BroadSoft is
now part of Cisco.

BroadWorks AS Mode IP Multimedia Subsystem

Solution Guide

Release 23.0

Document Version 1

BroadWorks® Guide

Copyright Notice

Trademarks

Document Revision History

Release	Version	Reason for Change	Date	Author
14.0	1	Created document from Release 13.0, Document Version 2.	September 20, 2006	Robb Surridge
14.0	1	Edited for technical accuracy.	October 2, 2006	Doug Sauder
14.0	1	Edited document.	October 18, 2006	Patricia Renaud
15.0	1	Updated document for Release 15.0.	July 21, 2008	Doug Sauder, Martin Piotte
15.0	1	Edited changes and published document.	September 9, 2008	Andrea Fitzwilliam
15.0	2	Added information about initial filter criteria.	September 17, 2008	Doug Sauder
15.0	2	Edited changes and published document.	October 2, 2008	Andrea Fitzwilliam
16.0	1	Updated document for Release 16.0.	May 20, 2009	Doug Sauder
16.0	1	Edited changes and published document.	August 18, 2009	Andrea Fitzwilliam
16.0	2	Updated section *6.1 BroadWorks Application Server Configuration Parameters: SIP* for EV 105823.	January 28, 2010	Goska Auerbach
16.0	2	Edited changes and published document.	February 5, 2010	Patricia Renaud
17.0	1	Updated document for Release 17.0.	May 20, 2010	Doug Sauder
17.0	1	Edited changes and published document.	May 26, 2010	Margot Hovey-Ritter
18.0	1	Updated document for Release 18.0.	November 14, 2011	Bob Russell
18.0	1	Edited changes and published document.	November 25, 2011	Jessica Boyle
18.0	2	Fixed graphic and re-published document.	December 28, 2011	Patricia Renaud
19.0	1	Updated document for Release 19.0.	September 21, 2012	Doug Sauder
19.0	1	Edited changes and published document.	October 25, 2012	Patricia Renaud
19.0	2	Added clarification of “Routing B2BUA” behavior in relation to the *routingMode* parameter in section *6.2.6 routingMode* for EV 167899.	November 7, 2012	Doug Sauder
19.0	2	Renamed the document file, edited changes, and published document.	December 18, 2012	Patricia Renaud
20.0	1	Changed the architecture information to remove old servers and add new servers. Updated document for Release 20 features.	October 14, 2013	Doug Sauder
20.0	1	Edited changes and published document.	November 8, 2013	Patricia Renaud
20.0	2	Updated document to refer to 3GPP Release 12 specifications.	November 15, 2013	Doug Sauder
20.0	2	Edited changes and published document.	November 18, 2013	Patricia Renaud

Release	Version	Reason for Change	Date	Author
20.0	3	Added a caution about unexpected consequences when enabling third-party registration or Sh interface for EV 191426.	November 19, 2013	Doug Sauder
20.0	3	Edited changes and published document.	December 13, 2013	Jessica Boyle
21.0	1	Updated document for Release 21.0.	October 27, 2014	Doug Sauder
21.0	1	Updated the BroadSoft legal notice.	October 28, 2014	Joan Renaud
21.0	1	Edited changes.	October 30, 2014	Joan Renaud
21.0	1	Rebranded and published document.	November 3, 2014	Joan Renaud
21.0	2	Updated document with rebranded server icons and published document.	February 23, 2015	Joan Renaud
21.0	3	Added further details on the steps the Application Server takes to select the CSCF URI for an out-of-the-blue request (PR-45114).	August 31, 2015	Doug Sauder
21.0	3	Edited changes and published document.	May 18, 2016	Jessica Boyle
22.0	1	Updated document for Release 22.0.	October 5, 2016	Doug Sauder
22.0	1	Edited changes and published document.	December 11, 2016	Patricia Renaud
23.0	1	Updated document for Release 23.0.	September 14, 2018	Doug Sauder
23.0	1	Edited changes and published document.	October 3, 2018	Jessica Boyle

Table of Contents

List of Figures

List of Tables

1 Summary of Changes

This section describes the changes to this document for each release and document version.

1.1 Changes for Release 23.0, Document Version 1

This version of the document includes the following changes:

- Added information about how the Application Server applies the system parameter *userPhoneErrorCorrection* to addresses other than the *Request-URI*.

1.2 Changes for Release 22.0, Document Version 1

This version of the document includes the following changes:

- The Application Server provides a SIP system parameter *pChargingFunction-AddressesFormat* to control the default syntax for the *P-Charging-Function-Addresses* header.
- The IMS parameter *includeDirectoryNumberInPAI* was moved from the IMS context to the SIP context in the CLI.
- The IMS parameter *userPhoneErrorCorrection* has a new value "fullEnforceUserPhone".

1.3 Changes for Release 21.0, Document Version 3

This version of the document includes the following changes:

- Added further details on the steps the Application Server takes to select the CSCF URI for an out-of-the-blue request (PR-45114).

1.4 Changes for Release 21.0, Document Version 2

This version of the document includes the following changes:

- Updated document with rebranded server icons.

1.5 Changes for Release 21.0, Document Version 1

This version of the document includes the following changes:

- Added a summary of the new Advice of Charge(AoC) capabilities:
  - The Application Server can query for AoC tariff information in accordance with 3GPP TS 32.280.
  - The Application Server supports redundant OCS servers.
- Replaced outdated references to the Instant Conferencing service with references to the Meet-Me Conferencing service.

1.6 Changes for Release 20.0, Document Version 3

This version of the document includes the following change:

- Added a caution about unexpected consequences when enabling third-party registration or the Sh interface. In summary, OOTB calls can fail if the served user is unregistered. (EV 191426)

1.7 Changes for Release 20.0, Document Version 2

This version of the document includes the following change:

- Updated the document to refer to 3GPP Release 12 specifications.

1.8 Changes for Release 20.0, Document Version 1

This version of the document includes the following changes:

- Updated the architecture description to remove information about obsolete servers (Web Server, Conferencing Server, Call Detail Server) and add information about current servers (Xtended Services Platform, Profile Server, Enhanced Call Logs Repository).
- Changed the name of the SIP parameter *usePAIForPrivateCLID* to its correct name *useAssertedIdentityForPrivateCLID*. (This name change occurred in Release 18.0.)
- No changes for Release 20.0 features.

1.9 Changes for Release 19.0, Document Version 2

This version of the document includes the following changes:

- Added clarification of "Routing B2BUA" behavior in relation to the *routingMode* parameter in section *6.2.6 routingMode* for EV 167899.
- Renamed the document file and title to include "AS Mode".

1.10 Changes for Release 19.0, Document Version 1

This version of the document includes the following change:

- Added a description of the *forceSipURIForClientOriginatedActions* IMS parameter.

1.11 Changes for Release 18.0, Document Version 2

This version of the document includes the following changes:

- Fixed graphic in *Figure 5 BroadWorks IMS Interfaces*.
- Made minor editorial changes.

1.12 Changes for Release 18.0, Document Version 1

This version of the document includes the following changes:

- Added information about the new *enableOIPCompliance, includeTrunkGroupPilotInPAITelURI*, and *forceDeflectedCallBeforeAnswerAsOOTB* parameters.
- Moved the *usePAIForPrivateCLID* parameter from section *6.2* to section *6.1 BroadWorks Application Server Configuration Parameters: SIP*.

1.13 Changes for Release 17.0, Document Version 1

This version of the document includes the following changes:

- Updated information on the Rf, Ro, and Sh interfaces in accordance with the new Diameter stack incorporated into BroadWorks in Release 17.0.
- Added information about the new *pServedUserSyntax* parameter.

1.14 Changes for Release 16.0, Document Version 2

This version of the document includes the following changes:

- Updated section *6.1 BroadWorks Application Server Configuration Parameters: SIP* for EV 105823.

1.15 Changes for Release 16.0, Document Version 1

This version of the document includes the following changes:

- Added information about new configuration parameters for the IMS Service Control (ISC) interface. Specifically, added information about the *connectedOrigination Handling* parameter.
- Added information about the Ro interface.
- Added information about the Advice of Charge supplementary service.

1.16 Changes for Release 15.0, Document Version 2

This version of the document includes the following change:

- Added information about initial filter criteria.

1.17 Changes for Release 15.0, Document Version 1

This version of the document includes the following change:

- Updated document for Release 15.0.

1.18 Changes for Releases 14.0

This version of the document includes the following change:

- Edited for technical accuracy in Release 14.0.

2 Introduction

2.1 Summary

The IP Media Subsystem (IMS) is a unified service delivery architecture for next generation converged voice and data services. Today's BroadWorks service offerings are both supported and being deployed within the IMS architecture in several markets.

BroadWorks brings a superior differentiated voice and data application solution to the IMS infrastructure beyond services provided by Internet Protocol private branch exchange (IP PBXs) and IN solutions. BroadWorks increases operator average revenue per unit (ARPU) through faster rollout of new services and faster integration and time-to-market of third-party applications using the standards-based IMS framework. Using the IMS architecture eliminates the need to deploy separate silo-based network/applications architectures and provides a common transport and subscriber data repository with lower operation, administration, and maintenance (OA&M) overhead.

The BroadWorks Application Server (AS) is an IMS Session Initiation Protocol (SIP) Application Server located within the IMS application layer. Most BroadWorks services reside with the Application Server. All servers use standard IMS interfaces, including Sh, ISC, Ro, Rf, Mb, and Mr to communicate with other BroadWorks servers and third-party IMS components.

The BroadWorks Media Server is an IMS Media Resource Function (MRF) that provides media services within the IMS data plane while being controlled within the IMS signaling plane.

Other supporting BroadWorks servers are deployed as optional add-on components associated with the BroadWorks Application Server. These include the Network Server, Element Management System (EMS), Xtended Services Platform, Profile Server, and Enhanced Call Logs Repository.

2.2 Scope

This document provides a system-level view of how BroadWorks fits into the IMS architecture. It includes a general overview of the IMS components most related to BroadWorks and includes specific considerations for configuring BroadWorks for use with IMS deployments. When applicable, guidelines are also provided for the configuration of associated non-BroadSoft components.

Topics covered in this document include:

- An overview of IMS architecture, describing the roles of key components within the IMS architecture as they relate to BroadWorks
- An overview of BroadWorks IMS components, including optional supporting servers
- An overview of key IMS interfaces as they relate to BroadWorks
- An introduction to BroadWorks signaling call flows in IMS deployments, including some detailed examples
- A review of BroadWorks operation in IMS deployments, with specific attention to IMS subscriptions and addressing mechanisms, distributed group calls, originator/terminator determination, call routing, P-header use, and charging
- A summary of key BroadWorks settings including operational parameters, application server configuration and deployment considerations

2.3 Intended Audience

This document is for use by current and potential BroadSoft customers and partners. It is also to be used by BroadSoft product managers, engineers, sales personnel, and management. Information in this document is to be treated as proprietary to BroadSoft.

It is assumed that the reader is familiar with the general features and capabilities of the BroadWorks product, with the use of SIP in both fixed and mobile networks, and with IP networking technologies. If not, contact your authorized BroadSoft sales representative for additional background information.

2.4 Access Independence

BroadWorks services are access independent. Note that this document describes how BroadWorks services can be deployed within the IMS architecture described in Third Generation Partnership Project (3GPP) Release 12, which is an access independent architecture in which services can be delivered over fixed and mobile networks of most types. Details to support service access in installations using Interim Standard (IS)-41 Code Division Multiple Access (CDMA) and 3GPP Global System for Mobile Communications (GSM) mobile networks, fixed line, or cable networks can be provided if relevant.

2.5 Standards

Various standards organizations present their own flavors of IMS adopted from the 3GPP, which use many of the protocols described by the Internet Engineering Task Force (IETF). This document refers primarily to standard documents provided by 3GPP and the IETF.

3GGP

The IP Multimedia Subsystem (IMS) has its origins in the mobile world. Initially, European Telecommunications Standards Institute (ETSI) defined the Global System for Mobile Communications (GSM), including the General Packet Radio Services (GPRS). A new organization was created, the 3rd Generation Partnership Program (3GPP), which built upon the ETSI standards to offer 3GPP Release 99. The next release, renamed to Release 4, introduced an all-IP infrastructure, while Release 5 introduced the IMS. Release 6 is an elaboration of the IMS specification. The BroadWorks IMS solution follows the 3GPP Release 12 standards, with development following newer 3GPP releases as they become available.

3GPP2

Similarly, for CDMA networks, the 3rd Generation Partnership Program 2 (3GPP2) was established. 3GGP2 specifies the same IMS architecture as the 3GPP with minor variations due to the mobile transport network (that is, Mobile IP versus GPRS). 3GPP2 provides a set of IMS-related documents under the X.S0013-xxx series, each directly related to a 3GPP document. For simplicity, this document refers primarily to the 3GPP reference specifications.

IETF

The Internet Engineering Task Force (IETF) offers documents that form a base reference for most IP communication protocols. 3GPP incorporates these protocols where possible within the IMS.

TISPAN

A technical committee within the ETSI group organized from the combined work of former ETSI bodies TC Services and Protocols for Advanced Networks (SPAN) and EP Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON). The committee is responsible for all aspects of standardization for present and future converged networks, including the Next Generation Network (NGN). Like 3GPP2, TISPAN has adopted much of the work done by 3GGP. However, its focus is on NGN wireline networks.

3 IMS Architecture Overview

This section describes the role of key components within the IMS architecture.

3.1 IMS Component Overview

The IMS architecture contains many functional components, described in *3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2* [15]. One or more of these functions can be part of an actual vendor product. *Figure 1* shows selected functional components in one possible representation of IMS. Each of the relevant functional components in the diagram is described in detail later in this section. For now, it should be noted that IMS brings together all types of networks for the delivery of converged services. BroadSoft primarily provides components involved in the delivery of application services.

Not all components and/or functions need to be in place to begin providing services using IMS. Existing packet-based and circuit-based products today can be integrated into IMS via gateways. It is important to assess if and when such products should be directly connected into the IMS core.

The left side of the diagram represents integration with existing non-IMS IP networks. The right side shows integration with existing time division multiplexing (TDM) networks. The bottom left shows integration with wireline devices via TISPAN. The bottom right shows integration to mobile networks via GPRS Gateway Support Node (GGSN). Note that a Packet Data Serving Node (PDSN) is used for CDMA networks.

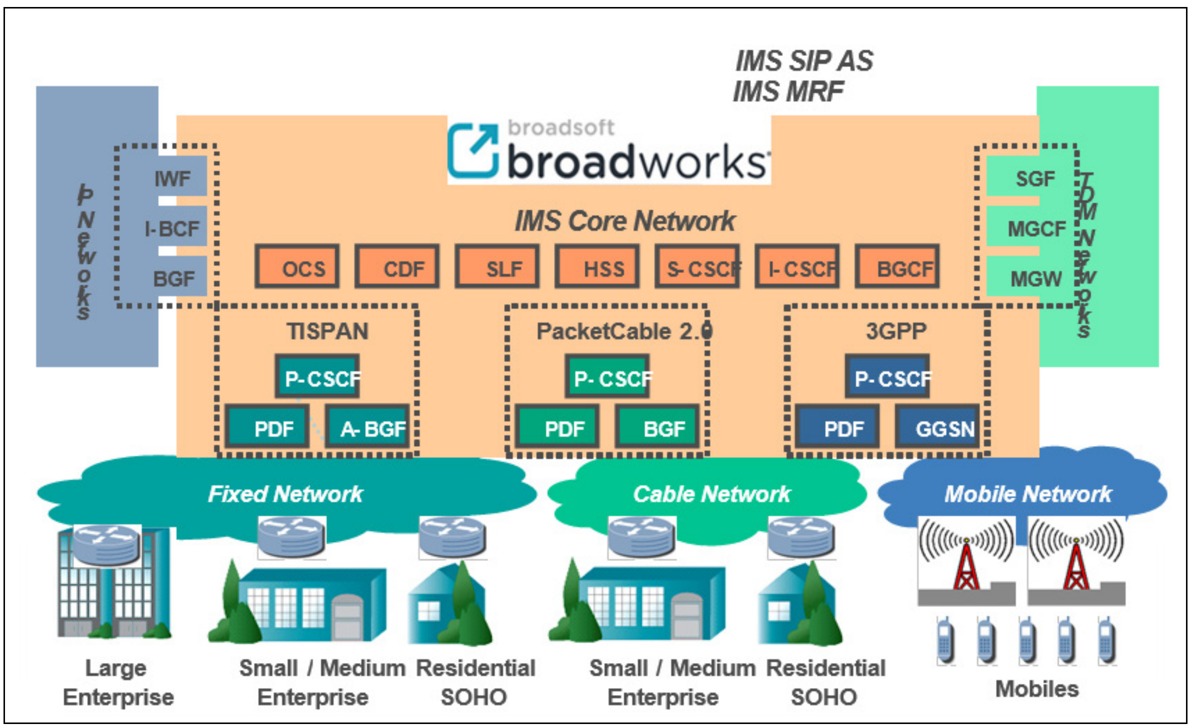

Figure 1 BroadWorks in IMS Network Architecture

The IMS standard defines each of the logical components, as well as the interfaces between them (referred to as "reference points"). This is a key advantage of IMS, allowing the vendor community to develop components with a limited number of well-defined interfaces. IMS offers a layered grouping of logical components. *Figure 2* shows the key IMS components, along with the interfaces between them (as per 3GPP). Each is briefly described below using descriptions paraphrased from 3GPP TS 23.002 [14].

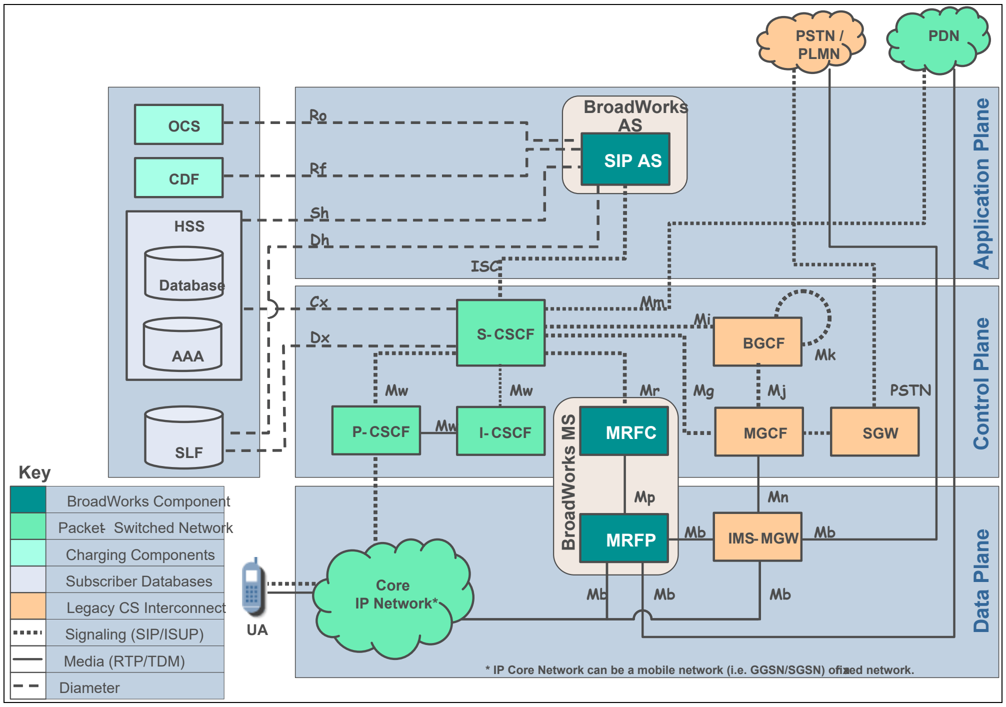

Figure 2 Key Logical Components and Interfaces of IMS (according to 3GPP)

The architecture can be viewed from many angles (architecture, transport, and protocol).

- **Architecture Plane**: IMS is a layered architecture, in which:
  - The *data plane* handles the switching of bearer media. This includes both packet data and circuit switched voice and the conversion between the two.
  - The *control plane* handles all signaling, including the conversion between integrated services user part (ISUP) and SIP. This includes user/device registration and location functions.
  - The *application plane* handles all service delivery capabilities and decisions and maps these to each subscriber based on profile information.
  - The *resource plane* (although not formally named in the standards or shown in the figure) provides a converged data repository in the form of subscriber profile and service data, as well as charging information and control.
- **Transport Type**: Traffic is primarily packet-switched or circuit-switched, indicated by the component colors in *Figure 2*.
  - **IP (green)**: In a pure IMS environment, all signaling and media traffic uses IP. Note that the core IP network in the diagram shows a 3G mobile phone. Not shown are IP-phones connected via public or private networks (the Packet Data Network [PDN] cloud is shown). Note that BroadWorks components are included in this grouping.

  - **Legacy Voice Interconnects (brown)**: To support both circuit-switched wireline phones and 2G/2.5G mobile phones (Public Land Mobile Network [PLMN]), as well as to interconnect with PSTN services, signaling and media conversion is required.
  - **Database Interconnects (light green and grey)**: These components deal with database and accounting functions.
- **Protocol Type**: Traffic is primarily signaling or media, indicated by the line types used in *Figure 2*:
  - **Signaling (dotted lines)**: Typically, IMS signaling is provided via the SIP protocol. Conversion to legacy TDM-based signaling such as ISUP is supported via gateways. Both are represented in the diagram by dotted lines.
  - **Media (solid lines)**: Typically, IMS media is supported using the Real-Time Transport Protocol (RTP) protocol. Conversion to legacy TDM circuits is supported via media gateways. Both are represented in the diagram by solid lines.
  - **Database/Accounting (dashed lines)**: Typically, IMS uses the Diameter protocol for database access. This includes access to subscriber information and authentication information held within the Home Subscriber Server (HSS), as well as offline and online accounting information.

3.1.1 Application Server

An Application Server (AS) offers value-added IMS services, residing in the user's home network or a third-party location. The third-party location could be a network or simply a stand-alone Application Server.

The SIP Application Server interacts with other network elements over the ISC, Sh, Rf, and Ro interfaces.

- The ISC interface is a SIP interface that connects the Application Server to SIP proxy servers, called Call Session Control Functions (CSCFs), to execute call processing services.
- The Sh interface is a Diameter interface that connects the Application Server to the Home Subscriber Server (HSS) to obtain IMS subscription information.
- The Rf interface is a Diameter interface that connects the Application Server to the Charging Data Function (CDF) for offline accounting information.
- The Ro interface is a Diameter interface that connects the Application Server to the Online Charging System (OCS) for real-time online accounting (for example, for prepaid services).

The BroadWorks Application Server is a SIP Application Server within the IMS architecture.

3.1.2 Call Session Control Function

The Call Session Control Function (CSCF) can act as Proxy-CSCF (P-CSCF), Serving-CSCF (S-CSCF), or Interrogating-CSCF (I-CSCF).

- The P-CSCF is the first contact point for the user equipment (UE), which offers SIP registration and session control.
- The S-CSCF handles the session states in the network for a given IMS subscriber.
- The I-CSCF assists with the registration and authentication of the UE (via HSS). It is the contact point for all IMS connections destined both to network subscribers and to roaming subscribers currently located within a network's service area.

For more information on the CSCF, see the *3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2* [15].

3.1.3 Multimedia Resource Function

The IMS Multimedia Resource Function (MRF) contains two individual components, the MRF Controller (MRFC) and MRF Processor (MRFP).

The BroadWorks Media Server is an MRF within the IMS architecture, containing both MRFC and MRFP functional components.

3.1.3.1 Multimedia Resource Function Controller

The Multimedia Resource Function Controller (MRFC) controls the media stream resources in the MRFP. It interprets information coming from an application server and/or the S-CSCF (that is, the session identifier) and controls the MRFP accordingly.

3.1.3.2 Multimedia Resource Function Processor

The Multimedia Resource Function Processor (MRFP) controls bearers on the Mb reference point. It mixes incoming media streams from multiple parties (such as for three-way calling or instant group call functions). It is a source of media streams for multimedia announcements (such as voice mail, custom ringback and so on). In addition, it processes media streams for analysis (such as dual-tone multi-frequency [DTMF] detection). MRFP resources are controlled by the MRFC.

3.1.4 Breakout Gateway Control Function

The Breakout Gateway Control Function (BGCF) selects the network in which PSTN breakout is to occur and within the network where the breakout is to occur by selecting which Media Gateway Control Function (MGCF) is to be used.

3.1.5 Signaling Gateway Function

The Signaling Gateway Function (SGW) performs bi-directional signaling conversion at transport level between the SS7-based transport of signaling used in pre-Release 4 networks, and the IP-based transport of signaling possibly used in post-R99 networks (for example, between SS7 MTP and Sigtran SCTP/IP). The SGW does not interpret the application layer messages (for example, MAP, CAP, BICC, ISUP), but may have to interpret the underlying SCCP or SCTP layer to ensure proper routing of the signaling.

3.1.6 Media Gateway Control Function

The Media Gateway Control Function (MGCF) is the signaling component within what is typically referred to as a softswitch. It is used as an interface to legacy networks (for example, PSTN or PLMN mobile). The MGCF selects the S-CSCF and communicates with it based on the routing number for incoming calls from the legacy network. It also provides protocol conversion between ISUP and SIP. The MGCF controls the parts of the call state that pertain to connection control for media channels in the IMS-MGW. It uses the Mn interface for dynamic sharing of transmission resources between domains, as the IP Multimedia Subsystem - Media Gateway Function (IMS-MGW) controls bearers and manages resources according to the H.248 protocols and functions for IMS.

3.1.7 IP Multimedia Subsystem – Media Gateway Function

The IP Multimedia Subsystem - Media Gateway Function (IMS-MGW) terminates media streams (RTP) from a packet network and it may offer media conversion and other media processing functions (for example, echo cancellation, conferencing). It is controlled by the MGCF using the Mn interface via H.248.

Note that this component may also be a Circuit-Switched Media Gateway (CS-MGW) if it terminates bearer channels.

3.2 BroadWorks IMS Components

Core BroadWorks servers are shown in the following table. BroadWorks also provides optional supporting server components as shown in the next table. All BroadWorks servers run on standard, off-the-shelf, Network Equipment Building Standards (NEBS)-compliant hardware and they are approved for use on IBM xSeries/BladeCenter (Linux) and the Sun Fire/Netra (Solaris).

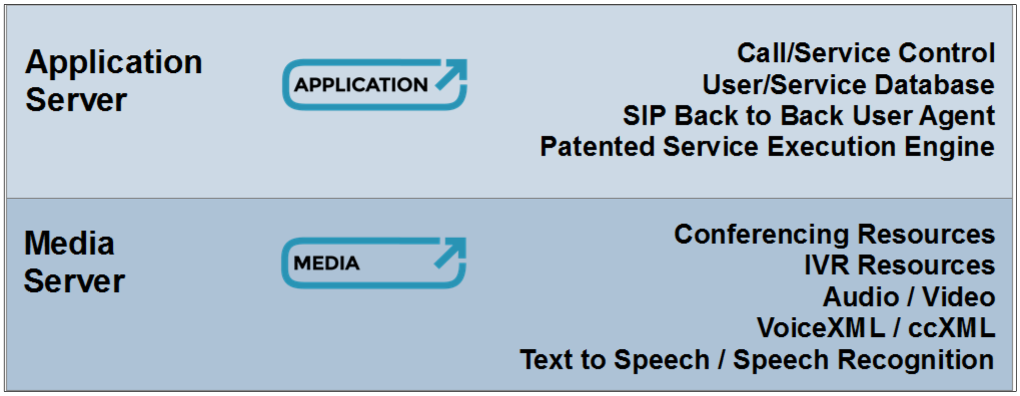

Figure 3 BroadWorks Core Servers

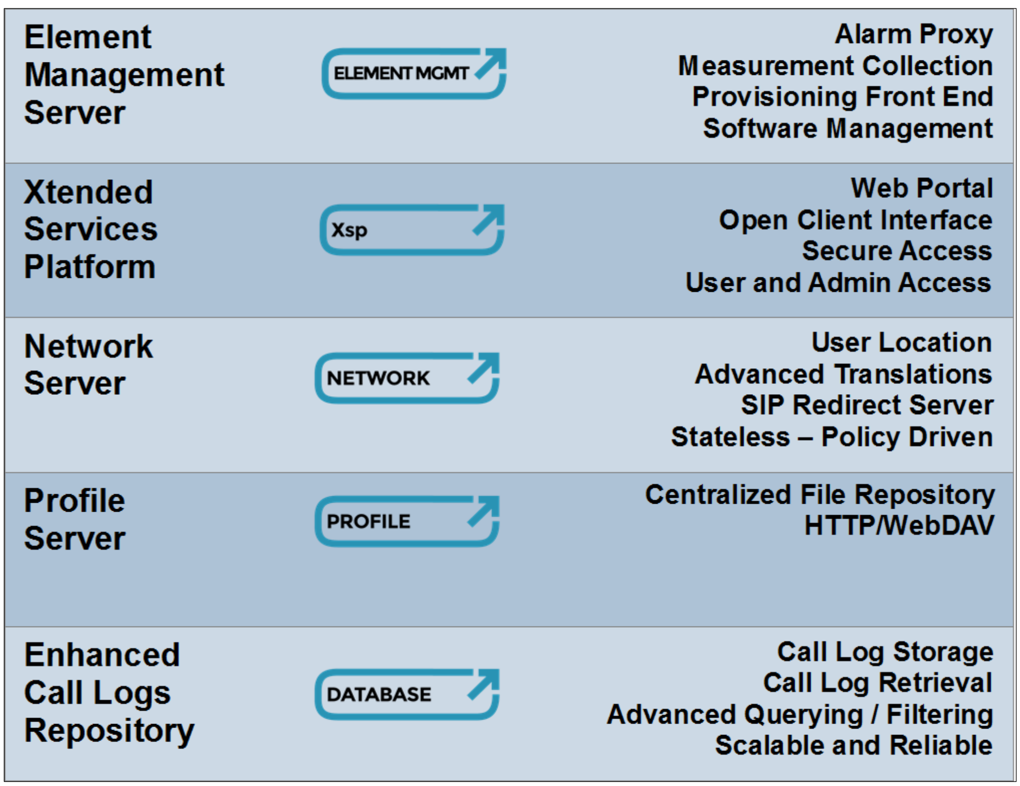

Figure 4 BroadWorks Optional Supporting Servers

3.2.1 IMS SIP Application Server – BroadWorks Application Server

Most advanced call services are provided by the BroadWorks Application Server (AS), which provides full-featured SIP application server functionality and is the heart of the BroadWorks solution. Note that many services also require the use of supporting servers, such as the BroadWorks Media Server.

Interaction between the Application Server and other IMS components occurs at a signaling level via SIP. If the BroadWorks Media Server is used, interaction also occurs at the media level via RTP/Real-Time Control Protocol (RTCP).

3.2.2 IMS MRF – BroadWorks Media Server

The BroadWorks Media Server provides an integrated MRF capability that includes both MRFC and MRFP IMS functions.

3.2.3 Optional Supporting Servers

BroadWorks provides a family of servers that integrate seamlessly into operator networks to provide a fully integrated solution.

- The Element Management System, a core server, provides an integrated point for Fault, Configuration, Accounting, Performance, and Security (FCAPS) access to all BroadWorks servers.
- The Xtended Services Platform provides an integrated point for service provisioning by operators with different levels of administrative privileges (system provider, service provider, group, and user).
- The Network Server provides enhanced network translations as well as a location service that reports the Application Server assigned to a BroadWorks user.
- The Profile Server provides a centralized file repository for use by media resources and device management.
- The Enhanced Call Logs Repository provides for the storage and retrieval of detailed call logs, enhancing customer service and OA&M functions.

3.3 Relevant BroadWorks IMS Interfaces

This section provides an overview of each external BroadWorks interface, focusing on those relevant to IMS deployments.

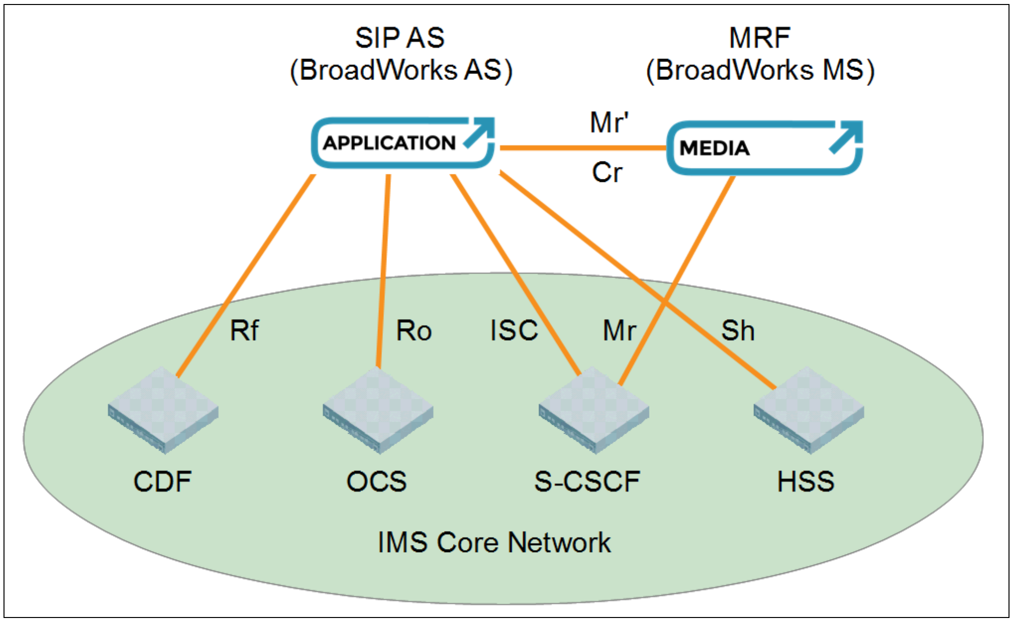

Figure 5 BroadWorks IMS Interfaces

3.3.1 Sh Interface

The Sh interface provides communication between the BroadWorks Application Server and the HSS. It is used to access subscriber profile data, which determines the services authorized to end-users. Subscriber profile data is transferred as eXtensible Markup Language (XML) data using the Diameter protocol. Messages contain both non-transparent data for service logic (IMS/subscriber-specific) and transparent data stored and used by Application Servers (application-specific).

3.3.2 Dh Interface

The Dh interface provides communication between the BroadWorks Application Server and the Subscription Locator Function (SLF). The SLF is used when there are multiple HSS entities within the network. It is not always shown in diagrams, as most networks initially have only one HSS. In general, it should be assumed this functionality is included when describing the BroadWorks Sh interface.

3.3.3 ISC Interface

The IMS Service Control (ISC) interface provides communication between an IMS-compliant application server, such as the BroadWorks Application Server, and the S-CSCF. It allows SIP requests to be routed from terminal devices to an application server, and supports application server-initiated SIP requests to the S-CSCF. SIP signaling is used, extended by several private headers (P-Headers) to meet telephony needs. P-Headers are extensions to SIP, defined by 3GPP in *TS 24.229* (see also *3GPP2 X.P0013.4*).

3.3.4 Mr Interface

The Mr interface provides communication between the MRFC/MRFP (for example, the BroadWorks Media Server) and the Application Server. It allows for SIP signaling to be used as the "control" protocol for the Media Server (MRFC). This includes Media Server Control Markup Language (MSCML), used for IVR functions, and NETwork ANNouncments (NETANN), used to differentiate interactive voice response (IVR), conferencing, fax, and conferencing control. It also serves as the means for the Application Server to establish a dedicated control channel with the MRF. This control channel is formally designated the Cr interface.

Typically, the BroadWorks Application Server maintains a list of available BroadWorks Media Servers. Media Server addressing should not need a public address (that is, it should not use an HSS entry).

NOTE: The Mr interface serves the same purpose as the Mr interface, the difference being that the Mr interface connects the Application Server and the MRF directly, whereas the Mr interface connects the Application Server and the MRF via the S-CSCF and the ISC interface. The BroadWorks Application Server sends SIP messages directly to the Media Server via the Mr interface, rather than routing them through the S-CSCF and the ISC and Mr interfaces.

3.3.5 Cr Interface

The Cr interface defines a dedicated control channel between an Application Server and an MRF. In a BroadWorks deployment, the BroadWorks Application Server and the BroadWorks Media Server interact for various services, such as conference mixing or call recording, using the Cr interface.

3.3.6 Rf Interface

The Rf interface provides communication between the Application Server and the IMS Charging Data Function (CDF). It is used to support an offline charging model (that is, postpaid/contract charging). Data is transferred using Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages. Charging information is stored and extracted in the following IMS-based P-headers: *P-Charging-Vector* and *P-Charging-Function-Addresses*.

3.3.7 Ro Interface

The Ro interface provides communication between the Application Server and the IMS Online Charging System (OCS). The Application Server uses the OCS to reserve and/or debit credits at call setup time, as well as at other times during a call, for the Prepaid service. Additionally, it may query the OCS for rate information to support the Advice of Charge service.

3.4 Summary of Key IMS Components and Interfaces

The following table summarizes the key IMS components and their interactions. Only IMS interfaces are shown. Other BroadWorks interfaces such as the BroadWorks Open Client Interface (OCI) are described in other BroadWorks documentation.

Component	Role	BroadWorks Interaction
BroadWorks Application Server (SIP AS)	Provides advanced SIP-based call control and services to all access device types	BroadWorks interactions are: ▪ CDF via the Rf interface for offline charging ▪ OCS via the Ro interface for online charging ▪ HSS via the Sh interface for subscriber profile access ▪ S-CSCF via the ISC interface for SIP signaling ▪ I-CSCF via the Ma interface for SIP signaling ▪ MRFC via the Mr’ interface for media resources ▪ MRFC via the Cr interface for media resources
BroadWorks Media Server MRF (MRFC and MRFP)	Provides media services (conference mixing, IVR, announcements, and so on)	BroadWorks interactions are: ▪ Application Server via the Mr’ interface for media control ▪ Application Server via the Cr interface for media control
HSS	Maintains non-transparent subscriber profile information and transparent application-specific information	Application Server (Sh) for subscriber profile access
S-CSCF	Entry point to mobile network, locates subscriber for inbound calls	Application Server (ISC) for signaling/routing MRF (Mr) for media resource control (via both the S-CSCF and the Application Server)
CDF	Collection of call detail records for offline charging	Application Server (Rf) for offline charging
OCS	Real-time, online charging for services such as Prepaid service	Application Server (Ro) for online charging.

Table 1 Key IMS Components and Interactions in BroadWorks Deployments

4 BroadWorks IMS Call Flows

To understand the delivery of services within IMS, it is best to separate what happens on the control plane from what happens on the data plane. To describe BroadWorks service delivery within the IMS, this section focuses on the signaling required to set up services. Signaling within the IMS uses SIP, regardless of the signaling origin (that is, from an IP phone or a signaling gateway).

4.1 Originating and Terminating Service Triggers

As shown earlier in *Figure 2*, the BroadWorks Application Server receives signaling from the S-CSCF over the IMS Service Control (ISC) interface. *Figure 6* shows a call entering the S-CSCF (from a P-SCSF or I-SCSF not shown). Based on the subscriber service profile, the S-CSCF first passes control to the BroadWorks Application Server over the ISC interface for originating services. Control is returned back to the S-CSCF for terminating services. A call termination is then triggered based on the service profile, passing control to a terminating Application Server (in this case, handled by the same Application Server). Control is then given back to the S-CSCF.

Note that the IMS defines a Service Capability Interaction Manager (SCIM), functionally located between the S-CSCF and the Application Server. The SCIM may dispatch calls via triggers to one or more Application Server components based on the subscriber profile (that is, first to a prepaid Application Server, then to BroadWorks, and so on).

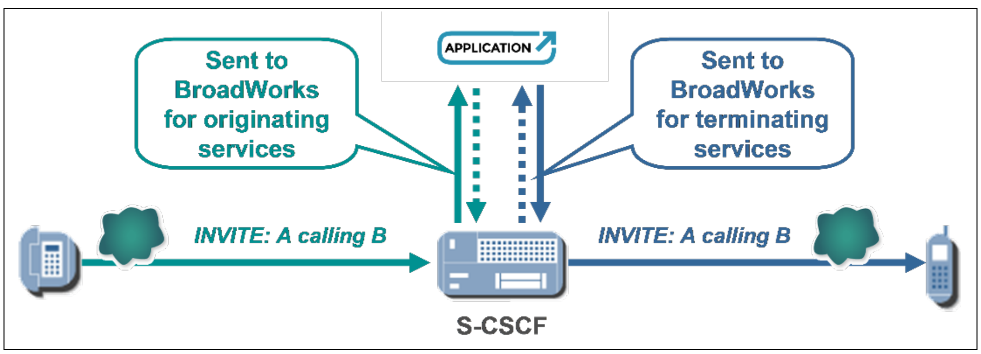

Figure 6 Originating and Terminating Service Triggers

4.2 Basic End-to-End Call Flow with Application Server Interaction

Other interactions are required to deliver a call from Party A to Party B. As illustrated in *Figure 7*, Party A may be located in a different part of the network from Party B, using a different P-CSCF or requiring the services of an I-CSCF for connection between different IMS core networks. The application of service logic is tied to the subscription associated with each user. In the case where Party A calls Party B, originating service logic is applied based on Party A and terminating logic is applied based on Party B. This includes the selection of services and the selection of required components (for example, Application Server or S-CSCF).

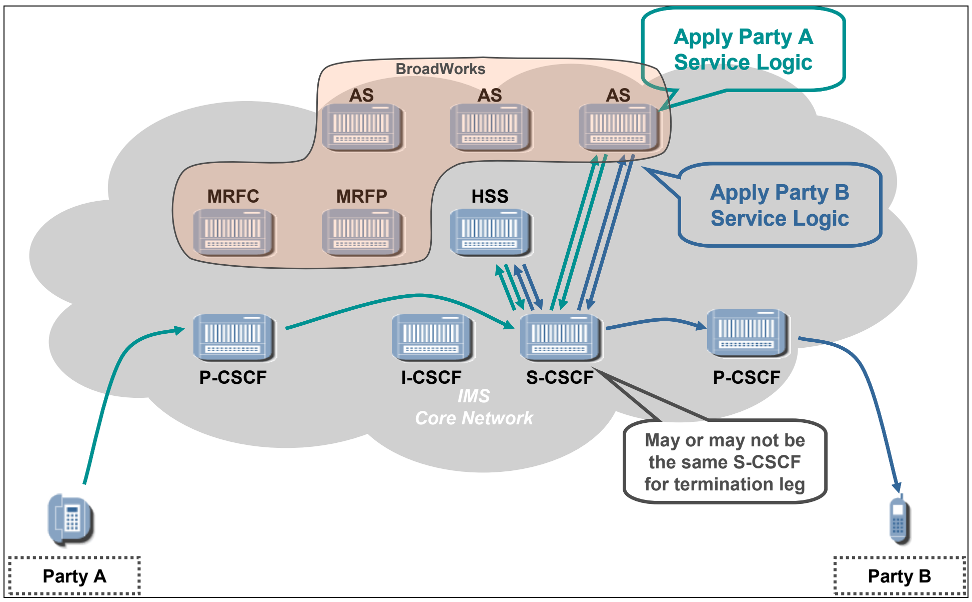

Figure 7 Party A to Party B Signaling Call Flow

To illustrate this at a deeper level, *Figure 8* shows a basic call flow between these components. Each user agent (UA) is assumed to be a SIP-enabled device. For non-SIP endpoint devices, the UA could be a gateway such as a mobile G-MSC with integrated softswitch.

UA A initiates a call with a SIP INVITE, which requests a call from A to B. This is sent to the proxy-CSCF assigned to UA A. Through user authentication methods (not shown) and subscriber information provided from the HSS, an S-CSCF is selected as a destination for the SIP INVITE. The S-CSCF receives the SIP INVITE. If UA A is not yet registered, the S-CSCF invokes a procedure with the HSS using a combination of the Cx-Put and Cx-Pull operations (for more information, see *3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2* [15]) that assigns an S-CSCF to the UA A Public User Identity and downloads user information required by the S-CSCF from the HSS. This procedure is mapped to the commands Server-Assignment-Request/Answer in the Diameter application specified in *3GPP TS 29.228, IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signaling flows and message contents* [17] and *3GPP TS 29.229, Cx and Dx interfaces based on the Diameter protocol; Protocol details* [18].

Based on the relevant user information, including the initial filter criteria (IFC), the S-CSCF selects an application server to service the origination requests and sends the SIP INVITE to the assigned SIP application server (for example, the BroadWorks Application Server). The application server applies the appropriate services and returns the SIP INVITE back to the S-CSCF. The same process is repeated for terminating services for UA B.

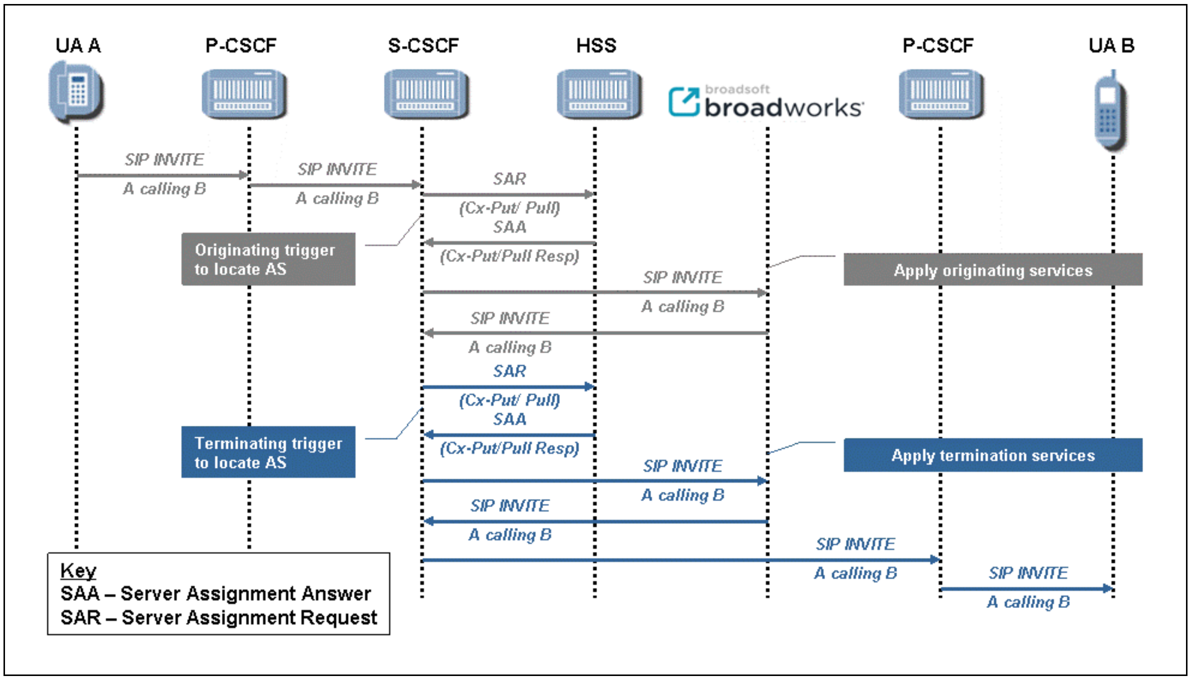

Figure 8 Call Completion: System View

Figure 9 shows the same interactions with more detail at the SIP messaging level.

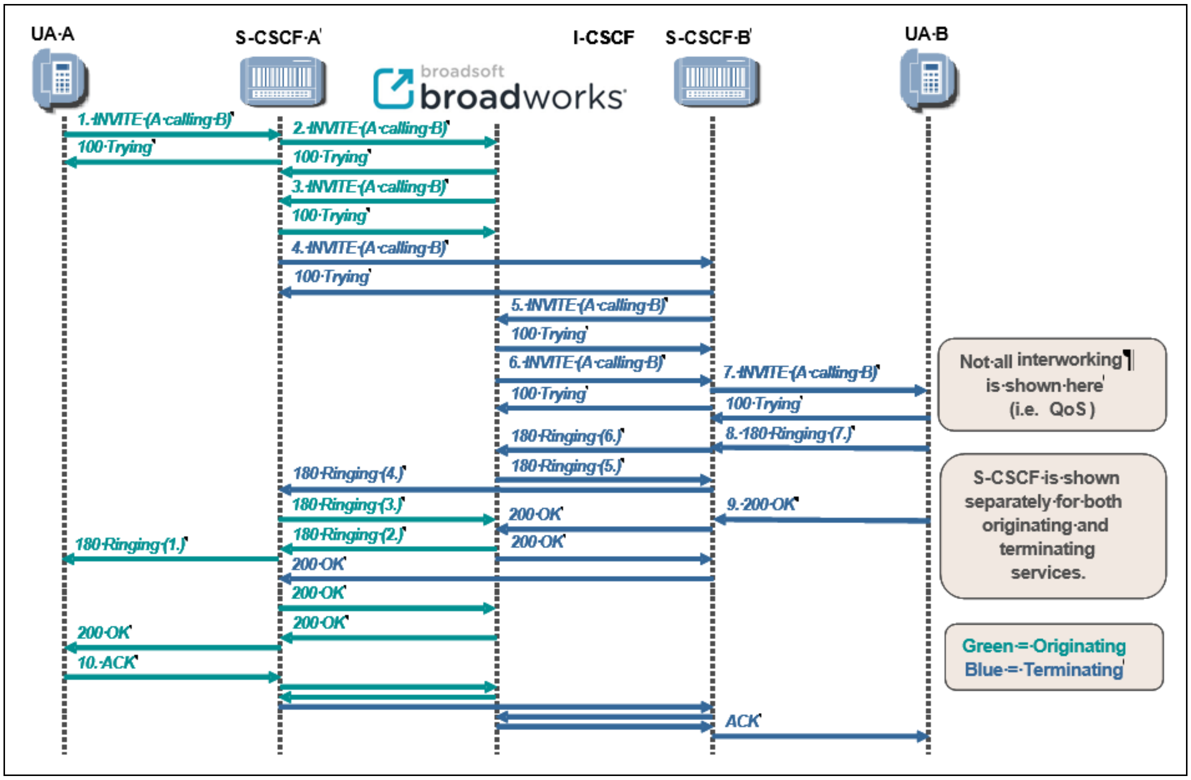

Figure 9 Call Completion: S-CSCF/Application Server Interoperation

Figure 9 shows the SIP signaling messages. It is helpful to note that end-to-end response messages (180 Ringing and 200 OK in the figure) propagate from user agent (UA) B to UA A over the same signaling path as the INVITE. To help illustrate this, each 180 Ringing arrow in the figure shows the message number of its corresponding SIP INVITE.

1) The Initial INVITE triggered from UA A calling UA B is sent to Party A's S-CSCF. (The invite may or may not go through a P-SCSF and I-SCSF, not shown).

2) The S-CSCF evaluates and approves the INVITE, triggering originating services. The S-CSCF then routes the INVITE to the BroadWorks Application Server.

3) The Application Server executes originating services for Party A, generating an INVITE based on these services, and sending it back to the S-CSCF to continue call processing.

4) Party A's S-CSCF evaluates and approves the INVITE, routing it to Party B's S-CSCF.

5) Party B's S-CSCF evaluates and approves the INVITE, triggering terminating services. The S-CSCF then routes the INVITE to the BroadWorks Application Server.

6) The Application Server executes terminating services for Party B, generating an INVITE based on these services, and sending it back to S-CSCF to continue call processing.

7) The S-CSCF performs termination routing, routing the INVITE to UA B.

8) UA B sends a 180 Ringing response back toward UA A. The 180 response propagates back through the network, following the reverse path of the initial INVITE request. For example, the 180 Ringing (5.) response is the response for the 5. INVITE request.

9) UA B answers the call, initiating a 200 OK response that propagates toward UA A, again following the reverse path of the initial INVITE request.

10) UA A sends an ACK request toward UA B, acknowledging the 200 response and completing the call setup.

The rest of this section shows flow diagrams for specific services. Processes going on in the background, such as HSS interactions and SIP response messages, are not shown. The diagrams only show SIP methods relevant to the delivery of each service.

4.2.1 Out-of-the-Blue Requests

It is important to note that the BroadWorks Application Server can initiate call services on its own, when required to execute a requested service. SIP requests originated by the Application Server, without an apparent association with a received request, are referred to as "out-of-the-blue" (OOTB) requests.

OOTB requests can be considered originating, terminating, or informational (not involving call processing). An originating OOTB request (always an INVITE request) is sent by the BroadWorks Application Server for a subscriber origination. The terminating party may or may not be a BroadWorks subscriber. If the Application Server knows the originating subscriber's S-CSCF, then it sends the INVITE request to that S-CSCF. Otherwise, depending on the configuration, it may send the INVITE request to a system-wide configured CSCF. A terminating OOTB request (again, always an INVITE request) is sent by the Application Server to terminate to a BroadWorks subscriber. The originating party may or may not be a BroadWorks subscriber. If the Application Server knows the S-CSCF for the terminating subscriber, then it sends the INVITE request to that S-CSCF. Otherwise, depending on the configuration, it may send the INVITE request to a system-wide configured CSCF. An informational OOTB request is a request that does not initiate a call, such as a NOTIFY message for Message Waiting Indication (MWI). The Application Server sends an informational request to an S-CSCF following a procedure similar to that for a terminating OOTB request.

In certain configurations, the Application Server sends OOTB requests when there appears to be a loose association with a received request. A good example of this is a blind transfer after answer scenario. When the transfer begins, the Application Server sends a new INVITE request to the transfer-to party. The new INVITE request has a loose association with the INVITE request the Application Server received when the call was set up. Depending on the configuration, this new INVITE request may be OOTB. If the new INVITE request is OOTB, then the Application Server sends it to the S-CSCF associated with the transferring party and generates a new IMS charging identifier (ICID) value in the *P-Charging-Vector* header. If it is not OOTB, then the Application Server sends it to the S-CSCF address taken from the *Route* header of the original INVITE request and copies the IMS charging identity (ICID) value of the original INVITE request. Thus, the OOTB and non-OOTB INVITE requests differ in two significant ways:

- The S-CSCF that the INVITE is routed to

  -and-

- The ICID value in the *P-Charging-Vector* header

There is also a hybrid configuration where the new INVITE is routed to the S-CSCF address from the received Route header, but with a new ICID value.

4.3 Service Flow Example – Call Transfer

Figure 10 shows a typical call transfer scenario that shows how SIP messages are used and propagated across the IMS control layer.

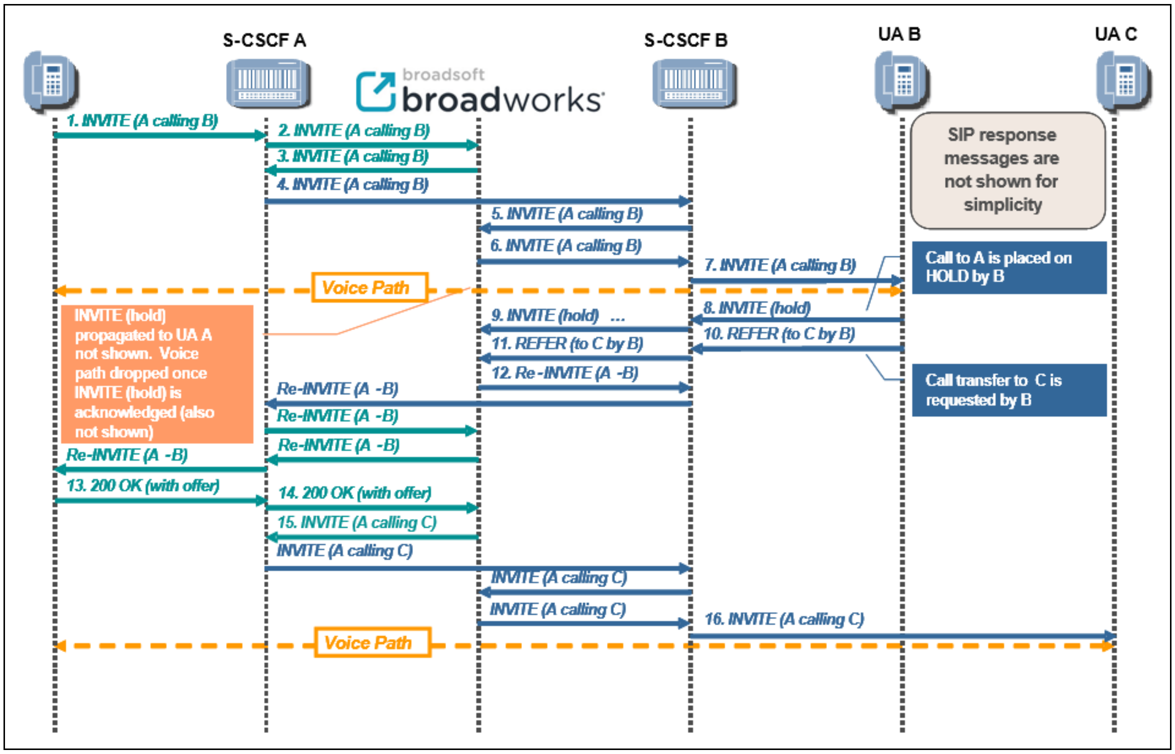

Figure 10 Call Transfer

A description of each signaling message follows:

1) The Initial INVITE triggered from UA A calling UA B is sent to the S-CSCF. (The invite may or may not go through a P-SCSF and I-SCSF, not shown).

2) The INVITE is evaluated and approved, triggering an originating service. The S-CSCF then passes the INVITE to the BroadWorks Application Server.

3) The Application Server executes originating services, generating an INVITE based on these services, and sends an INVITE to the S-CSCF to continue call processing.

4) The INVITE is evaluated and approved, triggering a terminating service. The S-CSCF then passes S-CSCF B to Party B.

5) S-CSCF B evaluates and approves the INVITE, triggering a terminating service. S-CSCF B then passes the INVITE to the BroadWorks Application Server.

6) BroadWorks executes originating services, generating an INVITE based on these services and sending an INVITE to S-CSCF B to continue call processing.

7) S-CSCF B performs termination routing, sending the INVITE to UA B.

8) UA B places the call on HOLD, triggering an INVITE (0.0.0.0) to cause a HOLD condition.

9) INVITE (0.0.0.0) is propagated to the BroadWorks Application Server. Propagation of the INVITE (hold) to UA A is not shown. UA B drops the voice path once the INVITE (hold) is acknowledged (also not shown). For blind transfer (or transfer through third-party call control), this INVITE hold may not occur.

10) UA B transfers the call to UA C, which triggers a REFER message.
11) The REFER message is propagated to the BroadWorks Application Server.
12) The Application Server now knows that UA A must connect to UA C, but first must get the available Session Description Protocol (SDP) information from UA A. To do this, a Re-INVITE on the A-B session is sent to UA A. The Re-INVITE is propagated to UA A.
13) UA A responds with a 200 OK, which includes the SDP offer.
14) The S-CSCF propagates the SDP information to the Application Server.
15) The Application Server creates a new INVITE on behalf of UA A, as if UA A were calling UA C. Depending on the Application Server's configuration, this INVITE may be an out-of-the-blue INVITE.
16) When the INVITE reaches UA C, a voice path is set up from UA C to UA A.

4.4 Service Flow Example – Simultaneous Ringing

Figure 11 shows the delivery of a simultaneous ringing scenario that shows how SIP messages are used and propagated across the IMS control layer.

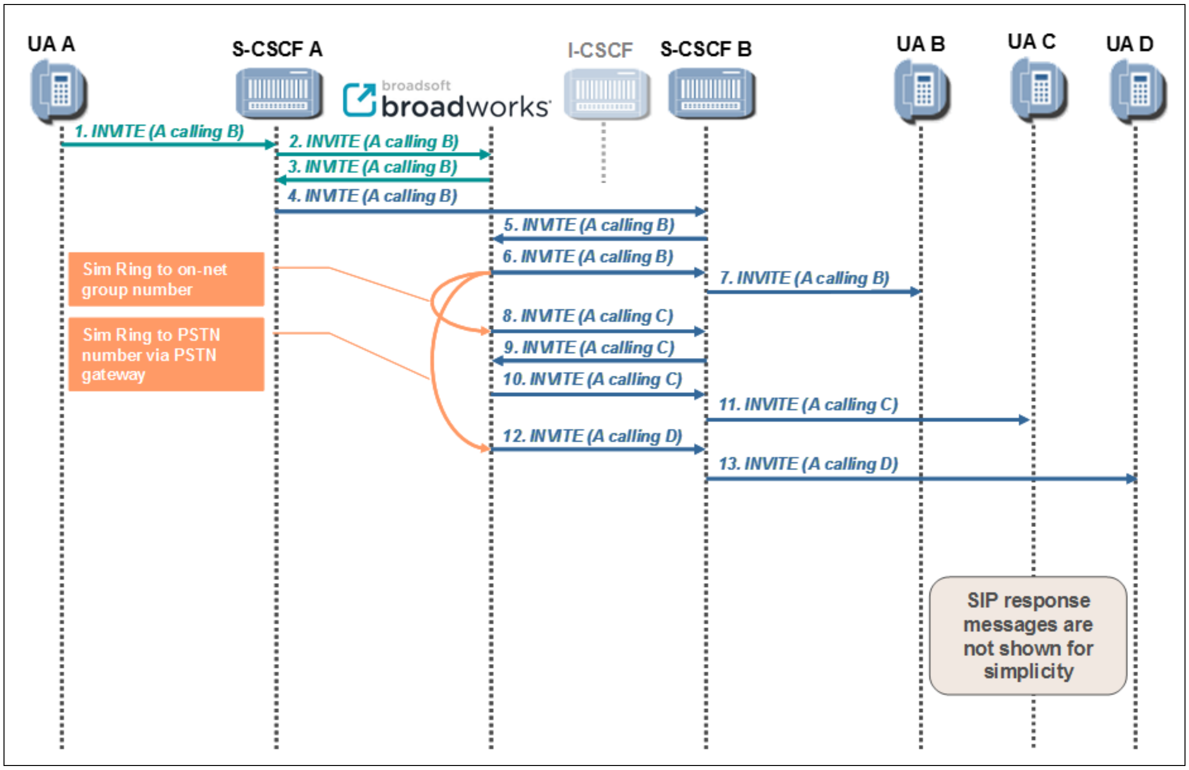

Figure 11 Simultaneous Ringing

A description of each signaling message follows:

1) The Initial INVITE triggered from UA A calling UA B is sent to the S-CSCF. (The invite may or may not go through a P-SCSF and I-SCSF, not shown).

2) The INVITE is evaluated and approved, triggering an originating service. The S-CSCF then passes the INVITE to the BroadWorks Application Server.

3) The Application Server performs originating services, generating an INVITE based on these services, and sends an INVITE to the S-CSCF to continue call processing.

4) The INVITE is evaluated and approved, triggering a terminating service. The S-CSCF then passes S-CSCF B to Party B.

5) The INVITE is evaluated and approved, triggering a terminating service. S-CSCF B then passes the INVITE to the BroadWorks Application Server.

6) The Application Server performs termination services, which rings three devices: the called number B, DN C hosted by BroadWorks (see step 8), and DN D hosted on the PSTN (see step 12). The Application Server sends an INVITE to the S-CSCF B to continue call processing.

7) S-CSCF B performs termination routing and sends the INVITE to UA B.

8) The Application Server sends a new origination INVITE to S-CSCF B destined for UA C. Depending on the Application Server's configuration, this INVITE may be an out-of-the-blue INVITE.

9) The INVITE is evaluated and approved by S-CSCF B, triggering a terminating service. S-CSCF B then passes the INVITE to the BroadWorks Application Server, since in this example UA C is an on-net BroadWorks user.

10) The Application Server performs termination services for UA C, generating an INVITE to S-CSCF B to continue call processing.

11) S-CSCF B performs termination routing and sends the INVITE to UA C.

12) The Application Server sends a new origination INVITE to S-CSCF B destined for UA D. Depending on the Application Server's configuration, this INVITE may be an out-of-the-blue INVITE.

13) S-CSCF B performs termination routing, determining that the call should be routed to a PSTN gateway, and sending the INVITE to UA D via the selected gateway.

NOTE: Simultaneous Ringing to B, C, and D (steps 6, 8, and 12) are initiated at the same time.

5 BroadWorks IMS Integration

Configuring BroadWorks for use in IMS architecture is a straightforward task. Although IMS offers the comfort of standard, well-defined interfaces, the format and interpretation of messages exchanged over these interfaces must be well understood. This section provides insight on these details, as well as guidelines for the deployment of BroadWorks in an IMS framework. Specific topics include:

- IMS subscriber information and Public User Identity configuration
- Distributed group calls (group/enterprise calls)
- Originator/Terminator determination
- Route header proxying
- Supported IMS P-headers
- Support for charging

For more information on this, see the *BroadWorks AS Mode ISC Interface Specification* [4].

5.1 User IMS Subscription and Addressing

For the Application Server to deliver services:

- Subscribers must be authorized to use services.
- There must be a way to find each subscriber within the service network.
- The types of services authorized for each subscriber must be known.
- Terminal characteristics must be known for the Application Server to determine how to deliver each service.

In IMS deployments, the first three items are defined by the IMS subscription stored in the HSS. The network authenticates and authorizes service use upon UE device registration. Device registration is also used to locate the subscriber. For both operations, each subscriber must be assigned a unique identity. This identity is in turn indexed within the HSS to the set of services that can be delivered.

Terminal characteristics are typically handled within the signaling protocols and may be associated with device identity modules, both of which are outside the scope of this section.

As shown in *Figure 12*, an IMS subscription consists of a Private User Identity (also, IP Multimedia Private Identity [IMPI]) which is a unique global identity defined by the home network operator. The IMPI uniquely identifies a subscription for an IMS subscriber. It uniquely identifies the subscription, and not the user, and it is used by devices to register with the network.

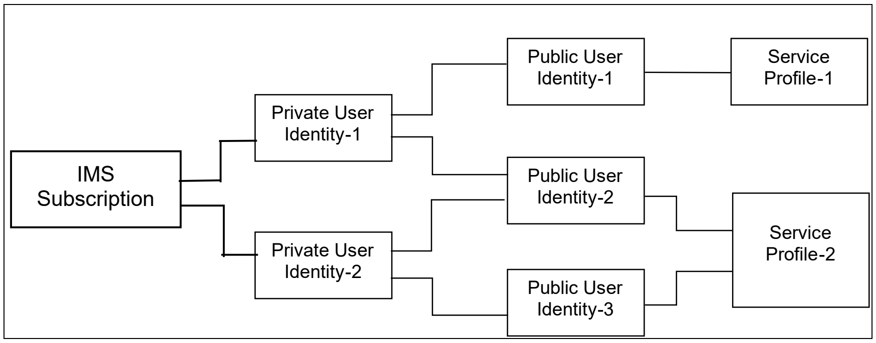

Figure 12 Public User Identity and Private User Identity Relationships

5.1.1 Private and Public User Identities

An IMPI defines a user subscription for authentication and accounting purposes. A home operator allocates an IMPI to each subscriber. The IMPI format is based on a Network Access Identifier (NAI) according to *RFC 2486* [21].

Example: subscriber@operator.com

An IMS subscription can be associated with multiple IMPIs. An IMPI can be associated with multiple Public User Identities (also, IP Multimedia Public Identity, [IMPU]), as shown in *Figure 12* (from *3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2* [15]). In essence, 3GPP allows a subscriber to have multiple PUIs containing both SIP URI and TEL URI addresses.

A Public User Identity (PUI) is a publicly routable address for the user for initiating sessions, equivalent to an Address of Record, as that term is defined in *RFC 3261*. A home operator allocates at least one PUI to each subscriber.

SIP URI example (according to *RFC 3261* [23]): SIP:alice.doe@broadsoft.com

Telephone URI example (E.164-style numbering according to *RFC 2806* [28]): Tel:+1-301-977-9440

A subscriber can have more than one PUI (for example, for business versus personal identification).

5.1.2 Configure PUIs for BroadWorks Subscribers

A BroadWorks subscriber definition is analogous to an IMS service profile. It contains both the PUI and an application service profile.

Each PUI should be associated with a BroadWorks subscriber. The PUI is configured on a per-subscriber basis within the BroadWorks Application Server.

Each BroadWorks subscriber has the following addressing options:

- Primary SIP PUI: The primary SIP PUI of each BroadWorks user is the Public Identity configured for the user’s primary identity/device profile. These PUIs are used both for network translations and for call originations and terminations.
- Other SIP PUIs: BroadWorks subscribers may have other SIP PUIs, determined by the following settings:
  - Aliases: A subscriber can have multiple aliases. These URIs are used only for network translations and optionally for terminations.
  - User ID: The BroadWorks user ID of each subscriber is also implicitly considered a SIP URI PUI analogous to the aliases described above.

- Shared Call Appearance PUIs: Each subscriber can have multiple additional SIP PUIs used for Shared Call Appearance (SCA) services. These PUIs are used only for call originations and terminations, not for network translations.
- Video Add-On PUI: Each subscriber may have an additional SIP PUI that represents a video-enabled endpoint used to deliver the video portion of calls. These URIs are used only for call originations and terminations, and not for network translations.[1]

- Primary TEL PUI: Each subscriber may have a primary telephone number configured for his or her account. These PUIs are used both for network translations and for call originations and terminations.
- Alternate TEL URI PUIs: Each subscriber may be assigned the Alternate Numbers service, which allows administrators to assign him or her additional telephone numbers. These PUIs are used only for network translations and optionally for terminations.

Most PUIs listed above are configured for each subscriber on the *Addresses* page of the Application Server web portal that follows.

[1] The full explanation of an origination from a VAO device is a little more complicated. If the Application Server receives an originating INVITE request that contains a subscriber's Video Add-On PUI as the originating party (for example, the VAO PUI is in the *P-Asserted-Identity* header), then it correctly identifies the subscriber, and the INVITE processing takes place in the context of that subscriber's originating service profile. In this sense, the VAO PUI is allowed for originations. However, originations are not allowed from a Video Add-On device, even in stand-alone mode. Therefore, the Application Server blocks the origination.

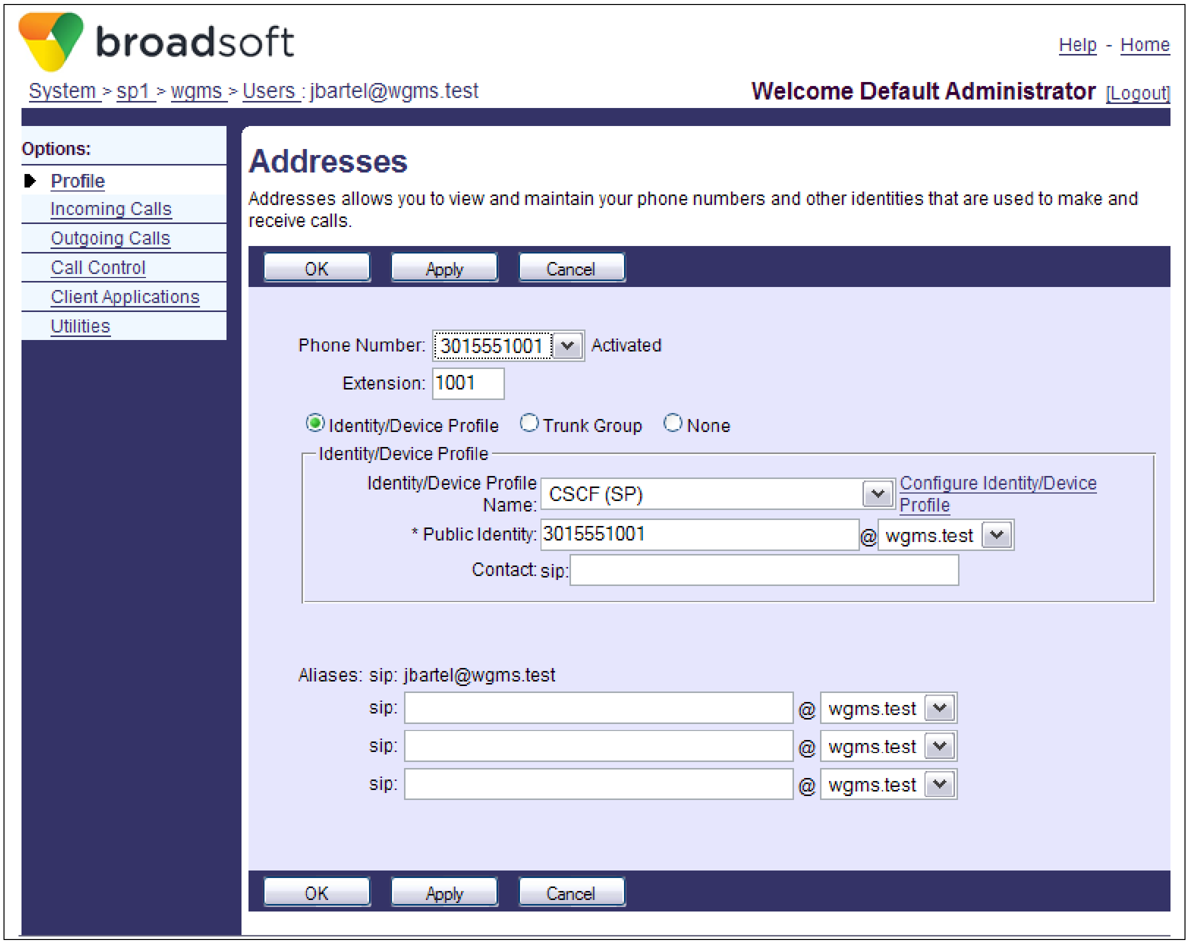

Figure 13 User Addresses Page

NOTE: Only devices that populate the host portion of their identity headers with a domain known to the Application Server can be used in IMS mode. Devices that use their own IP addresses or fully qualified domain names (FQDNs) are not supported.

Additional alternate SIP PUIs can be specified on the configuration pages for the Shared Call Appearance and Video Add-On services. Additional TEL PUIs can be specified on the configuration page for the Alternate Numbers service. For more information, see the *BroadWorks Application Server Group Web Interface Administration Guide, Part 2* [1].

5.1.3 Configure Service Profiles for BroadWorks Subscribers

Each user account on the BroadWorks Application Server can be assigned a wide range of individual call control services. In addition, the service profile of each subscriber is affected by services assigned to the group to which the subscriber belongs. These services, taken together, provide application service profiles for subscribers.

5.1.4 Public Service Identities

Public Service Identities (PSI)[2] are used to identify services. Examples of such services include:

- Auto Attendant
- Call Center
- Hunt Group
- Meet-Me Conferencing
- Voice Portal
- BroadWorks Anywhere Portal

A PSI, similar a PUI, can be either a Tel URI or a SIP URI. A home operator allocates a PSI to a service. For example:

SIP:vportal@operator.com

Tel:+1-301-555-1111

Using BroadWorks in IMS mode, a PSI is mapped to a virtual subscriber that has an assigned PUI, for the system to process calls on behalf of the virtual subscriber. This requires the virtual subscriber to have a unique PUI for use in the appropriate SIP headers (for example, *Request-URI, P-Asserted-Identity*, and so on).

[2] PSI is not an abbreviation within the IMS but is used as a convenience in this document.

Virtual subscribers are provisioned with PUIs in much the same way as regular subscriber accounts. However, virtual subscribers allow you to specify a primary SIP PUI without providing an identity/device profile, as follows.

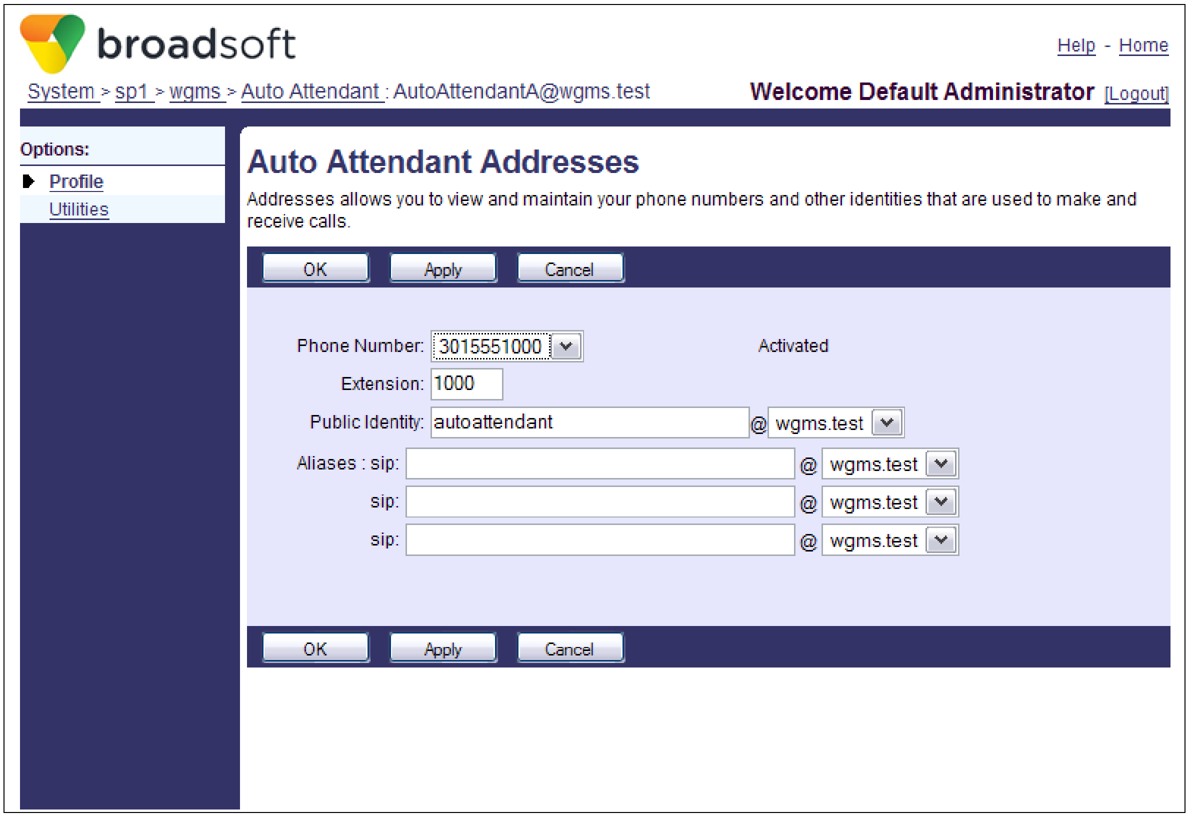

Figure 14 Auto Attendant Addresses Page

5.2 BroadWorks Distributed Group Calls in IMS

A BroadWorks distributed group call (DGC) is a group/enterprise call that is routed over the network from the originating call half to the terminating call half instead of being routed internally within the Application Server. In IMS mode, all group/enterprise calls are distributed group calls that go through the S-CSCF.

For the DGC information to be useful for the terminating call half, the terminating call half must be able to recognize the call as a group/enterprise call. This requires the terminating Application Server to retrieve information necessary for call processing.

DGCs include special information in the terminating INVITE that allows the terminating call half to provide group/enterprise services using the *X-BroadWorks-DGC* header.

NOTE: The CSCF must proxy certain BroadSoft-proprietary SIP headers for DGC calls to work correctly. These headers include the *X-BroadWorks-DGC* header and the *P-BroadWorks-Endpoint-Owner-ID* header. Additionally, BroadWorks includes proprietary parameters in the *Diversion, History-Info*, and *Reason* headers that MUST be proxied by CSCFs and other Application Servers for calls between BroadWorks subscribers to be processed correctly. This includes not only distributed group calls but also calls between BroadWorks subscribers in different groups.

5.3 Originator/Terminator Determination in IMS

When the BroadWorks Application Server receives an INVITE request, it must decide whether to execute originating services or terminating services. The rules for how the Application Server makes this decision are described in the *BroadWorks AS Mode ISC Interface Specification* [4]. Rather than depend on the Application Server to make the correct determination on its own, however, BroadSoft recommends that the IMS operator configure the S-CSCF and initial filter criteria (IFC) to indicate to the Application Server in the INVITE request whether it should execute originating or terminating services.

5.4 Call Routing in IMS

The BroadWorks Application Server interfaces with the S-CSCF via the ISC interface. Therefore, BroadWorks does not perform routing, as it does in stand-alone deployments, and it sends all outgoing INVITE requests to an S-CSCF. How the Application Server selects an S-CSCF depends on whether or not the request is out-of-the-blue. For more information regarding out-of-the-blue requests, see section *4.2.1 Out-of-the-Blue Requests*.

If the request is not out-of-the-blue, then the Application Server chooses the S-CSCF for the outgoing request by examining the *Route* headers of the corresponding incoming request. The first *Route* header entry of the incoming request must indicate the URI of the Application Server itself. The Application Server removes this first *Route* header when it creates the outgoing request. The second *Route* header entry of the incoming request contains the URI of the S-CSCF to which the Application Server sends the outgoing request. The Application Server copies this second *Route* header entry and any additional entries into the outgoing request.

If the request is out-of-the-blue, then the Application Server uses a combination of configured and dynamic data to obtain the S-CSCF URI for the outgoing request, depending on the system configuration. The Application Server can obtain the S-CSCF URI for a BroadWorks subscriber from Sh interface data, a third-party registration, a statically configured contact address, or a system-wide configured URI. The rules for the S-CSCF selection are described in section *6.2.9 support3rdPartyRegistration*.

5.5 IMS P-Headers

IMS requires the use of several private headers (P-Headers) to meet telephony needs, shown in the following table. P-Headers are optional extensions to SIP, defined in *RFC 3325* [25] and *RFC 3455* [26]. These parameters are also referenced in 3GPP specifications.

P-Header	Description
P-Asserted-Identity	Allows the network (that is, P-CSCF) to assert a public user identity used to identify the calling user.
P-Called-Party-ID	Allows the terminating UE to learn the dialed public user identity that triggered a call.
P-Access-Network-Info	Allows the UE to provide information related to the access network it is using (for example, cell ID).
P-Visited-Network-ID	Allows the home network to discover, via registration, the identities of other networks used by the user.
P-Associated-URI	Allows the home network (that is, S-CSCF) to return a set of URIs associated with the public user identity under registration.
P-Charging-Function-Addresses	Allows for distributing the addresses of charging function entities.

P-Header	Description
P-Charging-Vector	Allows for sharing of charging correlation information (for example, IMS Charging Identity [ICID]).

Table 2 IMS Private Header (P-Header) Summary

Most of these parameters are supported in BroadWorks Release 19. For more information, see the *BroadWorks AS Mode ISC Interface Specification* [4].

5.6 Charging in IMS

Charging in an IMS deployment is controlled primarily by two headers: *P-Charging-Vector* and *P-Charging-Function-Addresses*.

5.6.1 P-Charging-Vector Header

The *P-Charging-Vector* is the key component used to correlate calls between nodes in IMS.

Three types of correlation information are transferred: the IMS Charging Identity (ICID) value, the address of the SIP proxy that creates the ICID value, and the Inter-Operator Identifiers (IOI).

- The ICID is a value used to correlate charging records that identifies a dialog or a transaction outside a dialog. The ICID must be a globally unique value. One way to achieve global uniqueness is to generate the ICID by combining a locally unique value with the host name or IP address of the SIP proxy that generated the locally unique value.
- The *P-Charging-Vector* used by the BroadWorks Application Server is populated using the initial value received in the INVITE. For OOTB calls BroadWorks generates a unique *P-Charging-Vector* having the format <BroadWorks value>@<BroadWorks AS Address>.

  Example: icid-value="17100259105050419-901209215@192.168.0.8"

  BroadWorks also adds a *P-Charging-Vector* to the SIP INVITE if one is not received from a CSCF. The ICID value has the format <SIP Call-ID from the INVITE>+<BroadWorks value>@<BroadWorks AS Address>.

  Example: icid-value=e5882272-2866-435c-81c5-f7ab11680d50@192.168.0.36+16092950705050419-1234730916@192.168.0.8

5.6.2 P-Charging-Function-Addresses Header

The *P-Charging-Function-Addresses (PCFA)* header informs network elements of the addresses of entities used to receive and record charging information. The Application Server supports the PCFA header as follows:

- The PCFA header received in an INVITE is proxied in the INVITE the Application Server sends back to the S-CSCF.
- When a new call leg is created (for example, by the Call Forwarding or Simultaneous Ringing services), the PCFA received in the INVITE for the original leg is included in the INVITE sent to the S-CSCF for the new call leg.
- The PCFA header received in an 18x/200 OK response is proxied in the 18x/200 OK the Application Server sends back to the S-CSCF in normal call scenarios.

- When a new call leg is created (for example, by the Call Forwarding or Simultaneous Ringing services), the PCFA received in an 18x/200 OK response for the new leg is not proxied back to the original call leg. Instead, the 18x sent back to the original call leg contains no PCFA header, and the 200 OK sent back to the original call leg contains the PCFA received in the original INVITE.
- The Application Server captures the value of the PCFA header in its CDRs.

5.7 Sh Interface

The Sh interface is a Diameter connection established between BroadWorks Application Server and the Home Subscriber Server (HSS). BroadWorks uses this connection to retrieve from the HSS the identity of the S-CSCF associated with a BroadWorks user. The S-CSCF identity is used to route out-of-the-blue requests to the proper S-CSCF. For more information, see section *4.2.1 Out-of-the-Blue Requests*.

When a subscriber is first added, the Application Server registers to the HSS to be notified of changes in the public identity date, and retrieves the current value. The HSS is then responsible for keeping the Application Server up-to-date.

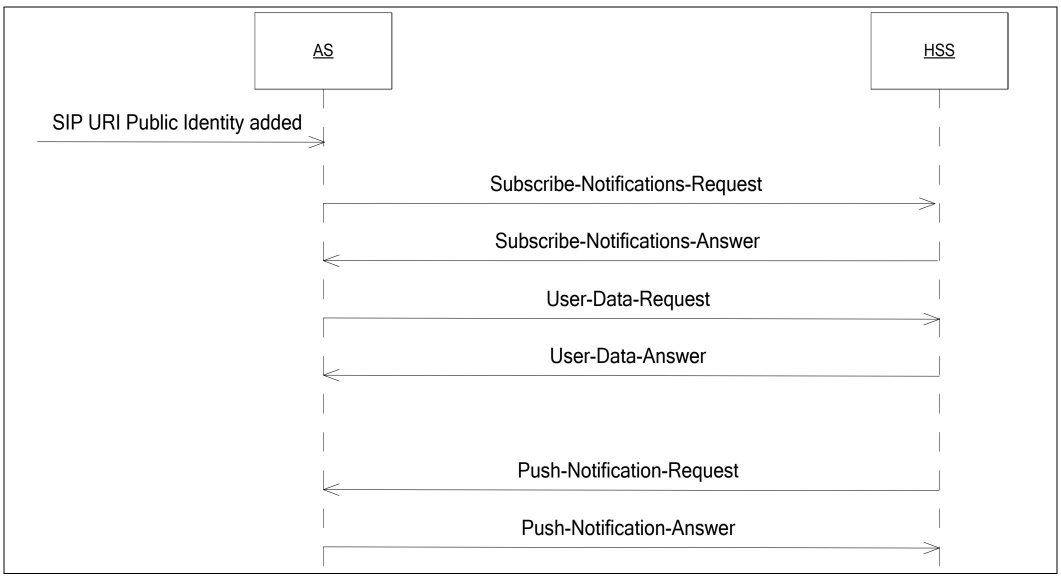

Figure 15 Message Flow between the Application Server and HSS

A refresh procedure that retrieves the profile of all existing users can also be initiated manually.

Detailed information on the Sh interface can be found in the *BroadWorks Sh Interface Specification* [5].

5.8 Rf Interface

The Rf interface is a Diameter connection established between the BroadWorks Application Server and a Charging Data Function (CDF) for billing purposes. BroadWorks records internally accounting information on the calls in progress, and transmits this information in real time over the Rf interface.

BroadWorks can connect to multiple CDFs simultaneously. The Application Server uses the information from the *P-Charging-Function-Addresses* header to select the CDF(s) that receive the accounting information for this specific call.

Billing information sent to the CDF over the Rf interface is divided between accounting sessions for answered calls and accounting events (ACR event) for unanswered calls. Accounting sessions are composed of one ACR Start, zero or more ACR Interims, and one ACR Stop.

The typical flow of events for an answered call is shown in *Figure 16*. In this figure, Party A calls Party B. The figure is valid for both the originating and the terminating party Application Server.

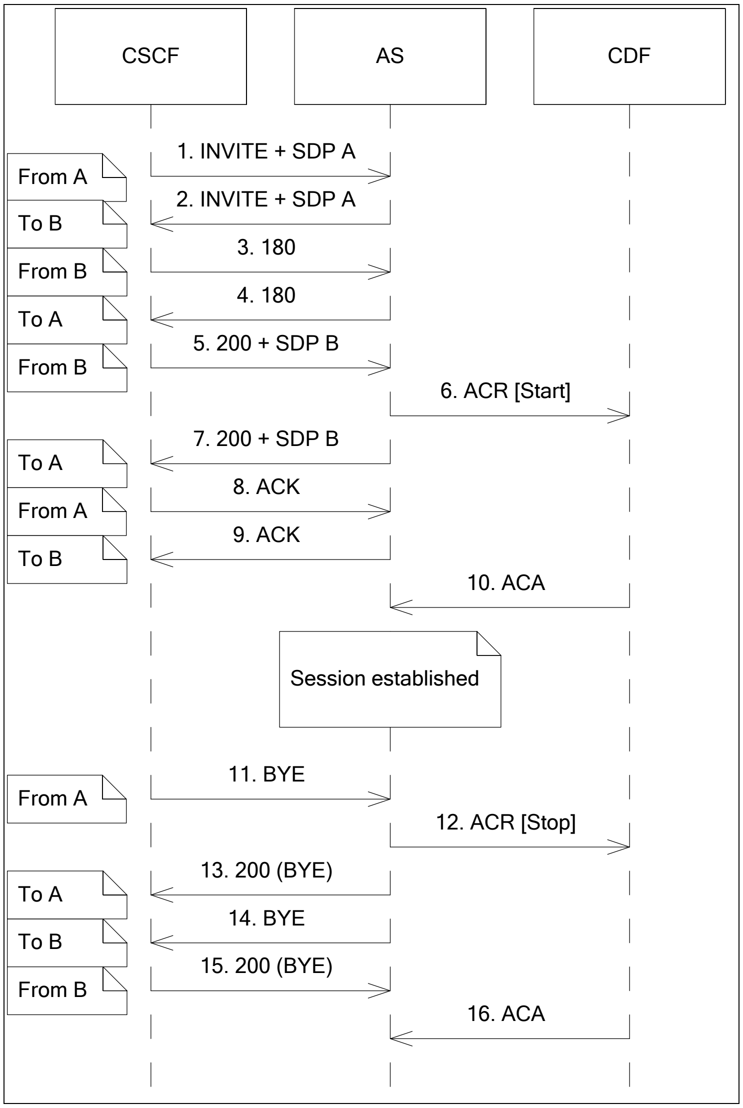

Figure 16 Rf Interface Messaging for Basic Call

For more information on the Rf interface, see the *BroadWorks Rf/Ro Interface Specification* [6].

5.9 Ro Interface

The Ro interface is a Diameter connection established between the BroadWorks Application Server and an Online Charging System (OCS) for online charging information, such as that used for prepaid services. The Application Server can use information from the OCS at call setup time to determine whether an originating or terminating subscriber has sufficient credits to allow the call to continue. It also reserves and debit credits when the call is allowed to proceed.

Online billing over the Ro interface is performed with BroadWorks sending a request to the OCS at call setup time, and waiting for a response before proceeding with the call, assuming enough credits can be granted. Credit control sessions are composed of one CCR Initial, zero or more CCR Updates, and one CCR Termination.

Figure 17 shows the sequence of events occurring in the simplest origination or termination scenario. In step 2, the CCR Initial blocks the call until authorization is obtained from the OCS in step 3. Reauthorization following media change is requested at step 10; however, reauthorization does not block call progression. The same behavior applies to Call Release at step 15.

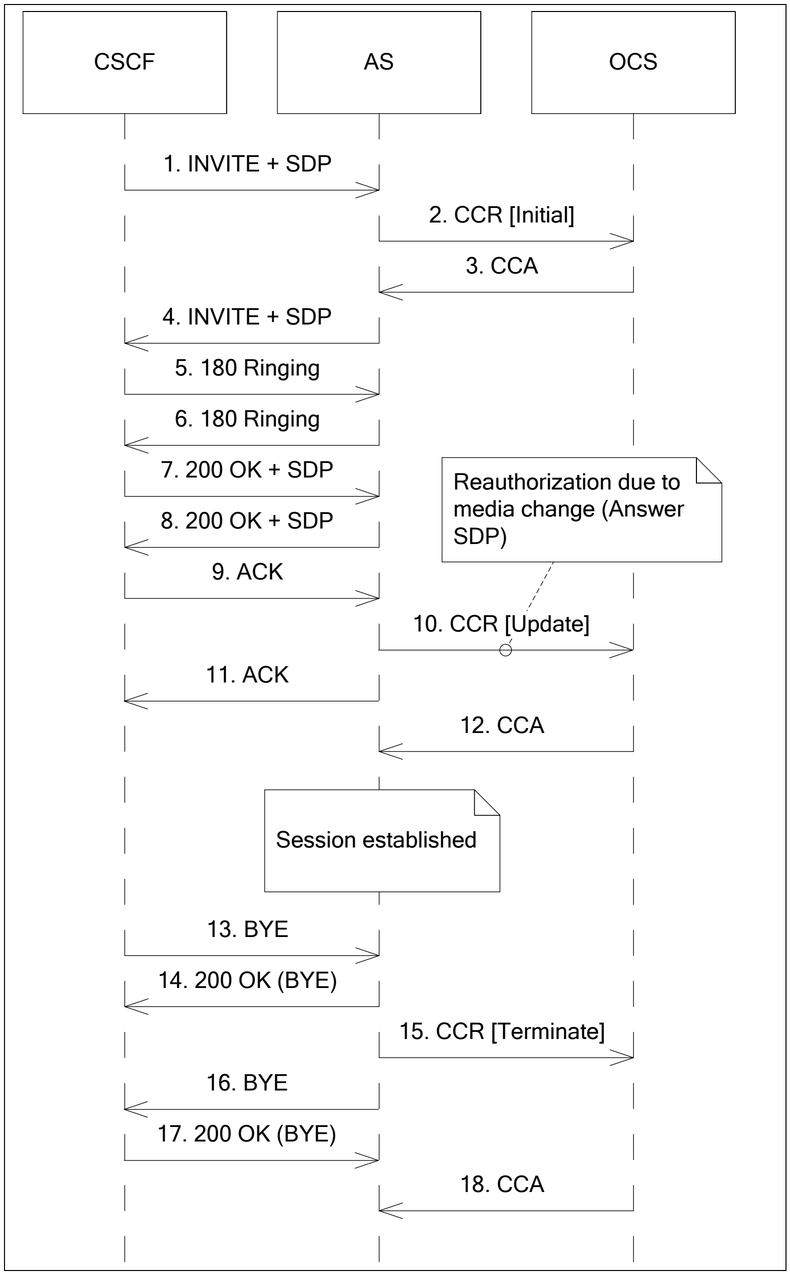

Figure 17 Ro Interface Messaging for Basic Call

Service Price Inquiry is also performed over the Ro interface to obtain tariff information for Advice of Charge (AoC). Upon answer, the Application Server sends a Service Price Inquiry CCR (Credit Control Information) to obtain tariff information. This tariff information is then used to periodically update the current charges and provide AoC to the user device. For more information on AoC, see section *5.10 Advice of Charge*.

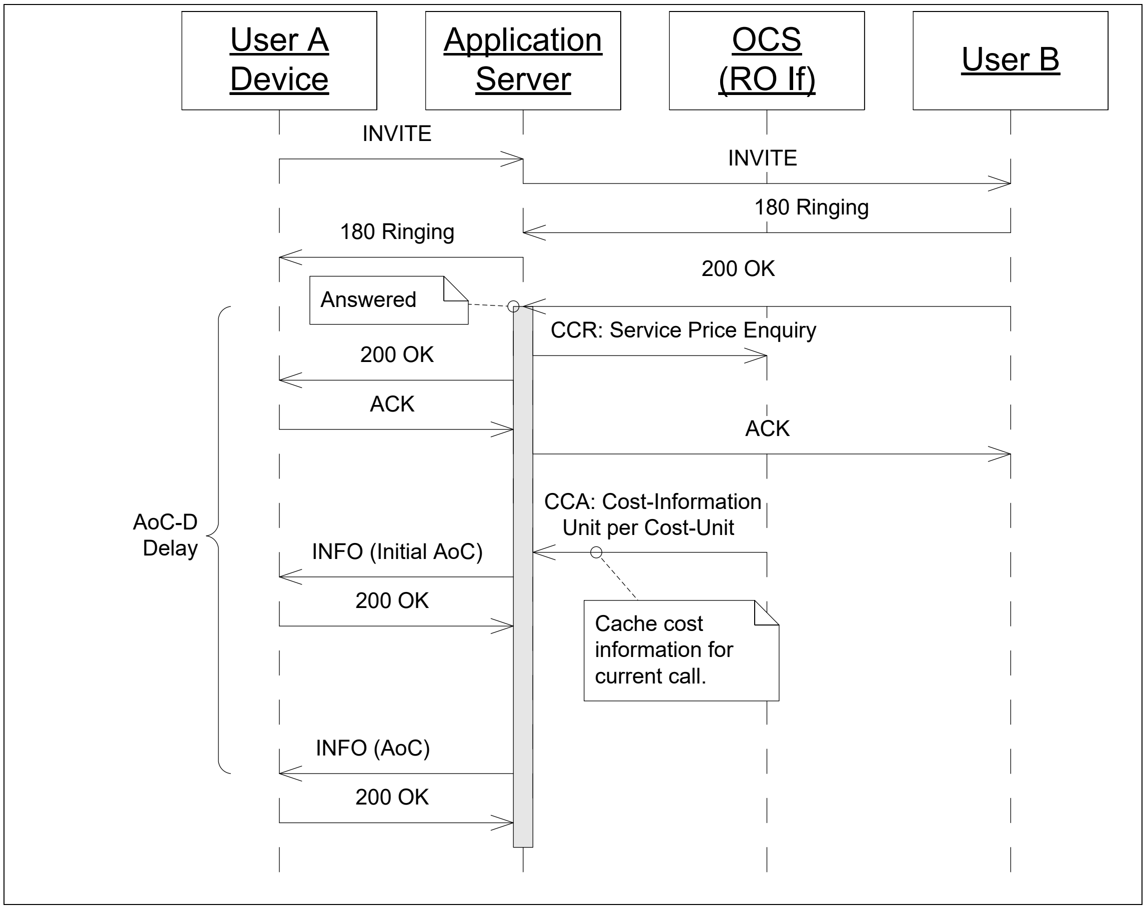

Figure 18 Ro Interface Messaging for Service Price Enquiry and Advice of Charge

5.10 Advice of Charge

BroadWorks supports the Advice of Charge supplementary service described in *3GPP TS 24.647* [16], *3GPP TS 29.658* [19], and *3GPP TS 32.280* [20]. More specifically, it supports AOC-D (during a call) and AOC-E (at the end of a call).

When Advice of Charge is implemented, the Application Server obtains tariff information at the time of a call, tracks the charges that accrue, and provides information about the charges to the originating UE (that is, the "advice of charge" information). The Application Server functions as a Charge Generation Point (CGP). It obtains the tariff information from a Charge Determination Point (CDP).

BroadWorks supports three methods for the Application Server to obtain the tariff information:

- The Application Server may receive tariff information in SIP messages from a downstream CDP, for example, in a SIP 183 response message. The tariff information is included in a message body with MIME type application/vnd.etsi.sci+xml.
- The Application Server may query an OCS via the Ro interface for charging information. Depending on configuration, the Application Server can perform either of the following actions:
  - Send a "Service Price Enquiry" Credit Control Request (CCR) message to the OCS and use the returned Cost-Information to establish the tariff information.

- Send an “AoC Enquiry” CCR message to the OCS and use the returned AoC-Information and Tariff-Information in accordance with *3GPP TS 32.280*. BroadWorks supports only AoCI (non-binding/estimation) information and not AoCC (binding/actual) information.

- The Application Server may query a BroadWorks Rating Function server (RFN) via the Ro interface, similar to the OCS.

The Application Server sends the Advice of Charge information to the originating UE in a SIP message, which may be an INFO or BYE request or a response. If AOC-D is enabled, the Application Server sends Advice of Charge information at regular intervals during the call and at the end of the call. If AOC-E is enabled, then it sends Advice of Charge information only at the end of the call. The information is sent in a message body with MIME type application/vnd.etsi.aoc+xml.

In an alternative implementation, a network element other than the BroadWorks Application Server may function as the CGP, and the Application Server may proxy the Advice of Charge information in SIP messages from the CGP back to the originating UE.

Figure 19 shows a simple call flow in which AOC-D is enabled. In this example, the Application Server obtains the tariff information from a downstream CDP. During the call, it calculates the charges that apply and sends regular SIP INFO requests to the originating UE with the Advice of Charge information. The terminating UE releases the call, and the Application Server includes the Advice of Charge in the final BYE request to the originating UE.

For more information about the Advice of Charge implementation in BroadWorks, see the *BroadWorks Advice of Charge Feature Description, Release 16.0* [10] and the *AoC Tariff Information from OCS Support Feature Description, Release 21.0* [11].

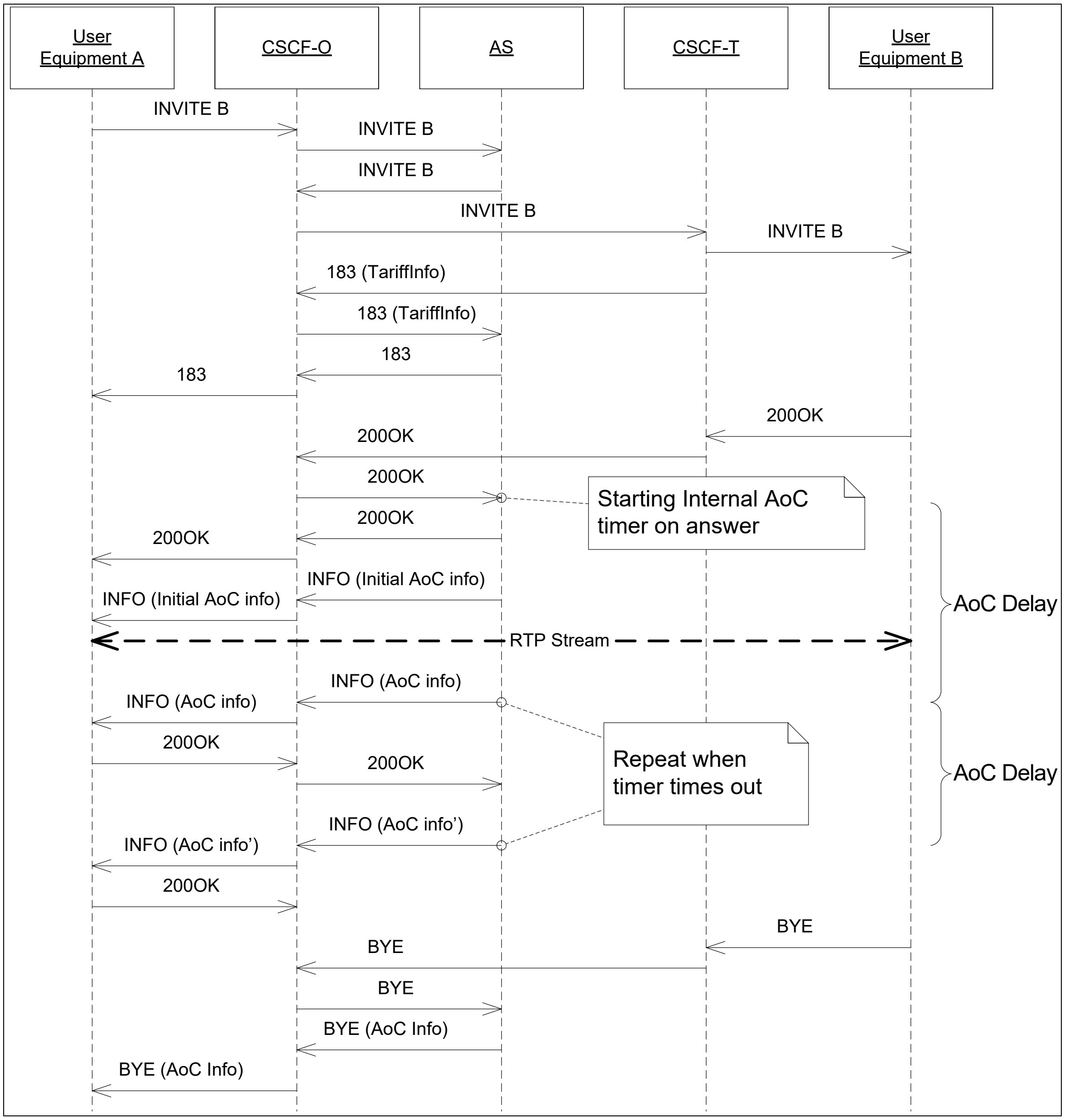

Figure 19 Basic Call Flow for Advice of Charge

6 BroadWorks IMS Operational Settings

This section provides details regarding configuration parameters that can be set for BroadWorks operation with IMS networks.

6.1 BroadWorks Application Server Configuration Parameters: SIP

This section describes the system parameters that can be set at the *Interface/SIP* level of the command line interface (CLI) on the BroadWorks Application Server. These parameters are in the SIP context instead of the IMS context because they affect the Application Server configuration in both IMS and stand-alone modes. The following table summarizes the relevant parameters. The parameters are described in detail in the subsections that follow.

Parameter	Release	Default Value	Comments
useDomainForSubscriber Address	Before Release 11.1	false	Should be set to "true" for IMS deployments.
sendE164	Before Release 11.1	false	Should be set to "true" for IMS deployments.
callingPartyE164-Normalization	Release 14.sp1	systemCountry Code	
supportRFC3966-PhoneContext	Release 14.sp2	true	
includePrivacyUser	Release 14.sp2	true	
useHistoryInfoHeaderOn-NetworkSide	Release 15.0	off	
useAssertedIdentityFor-PrivateCLID	Release 14.sp5 (in IMS context) Release 15.0 (in IMS context) Release 17.sp4 (moved to SIP context)	false	
supportPrivacyNone	Release 14.sp2 Release 15.0	false	
pChargingFunction-AddressesFormat	Release 22.0	RFC7315	
includeDirectoryNumberIn PAI	Release 14.sp5 Release 15.0 Release 22.0	true	

Table 3 Application Server CLI Configuration Parameters at *Interface/SIP* Level

6.1.1 useDomainForSubscriberAddress

useDomainForSubscriberAddress determines whether the Application Server uses the subscriber's domain for subscriber addressing (that is, the host portion of the *From* header when the subscriber originates a call). This parameter should be set to "true" for IMS deployments.

6.1.2 sendE164

sendE164 determines whether the Application Server sends directory numbers in E.164 format. This parameter should be set to "true" for IMS deployments.

6.1.3 callingPartyE164Normalization

callingPartyE164Normalization determines whether the Application Server attempts to normalize a network originator's CLID when that CLID is a phone number not already in E.164 format. If normalization is allowed, then the parameter also determines how the Application Server performs the normalization.

- When the *callingPartyE164Normalization* parameter is set to "none", the Application Server does not attempt to normalize CLID to E.164 format. However, if the CLID is a phone number in E.164 format and the country code matches the terminating subscriber's country code, then the Application Server normalizes the number to a prefixed national format for the termination to the subscriber.
- When the *callingPartyE164Normalization* parameter is set to "systemCountryCode", the Application Server attempts to normalize the CLID to E.164 using the system country code. If the system country code matches the terminating subscriber's country code, then the Application Server further normalizes the CLID to a prefixed national format for the termination to the subscriber.
- When the *callingPartyE164Normalization* parameter is set to "calledCountryCode", the Application Server attempts to normalize the CLID to E.164 using the called country code for the INVITE. The called country code is the country code for the called address. The called address is normally the Request-URI of the INVITE; however, it may come from the *P-Called-Party-ID* header or *Diversion* header for a mobile device. If the called address is not a phone number in E.164 format, then the Application Server uses the system country code instead (that is, the behavior is identical to the "systemCountryCode" setting). If the called country code matches the terminating subscriber's country code, then the Application Server further normalizes the CLID to a prefixed national format for the termination to the subscriber.

The default value of the *callingPartyE164Normalization* parameter is "systemCountryCode".

6.1.4 supportRFC3966PhoneContext

supportRFC3966PhoneContext configures how the Application Server handles the phone-context received in a URI.

- If the *supportRFC3966PhoneContext* system parameter is set to "false", then the phone-context (if any) received in a URI is normally prepended to the number portion of the URI or it is completely ignored.
- If the *supportRFC3966PhoneContext* system parameter is set to "true", then the phone-context (if any) received in a URI is handled as described in the subsections that follow. Note that the phone-context is still stripped of any visual separators when received just as the number portion of the URI is.

The default value for the *supportRFC3966PhoneContext* system parameter is "true".

The phone-context is only valid and used for SIP URIs with user=phone present and for TEL URIs.

6.1.4.1 User Origination/Redirection Destination URI Handling

When the *supportRFC3966PhoneContext* system parameter is set to "true", the phone-context (if any) received in the destination uniform resource identifier (URI) for a user origination/redirection is used as follows:

IMS mode with the *userPhoneErrorCorrection* system parameter set to "full":

- If the phone-context is global-number-digits (starts with a +), then it is used as applicable for directory number (DN) translations. Extension translations are also allowed, but do not use the phone-context. If no group/enterprise match is found, then the Request-URI sent to the Network Server/network contains the phone-context.
- If the phone-context is a domain name (does not start with a +), then group/enterprise digit translations (DN, extension, location code + extension) are performed. If no group/enterprise match is found, then the Request-URI sent to the Network Server/network contains the phone-context.

IMS mode with the *userPhoneErrorCorrection* system parameter set to "identityDomain" or "none":

- If the phone-context is global-number-digits, then it is used as applicable for DN translations. Extension translations are also allowed, but do not use the phone-context. If no group/enterprise match is found, then the Request-URI sent to the Network Server/network contains the phone-context.
- If the phone-context is a domain name and the domain is a valid Application Server domain, then group/enterprise digit translations are performed. If no group/enterprise match is found, then the Request-URI sent to the Network Server/network contains the phone-context.
- If the phone-context is a domain name but the domain is not a valid Application Server domain, then group/enterprise digit translations are not performed and the Request-URI sent to the Network Server/network contains the phone-context.

6.1.4.2 Network Origination Request-URI Handling

When the *supportRFC3966PhoneContext* system parameter is set to "true", the phone-context (if any) received in the Request-URI for a network origination (that is, a user termination from the network) is used as follows. Note that the handling in IMS mode depends on the *userPhoneErrorCorrection* system parameter setting.

IMS mode with *userPhoneErrorCorrection* system parameter set to "full":

- If the phone-context is global-number-digits, then it is used as applicable for DN translations.
- If the phone-context is a domain name, then DN translations are performed.

IMS mode with *userPhoneErrorCorrection* system parameter set to "identityDomain" or "none":

- If the phone-context is global-number-digits, then it is used as applicable for DN translations.
- If the phone-context is a domain name and the domain is a valid Application Server domain, then DN translations are performed.
- If the phone-context is a domain name but the domain is not a valid Application Server domain, then the call is rejected as a network loopback.

6.1.4.3 Other Handling

When the *supportRFC3966PhoneContext* system parameter is set to "true", the phone-context (if any) is proxied in the *From*, *Diversion*, *History-Info*, *P-Asserted-Identity*, and *P-Called-Party-ID* headers.

6.1.5 includePrivacyUser

includePrivacyUser configures whether the Application Server includes the "user" value in the *Privacy* header when privacy is restricted.

- When the *includePrivacyUser* system parameter is set to "true" and privacy is restricted, then the "user", "id", and "critical" values are present in the *Privacy* header sent by the Application Server.
- When the *includePrivacyUser* system parameter is set to "false" and privacy is restricted, then the "id" and "critical" values are present in the *Privacy* header sent by the Application Server. The "user" value is omitted.

The default value for the *includePrivacyUser* system parameter is "true".

6.1.6 useHistoryInfoHeaderOnNetworkSide

useHistoryInfoHeaderOnNetworkSide configures whether BroadWorks should insert a *History-Info* header rather than a *Diversion* header to propagate redirection information on the network side. If it is set to the default value "off", then the Application Server uses the *Diversion* header to convey the redirection information. However, if it is set to "on", then the Application Server uses the *History-Info* header instead of the *Diversion* header.

Note that the choice between *Diversion* and *History-Info* on the access side is not affected by this parameter, since the access side is configured from the Identity/Device Profile policies.

6.1.7 useAssertedIdentityForPrivateCLID

useAssertedIdentityForPrivateCLID determines whether the Application Server uses the *P-Asserted-Identity* (PAI) header for the CLID of a network caller when privacy is requested.

For calls from the network without privacy requested, the Application Server determines the CLID from the *From* header of the incoming INVITE request. In this case, the value of *useAssertedIdentityForPrivateCLID* does not matter. However, if the incoming INVITE requests privacy, by including an appropriate *Privacy* header, the Application Server's behavior depends on the value of *useAssertedIdentityForPrivateCLID*.

If *useAssertedIdentityForPrivateCLID* has its default value of "false" and if the Application Server receives an INVITE request with privacy requested from a network caller, then it determines the CLID from the *From* header. Thus, the behavior is the same as it is for a call without privacy requested.

However, if *useAssertedIdentityForPrivateCLID* is set to "true", then the Application Server determines the CLID from the *P-Asserted-Identity* header of the incoming INVITE. The Application Server prefers a TEL URI over a SIP URI in the *P-Asserted-Identity* header. Therefore, if the *P-Asserted-Identity* header has a TEL URI, then the Application Server determines the CLID from that TEL URI. If the *P-Asserted-Identity* header has no TEL URI, but has a SIP URI, then it determines the CLID from the SIP URI. This behavior is desired when the IMS core network sets an anonymous address in the *From* header (for example, sip:anonymous@anonymous.invalid). The Application Server requires the authentic CLID for services such as CLID Blocking Override, Malicious Call Trace, Selective Call Rejection, and Accounting.

6.1.8 supportPrivacyNone

supportPrivacyNone determines whether the Application Server respects the “none” value in the *Privacy* header for an origination from a BroadWorks subscriber.

When *supportPrivacyNone* has its default value set to “false”, the Application Server ignores the “none” value. If an incoming INVITE request for a subscriber’s origination has “none” in the *Privacy* header, and if the subscriber has CLID Delivery Blocking enabled, then the Application Server honors the CLID Blocking service and indicates that privacy is desired in the outgoing INVITE.

However, when *supportPrivacyNone* is set to “true”, the Application Server respects the “none” value. If an incoming INVITE request for a subscriber’s origination has “none” in the *Privacy* header, then the Application Server honors this header and indicates that no privacy is desired in the outgoing INVITE. In other words, the privacy “none” indication in the incoming INVITE request has precedence over the subscriber’s BroadWorks service profile.

In all cases, a per-call privacy feature access code (FAC) in the request URI has highest precedence.

6.1.9 pChargingFunctionAddressesFormat

pChargingFunctionAddressesFormat controls the default syntax for the *P-Charging-Function-Addresses* header. When the Application Server relays a *P-Charging-Function-Addresses* header, it retains the syntax of the received header. However, when the Application Server generates a new *P-Charging-Function-Addresses* header, it uses syntax according to the value of the *pChargingFunctionAddressesFormat* parameter. If *pChargingFunctionAddressesFormat* is set to “RFC3455”, then the Application Server uses RFC 3455 syntax. If *pChargingFunctionAddressesFormat* is set to “RFC7315”, then the Application Server uses RFC 7315 syntax. The default value is “RFC7315”.

6.1.10 includeDirectoryNumberInPAI

If *includeDirectoryNumberInPAI* is set to the default value “true”, then for originations, the Application Server adds a TEL URI in the *P-Asserted-Identity* header that contains the BroadWorks subscriber’s principal number. If *includeDirectoryNumberInPAI* is “false”, then the Application Server uses the originating subscriber’s display address to set the *P-Asserted-Identity* header’s TEL URI. Additionally, if a policy or service modifies the CLID in the *From* header, then the policy or service also modifies the *P-Asserted-Identity* header’s TEL URI, provided the modified CLID is trusted.

6.2 BroadWorks Application Server Configuration Parameters: IMS

This section describes the system parameters that can be set from the *Interface/IMS* CLI level. Table 4 summarizes the available parameters. The parameters are described in more detail in the subsections that follow.

Parameter	Release	Default Value	Comments
cscfAddressHost	Release 11.1	none (not set)	IP address or FQDN of the S-CSCF
cscfAddressPort	Release 11.1	none (not set)	Default value is appropriate for most installations.
cscfAddressTransport	Release 14.0	unspecified	Default value is appropriate for most installations.

Parameter	Release	Default Value	Comments
includeEnhancedPChargingVectorInfo	Release 14.0	false	
setPriorityHeaderForEmergency	Release 14.sp1 Release 15.0	false	
addNoServicesParameterForOOTB	Release 14.sp1 Release 15	false	
supportImplicitIdentities	Release 14.sp1 Release 15.0	true	
routingMode	Release 14.sp2 Release 15.0	routingB2BUA	
useEnhancedNetworkTranslations	Release 14.sp1 Release 15.0	false	
userPhoneErrorCorrection	Release 14.sp2 Release 15.0 Release 22.0	identityDomain	
support3rdPartyRegistration	Release 14.sp1 Release 15.0	disabled	
supportShSCscfName	Release 14.sp1 Release 15.0	false	
includeCscfParameterInToHeader	Release 14.sp2 Release 15.0	true	
connectedOriginationRouteHandling	Release 14.sp7 Release 15.sp2 Release 16.0	default	
pServedUserSyntax	Release 17.0	p-served-user	
enableOIPCompliance	Release 17.sp2 Release 18.0	false	
includeTrunkGroupPilotInPAITelURI	Release 17.sp3 Release 18.0	false	
forceDeflectedCallBeforeAnswerAsOOTB	Release 18.0	false	
forceSipURIForClientOriginatedActions	Release 19.0	false	

Table 4 Application Server CLI Configuration Parameters at Interface/IMS Level

6.2.1 cscfAddressHost, cscfAddressPort, cscfAddressTransport

- *cscfAddressHost* configures the default IP address or fully qualified domain name (FQDN) for the S-CSCF. Depending on the configuration, the Application Server can use this address to send out-of-the-blue requests in some situations.
- *cscfAddressPort* defines the listening port for the S-CSCF, used in conjunction with the *cscfAddressHost* parameter described above. If this parameter is not set, the Application Server can use the DNS SRV lookup if enabled. If this parameter is set, DNS SRV is not used.

- *cscfAddressTransport* determines the transport used for out-of-the-blue SIP requests sent to the S-CSCF at the address specified by *cscfAddressHost* and *cscfAddressPort*. The allowed values are "udp", "tcp", and "unspecified". If the value is "unspecified", then the Application Server uses the mechanism described in *RFC 3263* [29] to determine the transport, including naming authority pointer (NAPTR) and service locator (SRV) domain name system (DNS) queries when these queries are enabled. Otherwise, if the value is "udp" or "tcp", then the Application Server uses User Datagram Protocol (UDP) or Transmission Control Protocol (TCP), respectively.

6.2.2 includeEnhancedPChargingVectorInfo

When *includeEnhancedPChargingVectorInfo* is set to "true", BroadWorks adds proprietary *bw-speid* and *bw-calltype* parameters to the *P-Charging-Vector* header.

The *bw-speid* parameter contains a service provider/enterprise ID as a SIP quoted string.

The *bw-calltype* parameter contains one of the following SIP token values:

- local: Call is between users within the same group.
- on-net: Call is between users in different groups but within the same service provider/enterprise.
- off-net: Call is not within the same service provider/enterprise.

The following is an example of the *P-Charging-Vector* header with the proprietary parameters.

```
P-Charging-Vector:icid-
value="2+BW165212905120905454663316@192.168.40.34";bw-speid="spe1";bw-
calltype=local
```

6.2.2.1 Originating Execution

When the Application Server sends an INVITE to an S-CSCF for a BroadWorks user origination and the *includeEnhancedPChargingVectorInfo* parameter is set to "true", the *P-Charging-Vector* header in the INVITE request has:

- *bw-speid* parameter set to the originating user's service provider/enterprise ID

-and-

- *bw-calltype* set according to the call type from the originating user to the terminator

6.2.2.2 Terminating Execution

When the Application Server sends an INVITE to an S-CSCF for a BroadWorks user termination and the *includeEnhancedPChargingVectorInfo* parameter is set to "true", the *P-Charging-Vector* in the INVITE has the *bw-speid* parameter set to the terminating user's service provider/enterprise ID.

If the INVITE received from the S-CSCF for the termination, contained a *P-Charging-Vector* with a *bw-calltype* parameter already present, then this same *bw-calltype* value is included in the *P-Charging-Vector* of the INVITE sent to the S-CSCF. Otherwise, the *bw-calltype* is set according to the call type from the originating (or redirecting if the call was redirected) party to the terminator.

6.2.2.3 Redirecting Execution

When the Application Server sends an INVITE to an S-CSCF for a BroadWorks user redirection and the *includeEnhancedPChargingVectorInfo* parameter is set to "true", the *P-Charging-Vector* in the INVITE has the *bw-speid* parameter set to the redirecting user's service provider/enterprise ID and the *bw-calltype* set according to the call type from the redirecting user to the redirect destination.

6.2.3 setPriorityHeaderForEmergency

If *setPriorityHeaderForEmergency* is set to "true" and if the Application Server determines that a call is an emergency call, then the Application Server adds a *Priority* header with the value "emergency" to the outgoing INVITE request. This processing applies when the Application Server runs originating services, including when it redirects a termination to an emergency number.

If the value is "false" or if the call is not an emergency call, then the Application Server proxies a *Priority* header from the incoming INVITE request to the outgoing INVITE request, but it never adds or modifies a *Priority* header.

6.2.4 addNoServicesParameterForOOTB

If *addNoServicesParameterForOOTB* is set to "true", then the Application Server adds a *no_services* parameter to the *Route* header of an out-of-the-blue INVITE request. The parameter signals to the S-CSCF that it should not run services for the INVITE request.

If the value is "false" (the default value), then the Application Server omits the *no_services* parameter.

6.2.5 supportImplicitIdentities

When *supportImplicitIdentities* is set to the default value "true", the Application Server provides no special treatment for implicit identities such as aliases or alternate numbers. This configuration applies when an S-CSCF has knowledge of implicit identities and can terminate to them.

In some deployments, the S-CSCF is unaware of implicit identities, and it depends on the Application Server to translate all implicit identities to the associated subscriber's primary SIP PUI. Therefore, if *supportImplicitIdentities* is "false", and if a call terminates to a BroadWorks subscriber, then the Application Server puts the subscriber's primary SIP PUI into the request URI in the terminating INVITE. The S-CSCF recognizes the PUI and correctly routes the INVITE.

Example:

User A has a primary SIP PUI sip:3015551001@example.net and an alternate number of +13015551009. The Application Server receives a terminating INVITE with a *Request-URI* sip:+13015551009@example.net;user=phone. The Application Server determines that this is a termination attempt to User A by way of User A's alternate number. If *supportImplicitIdentities* is "true", then the Application Server sends the terminating INVITE with the same *Request-URI*. However, if *supportImplicitIdentities* is "false", then the Application Server sends the terminating INVITE with the *Request-URI* sip:3015551001@example.net, User A's primary SIP PUI.

6.2.6 routingMode

routingMode determines how the Application Server routes incoming requests, particularly, when there is any kind of diversion or forking. The value of the parameter determines, among other things, which SIP requests are sent out-of-the-blue and to which S-CSCF a request is sent. There are three allowed values for the parameter: "routingB2BUA" (default), "asRoute", and "receivedRouteLocation".

- **routingB2BUA** – In this mode, outgoing INVITE requests for scenarios such as Blind Transfer are not out-of-the-blue.
- **asRoute** – When the *routingMode* is set to "asRoute", the Application Server sends outgoing INVITE requests for scenarios such as Blind Transfer as out-of-the-blue originating requests. For these out-of-the-blue requests, the Application Server generates a new *Route* header, generates a new *P-Charging-Vector* header, and sends a *P-Served-User* header.
- **receivedRouteLocation** – When the *routingMode* is set to "receivedRouteLocation", the Application Server sends outgoing INVITE requests for scenarios such as Blind Transfer as out-of-the-blue originating requests. In this way, it is like "asRoute" mode. However, it is different because, if possible, the Application Server sends the outgoing INVITE request to the S-CSCF domain name or IP address from the *Route* header of the incoming INVITE.

The differences between the different routing modes are best shown by a simple example. In this example, User X calls BroadWorks subscriber User A. User A answers the call, and then Blind Transfers User X to User Y. The following table shows differences in the INVITE request the Application Server sends to the S-CSCF for the transfer.

	routingB2BUA	asRoute	receivedRouteLocation
INVITE is OOTB	No	Yes	Yes
S-CSCF address	Received	Configured or Sh or Third-party registration	Received
ODI in *Route* header	Yes	No	No
orig parameter in *Route* header	No	Yes	Yes
Route header	Copied from received INVITE	Generated by Application Server using S-CSCF URI from Sh, third-party registration, or configured value	Generated by Application Server, with S-CSCF URI constructed using the host from the received S-CSCF URI
Charging-Vector icid-value source	Received value	Generated by Application Server	Generated by Application Server
P-Served-User header	Omitted	Sent	Sent

Table 4 Outgoing INVITE for Blind Transfer in Different Application Server Routing Modes

NOTE: For sessions in which there is a redirection or forking, the Application Server may behave as a "Routeing B2BUA" or as an "Initiating B2BUA". Whether the Application Server behaves as a "Routeing B2BUA" or an "Initiating B2BUA" for specific redirection or forking scenarios is controlled by the *routingMode* parameter. The details of specific scenarios are covered in the *BroadWorks AS Mode ISC Interface Specification* [4] in section about Out-of-the-Blue requests.

6.2.7 useEnhancedNetworkTranslations

In IMS mode, the Application Server does not use the Network Server for routing as it does in stand-alone mode. However, the Network Server also provides network translations, which are useful in IMS mode as well as stand-alone mode. When *useEnhancedNetworkTranslations* is set to "true", the Application Server uses the Network Server for translations, but not for routing. However, when *useEnhancedNetworkTranslations* is "false" the Application Server does not use the Network Server. For more information on enhanced Network Server translations, see the *BroadWorks IMS ISC Interoperability Enhancements Feature Description, Release 14.sp1* [9].

6.2.8 userPhoneErrorCorrection

The parameter *userPhoneErrorCorrection* determines the extent to which the Application Server performs an error correction when handling a SIP URI that is missing a *user=phone* parameter. In the standards-compliant scenarios, the Application Server treats the user part of the request URI as dialed digits only when the request URI has a *user=phone* parameter.

Example:

sip:+12405552001@as.broadsoft.com;user=phone

In certain deployments, however, the S-CSCF expects the Application Server to treat the user part as dialed digits, even if there is no *user=phone* parameter. Therefore, the S-CSCF requires the Application Server to provide an error correction.

In some cases, the Application Server adds a *user=phone* parameter when error correcting. In other cases, the Application Server does not add *user=phone*, but it still treats the user part of the request URI as dialed digits, and performs digit translations.

userPhoneErrorCorrection also affects when the Application Server attempts alias translations.

The following table shows the behavior of the Application Server for the different values of *userPhoneErrorCorrection*.

	none	**identityDomain**	**full**	**fullEnforceUser-Phone**
Application Server adds user=phone before translations	Never	Yes, if the originator is a BroadWorks user, the URI user is all digits, and the URI domain matches the domain of the originating user's SIP PUI.	Yes, if the originator is a BroadWorks user, the URI user is all digits, and the URI domain matches the domain of the originating user's SIP PUI.	Yes, if the originator is a BroadWorks user and the URI user is all digits.
Application Server attempts digit translations	Yes, if the URI has *user=phone* and the domain matches an Application Server domain.	Yes, if the URI has *user=phone* and the domain matches an Application Server domain.	Yes, if the URI user is all digits.	Yes, if the URI user is all digits.

	none	identityDomain	full	fullEnforceUser-Phone
Application Server attempts alias translations	Yes, if *user=phone* is absent.	Yes, if *user=phone* is absent.	Always	Always

Table 5 Application Server Behavior for Different Values of *userPhoneErrorCorrection*

In addition to error correction for the *Request-URI*, the parameter may also affect how the Application Server processes addresses for other purposes. The following list describes some of these cases:

- Trunk group origination: *P-Asserted-Identity* header URI lookup to determine the originating trunk group via the pilot user DN.
- Trunk group origination: DN lookup to determine the originating user.
- Trunk group origination: Originator address for unscreened trunk group origination.
- Trunk group origination: Presentation identity from received *From* header.
- Out-of-dialog PBX Redirection: DN lookup to identify redirecting user or originating user.
- In-dialog PBX Redirection: DN lookup to identify redirecting user.
- User origination: Unscreened originator address.
- Redirection: Destination address for the redirection.
- BroadWorks Mobility: Look up originator's BroadWorks Anywhere location.

6.2.9 support3rdPartyRegistration

The parameter *support3rdPartyRegistration* controls whether or not the Application Server supports third-party registration as defined in 3GPP TS 24.229.

If *support3rdPartyRegistration* is set to "enabled", then the Application Server accepts third-party REGISTER requests from the S-CSCF. It accepts registrations for the subscriber's primary identity/device profile, as well as the subscriber's Shared Call Appearance and Video Add-On identity/device profiles. A REGISTER request may contain a TEL URI as the target address (that is, the "address of record"), in which case the Application Server binds the registration to the primary identity/device profile of the subscriber identified by the TEL URI (that is, the subscriber whose primary DN matches the TEL URI).

If *supportThirdPartyRegistration* is set to "enabled", depending on the circumstances, the Application Server may then use the S-CSCF URI from the third-party registration for out-of-the-blue requests.

If *supportThirdPartyRegistration* is set to "enableRegistrarOnly", then the Application Server accepts third-party REGISTER requests from the S-CSCF and associates them with the subscriber's identity/device profiles; however, it does not use the S-CSCF URI for out-of-the-blue requests. "enableRegistrarOnly" is a transitional setting that allows all subscribers to register before the value is set to "enabled".

If *support3rdPartyRegistration* is set to the default value "disabled", then the Application Server rejects third-party registrations.

If *support3rdPartyRegistration* is set to "enabled", then the S-CSCF URI for a BroadWorks subscriber can also be statically configured, in what is sometimes referred to as "static registration". However, the contact URI from a SIP dynamic registration has precedence over a statically configured contact URI.

The Application Server does not support third-party registration for virtual subscribers.

The steps that the Application Server takes to select the S-CSCF URI for an out-of-the-blue request involve several system parameters and dynamic conditions. In short, the Application Server selects the CSCFName, the third-party registration, or the system-wide CSCF address, in that order. These steps are described in detail in the following list.

- If the IMS parameter *supportShSCSCFName* is set to "true" and the Application Server has a value for the S-CSCF name from the HSS, then it selects that value. For more information about this parameter, see section *6.2.10 supportImplicitIdentities*.
- If *support3rdPartyRegistration* is set to "enabled" and the Application Server has a valid registered URI, then it selects that URI.
- If the subscriber is a virtual subscriber, then the Application Server selects a URI constructed from the values of the IMS parameters "cscfAddressHost", "cscfAddressPort", and "cscfAddressTransport". For more information about these parameters, see section *6.2.1 cscfAddressHost, cscfAddressPort, cscfAddressTransport*.
- If the subscriber is a regular subscriber (that is, not a virtual subscriber), then the Application Server may select a URI constructed from the values of the IMS parameters "cscfAddressHost", "cscfAddressPort", and "cscfAddressTransport". However, the Application Server may select this "system" URI only if *supportShSCSCFName* is set to "false" and *support3rdPartyRegistration* is set to "enableRegistrarOnly" or "disabled".

NOTE: If the CSCFName option is enabled (*supportShSCSCFName* is set to "true") or third-party registration is enabled (*support3rdPartyRegistration* is set to "enabled"), then the Application Server cannot select the system CSCF address for a regular subscriber. This restriction is not applied to virtual subscribers.

CAUTION: If third-party registration is enabled, that setting prevents the Application Server from using the CSCF address provisioned at the system level (that is, *cscfAddressHost*, *cscfAddressPort*, *cscfAddressTransport*) for BroadWorks users. This means the Application Server is unable send an OOTB request for an unregistered user. When *routingMode* is set to "routingB2BUA", this is generally not a problem. However, it could be a problem when: (1) routingMode is set to "asRoute", because this causes the Application Server to send OOTB requests for more services (compared to "routingB2BUA"), (2) when *forceDeflectedCallsBeforeAnswerAsOOTB* is set to "true".

For example, if *support3rdPartyRegistration* is set to "enabled", *routingMode* is set to "asRoute" and *forceDeflectedCallsBeforeAnswerAsOOTB* is set to "true", then the Application Server cannot perform a Call Forwarding operation for an unregistered user. First, because of the *routingMode* setting and the *forceDeflectedCallsBeforeAnswerAsOOTB* setting, the Application Server must send the outgoing INVITE request out of the blue. Second, because the user is unregistered, the Application Server does not have an S-CSCF address to send the OOTB INVITE request to. Third, because third-party registration is enabled, the Application Server cannot use the CSCF address configured at the system level. Therefore, the Application Server cannot complete a Call Forwarding operation. If the user has Call Forwarding Always enabled, the Application Server will reject all incoming calls while that user is unregistered, which is probably not what one would expect.

6.2.10 supportShSCscfName

supportShSCscfName controls whether the Sh-provided S-CSCF name is expected and if it is allowed to be used.

- If *supportShSCscfName* is "false", then the Sh-provided S-CSCF name is not used even if present.
- If *supportShSCscfName* is "true", then the Sh-provided S-CSCF name can be used.

For more information on the rules that the Application Server uses to determine the route for an out-of-the-blue request, see section *6.2.9 support3rdPartyRegistration*.

CAUTION: If *supportShSCscfName* is set to "true", that setting prevents the Application Server from using the CSCF address provisioned at the system level (that is, *cscfAddressHost*, *cscfAddressPort*, *cscfAddressTransport*) for BroadWorks users. See the note in section *6.2.9 support3rdPartyRegistration*, which describes a similar situation for *supportThirdPartyRegistration*.

6.2.11 includeCscfParameterInToHeader

includeCscfParameterInToHeader determines whether the Application Server adds a *cscf* parameter to the *To* header of an out-of-the-blue (OOTB) terminating INVITE request.

When the Application Server sends an OOTB terminating INVITE request for the first call leg of a click-to-dial call, the IMS core should route that INVITE directly to the subscriber's UE. However, some IMS cores mistakenly route the INVITE back to the Application Server for terminating services. The Application Server should not execute terminating services in this situation, and to prevent this, the Application Server adds a *cscf* parameter to the *To* header of the OOTB INVITE request. If the IMS core routes this INVITE back to the Application Server, then the Application Server finds the *cscf* parameter and proxies the INVITE back to the S-CSCF without executing terminating services.

Some IMS core implementations do not route the OOTB terminating INVITE back to the Application Server. For such implementations, the administrator can set *includeCscfParameterInToHeader* to "false", causing the Application Server to send the OOTB terminating INVITE request without the *cscf* parameter.

The default value is "true".

6.2.12 connectedOriginationRouteHandling

The *connectedOriginationHandling* parameter takes effect if *routingMode* is not set to "routingB2BUA". If *routingMode* is set to "routingB2BUA", then the Application Server behaves as if *connectedOriginationHandling* were set to "Default".

In the case of Account Codes, Authorization Codes, and some Feature Access Code (FAC) services, the Application Server sends a final 200 response to the originating INVITE request, collects DTMF digits, and then sends an outgoing INVITE request to continue the origination. Depending on the value of *connectedOriginationHandling*, the Application Server may or may not send the outgoing INVITE request out of the blue. If the value of *connectedOriginationHandling* is *OOTB*, then it sends the INVITE request as an out-of-the-blue originating request. Otherwise, if the value of *connectedOriginationHandling* is “Default”, it sends the outgoing INVITE as if it were a continuation of the incoming INVITE request.

6.2.13 pServedUserSyntax

The *pServedUserSyntax* parameter determines the syntax that the Application Server uses for served user information. If the parameter is set to “p-served-user”, which is the default value, then the Application Server uses the *P-Served-User* SIP header according to the syntax described in *RFC 5502*. If the parameter is set to “p-served-user-identity”, then the Application Server uses the *P-Served-User-Identity* SIP header. If the parameter is set to “both”, then the Application Server uses both the *P-Served-User* SIP header and the *P-Served-User-Identity* SIP header.

Note that the semantics for the *P-Served-User* header and the *P-Served-User-Identity* header are the same. Thus, this parameter, as its name implies, affects only syntax.

Also, note that when the Application Server uses the *P-Served-User* header, it adds the *sescase* header parameter but not the *regstate* header parameter.

6.2.14 enableOIPCompliance

When the *enableOIPCompliance* parameter is set to true, the P-Asserted-Identity and Privacy headers can be stripped from the access side invitations based on the relevant Calling Line Identity Delivery service. The conditions for omitting the P-Asserted-Identity header are:

- The request is a terminating request for a BroadWorks user.
- The device profile for the user’s device indicates that it is not a trusted device.
- The user’s service profile does not have an appropriate calling line identity delivery service (External Calling Line ID, Internal Calling Line ID, Calling Name Delivery, and Calling Number Delivery).

For Calling Name Delivery and Calling Number Delivery, when one or the other is assigned, the following behavior occurs:

- If only Calling Number Delivery service is active, then the display name is removed from the From header and the PAI header.
- If only Calling Name Delivery service is active, then the user portion of the From and the PAI headers is replaced with the value in the *disabledCLIDNumberValue* parameter. When the calling number is not present and the calling name is present, the PAI header does not contain a Tel URL.

6.2.15 includeTrunkGroupPilotInPAITelURI

The *includeTrunkGroupPilotInPAITelURI* parameter when set to true, always populates the pilot user's DN in the Tel URI of the P-Asserted-Identity header for all trunk group-originating calls regardless of the Calling Line ID policy configuration. Calls forwarded from the Private Branch Exchange (PBX) or from the trunk group are treated the same way as the usual calls originating from the PBX. That is, the phone number in the Tel URI is that of the pilot user's DN for the trunk group where the call is redirected. Whenever the pilot user's DN is used in the Tel URI, the corresponding pilot user's display name is also populated in the Tel URI.

This function assumes that the pilot user's DN exists. In "error" cases when the pilot user's DN does not exist, the Application Server uses the pilot user's CLID instead. The CLID configuration behavior is defined in the *Calling Line ID Enhancements Feature Description* [13].

6.2.16 forceDeflectedCallBeforeAnswerAsOOTB

When the *forceDeflectedCallBeforeAnswerAsOOTB* parameter is set to "true", calls deflected before answer, are treated as OOTB originating requests. For a deflected call to be initiated as an OOTB originating request, the *routingMode* system parameter must be set to "Route" or "receivedRouteLocation". If the *routingMode* system parameter is set to "routingB2BUA", a deflected call is not an OOTB request.

The following table shows the routing behavior for the different user scenarios and *forceDeflectedCallBeforeAnswerAsOOTB* setting compared to the different deflection services.

User Scenarios	Force Deflected Call Before Answer as OOTB Setting	User Deflecting Service	Trunk Group Deflecting Service	In-Dialog PBX Deflection	Out-Dialog Deflection
Normal User (non-trunking)	No	non-OOTB	Not applicable	OOTB [NOTE 1]	non-OOTB
	Yes	OOTB	Not applicable		OOTB
Trunk Mode Setting – Proxy	No	non-OOTB	non-OOTB	non-OOTB	non-OOTB
	Yes	OOTB	OOTB	OOTB	OOTB
Trunk Mode Setting – User	No	non-OOTB	OOTB [NOTE 1]	OOTB [NOTE 1]	non-OOTB
	Yes	OOTB			OOTB
Trunk Mode Setting – Pilot	No	OOTB [NOTE 1]	OOTB [NOTE 1]	OOTB [NOTE 1]	non-OOTB
	Yes				OOTB

Table 6 Routing Behavior for Different User Scenarios and *forceDeflectedCallBefore AnswerAsOOTB*

NOTE 1: The *forceDeflectedCallBeforeAnswerAsOOTB* does not affect these deflected calls. These calls always route as “Out of the Blue” regardless of the *forceDeflectedCallBefore AnswerAsOOTB* setting.

6.2.17 forceSipURIForClientOriginatedActions

When a call client sends BroadWorks a request to originate or transfer a call, the client may send the destination address as a sip URI or a tel URI. By default, when BroadWorks carries out the client action, it matches the URI scheme in the SIP signaling to the URI scheme in the client request. For example, if the client initiates a Click-To-Dial call with a tel URI as the destination address, then BroadWorks places a tel URI in the Request URI of the originating INVITE request.

If the value of *forceSipURIForClientOriginatedActions* is set to “true”, then this default behavior is changed, and BroadWorks converts any tel URI to a sip URI in the SIP signaling. Setting this parameter to “true” allows BroadWorks to accommodate CSCFs that cannot route a tel URI.

The default parameter value is “false”.

6.3 BroadWorks Application Server Configuration Parameters: Server Addresses

This section provides details regarding configuration parameters that must be set at the *System/ClientSession/ServerAddresses* level of the CLI on the BroadWorks Application Server.

Parameter	Description	Default Value	Required Value for IMS Deployments
publicClusterFQDN	Configures the cluster FQDN encompassing the primary and secondary Application Servers.	none	Dependent on network settings
primaryPublicFQDN	Configures the public FQDN for the primary Application Server in the cluster when there is no BroadWorks Location Server in the network. If there is a Location Server in the network, this parameter can be omitted.	none	Dependent on network settings
secondaryPublicFQDN	Configures the public FQDN for the secondary Application Server in the cluster when there is no BroadWorks Location Server in the network. If there is a Location Server in the network, this parameter can be omitted.	none	Dependent on network settings
primaryPrivateFQDN	Configures the private FQDN for the primary Application Server in the cluster when there is no BroadWorks Location Server in the network. If there is a Location Server in the network, this parameter can be omitted.	none	Dependent on network settings
secondaryPrivateFQDN	Configures the private FQDN for the secondary Application Server in the cluster when there is no BroadWorks Location Server in the network. If there is a Location Server in the network, this parameter can be omitted.	none	Dependent on network settings

Table 7 Application Server CLI Configuration Parameters at *ServerAddresses* Level

6.4 BroadWorks Application Server Configuration: Diameter

BroadWorks uses Diameter for the Rf, Ro, and Sh interfaces. Configuring the Diameter interface involves the following steps:

1) Set Diameter base system data (Diameter identities, realms, listening addresses, ports, and so on).
2) Use the CLI "add peers" command. This is the list of Diameter peers with which the Diameter stack instance(s) directly communicate. Connection to peers is done once either Rf, Ro, or Sh is enabled.
3) Use the CLI "add Routing Realms" command (optional – only if *Realm Routing* is used). For each Routing Realm added, add associated routing peers and associated priority/weight.
4) Set the Offline Charging, Online Charging, and Sh interface specific configuration data if applicable.

For more information on Diameter configuration, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.5 BroadWorks Application Server Configuration: Rf and Ro Interface

The Rf and Ro interface configurations are set at the *Interface/Accounting/BroadWorksCDRInterface* level and sublevels of the command line interface (CLI) on the BroadWorks Application Server.

The BroadWorksCDRInterface menu is used to configure BroadWorks accounting settings common to all accounting interfaces, including the Rf and Ro interfaces. The master control for all accounting operations, *enabled*, is found at this level.

The BroadWorksCDRInterface menu also contains the Diameter submenu, which itself contains the Offline, Online, and ChargingFunctionElement submenus.

For more information, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.5.1 Offline

The *Interface/Accounting/BroadWorksCDRInterface/Diameter/Offline* menu is used to enable the Rf interface and configure the message content. This menu is also used to control whether ACR messages that cannot be delivered are queued to disk for later retransmission.

For more information, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.5.2 Online

The *Interface/Accounting/BroadWorksCDRInterface/Diameter/Online* menu is used to enable and configure the Ro interface.

For more information, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.5.3 ChargingFunctionElement

The *Interface/Accounting/BroadWorksCDRInterface/Diameter/ChargingFunctionElement* menu is used to configure the system default value for the *P-Charging-Function-Addresses SIP* header. When received over the SIP signaling, the received *P-Charging-Function-Addresses* header value takes precedence over the system default. However, in scenarios where the *P-Charging-Function-Addresses SIP* header has not been received, the system uses the default value configured here.

This default value is used both to select the CCF that receives the billing information and to populate an outgoing *P-Charging-Function-Addresses SIP* header. A scenario where the default P-Charging-Function-Addresses value is used is an out-of-the-blue call that is cancelled before receiving a reliable provisional response.

For more information, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.6 BroadWorks Application Server Configuration Parameters: Sh Interface

Enabling the Sh interface requires the following steps:

1) Enabling Public Identity Reporting.
2) Configuring Diameter stack, HSS Peers, and Realms.
3) Enabling ShInterface Input Channel.
4) Configuring HSS Realm.
5) Configuring DNS SRV Records.

For more information, see the *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide* [7].

6.7 BroadWorks Application Server Configuration Parameters: Advice of Charge

The Advice of Charge service has the following parameters in the CLI level */Service/AdviceOfCharge*:

- **delayBetweenNotificationsInSeconds** – The value of this parameter determines the time interval in seconds between the Advice of Charge notifications the Application Server sends for AOC-D. Values in the range of 5 through 1800 are allowed. The default value is “60”.
- **incomingAocHandling** – If the value is “charge” and if the Application Server is configured as a CGP, then the Application Server applies the incoming Advice of Charge information from a downstream CGP to the current call and sends a new SIP message toward the originating UE with the cumulative charges. If the value is “ignore”, then the Application Server ignores the incoming Advice of Charge information.
- **useOCSEnquiry** – When set to ”true”, the service performs a tariff enquiry to the OCS during call setup time to fetch tariff information that is used to provide Advice of Charge service information to the access device. When set to “false”, there is no tariff enquiry sent to the OCS. The default value is “false”.
- **OCSEnquiryType** – This parameter indicates what type of enquiry request should be sent to the cost information source. The parameter can be set to “ServicePrice” or “AoC”. The default value is “AoC”. When the *CostInformationSource* servers are properly configured, based on the *OCSEnquiryType,* a CCR AoC Enquiry or a CCR Service Price Enquiry request is sent to the provisioned remote Diameter peer.

The cost source for the Advice of Charge service is configured at the CLI level */Service/AdviceOfCharge/CostInformationSource*. The Application Server supports redundant OCS locations, allowing up to ten entries. Each entry comprises the IP address or URL of the Diameter peer as well as a priority. The following is an example of the CLI configuration.

```
AS_CLI/Service/AdviceOfCharge/CostInformationSource> get

                Peer Identity   Priority
========================================
 ro1.server.mtl.broadsoft.com          0
 ro2.server.mtl.broadsoft.com          1
```

To allow the Application Server to proxy incoming Advice of Charge information from a downstream CGP, the Application Server must have the MIME type *application/vnd.etsi.aoc+xml* in the CLI at the */Interface/SIP/ContentType/Content* level.

To allow the Application Server to send Advice of Charge to a UE, the identity/device profile type for the device must have the *Advice of Charge Capable* policy enabled.

Advice of Charge is a user service that must be authorized to a service provider or enterprise, and group, and assigned to a user. The service may be enabled or disabled for each user.

For more information about configuring Advice of Charge in BroadWorks, see the *BroadWorks Advice of Charge Feature Description, Release 16.0* [10] and the *AoC Tariff Information from OCS Support Feature Description, Release 21.0* [11].

6.8 BroadWorks Operational Settings

6.8.1 BroadWorks IMS Addressing

The Public User Identity must be configured on the BroadWorks Application Server for each user account, from the subscriber address in 3GPP. It consists of the address of record (AoR) of the subscriber (for example, sip:bob@broadsoft.com) and is used for all communication between CSCF and Application Servers in the IMS network. For information on configuration, see section *5.1 User IMS Subscription and Addressing*.

6.9 BroadWorks Operational Considerations

This section provides some additional information regarding considerations that should be reviewed for IMS deployments.

6.9.1 Proxying Pre-loaded Routes

The BroadWorks Application Server only proxies pre-loaded routes if the following conditions are all true:

- A ROUTE header is included in the INVITE.
- The first ROUTE entry contains a known identity of the application server and is a loose route. The verification of the first ROUTE entry is done using the maddr. If the maddr is not within the first ROUTE entry, the host portion shall be used for the verification to ensure the ROUTE is identifying the Application Server.
- The second ROUTE entry is also a loose route.

6.9.2 Proxy Addressing Devices

When configured for operation within the IMS, BroadWorks only supports proxy addressing identity/device profiles because the CSCF translates all access attempts (origination, termination, and so on) to the public user identity. However, the Application Server must own the address space for the identity/device profile. Therefore, the identity/device profile type that the identity/device profile is based on must use either the "intelligent proxy addressing" or the "non-intelligent proxy addressing" signaling address types. Such identity/device profile types typically define registering devices and other intelligent SIP devices.

6.10 Best Practices for Configuring for IMS

While the best practices for configuring BroadWorks for IMS depend on the actual deployment details and associated IMS vendor equipment, general considerations fall into two categories: common practices and vendor-specific practices.

6.10.1 Common Practices

In general, configuration guidance is provided in section *5 BroadWorks IMS Integration* and section *6 BroadWorks IMS Operational Settings*.

6.10.2 Vendor-specific Practices

Ask your authorized BroadSoft sales representative for documentation concerning integration with products from particular vendors.

Appendix A: Initial Filter Criteria

A subscription in IMS can contain initial filter criteria (iFC), which are applied by an S-CSCF to determine when a SIP request should be routed to an Application Server for service execution. The application of the iFC is described in *3GPP TS 24.229* [18]. The model and the syntax of the iFC are described in *3GPP TS 29.228* [16].

This appendix provides examples of iFC that have been demonstrated to work correctly to integrate a BroadWorks Application Server into the IMS core network.

The following describes the iFC in textual format and in the XML syntax of *3GPP TS 29.228* [16].

IFC 1 – Originating Services

NOTE: BroadSoft can change the content of the *Via* header, which can break this trigger point. Implementers should consider this before choosing this alternative.

Priority: 0

Trigger Point:

- Session case is Originating

  -and-

- Method is INVITE

  -and-

- *Via* header does not contain "BroadWorks".

XML:

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If the session case is ORIGINATING_SESSION ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SessionCase>0</SessionCase>
  </SPT>
  <!-- ... and it's an INVITE request ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>INVITE</Method>
  </SPT>
  <!-- ... and "BroadWorks" is not in the Via header. -->
  <SPT>
    <ConditionNegated>1</ConditionNegated>
    <Group>1</Group>
    <SIPHeader>
      <Header>Via</Header>
      <Content>.*;branch=.*BroadWorks.*</Content>
    </SIPHeader>
  </SPT>
</TriggerPoint>
```

IFC 1a – Originating Services (Alternate)

NOTE: This iFC is an alternative to iFC 1.

Priority: 0

Trigger Point:

- Session case is Originating

  -and-

- Method is INVITE

  -and-

- *Contact* header does not contain the URI of a BroadWorks Application Server.

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If the session case is ORIGINATING_SESSION ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SessionCase>0</SessionCase>
  </SPT>
  <!-- ... and it's an INVITE request ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>INVITE</Method>
  </SPT>
  <!-- ... and the Contact header does not contain an Application
       Server network address.  (Note that the value given is only
       an example.) -->
  <SPT>
    <ConditionNegated>1</ConditionNegated>
    <Group>1</Group>
    <SIPHeader>
      <Header>Contact</Header>
      <Content>.*sip:as.broadworks.net.*</Content>
    </SIPHeader>
  </SPT>
</TriggerPoint>
```

IFC 2 – Terminating Services

Priority: 1

Trigger Point:

- Session case is Terminating Registered

  -and-

- Method is INVITE

  -and-

- *To* header does not contain ";cscf".

XML:

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If the session case is TERMINATING_REGISTERED ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SessionCase>1</SessionCase>
  </SPT>
  <!-- ... and it's an INVITE request ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>INVITE</Method>
  </SPT>
  <!-- ... and the To header does not contain cscf. -->
  <SPT>
    <ConditionNegated>1</ConditionNegated>
    <Group>1</Group>
    <SIPHeader>
      <Header>To</Header>
      <Content>.*;cscf.*</Content>
    </SIPHeader>
  </SPT>
</TriggerPoint>
```

IFC 2a – Terminating Services (Alternate)

NOTE: This iFC is an alternative to iFC 2.

Priority: 1

Trigger Point:

- Session case is Terminating Registered

  -and-

- Method is INVITE

  -and-

- *Contact* header does not contain the URI of a BroadWorks Application Server.

XML:

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If the session case is TERMINATING_REGISTERED ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SessionCase>1</SessionCase>
  </SPT>
  <!-- ... and it's an INVITE request ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>INVITE</Method>
  </SPT>
```

```
    <!-- ... and the Contact header does not contain an Application
         Server network address.  (Note that the value given is only
         an example.) -->
    <SPT>
      <ConditionNegated>1</ConditionNegated>
      <Group>1</Group>
      <SIPHeader>
        <Header>Contact</Header>
        <Content>.*sip:as.broadworks.net.*</Content>
      </SIPHeader>
    </SPT>
  </TriggerPoint>
```

IFC 3 – SUBSCRIBE Request

Priority: 2

Trigger Point:

- Method is SUBSCRIBE

  -and-

- Session case is Terminating Registered.

XML:

```
  <TriggerPoint>
    <ConditionTypeCNF>0</ConditionTypeCNF>
    <!-- If it's a SUBSCRIBE request ... -->
    <SPT>
      <ConditionNegated>0</ConditionNegated>
      <Group>1</Group>
      <Method>SUBSCRIBE</Method>
    </SPT>
    <!-- ... and the session case is TERMINATING_REGISTERED ... -->
    <SPT>
      <ConditionNegated>0</ConditionNegated>
      <Group>1</Group>
      <SessionCase>1</SessionCase>
    </SPT>
  </TriggerPoint>
```

IFC 4 – Call Type Query

> **NOTE**: This iFC is required only if BroadWorks is configured to support call type queries via INFO.

Priority: 3

Trigger Point:

- Method is INFO

  -and-

- Session case is Originating.

  -and-

- *Required* header contains “broadworkscalltypequery”.

XML:

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If it's an INFO request ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>INFO</Method>
  </SPT>
  <!-- ... and if the session case is ORIGINATING_SESSION ... -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SessionCase>0</SessionCase>
  </SPT>
  <!-- ... and if the Required header contains
       "broadworkscalltypequery". -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <SIPHeader>
      <Header>Required</Header>
      <Content>.*broadworkscalltypequery.*</Content>
    </SIPHeader>
  </SPT>
</TriggerPoint>
```

IFC 5 – Third-Party Registration

This iFC is required only if the BroadWorks Application Server is integrated into the IMS network with the third-party registration option.

Priority: 4

Trigger Point:

Method is REGISTER.

XML:

```
<TriggerPoint>
  <ConditionTypeCNF>0</ConditionTypeCNF>
  <!-- If it's a REGISTER request … -->
  <SPT>
    <ConditionNegated>0</ConditionNegated>
    <Group>1</Group>
    <Method>REGISTER</Method>
  </SPT>
</TriggerPoint>
```

Acronyms and Abbreviations

This section lists the acronyms and abbreviations found in this document. The acronyms and abbreviations are listed in alphabetical order along with their meanings.

3GGP2	Third-Generation Partnership Project 2
3GPP	Third-Generation Partnership Project
Abbr	Abbreviation
ACA	Accounting-Answer
ACR	Accounting-Request
Admin	Administrator
API	Application Programming Interface
ARPU	Average Revenue Per Unit
AS	Application Server
BGCF	Breakout Gateway Control Function
BW	BroadWorks
CAP	Client Application Protocol
CCF	Charging Collection Function
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CDP	Charge Determination Point
CDR	Call Detail Record
CGP	Charge Generation Point
CLI	Command Line Interface
CLID	Calling Line Identifier
CS	Conferencing Server
CSCF	Call Session Control Function
CS-MGW	Circuit-Switched Media Gateway
CWT	Call Waiting Tone
dBm	The power ratio in decibel (dB) of the measured power referenced to one milliwatt (mW).
Dbmo	The level of a signal as specified in dBmO, is the level of that signal (in dBm) as measured at the reference point of the network.
DGC	Distributed Group Call
DID	Direct Inward Dialing
DN	Directory Number
DNS	Domain Name System
DTMF	Dual-Tone Multi-Frequency

ECF	Event Charging Function
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FAC	Feature Access Code
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FQDN	Fully Qualified Domain Name
GGSN	GPRS Gateway Support Node
G-MSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSS	Home Subscriber Server
HTML	Hypertext Markup Language
Hz	Hertz
ICID	IMS Charging Identity
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
IFC	Initial Filter Criteria
IMS	IP Multimedia Subsystem
IMS-MGW	IP Multimedia Subsystem - Media Gateway Function
IOI	Inter-Operator Identifiers
IP	Internet Protocol
IP-PBX	Internet Protocol-Private Branch Exchange
IS	Interim Standard
ISC	IMS Service Control
ISUP	Integrated Services User Part
IVR	Interactive Voice Response
IWF	Inter-Working Function
MGCF	Media Gateway Control Function
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MNO	Mobile Network Operator
Mobile Endpoint	A generic term for any service-termination device connected via wireless access technology.
MRF	Multimedia Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor

MSCML	Media Server Control Markup Language
MSIDSN	Mobile Station ISDN number
M-SRN	Mobile Station Roaming Number
NAI	Network Access Identifier
NAPTR	Naming Authority Pointer
NEBS	Network Equipment Building Standards
NETANN	NETwork ANNouncments
NGN	Next Generation Network
NS	Network Server
NSSync	Network Server Synchronization
OA&M	Operation, Administration, and Maintenance
OCS	Online Charging System
OCI	Open Client Interface
OCI-P	Open Client Interface-Provisioning
OOTB	Out-of-the-Blue A SIP INVITE request originated by an Application Server used to initiate a call. Services that cause out-of-the-blue requests include Simultaneous Ringing, Call Center, and Hunt Group.
OS	Operating System
OSS	Operations Support System
PAI	P-Asserted-Identity
PCFA	P-Charging-Function-Addresses
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PDSN	Packet Data Serving Node
PLMN	Public Land Mobile Network
PM	Performance Measurement
PSI	Public Service Identity
PUI	Public User Identity
PVI	PriVate User Identity
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
RTU	Right-To-Use
SCA	Shared Call Appearance
SCIM	Service Capability Interaction Manager
S-CSCF	Serving-Call Session Control Function
SDP	Session Description Protocol

SGW	Signaling Gateway Function
SIGTRAN	The name given to the IETF working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols.
SIP	Session Initiation Protocol
SLF	Subscription Locator Functional Entity
SOAP	Simple Object Access Protocol
SPAN	Services and Protocols for Advanced Networks
SRV	Service Locator
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TG	Trunk Group
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
UA	User Agent
UDP	User Datagram Protocol
UE	Unit Equipment
URI	Uniform Resource Identifier
XML	eXtensible Markup Language

References

[1] BroadSoft. 2016. *BroadWorks Application Server Group Web Interface Administration Guide, Part 2, Release 22.0*. Available from the BroadSoft Xchange at xchange.broadsoft.com.

[2] BroadSoft. 2016. *BroadWorks Feature Overview (Through Release 21.0)*. Available from the BroadSoft Xchange at xchange.broadsoft.com.

[3] BroadSoft. 2016. *BroadWorks SIP Network Interface Interworking Guide, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[4] BroadSoft. 2016. *BroadWorks AS Mode ISC Interface Specification, Release 22.0*. Available from the BroadSoft Xchange at xchange.broadsoft.com.

[5] BroadSoft. 2016. *BroadWorks Application Server Sh Interface Specification, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[6] BroadSoft. 2016. *BroadWorks Rf/Ro Interface Specification, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[7] BroadSoft. 2016. *BroadWorks Diameter, Rf, Ro, and Sh Interfaces Configuration Guide, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[8] BroadSoft. 2016. *BroadWorks Accounting Call Detail Record Interface Specification, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[9] BroadSoft. 2007. *IMS ISC Interoperability Enhancements Feature Description, Release 14.sp1.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[10] BroadSoft. 2014. *BroadWorks Advice of Charge Feature Description, Release 16.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[11] BroadSoft. 2014. *AoC Tariff Information from OCS Support Feature Description, Release 21.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[12] BroadSoft. 2016. *BroadWorks Application Server Group Web Interface Administration Guide, Part 2, Release 22.0.* Available from the BroadSoft Xchange at xchange.broadsoft.com.

[13] BroadSoft, Inc. 2010. *Calling Line ID Enhancements Feature Description*, Release 16.0. Available from xchange.broadsoft.com.

[14] 3rd Generation Partnership Project (3GPP). 2014. *3GPP TS 23.002, Network Architecture, (Release 12).* Available from http://www.3gpp.org/.

[15] 3rd Generation Partnership Project (3GPP). 2014. *3GPP TS 23.228, IP Multimedia Subsystem (IMS); Stage 2 (Release 12).* Available from http://www.3gpp.org/.

[16] 3rd Generation Partnership Project (3GPP). 2014. *3GPP TS 24.647, Advice of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem, (Release 12).* Available from http://www.3gpp.org/.

[17] 3rd Generation Partnership Project (3GPP). 2014. 3*GPP TS 29.228, IP Multimedia (IM) Subsystem Cx, and Dx interfaces; Signaling flows and message contents, (Release 12).* Available from http://www.3gpp.org/.

[18] 3rd Generation Partnership Project (3GPP). 2014. *3GPP TS 29.229, Cx and Dx interfaces based on the Diameter protocol; Protocol details, (Release 12).* Available from http://www.3gpp.org/.

[19] 3rd Generation Partnership Project (3GPP). 2013. *3GPP TS 29.658, SIP Transfer of IP Multimedia Service Tariff Information; Protocol specification (Release 12).* Available from http://www.3gpp.org/.

[20] 3rd Generation Partnership Project (3GPP). 2014. *3GPP TS 32.280, Advice of Charge (AoC) service (Release 12)*. Available from www.3gpp.org/.

[21] Aboba, B., and Beadles, M., "The Network Access Identifier", RFC 2486, Internet Engineering Task Force, January 1999. Available from http://www.ietf.org/.

[22] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, Internet Engineering Task Force, December 2004. Available from http://www.ietf.org/.

[23] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J, Sparks R., Handley, M., and Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, Internet Engineering Task Force, June 2002. Available from http://www.ietf.org/.

[24] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, Internet Engineering Task Force, November 2002. Available from http://www.ietf.org/.

[25] Jennings, C., Peterson, J., and Watson, M., "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, Internet Engineering Task Force, November 2002. Available from http://www.ietf.org/.

[26] Garcia-Martin, M., Henrikson, E., and Mills, D., "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the Third-Generation Partnership Project (3GPP)", RFC 3455, Internet Engineering Task Force, January 2003. Available from http://www.ietf.org/.

[27] Barnes, E., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, Internet Engineering Task Force, November 2005. Available from http://www.ietf.org/.

[28] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806. Internet Engineering Task Force, April 2000. Available from http://www.ietf.org/.

[29] Rosenberg, J., Schulzrinne, H., "Session Initiation Protocol (SIP): Locating SIP Servers" RFC 3263, Available from http://www.ietf.org/.

Index