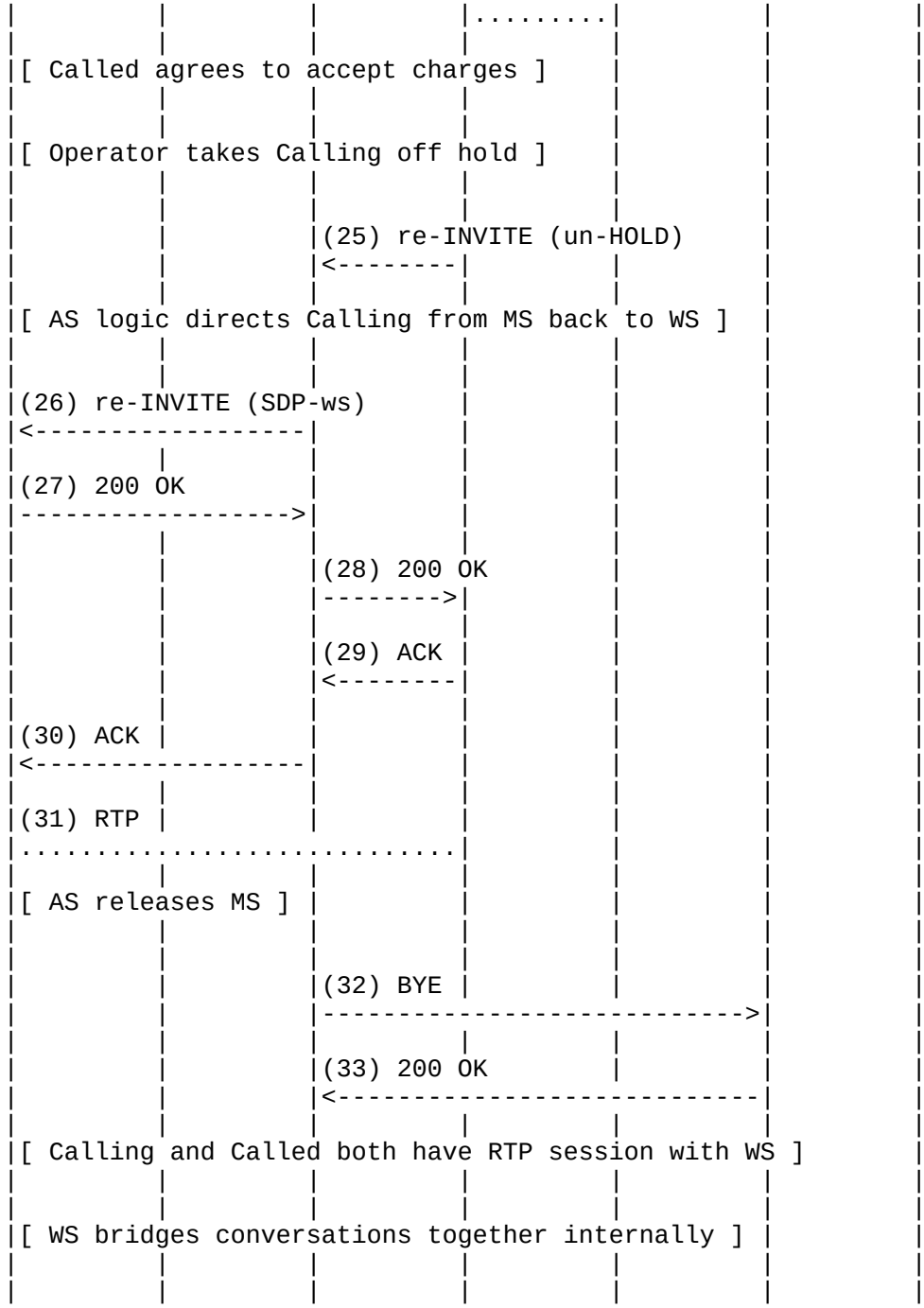
Figure 23 Intercept Request Via PSTN

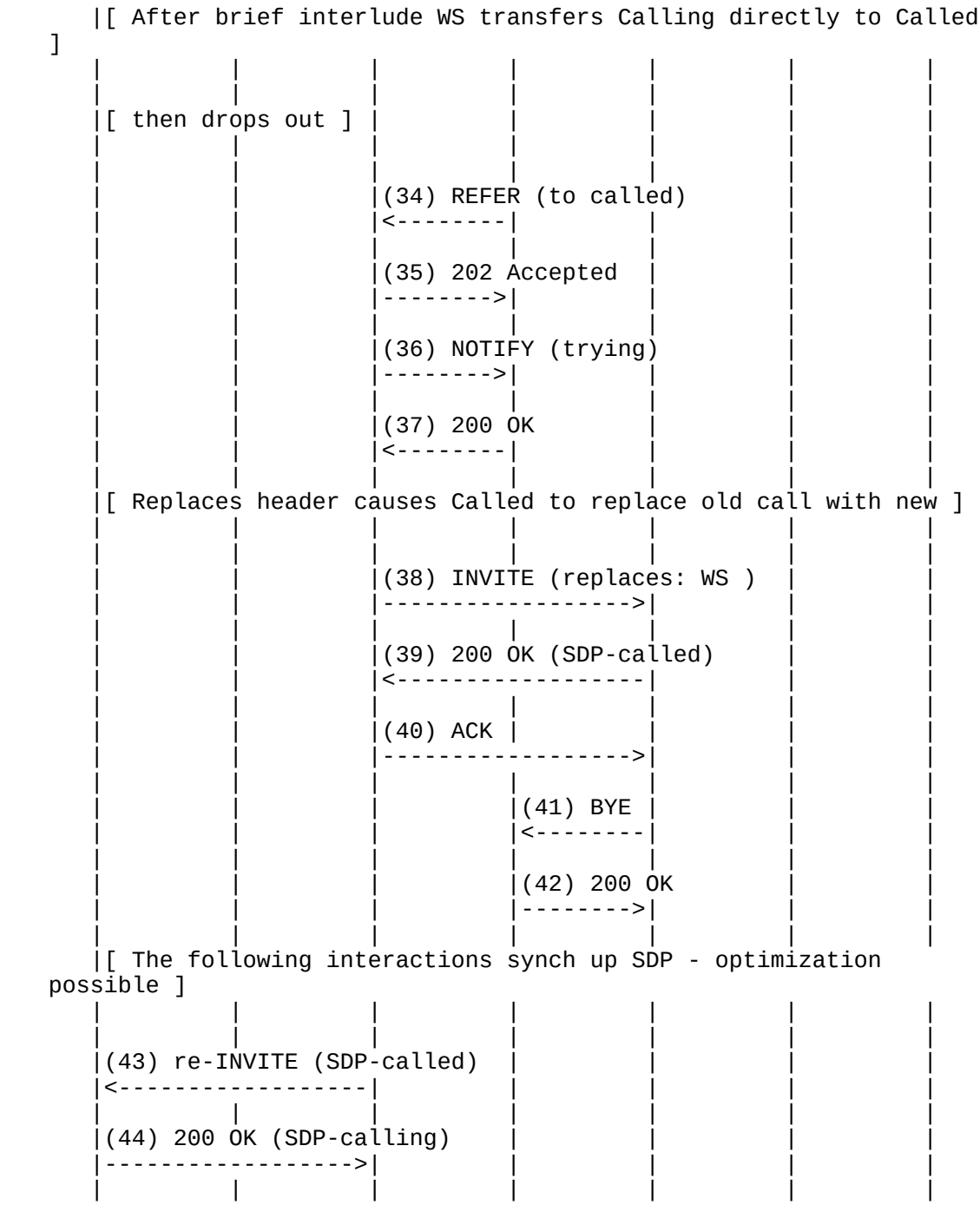
11.5. Operator Assisted Collect Call

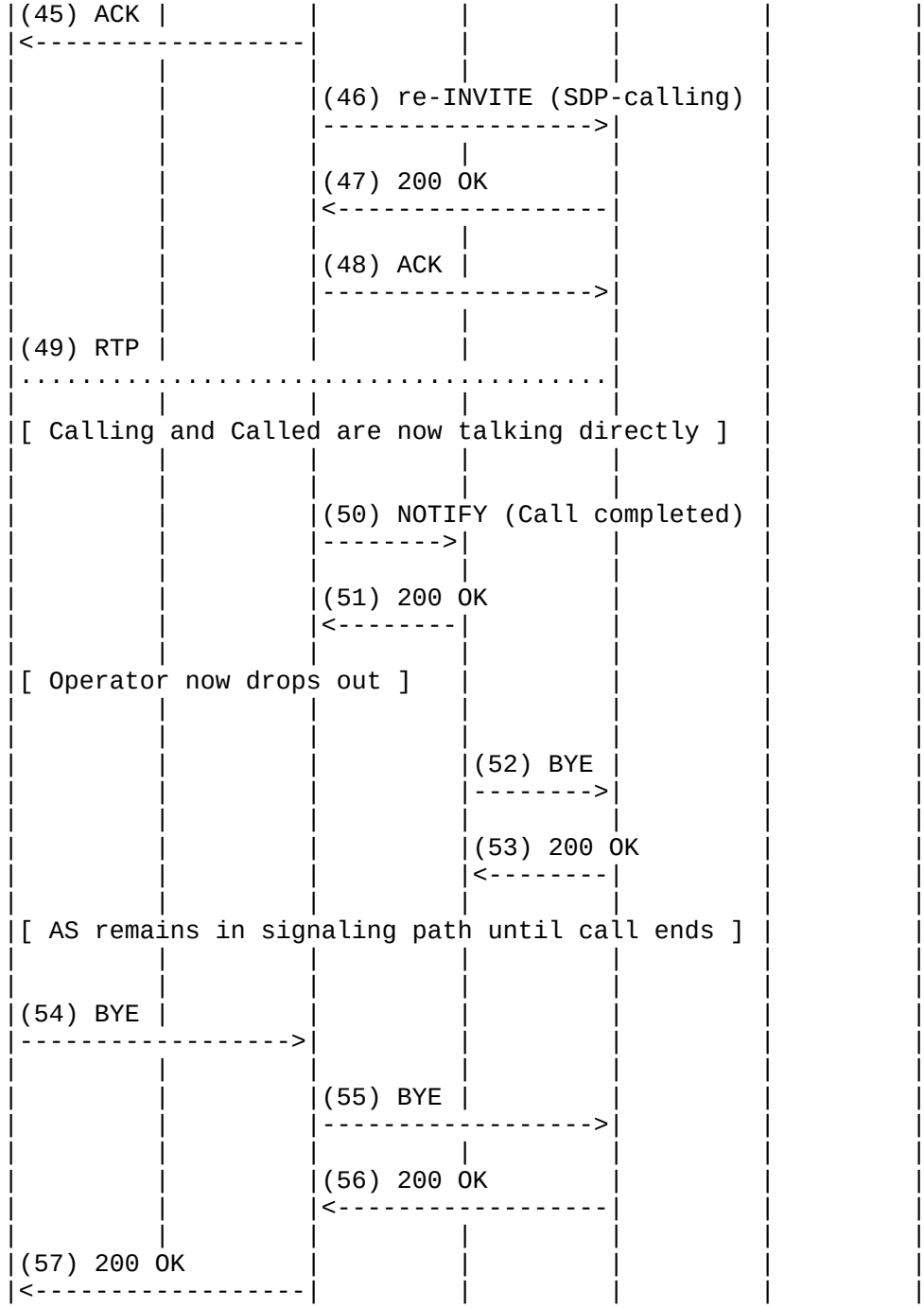
The following call flow provides examples of how a specific operator service, Operator Assisted Collect Call, could be implemented using the mechanisms described in this document. The purpose is to illustrate one way to implement this service using the proposed signaling mechanisms. In practice, this particular service could be implemented in an automated fashion without human intervention.


Caller
Proxy
AS
WS
Called
MS
ACD
[Caller dials 0+ or 0-]
(1) INVITE
(2) 100 Trying
[AS determines operator is needed, performs 3PCC]
(3) INVITE
(4) 3xx redirect to WS where selected operator registered
(5) INVITE
(6) 200 OK
(7) ACK
(8) 200 OK
(9) ACK
[Caller is now connected to operator]
(10) RTP
[Operator determines calling's request and places on hold]


(11) re-INVITE (HOLD)
(12) 200 OK
(13) ACK
[AS logic determines announcements should be played instead]
(14) INVITE (play announcements)
(15) 200 OK (SDP-MS)
(16) ACK
(17) reINVITE (SDP-MS)
(18) 200 OK (SDP-calling)
(19) ACK
(20) RTP (MS plays announcements to calling)
[Operator calls called party]
(21) INVITE
(22) 200 OK
(23) ACK
(24) RTP


[Called agrees to accept charges]
[Operator takes Calling off hold]
(25) re-INVITE (un-HOLD)
[AS logic directs Calling from MS back to WS]
(26) re-INVITE (SDP-ws)
(27) 200 OK
(28) 200 OK
(29) ACK
(30) ACK
(31) RTP
[AS releases MS]
(32) BYE
(33) 200 OK
[Calling and Called both have RTP session with WS]
[WS bridges conversations together internally]


[After brief interlude WS transfers Calling directly to Called]
[then drops out]
(34) REFER (to called)
(35) 202 Accepted
(36) NOTIFY (trying)
(37) 200 OK
[Replaces header causes Called to replace old call with new]
(38) INVITE (replaces: WS)
(39) 200 OK (SDP-called)
(40) ACK
(41) BYE
(42) 200 OK
[The following interactions synch up SDP - optimization possible]
(43) re-INVITE (SDP-called)
(44) 200 OK (SDP-calling)


(45) ACK
(46) re-INVITE (SDP-calling)
(47) 200 OK
(48) ACK
(49) RTP
[Calling and Called are now talking directly]
(50) NOTIFY (Call completed)
(51) 200 OK
[Operator now drops out]
(52) BYE
(53) 200 OK
[AS remains in signaling path until call ends]
(54) BYE
(55) BYE
(56) 200 OK
(57) 200 OK

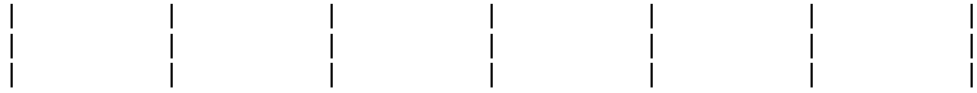


Figure 24 Operator Assisted Collect Call

The caller initiates the call by dialing 0+ or 0-.

The call is routed to the AS. The AS examines the calling party number and calling party's home provider, which are derived from the P-Asserted-Identity header. The charge number is also needed, in case the caller's service is determined by agreements with another party, such as the caller's employer. The employer may have a large number of calling identities representing its employees, which are covered under its agreement with the OISP. Rather than provision every possible calling number/identity with the OISP (and this may be constantly changing), the ability to pass a charge number would allow the OISP to determine whether this charge number has any associated treatment on a per charge number basis.

In any case, in our example, the AS examines the request and determines that the call is for an operator assisted collect call. Typically a MS could be initially connected to prompt the user for the type of call. This step is omitted in this example.

The AS performs third party call control (3PCC). It sends a 18x response towards the caller. It needs to initiate a call leg to an operator workstation. It populates the selection criteria in an INVITE message (the exact mechanism for this is under study) which it sends to the ACD server in (3). The ACD server identifies the best match available operator and returns the contact information for the workstation where that operator is currently registered in a 3xx redirection response.

In (5) the AS sets up a call to the workstation identified by the ACD server, and using 3PCC connects the caller to the WS, resulting in an RTP session in (10).

The operator determines the caller's requested number, and sends an INVITE toward the AS to put the caller on hold. The logic in the AS determines that instead the caller should be connected to custom announcements, and in (14) through (20) creates a session between the caller and a MS.

Meanwhile, in (21) the WS places a call to the called party, and asks whether the called party would accept the charges for a collect call. In this example, the called party agrees to the request.

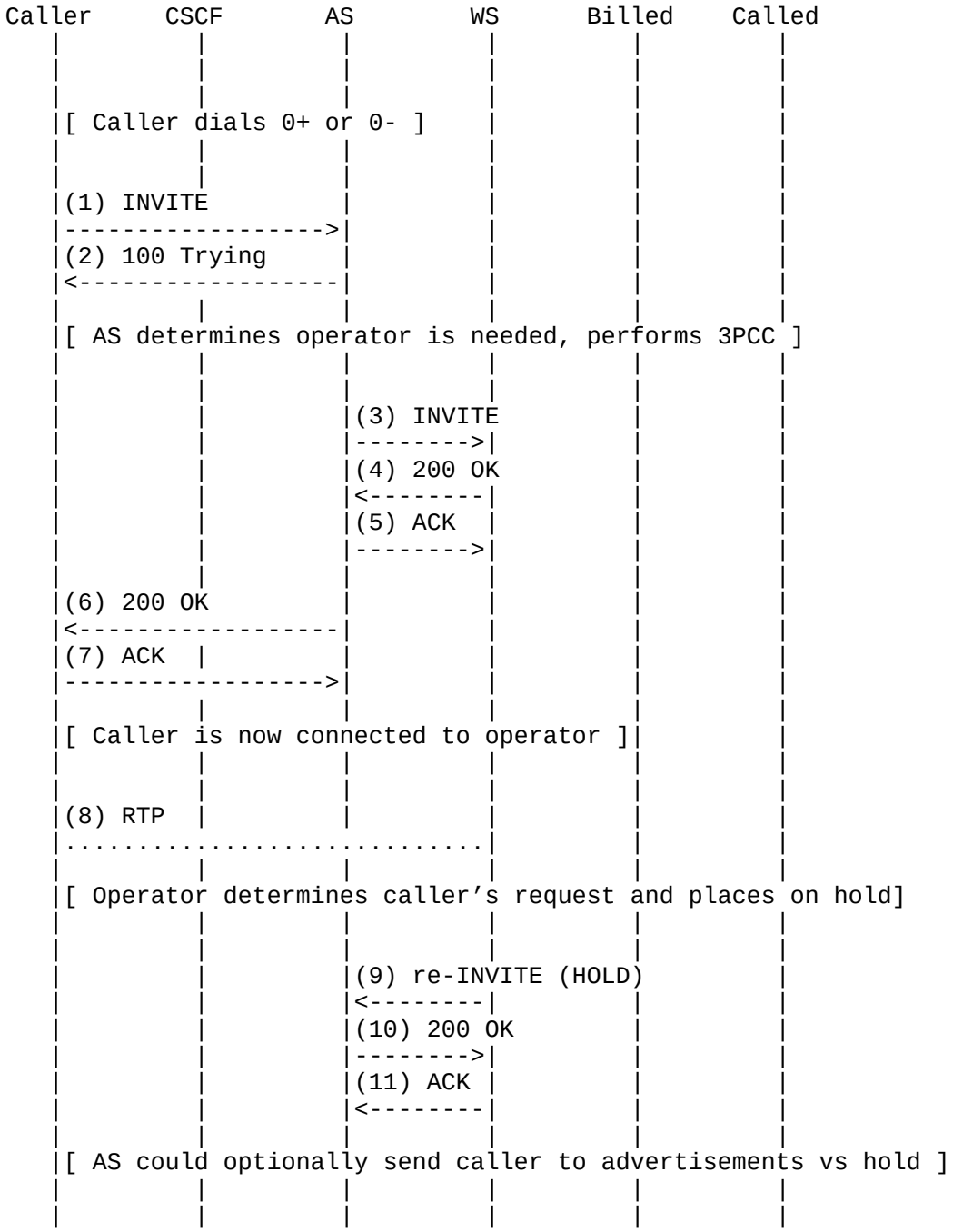
In (25), the operator takes the caller off hold (recall that it believes it has placed the caller on hold). The AS, in (26) through (33), performs 3PCC, and removes the caller from the MS which is playing custom announcements, and reconnects the caller back to the WS. The WS uses its own internal bridging functionality to conference the operator, calling, and called parties.

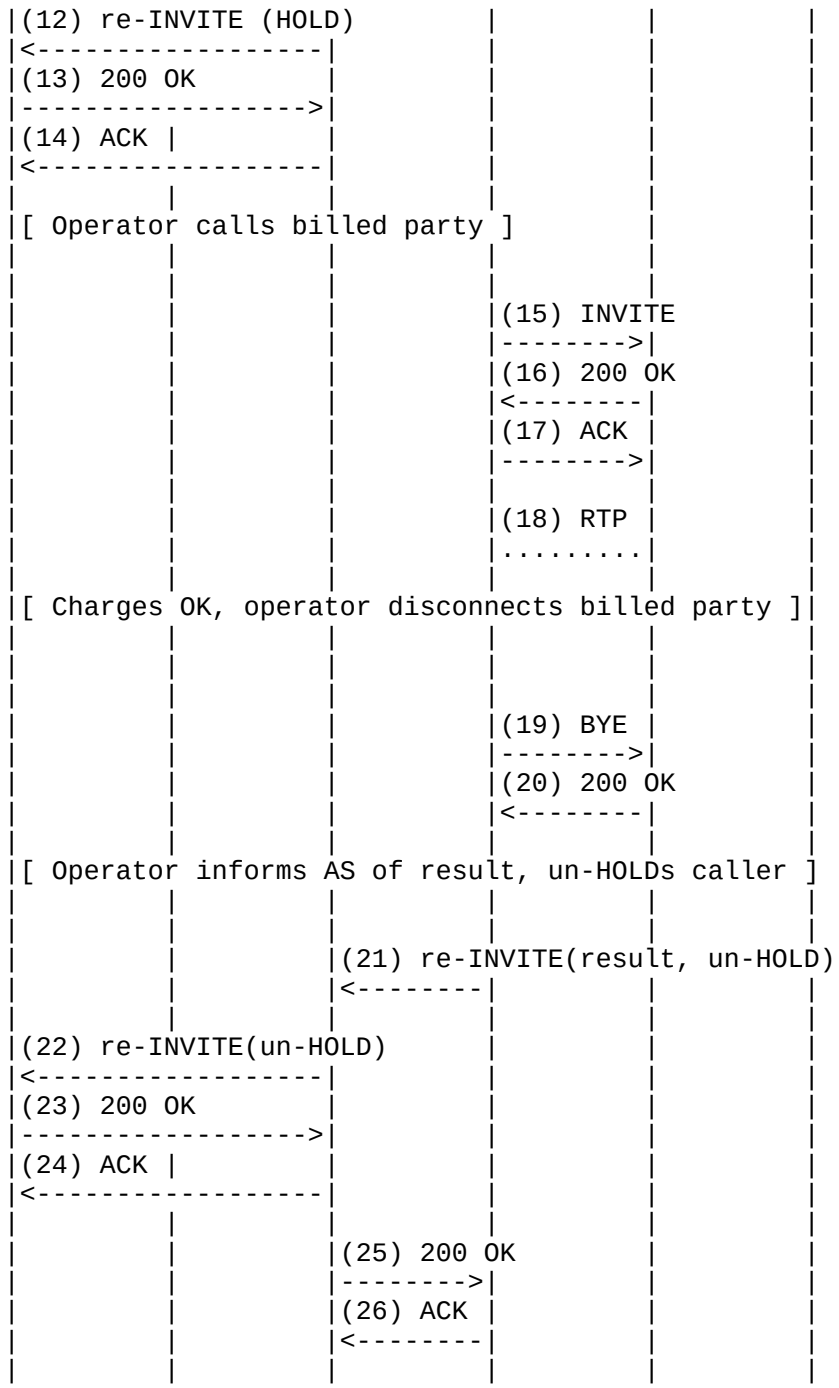
After a brief interlude, the operator initiates a transfer of the calling and called parties directly together using a REFER in (34) through (37). The AS, performing 3PCC, utilizes the SIP Replaces mechanism beginning in (38) to complete the transfer. When the transfer is complete, the operator drops out completely. Note that the AS, performing 3PCC, remains in the signaling path until the call is torn down in (54) through (57).

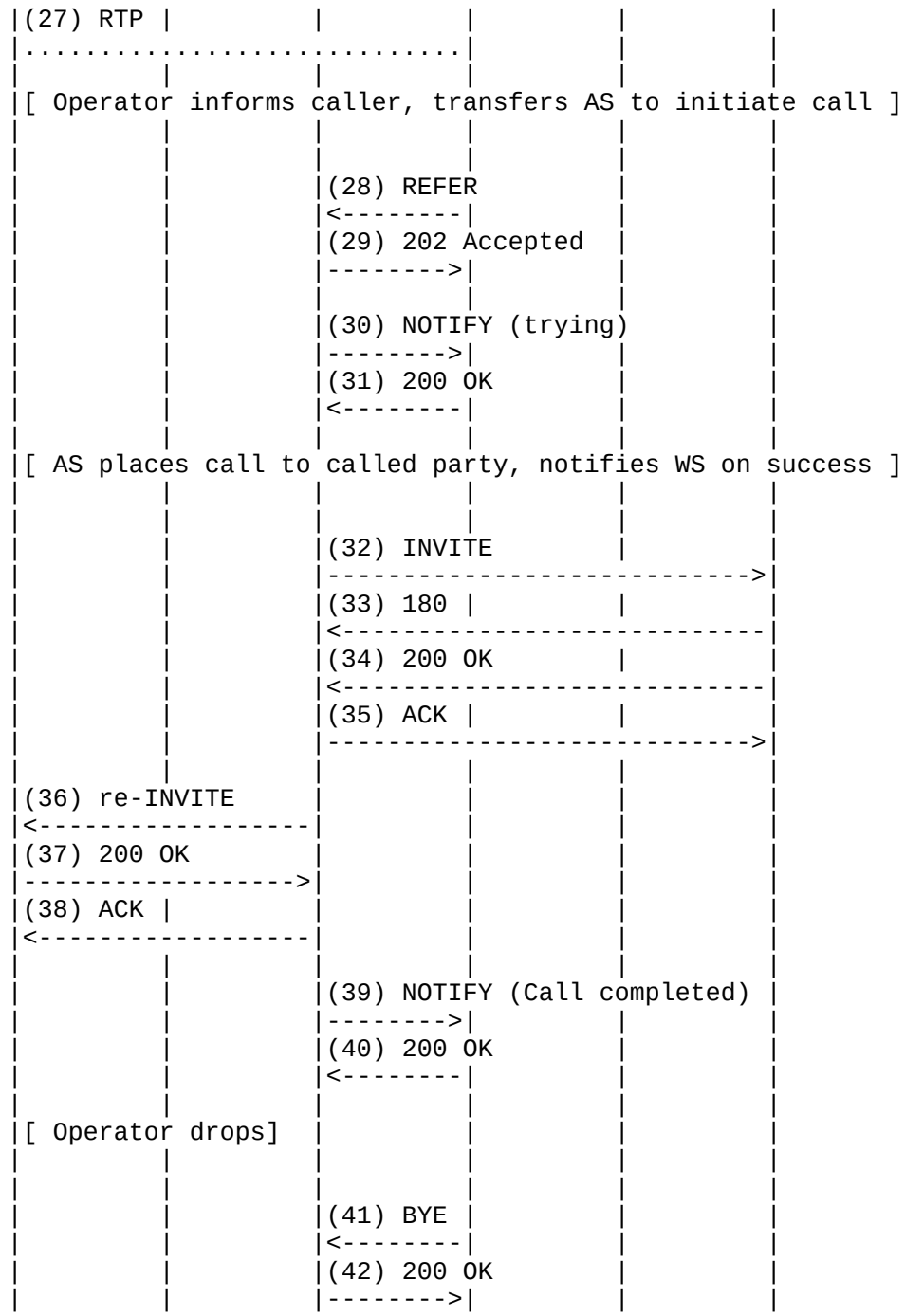
11.6. Operator Assisted Third Party Billing

The Operator Assisted Third Party Billing service allows a caller to request billing of a call to a third party. In such a service, the caller calls the operator, who places a call to the billed party to obtain authorization for billing. If authorized, the OISP places the call to the called party, and bills it to the billed party. This document focuses on the call flow and SIP signaling, and does not discuss the billing mechanisms.

In 1 through 8 below, the caller is connected to the operator. In 9 through 14, the operator places the caller on hold, and in 15 through 18 the operator calls the billed party to ask for authorization. In 21, the operator un-holds the caller and informs of the authorization. In 18 the operator initiates a call to the called party via the AS by sending a REFER to the AS.


Caller
CSCF
AS
WS
Billed
Called
[Caller dials 0+ or 0-]
(1) INVITE
(2) 100 Trying
[AS determines operator is needed, performs 3PCC]
(3) INVITE
(4) 200 OK
(5) ACK
(6) 200 OK
(7) ACK
[Caller is now connected to operator]
(8) RTP
[Operator determines caller’s request and places on hold]
(9) re-INVITE (HOLD)
(10) 200 OK
(11) ACK
[AS could optionally send caller to advertisements vs hold]


(12) re-INVITE (HOLD)
(13) 200 OK
(14) ACK
[Operator calls billed party]
(15) INVITE
(16) 200 OK
(17) ACK
(18) RTP
[Charges OK, operator disconnects billed party]
(19) BYE
(20) 200 OK
[Operator informs AS of result, un-HOLDs caller]
(21) re-INVITE(result, un-HOLD)
(22) re-INVITE(un-HOLD)
(23) 200 OK
(24) ACK
(25) 200 OK
(26) ACK


(27) RTP
[Operator informs caller, transfers AS to initiate call]
(28) REFER
(29) 202 Accepted
(30) NOTIFY (trying)
(31) 200 OK
[AS places call to called party, notifies WS on success]
(32) INVITE
(33) 180
(34) 200 OK
(35) ACK
(36) re-INVITE
(37) 200 OK
(38) ACK
(39) NOTIFY (Call completed)
(40) 200 OK
[Operator drops]
(41) BYE
(42) 200 OK

| | | | | |

Figure 25 Operator Assisted Third Party Billed Call

11.7. Offerless INVITE

In some cases, notably including calls originating from enterprise systems, it may occur that the incoming SIP INVITE message does not contain an SDP offer. Such "offerless INVITEs" are the source of much discussion and are often characterized as troublesome. The intention of this section is to identify the possibility of receiving such an INVITE. An example flow illustrating one way of addressing this is shown; however any particular solution may need to take into account factors such as equipment capabilities, operator policies, etc.

The most significant impact of this on a typical call is that when the application server receives such an INVITE and needs to perform third party call control, it does not have an SDP offer to send to the destination. In the example flow below, the media server receives such an INVITE from the application server, and it will not be able to formulate an SDP answer as usual, nor will it know which codec to use, nor will it know where to send the RTP stream. It will thus be delayed from sending media toward the caller until the SDP offer/answer exchange has completed.

Instead of sending an SDP answer, the media server needs to formulate an SDP offer of its own and include this in the next SIP message send toward the user. It will require some basis for selecting the appropriate media type (e.g., audio) and codec set. This should be configurable via operator policy. One possibility is to include all codecs supported by the media server in the SDP offer. If the caller finds one of the codecs acceptable it will make it selection and include in its SDP answer.

The flow below shows the media server returning a 183 Session Progress message with its SDP offer, and the caller including the SDP answer in the PRACK message sent in response to the 183. This is only one example; other flows are possible. For example the 183 could be omitted, and the media server could simply send a 200 OK message with the SDP offer. In that case the caller would include the SDP answer in the ACK message.

For normative information on the SDP offer/answer procedures, please refer to [RFC3264].

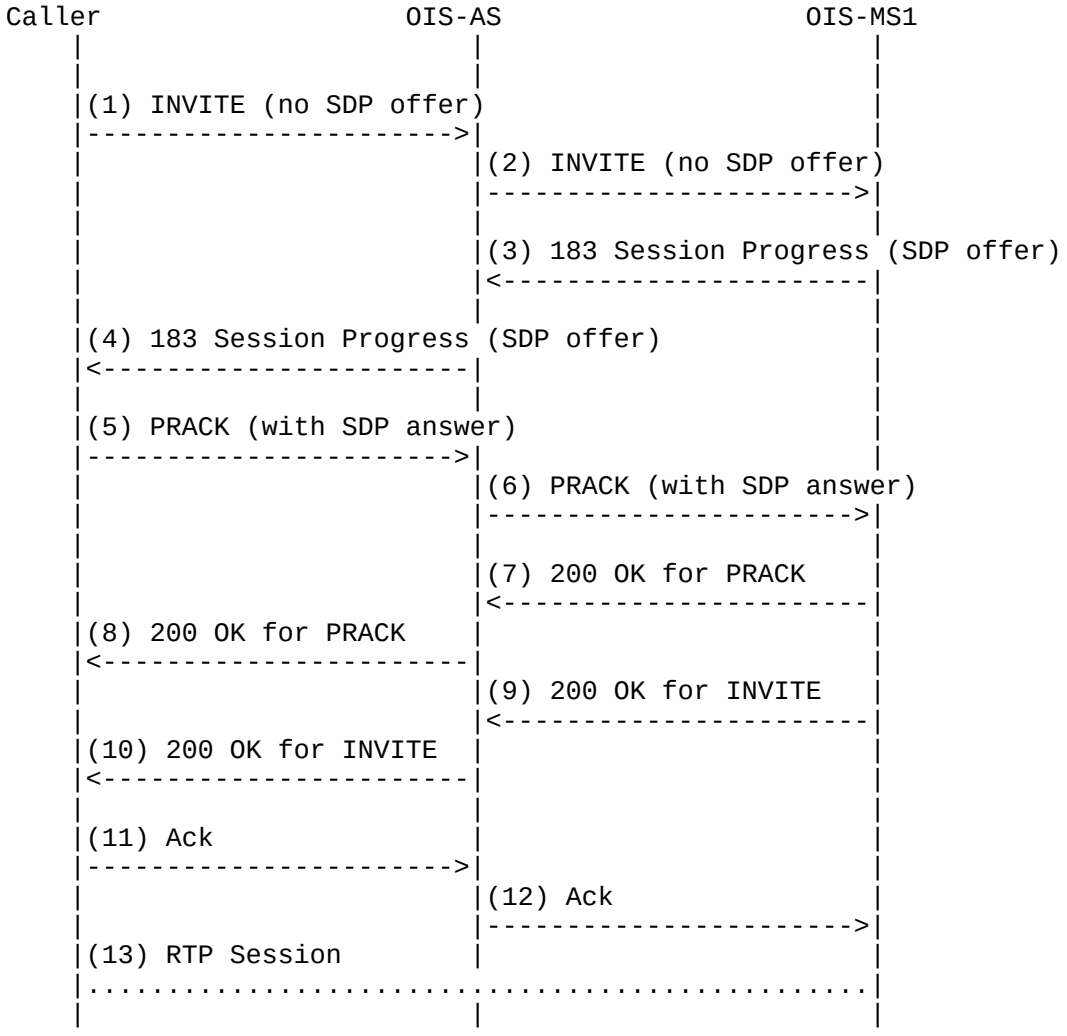


Figure 26 Offerless INVITE

12. Summary and Conclusions

The intent of this document is to explain how Directory Assistance and Operator Services work, and explore how they could be implemented with SIP. This includes both SIP originated requests as well as interworking with requests from the PSTN.

A basic architecture utilizing an application server as the primary controller, performing third party call control to route incoming calls among media servers, operator workstations, etc. is described. Interface to the PSTN is described using PSTN gateways which interwork between ISUP or MF signaling and SIP.

Operator services in the North American PSTN often utilize MF trunks. As there is currently no specific specification for MF/SIP interworking, we assume that the PSTN gateway performs an internal MF to ISUP translation.

The use of existing SIP mechanisms is described where possible. Some of the main mechanisms described include third party call control, the REFER method with several extensions (e.g. Replaces), the Join header, Netann, and some of the ongoing work in the MEDIACTRL working group.

Several protocol gaps and issues were identified. These include:

Charge Number

Coin Deposit Tones

Carrier Information: ISUP TNS, CIP, and CSI parameters, and "cic", "dai" tel URI parameters/

For conveyance of coin deposit tones, the document suggests that extensions to KPML are one potential option, and shows how KPML could be used to this end. Definition of an operator services SIP event package is mentioned as another alternative.

The desired next steps include soliciting feedback from the IETF community on the choices and intended usages of the proposed mechanisms.

13. Security Considerations

This document describes the use of existing and currently proposed protocol mechanisms. Detailed security analysis of services provided using these mechanisms should be performed, and needs to take into account the security implications of the individual mechanisms, which are documented in the defining documents for each mechanism. Security analysis of service provider use of these mechanisms also needs to take into account the interactions between individual mechanisms, as well as the overall context, including interactions with other providers, with which the provider may have differing levels of trust, in which these services are deployed.

Note that signaling for Operator and Information Services may convey information of a private nature, and may also convey information about deposit of coins by customers into coin phones. Thus, appropriate measures should be taken to ensure the confidentiality, integrity, and data origin authenticity of such signaling.

14. IANA Considerations

This document identifies how existing and currently proposed protocol mechanisms can be used, and does not request any action on the part of IANA.

15. Acknowledgements

The authors would like to thank Martin Dolly, Gary Munson, Spencer Dawkins, and Cullen Jennings for their review, comments, and advice with this document.

16. References

16.1. Normative References

[RFC3261] Rosenberg, et al, J., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC4474] Peterson, Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC3325] Jennings, et al, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

16.2. Informative References

[CSI] Loreto, Terril, "Input 3rd-Generation Partnership Project (3GPP) Communications Service Identifiers Requirements on the Session Initiation Protocol (SIP)", draft-loreto-sipping-3gpp-ics-requirements-00.txt, June 2006. (work in progress)

[RFC3324] Watson, "Short Term Requirements for Network Asserted Identity", RFC 3324, November 2004.

[RFC3263] Rosenberg, Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC4240] Burger, et al, "Basic Network Media Services with SIP", RFC 4240, December 2005.

[RFC3725] Rosenberg, et al, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", RFC 3725, April 2004.

[IMS] 3GPP TS 23.228 V7.4.0 (2006-06) - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 7)

[NSS] American National Standards Institute, Inc., "ANSI Extensions to the Narrowband Signaling Syntax (NSS) - Syntax Definition", ATIS-1000008.2006, January 2006.

[RFC4904] Gurbani, et al, "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)", RFC 4904, June 2007.

[RFC4730] Burger, Dolly, "A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)", RFC 4730, November 2006.

[RST] PacketCable, " Residential SIP Telephony Feature Specification", PKT-SP-RSTF-I01-060927, September 2006.

[RFC4235] Rosenberg, et al, "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", RFC 4235, November 2005.

[RFC3911] Mahy, et al, "The Session Initiation Protocol (SIP) "Join" Header", RFC 3911, October 2004.

[RFC3398] Camarillo, et al, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", RFC 3398, December 2002.

[RFC3840] Rosenberg, et al, "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", RFC 3840, August 2004.

[RFC4483] Burger, et al, "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", RFC 4483, May 2006.

[RFC2045] Freed, et al, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[RFC3204] Zimmerer, et al, "MIME media types for ISUP and QSIG Objects", RFC 3204, November 2001.

[RFC3325] Jennings, et al, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC4244] Barnes, et al, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

[RFC4694] Yu, J., "Number Portability Parameters for the "tel" URI", RFC 4694, October 2006.

[RFC5552] Burke, D. and Scott, M., "SIP Interface to VoiceXML Media Services", RFC 5552, May 2009.

[DAI] Yu, et al, "DAI Parameter for the tel URI", draft-yu-tel-dai-07, July 2009. (work in progress)

[T1679] Alliance for Telecommunications Industry Solutions (ATIS) Committee T1, "American National Standard for Telecommunications - Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part", ATIS T1.679-2004, June 2004.

[PCI] York, et al, "P-Charge-Info: A Private Header (P-Header) Extension to the Session Initiation Protocol (SIP)", draft-york-sipping-p-charge-info-07, August 2009. (work in progress)

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[draft-mahy-iptel-cpc] Mahy, R., "The Calling Party’s Category tel URI Parameter (SIP)", draft-mahy-iptel-cpc-06.txt, March 2007.

[RFC3891] Mahy, R. et al., "The Session Initiation Protocol (SIP) "Replaces" Header", RFC 3891, September 2004.

[RFC5079] Rosenberg, J., "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)", RFC 5079, December 2007.

[TS24229] xxx.

[RFC5009] Ejzak, R., "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media", RFC 5079, September 2007.

[GR506] GR-506-CORE, "LSSGR: Signaling for Analog Interfaces". Telcordia Technologies, Issue 2, December 2006.

[RFC3264] Rosenberg, J., et al. "An Offer/Answer Model with the Session Description Protocol (SDP)", RFC 3264, June 2002.

Author's Addresses

John Haluska
Telcordia Technologies, Inc.
331 Newman Springs Road
Room 2Z-323
Red Bank, NJ 07701-5699
USA

Phone: +1 732 758 5735
Email: jhaluska@telcordia.com

Renee Berkowitz
Telcordia Technologies, Inc.
One Telcordia Drive
Piscataway, NJ 08854-4157
USA

Phone: +1 732 699 4784
Email: rberkowi@telcordia.com

Paul Roder
Telcordia Technologies, Inc.
One Telcordia Drive
Room RRC-4A619
Piscataway, NJ 08854-4157
USA

Phone: +1 732 699 6191
Email: proder2@telcordia.com

Wesley Downum
Telcordia Technologies, Inc.
One Telcordia Drive
Piscataway, NJ 08854-4157
USA

Phone: +1 732 699 6201
Email: wdownum@telcordia.com

Richard Ahern
AT&T Customer Information Services
1876 Data Drive
Room 314

Hoover, AL 35244
USA

Email: Richard.Ahern@bellsouth.com

Paul Lum Lung

Marty Cruze
CenturyLink
Email: marty.cruze@centurylink

Nicholas S. Costantino
Soleo Communications, Inc.
300 Willowbrook Drive
Fairport, NY 14450

Email: ncostantino@soleocommunications.com

Chris Blackwell

D. E. Scott
VoltDelta
2401 N. Glassell St.
Orange, CA 92865-2705

Email: dscott@voltdelta.com