Cisco BroadWorks

SIP Trunking

Solution Guide

Release 23.0

Document Version 2

Notification

The BroadSoft BroadWorks has been renamed to Cisco BroadWorks. Beginning in September 2018, you will begin to see the Cisco name and company logo, along with the new product name on the software, documentation, and packaging. During this transition process, you may see both BroadSoft and Cisco brands and former product names. These products meet the same high standards and quality that both BroadSoft and Cisco are known for in the industry.

Copyright Notice

Trademarks

Document Revision History

Release	Version	Reason for Change	Date	Author
19.0	1	Created document.	October 1, 2012	Doug Sauder
19.0	1	Updated document after review meeting.	November 7, 2012	Doug Sauder
19.0	1	Added case studies to the appendix.	November 15, 2012	Don Gilchrist
19.0	1	Edited document.	November 16, 2012	Patricia Renaud
19.0	1	Edited and published document.	December 14, 2012	Patricia Renaud
19.0	2	Added an Index, updated the Abbreviations section, and published document.	December 20, 2012	Patricia Renaud
19.0	3	Added new text to explain that every pilot user must have a DN or an extension for EV 154670.	March 5,2013	Doug Sauder
19.0	3	Edited changes and published document.	March 21, 2012	Jessica Boyle
20.0	1	Updated document with Release 20.0 features.	August 19, 2013	Doug Sauder
20.0	1	Edited changes and published document.	October 11, 2013	Joan Renaud
20.0	2	Corrected information about trunk group lookups for EV 208570 and added clarifying information about preferred carrier for EV 195369.	November 19, 2013	Doug Sauder
20.0	2	Edited changes and published document.	December 30, 2013	Jessica Boyle
20.0	3	Added explanations of license parameters for EV 210785.	January 30, 2014	Doug Sauder
20.0	3	Edited changes and published document.	May 16, 2014	Joan Renaud
21.0	1	Updated document with Release 21.0 features.	December 1, 2014	Doug Sauder
21.0	1	Updated the legal notice and edited changes.	December 5, 2014	Joan Renaud
21.0	1	Rebranded and published document.	December 15, 2014	Joan Renaud
21.0	2	Updated and corrected information about PBX redirections for EVs 206445 and 247709. Made correction for EV 245717.	February 9, 2015	Doug Sauder
21.0	2	Added rebranded server icons.	March 20, 2015	Joan Renaud
21.0	2	Edited changes and published document. Verified *Table of Figures*.	May 3, 2015	Jessica Boyle
21.0	3	Added complete list of conditions that cause the Application Server to ignore the *Calling Line Identity Source for Screened Trunk Group Calls Policy* (PR-47928).	August 31, 2015	Doug Sauder
21.0	3	Added a note that the Application Server rejects a REFER request for a dialog that was set up as an out-of-dialog PBX redirection (PR-48036).	September 17, 2015	Doug Sauder

Release	Version	Reason for Change	Date	Author
21.0	3	Added more information about how the Application Server processes an initial INVITE request that contains a *History-Info* or *Diversion* header (PR-49102).	December 15, 2015	Doug Sauder
21.0	3	Added a note that an administrator may need to set container options on the Network Server for case-insensitive matching of the *tgrp* parameter (PR-49284).	January 29, 2016	Doug Sauder
21.0	3	Edited changes and published document.	February 10, 2016	Jessica Boyle
22.0	1	Updated document with Release 22.0 features.	October 29, 2016	Doug Sauder
22.0	1	Added information about the container option *bw.oodPbxRedirection.force-PresentationIdentityForOriginatorLookup* (PR-50281).	November 16, 2016	Doug Sauder
22.0	1	Edited changes and published document.	December 11, 2016	Patricia Renaud
22.0	2	Updated the document for PR-45120.	December 15, 2016	Doug Sauder
22.0	2	Edited changes and published document.	June 12, 2017	Jessica Boyle
22.0	3	Updated the document for PR-56320.	January 26, 2018	Karine Leduc
22.0	3	Edited changes and published document.	April 13, 2018	Jessica Boyle
23.0	1	Updated document with Release 23.0 features.	September 7, 2018	Geng Chen
23.0	1	Added a special exception for the “Calling Line Identity Source for Screened Trunk Group Calls Policy” for PR-58063.	September 18, 2018	Doug Sauder
23.0	1	Rebranded document for Cisco. Edited changes and published document.	November 7, 2018	Joan Renaud
23.0	2	Rebranded product name for Cisco and published document.	March 10, 2019	Joan Renaud

Table of Contents

Table of Figures

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 2

This version of the document includes the following change:

- Rebranded product name for Cisco.

1.2 Changes for Release 23.0, Document Version 1

This version of the document includes the following changes:

- Added information about the new Terminating Alternate Trunk Identity service (FR11960).
- Added information about the new system-wide parameter *useUnmappedSessionsForTrunkUsers* (FR10536).
- Added information about the new optional field named Physical Location added against user trunking addresses (FR12083).
- Added information about the new system parameters, *allowPAILookupForOutOfDialogPBXRedirection*, *outOfDialogPBXRedirectionOriginatorLookupPolicy*, *allowTrunkIdentityForAllOriginations*, the new option “Basic Lookup Prefer From” for Trunk Group User Lookup Policy, and new call blocking service value *ETRouteExhaustUnreachable* for configurable treatment (FR17119).
- Added a special exception for the “Calling Line Identity Source for Screened Trunk Group Calls Policy” for PR-58063.

1.3 Changes for Release 22.0, Document Version 3

This version of the document includes the following changes:

- Updated the document for PR-56320.

1.4 Changes for Release 22.0, Document Version 2

This version of the document includes the following changes:

- Updated the description of the Trunk Group identification processing steps for an out-of-dialog PBX redirection (PR-45120).
- Revised the description of the Trunk Group identification processing steps for an outbound call.
- Updated the description of how the Application Server selects the caller identity for an out-of-dialog PBX redirection.

1.5 Changes for Release 22.0, Document Version 1

This version of the document includes the following changes:

- Added information about the new Direct Route service and Direct Route terminations.
- Added information about the new Enterprise Trunk Number Prefixes.

- Added a clarification that the Application Server does not advance to the next IP address if it fails to receive a response to a SIP OPTIONS request (PR-53411).
- Added information about the container option *bw.oodPbxRedirection.forcePresentationIdentityForOriginatorLookup* (PR-50281).

1.6 Changes for Release 21.0, Document Version 3

This version of the document includes the following changes:

- Added complete list of conditions that cause the Application Server to ignore the *Calling Line Identity Source for Screened Trunk Group Calls Policy* (PR-47928).
- Added a note that the Application Server rejects a REFER request for a dialog that was set up as an out-of-dialog PBX redirection (PR-48036).
- Added more information about how the Application Server processes an initial INVITE request that contains a *History-Info* or *Diversion* header (PR-49102).
- Added a note that an administrator may need to set container options on the Network Server for case-insensitive matching of the *tgrp* parameter (PR-49284).

1.7 Changes for Release 21.0, Document Version 2

This version of the document includes the following changes:

- Corrected the Application Server case-sensitive matching algorithm for the *tgrp* parameter for EV 245717.
- Added more details for in-dialog PBX redirections: service execution and identity information in the outgoing INVITE request for EV 206445.
- Added more details for out-of-dialog PBX redirections: CLID mapping, license check, service execution, and identity information in the outgoing INVITE request.
- Added Flexible Seating Guest calls to the list of calls that require a business trunking license unit.
- Added rebranded server icons.

1.8 Changes for Release 21.0, Document Version 1

This version of the document includes the following changes for new Release 21.0 features:

- Enterprise Trunk Number Range and Route List service functionality, which provides a capability for basic connectivity with efficient provisioning using number ranges.
- Capacity management at the Enterprise Trunk level, based on license usage.
- Alternate Trunk Identity in IP Multimedia Subsystem (IMS) now consists of both a user part and a domain part, and can function as a trunking user's primary public identity.
- Capability to use SIP caller preferences to support routing in IMS.
- Capability to allow the PBX to provide the connected identity for inbound calls.
- *ETRouteExhaust* internal blocking action, to permit the use of configurable treatments to handle an Enterprise Trunk route exhaustion condition.
- Capability to merge the *History-Info* header and *Diversion* header according to *RFC 6044*.
- CLID mapping capability to mitigate CLID spoofing in out-of-dialog PBX redirections.

- Capability to configure a Trunk Group's incoming or outgoing call capacity at zero, which has the effect of disabling originations or terminations via that Trunk Group.
- Capability to configure which SIP responses to an OPTIONS request indicate that the PBX is reachable.
- New counters (performance measurements).
- Call detail record (CDR) fields *btluExceeded* and *enterpriseTrunkCapacityExceeded*.

The following changes provide additional detail or clarification for previously existing functionality:

- Additional details on the processing steps for inbound calls, including translations, license check, and capacity check.
- Additional details on the processing steps for out-of-dialog PBX redirections, including calling user identification, CLID processing, and capacity check.

The following change was made in response to problem reports (ExtraView):

- (EV 217151) The order of the capacity check and license check is reversed, so that the license check is first and the capacity check second. This change is available in the following releases via a patch: 17.sp4, 18.0, 18.sp1, 19.0, 19.sp1, 20.0, and 20.sp1.

1.9 Changes for Release 20.0, Document Version 3

This version of the document includes the following changes:

- Added section *4.3 License Parameters* with descriptions of the various license parameters for SIP trunking.
- Added additional examples of bursting capacity to *Appendix C – Bursting Call Capacity*.

1.10 Changes for Release 20.0, Document Version 2

This version of the document includes the following changes:

- Corrected information about originating Trunk Group lookups when a Trunk Group has no Pilot User for EV 208570.
- Added clarifying information that the Application Server does not apply the preferred carrier information of a Pilot User to all originations via the associated Trunk Group for EV 195369.

1.11 Changes for Release 20.0, Document Version 1

This version of the document includes the following changes:

- Updated with Release 20.0 functionality covered under FR 173898.
- Added significant clarifying information about Enterprise Trunk route advancing.
- Added various minor clarifications.

1.12 Changes for Release 19.0, Document Version 3

This version of the document includes the following change:

- Added new text in section *5.2 Pilot User* to explain that every pilot user must have a DN or an extension for EV 154670.

1.13 Changes for Release 19.0, Document Version 2

This version of the document includes the following changes:

- Added an Index and updated the Abbreviations section.

1.14 Changes for Release 19.0, Document Version 1

This is the initial document version.

2 Document Purpose

This guide describes the Cisco BroadWorks SIP Trunking solution. In contrast to a Hosted Centrex solution, in which Cisco BroadWorks provides a self-contained telephony services platform, and the Business Line solution, in which Cisco BroadWorks provides dial-tone to the customer premise-based Key Telephony System (KTS), the SIP Trunking solution enables Cisco BroadWorks to integrate with a Private Branch Exchange (PBX) residing within an enterprise's own network. In this integrated model, Cisco BroadWorks provides connectivity to the Public Switched Telephone Network (PSTN), as well as services that integrate with services provided by the PBX.

As a solution guide, this document targets a broad audience, providing both a high-level overview of the solution, as well as finer details and reference information. This guide is intended to be complete and up-to-date, with new information incorporated as new features are added.

This guide is structured so that concepts and functionality are explained in the first part of the guide. The second part of the guide explains the Cisco BroadWorks SIP Trunking configuration, including step-by-step provisioning procedures. Various other aspects of SIP Trunking, which are considered useful but not central to the guide, are provided in the *Appendices.*

This guide follows the convention of using initial capital letters for well-defined concepts within Cisco BroadWorks. This convention adds clarity to explanations. For example, the term "enterprise", which is not capitalized, refers to a business or other organization, while the term "Enterprise", which is capitalized, refers to the organizational unit recognized in Cisco BroadWorks' provisioning model. The terms are different, and an "enterprise" does not necessarily correspond to an "Enterprise" in Cisco BroadWorks.

3 Network Architecture

The Cisco BroadWorks SIP Trunking solution provides flexibility to adapt to widely varying network architectures. Some key aspects of this flexibility include:

- Support for redundant network elements and redundant routes
- Support for IMS, including Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) Business Trunking specifications
- Support for non-IMS all-IP networks (referred to in this guide as a stand-alone deployment), including SIPconnect-compliant deployments
- Support for legacy Time Division Multiplexing (TDM) PBXs via an Integrated Access Device (IAD) or other gateway

The Cisco BroadWorks Application Server can be installed in one of two different deployment modes, referred to as "IMS deployment" and "stand-alone deployment". An IMS deployment is appropriate for network architectures in which the Cisco BroadWorks Application Server takes the role of a Telephony Application Server in an IMS network – that is, it interfaces with an Interrogating Call Session Control Function (I-CSCF) or Serving – Call Session Control Function (S-CSCF). Note that a stand-alone deployment is appropriate for all other network architectures including the SIPconnect-compliant deployments. Because the selection of the deployment mode fundamentally affects the external interfaces of the Application Server, the following sections describe the IMS architecture and stand-alone architecture separately.

3.1 Stand-Alone Deployment

The network architecture for a stand-alone deployment features a direct connection from a carrier's network to a customer's network. In accordance with common usage in other specifications, this document refers to the carrier as the "service provider" and the customer as the "enterprise". Therefore, the Cisco BroadWorks network elements are deployed in the service provider's network and the customer premises network elements in the enterprise's network.

Real-world deployments are expected to be quite diverse, and descriptions of the possible deployment architectures would be lengthy. For this reason, the following sections provide sample deployment architectures as "reference" architectures, which are suitable as references for SIP trunking features supported by Cisco BroadWorks. These reference architectures also provide a starting point for more complex real-world deployments.

3.1.1 IP PBX Reference Architecture

In the IP PBX reference architecture, the enterprise deploys a SIP PBX, which communicates with Cisco BroadWorks directly using SIP. A diagram for this reference architecture is shown in *Figure 1*.

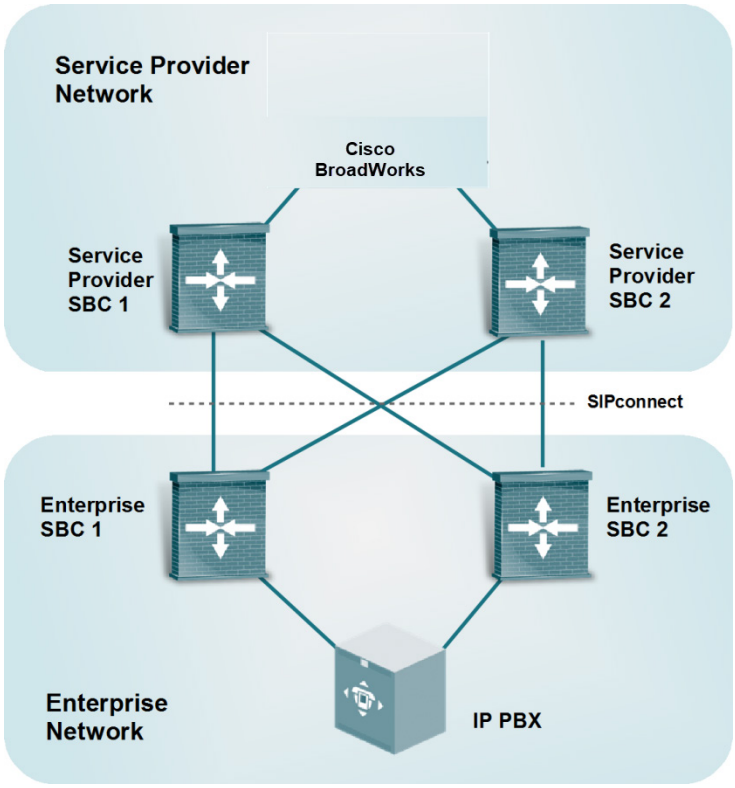

Figure 1 Reference Architecture for IP PBX

The diagram shows Cisco BroadWorks with connections to session border controllers (SBCs) in the service provider's network. Cisco BroadWorks supports redundant service provider SBCs for added reliability. The enterprise may also deploy SBCs at its network boundary. The diagram shows two redundant SBCs deployed by both the service provider and the enterprise. This basic diagram also shows redundant routes, which provide resilience against the failure of a single SBC.

Best Practice

Cisco recommends that the service provider deploy SBCs at its network border to address security issues (DoS/DDoS, Signaling Encryption – IPSec/TLS, topology hiding), NAT traversal, and Quality of Service (QoS) policy and prioritization of flows.

Cisco BroadWorks fully supports the SIP Forum's SIPconnect recommendation [15]. The SIPconnect specification also describes a reference architecture, which makes a clear distinction between the service provider and the enterprise. The diagram in *Figure 1* shows the reference point that is subject to the SIPconnect recommendation.

3.1.2 TDM PBX Reference Architecture

Cisco BroadWorks can provide advanced, IP-based services to legacy TDM PBXs when the PBX is fronted by an IAD or other gateway. The IAD supports a TDM interface to the PBX and a SIP interface to Cisco BroadWorks, and provides interworking between the two.

Figure 2 shows a reference architecture in which the service provider manages redundant IADs and redundant T1/E1 links to the TDM PBX in the enterprise network. Cisco BroadWorks supports the redundant IADs in the same way it supports redundant SBCs in an all-IP network.

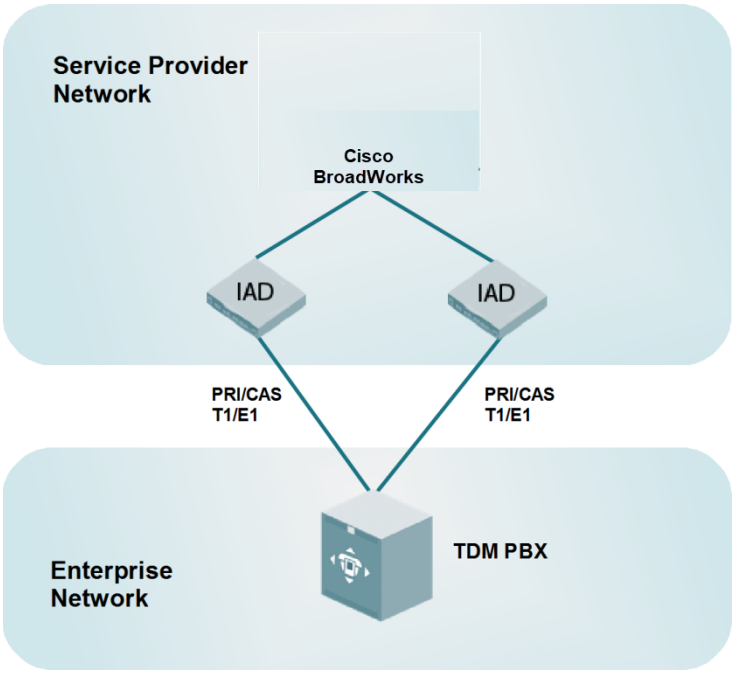

Figure 2 Reference Architecture for TDM PBX with IAD in Service Provider's Network

Figure 3 shows a reference architecture in which the enterprise manages redundant IADs. In this architecture, the TDM to IP interworking is performed within the enterprise. The connection between the service provider and the enterprise is IP. As in the case of the all-IP reference architecture, Cisco recommends that the service provider deploy SBCs at its network border. *Figure 3* shows redundant SBCs.

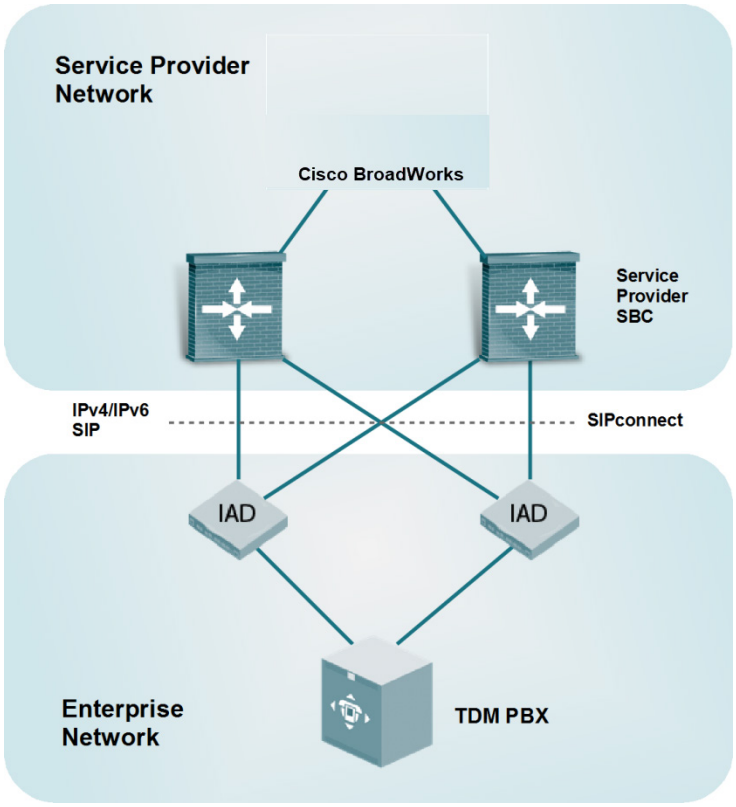

Figure 3 Reference Architecture for TDM PBX with IAD in Enterprise Network

3.2 IMS Deployment

The network architecture for an IMS deployment features the Cisco BroadWorks Application Server taking the role of a Telephony Application Server in an IMS network. The Application Server interfaces with an S-CSCF or I-CSCF and provides originating or terminating services for Cisco BroadWorks subscribers who are reachable via the PBX.

The 3GPP specification *TS 24.525* [18] specifies the business trunking architecture for the Next Generation Network. This document describes two different reference architectures: subscription-based and peering-based. Cisco BroadWorks supports both of these architectures. For example call flows, see *Appendix B – IMS Deployment Examples*.

3.2.1 TISPAN Subscription-Based Reference Architecture

In this architecture, the IP PBX takes a role similar to that of a User Equipment (UE) in an IMS network. The IP PBX interfaces with the Proxy Call Session Control Function (P-CSCF) as its entry point to the IMS. The Cisco BroadWorks Application Server takes the role of a Telephony Application Server, providing originating and terminating services to the business trunking subscribers. If the IP PBX registers, the registration is handled by the S-CSCF. A diagram for this architecture is shown in the *Figure 4*.

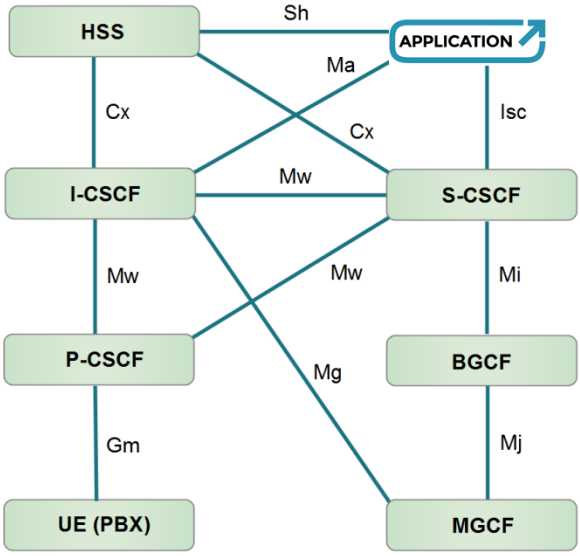

Figure 4 Reference Architecture for TISPAN Subscription-Based Business Trunking

Outbound calls from the PBX are routed through the P-CSCF to the S-CSCF to the Cisco BroadWorks Application Server for originating services. Outbound calls to the PSTN are further routed by the Cisco BroadWorks Application Server to the S-CSCF, the Breakout Gateway Control Function (BGCF), and the Media Gateway Control Function (MGCF). Inbound calls from the PSTN are routed from the MGCF to the I-CSCF, the S-CSCF, and the Cisco BroadWorks Application Server, where the Application Server can execute terminating services. To reach the PBX, the call is further routed back to the S-CSCF, the P-CSCF, and the PBX.

In some cases, the incoming call from the MGCF could be routed to the I-CSCF, then directly to the Cisco BroadWorks Application Server. This scenario is expected when the routing within the IMS is based on a “wildcarded” public service identity (PSI) that routes to the Application Server.

3.2.2 TISPAN Peering-Based Reference Architecture

In this architecture, the enterprise network is treated as a peering network by the service provider. A diagram for this architecture is shown in *Figure 5*.

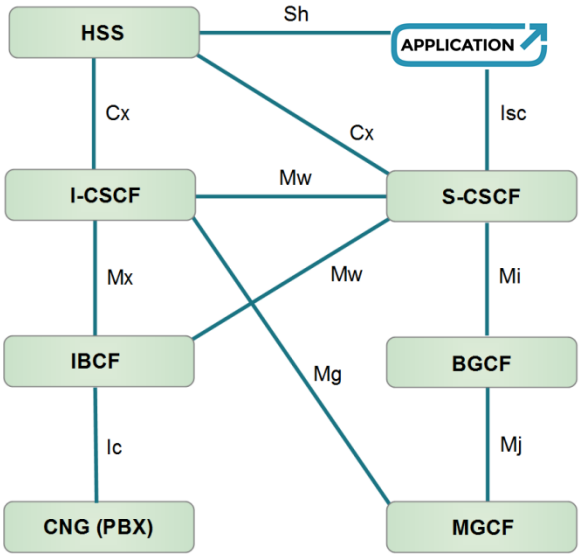

Figure 5 Reference Architecture for TISPAN Peering-Based Business Trunking

3.3 Abstract Architecture

Underlying each reference architecture is an abstract architecture, which defines a model that is important to the provisioning of the Application Server and the SIP signaling exchanged between Cisco BroadWorks and the other network elements. This abstract architecture is illustrated in *Figure 6*.

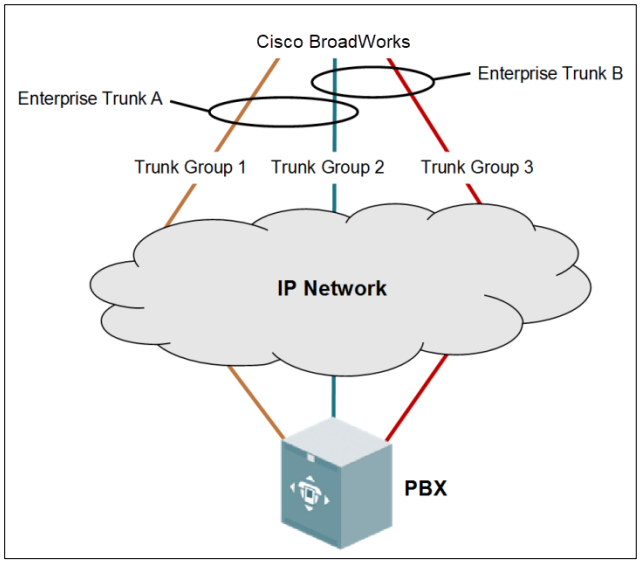

Figure 6 Abstract Architecture

This diagram illustrates key concepts. Understanding these concepts is essential to understand the flexibility that Cisco BroadWorks provides and to apply that flexibility to actual deployment architectures.

A *Trunk Group* is a route to the PBX, as recognized by Cisco BroadWorks. Service providers have some flexibility in defining Trunk Groups. Not every possible path from Cisco BroadWorks to the PBX need be provisioned as a Trunk Group. However, SIP trunking routing procedures in Cisco BroadWorks have direct control only over Trunk Groups. For example, Cisco BroadWorks could be configured to choose between Trunk Group 1 and Trunk Group 2, based on which Trunk Group is the least used, or based on a number of other policies. Other routing procedures, such as routing based on resolving domain names in the Domain Name System (DNS), offer less flexibility. Therefore, the decision as to whether a particular route should be defined in Cisco BroadWorks as a Trunk Group really depends on whether Cisco BroadWorks' routing policies need to identify that route specifically.

An *Enterprise Trunk* is an aggregation of Trunk Groups, primarily for applying a routing policy to select a Trunk Group for a call terminating to the PBX from Cisco BroadWorks. *Figure 6* shows two Enterprise Trunks. Enterprise Trunk A comprises Trunk Group 1 and Trunk Group 2. Enterprise Trunk B comprises Trunk Group 2 and Trunk Group 3. This arrangement shows that the relationship between Enterprise Trunks and Trunk Groups is many-to-many. Therefore:

- An Enterprise Trunk can contain zero or more Trunk Groups.

  Note that if an Enterprise Trunk contains zero Trunk Groups, then Cisco BroadWorks cannot route any calls via that Enterprise Trunk.

- A Trunk Group can belong to zero or more Enterprise Trunks.

  Note that if a Trunk Group does not belong to an Enterprise Trunk, then it is not used in an Enterprise Trunk routing policy, but Cisco BroadWorks can still route calls to the PBX via that Trunk Group directly.

4 SIP Trunking Licensing

4.1 Licensing Concepts

In Cisco BroadWorks, business trunking users are distinctly different from (non-trunking) regular users. One distinction concerns inbound or outbound calls over a Trunk Group, as only business trunking users are permitted to originate or terminate calls via a Trunk Group. Another distinction concerns licensing: business trunking users are licensed differently from regular users. While a regular user requires a Cisco BroadWorks user license at provisioning time, a business trunking user does not. A business trunking user, however, dynamically seizes a business trunking license unit (BTLU) at call setup and releases the license unit when the call is released.

Business trunking users are otherwise much like regular users in a Group or Enterprise, in that they can reach other users via extension dialing, can participate in group services such as Hunt Group or Call Pickup, can integrate with Cisco BroadWorks client applications, and can benefit from Cisco BroadWorks advanced features such as BroadWorks Anywhere. These advanced services work transparently whether the users involved are business trunking users or regular users.

The Cisco BroadWorks license file provided to a System Provider does not place a hard limit on the number of business trunking users that can be provisioned in the system. However, the license file does place a strict limit on the number of simultaneous calls that are permitted by trunking users in the system. The restriction is enforced by means of BTLUs, with one license unit being required for each call. Therefore, if a System Provider has a license for, say, 10,000 simultaneous trunking user calls (thus, 10,000 BTLUs), then the number of simultaneous calls by trunking users is limited system wide to 10,000.

BTLUs are not shared system wide. Instead, they are allocated into smaller pools, from which business trunking users can dynamically seize them when needed. Business trunking users in an Enterprise seize their license units from a pool allocated to their Enterprise. Business trunking users in a Service Provider seize their license units from a pool allocated to their Group. These pools, therefore, place additional strict limits on simultaneous calls by business trunking users. If, say, 1000 license units are allocated to an Enterprise, then the number of simultaneous calls by business trunking users in that Enterprise is limited to 1000.

The creation of the license pools is an explicit provisioning activity. A System Provider administrator can allocate BTLUs to an Enterprise to create that Enterprise's license pool. A System Provider administrator can also reserve BTLUs for a Service Provider, and a Service Provider administrator can then allocate the license units to Groups to create those Groups' license pools. Reserving license units for a Service Provider is optional. When a Service Provider has no reserved license units, the Groups in that Service Provider can take license units directly from the system's stock of unallocated and unreserved license units.

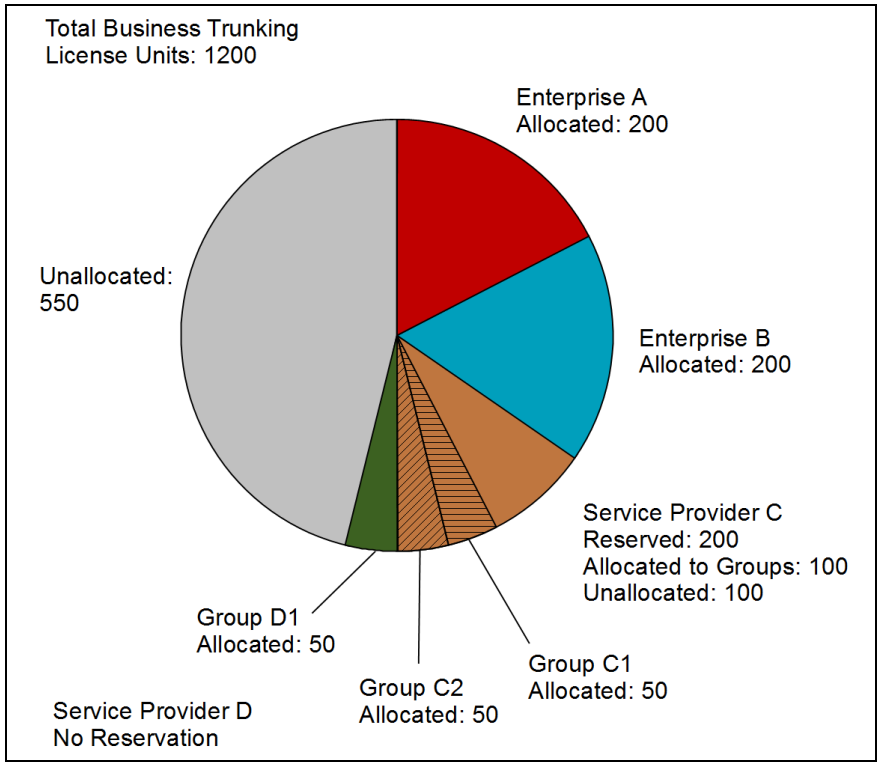

Figure 7 Business Trunking License Unit Allocation

Figure 7 shows an example of BTLU allocation. Enterprise A and Enterprise B, each have 200 license units allocated. Service Provider C has 200 license units reserved. Of those 200 units, 50 units have been allocated to Group C1 (in Service Provider C) and 50 units have been allocated to Group C2 (also in Service Provider C). Service Provider D has no license units reserved, and Group D1 (in Service Provider D) has 50 license units allocated directly from the system. The figure shows 550 license units still available in the system. These license units are available to be allocated to new Enterprises or Groups, or to be reserved for a new Service Provider.

When a business trunking user makes or receives a call, that user must dynamically seize a BTLU at call setup time and retain that seizure for the duration of the call. If all trunking license units in the pool are already seized by other trunking users, then Cisco BroadWorks blocks the call. If the license seizure succeeds, then Cisco BroadWorks allows the call to proceed. When the call is released, the trunking user releases the trunking license unit, which then becomes available for another call.

If Cisco BroadWorks blocks a call because it cannot satisfy a request to seize a BTLU, then it sends a Simple Network Management Protocol (SNMP) *bwTrunkingLicensedCapacityExceeded* notification. Additionally, it indicates the failure condition in the CDR in the *btluExceeded* field.

The pool from which a trunking user seizes a trunking license depends on the provisioning model for that user. In the Service Provider model, the trunking user must seize a license from the pool of license units allocated to the user's Group. In the Enterprise model, the trunking user must seize a license from the pool of license units allocated to the user's Enterprise.

Because trunking users do not have a regular user license, Cisco BroadWorks applies the enforcement of trunking license units for trunking users broadly, meaning that a business trunking user requires a trunking license unit for every call, even if the call does not involve a Trunk Group. For example, if a trunking user receives a call via a Shared Call Appearance device, Cisco BroadWorks requires a trunking license unit for that call. The exception to this general rule is for services that have a separate license that can be deemed sufficient for the service, such as Call Forwarding, where the Call Forwarding user license alone is considered sufficient to allow the forwarded call.

The following points summarize the use of BTLUs with certain Cisco BroadWorks services:

- BroadWorks Anywhere termination or origination uses a BTLU.
- Remote Office origination or termination uses a BTLU.
- Voice Portal origination uses a BTLU.
- Shared Call Appearance termination to a secondary device uses a BTLU.
- Shared Call Appearance origination from a secondary device uses a BTLU.
- Call Forwarding services, such as Call Forwarding No Answer (CFNA), do not use a BTLU when a call is forwarded.
- Simultaneous Ringing and Sequential Ringing do not use a BTLU if the call is answered at a secondary location.
- A Flexible Seating Guest origination or termination uses a BTLU.

The topic of Trunk Group capacity management is unrelated to business trunking user licensing. Nevertheless, a perceived connection between them can be the source of confusion, and so a brief explanation of capacity management is provided here for clarity. An administrator can provision capacity limits for a Trunk Group, with distinct limits for Active Calls, Incoming Calls, and Outgoing Calls. The enforcement of these capacity limits is unrelated to trunking license enforcement. Thus, a Trunk Group capacity limit can cause Cisco BroadWorks to block a call even if a trunking license unit is available. Conversely, if no trunking license units are available, Cisco BroadWorks blocks a Trunk Group call even if the Trunk Group has available capacity. The superficial connection between trunking license enforcement and Trunk Group capacity management arises from the fact that the number of trunking license units allocated to the relevant pool establishes an upper limit on the value that can be provisioned for Trunk Group capacity. For example, if 1,000 trunking license units are allocated to an Enterprise, then no Trunk Group in that Enterprise can be provisioned with a capacity that exceeds 1,000.

4.2 Enterprise Trunk Capacity Management

The requirement of one BTLU per call is an integral part of Cisco BroadWorks licensing structure. Apart from that, however, Cisco BroadWorks also allows an administrator to limit the number of BTLUs allowed to an Enterprise Trunk. This use of BTLUs is optional. It is available to an Enterprise or Group administrator as a capacity management tool within the Enterprise or Group.

An administrator may set a limit on the number of license units that can be seized by users who are assigned to a specific Enterprise Trunk. This limit is a configuration parameter of the Enterprise Trunk. Because this limit depends on license units, it is independent of Trunk Group capacity and can restrict the number of active calls across the multiple Trunk Groups assigned to an Enterprise Trunk. For example, an Enterprise Trunk may have two constituent Trunk Groups, each with a call capacity of 40 calls. With no limit set at the Enterprise Trunk, the maximum number of active calls for that Enterprise Trunk is 80, which is the sum of the capacities of the constituent Trunk Groups. However, an administrator may choose to set a limit of 40 BTLUs for the Enterprise Trunk. In such case, the Application Server does not allow more than 40 active calls for that Enterprise Trunk, regardless of how those calls are distributed between the two Trunk Groups.

Because Enterprise Trunk capacity management is based on license units, many of the general principles that apply to license units also apply to Enterprise Trunk capacity management. Particularly, Cisco BroadWorks applies license usage broadly. When a trunking user establishes a new call, the Application Server seizes a license unit from the user's Enterprise or Group, even if that call does not require a Trunk Group. If the user is assigned to an Enterprise Trunk, and if that Enterprise Trunk has capacity management enabled, then the Application Server counts that license unit toward the Enterprise Trunk's limit. For example, if the user makes a BroadWorks Anywhere call, then that call also requires a license unit and the Application Server counts it against the limit of the Enterprise Trunk. For another example, if the user makes an originating call that uses a Trunk Group and that Trunk Group is not a constituent of the user's assigned Enterprise Trunk, then the Application Server counts that call against the limit of the user's assigned Enterprise Trunk. The Enterprise Trunk limit, therefore, applies to all calls made by all users that are assigned to that Enterprise Trunk.

NOTE: Enterprise Trunk Capacity Management limits the number of BTLUs that may be seized by the users that are assigned to the Enterprise Trunk. Because those users must seize a BTLU for non-Trunk Group calls, such as Shared Call Appearance calls, this form of capacity management may not be a perfect solution for limiting SIP trunking calls to an enterprise.

If the Application Server blocks a call because it reaches the limit of calls allowed by an Enterprise Trunk, then it sends an SNMP *bwEnterpriseTrunkCapacityExceeded* notification (subject to throttling, see section *20.2 Enterprise Trunk Attributes*). Additionally, it indicates the failure condition in the CDR in the *enterpriseTrunkCapacityExceeded* field.

The Application Server allows an emergency call to continue, even if the call causes the Enterprise Trunk's license unit count to exceed the limit. For an emergency call, the Application Server increments the license unit count, even if that action causes the count to exceed the limit for a time.

The call capacity limit configured for an Enterprise Trunk does not create a license pool in the way that license allocation to an Enterprise or Group does. An administrator cannot allocate license units to an Enterprise Trunk.

4.3 License Parameters

The Cisco BroadWorks license file defines three parameters related to SIP trunking. These parameters set certain limits that are applied system wide and are described in the following subsections.

The parameters are viewable from the command line interface (CLI). The following is a sample of the CLI output.

```
AS_CLI/System/Licensing> get

[... elided ...]

  System Parameter Licenses:
                                    Name  Licensed  Used  Available
  ================================================================
                  Trunking Call Capacity     10000    50       9950
        Trunking Bursting Call Capacity      10000     0      10000
  Trunking Bursting Over Max Percentage         25    NA         NA
                       Concurrent Calls      10000    NA         NA
   Number of Meet-Me Conferencing Ports      10000    NA         NA

  5 entries found.

[... elided ...]
```

4.3.1 Trunking Call Capacity License Parameter

The *Trunking Call Capacity* license parameter (alias *maxTrunkGroupCallCapacity*) defines the total number of BTLUs granted by the license file. Because each trunking call requires one BTLU, this parameter sets the maximum number of simultaneous trunking calls allowed in the entire system.

4.3.2 Trunking Bursting Call Capacity License Parameter

The *Trunking Bursting Call Capacity* license parameter (alias *burstingMaxTrunkGroupCallCapacity*) defines the bursting capacity for the entire system. For more information about Bursting, see *Appendix C – Bursting Call Capacity*.

4.3.3 Trunking Bursting Over Max Percentage License Parameter

The *Trunking Bursting Over Max Percentage* license parameter (alias *burstingOverMaxPercentage*) defines the maximum ratio of trunk group bursting capacity to regular capacity. For example, if *burstingOverMaxPercentage* is set to 25% and a trunk group has regular capacity of 48 calls, then the maximum bursting capacity allowed for that Trunk Group is 12, which is 25% of 48. For more information about Bursting, see *Appendix C – Bursting Call Capacity*.

4.4 License Utilization Reporting

Compared to licensing for hosted users, the structure of SIP Trunking licensing in Cisco BroadWorks operates under a different model. In particular, SIP Trunking licensing allows a system provider to take advantage of statistical averaging to "oversubscribe" on license units by provisioning more trunking users than allocated trunking license units. For example, a system provider can decide to allocate 200 trunking license units to an Enterprise, and then provision substantially more than 200 trunking users, who share those licenses. The system engineering required to determine the optimal number of licenses typically follows well-established practices for capacity planning. However, Cisco BroadWorks also provides a tool, in the form of license utilization reports, to assist the network engineer in these planning activities.

Cisco BroadWorks' business trunking license utilization reporting facility produces a daily record of the high-water mark of simultaneous calls by business trunking users. Because each such call requires one BTLU, this record also reveals the maximum number of BTLUs in use at the busiest time of each day. Based on the report, a system provider can gain insight into the license utilization, which could assist their effort to properly allocate their BTLUs.

A basic license utilization report provides a summary of the license utilization in the entire Application Server cluster. Available as a text file in comma-separated value (CSV) format, this report provides the following information for each of the trailing 30 days:

- Date
- Host ID
- Host Name
- Total number of BTLUs
- Total number of BTLUs allocated
- License unit utilization high-water mark for the 24-hour period beginning at midnight

A detailed license utilization report provides the summary information as well as additional information about utilization within Enterprises and Groups. For each Enterprise or Group, the detailed report provides the following information for each of the trailing 30 days:

- Enterprise or group ID information
  - For an Enterprise, this information consists of:
    - Enterprise ID
    - Enterprise name
  - For a Group (within a Service Provider), this information consists of:
    - Service provider ID
    - Service provider name
    - Group ID
    - Group name
- Number of BTLUs allocated to the Enterprise or Group
- License utilization high-water mark over the 24-hour period beginning at midnight
- The time of day during which the high-water mark was recorded

The following is a sample detailed license utilization report.

```
#System

"Report date","Host ID","Hostname","Total number of BTLU","Total BTLU
allocated","System usage summary","Date"

03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,8888, 03/30/2012 EDT
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,10000, 03/29/2012 EDT
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,3534, 03/28/2012 EDT
.
.
.
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,6346, 03/04/2012 EDT
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,122, 03/03/2012 EDT
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,5344, 03/02/2012 EDT
03/31/2012,a8c01b0d,t3-blade17-vm4,12000,10000,8192, 03/01/2012 EDT


#Enterprises

"Enterprise ID","Enterprise Name","Total number of BTLU allocated to the
enterprise","High-water mark BTLU utilization","Time which the high-water mark
occurred"

Enterprise-1-ID,Enterprise One,8000,5555, March 30 2012 3:33:58 EDT
Enterprise-1-ID,Enterprise One,8000,3453, March 29 2012 12:24:11 EDT
Enterprise-1-ID,Enterprise One,8000,3534, March 28 2012 9:03:13 EDT
.
.
.
Enterprise-1-ID,Enterprise One,8000,122, March 03 2012 21:32:11 EDT
Enterprise-1-ID,Enterprise One,8000,5344, March 02 2012 10:13:14 EDT
Enterprise-1-ID,Enterprise One,8000,812, March 01 2012 2:31:25 EDT

Enterprise-2-ID,Enterprise Two,8000,5555, March 30 2012 4:22:28 EDT
Enterprise-2-ID,Enterprise Two,8000,3453, March 29 2012 8:18:51 EDT
Enterprise-2-ID,Enterprise Two,8000,3534, March 28 2012 19:30:41 EDT
.
.
.
Enterprise-2-ID,Enterprise Two,8000,122, March 03 2012 2:24:11 EDT
Enterprise-2-ID,Enterprise Two,8000,5344, March 02 2012 7:11:19 EDT
Enterprise-2-ID,Enterprise Two,8000,8192, March 01 2012 19:30:41 EDT

#Groups

"Service Provider ID","Service Provider Name","Group ID","Group Name","Total number
of BTLU allocated to the Group","High-water mark BTLU utilization","Time which the
high-water mark occurred"

SP-1-ID,SP One,Group-1-ID,Group One,8000,5555, March 30 2012 5:16:24 EDT
SP-1-ID,SP One,Group-1-ID,Group One,8000,3453, March 29 2012 12:24:11 EDT
SP-1-ID,SP One,Group-1-ID,Group One,8000,3534, March 28 2012 22:13:19 EDT
.
.
.
SP-1-ID,SP One,Group-1-ID,Group One,8000,6346, March 04 012 1:42:11 EDT
SP-1-ID,SP One,Group-1-ID,Group One,8000,122, March 03 2012 2:11:51 EDT
SP-1-ID,SP One,Group-1-ID,Group One,8000,5344, March 02 2012 3:24:14 EDT
SP-1-ID,SP One,Group-1-ID,Group One,8000,8192, March 01 2012 4:13:35 EDT
```

A license utilization report can be generated either on demand, or as a recurring scheduled task. To generate a basic report on demand, an administrator executes the following command at the Application Server CLI.

```
$ CLI/System/Util/BTLU> generateReport
.. Done
```

To generate a detailed report, the administrator executes the following command.

```
$ CLI/System/Util/BTLU> generateReport detail
.. Done
```

When the Application Server generates a report on demand, it writes the report to the file system in the directory */var/broadworks/reports/btlu*. The file name is *btluReport<timestamp>.csv* (<timestamp> is replaced with the actual timestamp).

To enable automatic, recurring report generation, the administrator executes a command similar to the following.

```
$ CLI/Maintenance/Scheduler> add btluReport daily 15 30
```

5 User Classification

In the Cisco BroadWorks SIP Trunking solution, users can have different characteristics or roles, which affect Cisco BroadWorks' provisioning and call processing behavior. This section describes the different types of users, including their characteristics and roles, in relation to SIP Trunking.

5.1 Hosted Users and Business Trunking Users

From a licensing perspective, every Cisco BroadWorks user can be classified as a either a hosted user or a business trunking user. This fundamental distinction is made at the time a user is provisioned in the system. A hosted user, sometimes referred to as a "regular" user to distinguish the user from a trunking user, requires a user license at provisioning time, but does not require a license for each call. In contrast, a business trunking user does not require a user license, but *does* require a BTLU for each call.

The CommPilot web pages that show lists of users indicate clearly which users are hosted users and which users are business trunking users. As seen in *Figure 8*, each business trunking user has a check mark symbol under the column labeled "In Trunk Group".

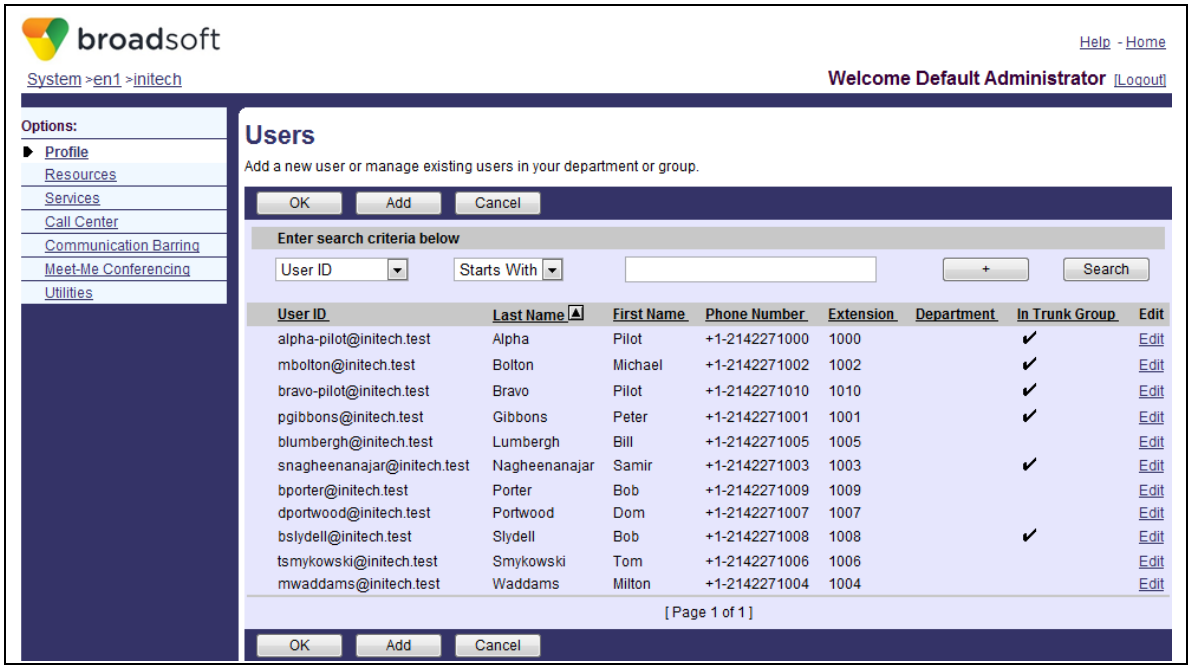

Figure 8 List of Users – Indicating which Users are Hosted Users and which are Trunking Users

Generally, a business trunking user is hosted on a PBX within an Enterprise. The PBX can provide telephony services, such as Extension Dialing or Voice Mail, within the Enterprise. Cisco BroadWorks can provide services in addition to, or instead of, services typically provided by a PBX. Whenever possible, the services Cisco BroadWorks provides to hosted users and to business trunking users are identical. In other words, if Cisco BroadWorks provides service X, it provides that service identically to both hosted users and business trunking users.

5.2 Pilot User

Every Trunk Group configured in Cisco BroadWorks should have a unique association with a trunking user designated the “pilot” user. The Pilot User defines various characteristics of the Trunk Group, such as the Address of Record (AoR) of that Trunk Group.

In Cisco BroadWorks’ provisioning model, some attributes that can apply to the Trunk Group are provisioned against the Pilot User. For this reason, many features of Cisco BroadWorks SIP trunking solution require that each Trunk Group have a Pilot User assigned. In particular, addresses that are associated with the Trunk Group as a whole must be provisioned as the Pilot User’s addresses. These addresses include:

- The Pilot User’s Line/Port (explained in section *6 Trunking User Addresses*), which serves as the AoR for the Trunk Group.
- The Pilot User’s contact Uniform Resource Identifier (URI), which serves as the contact URI for the Trunk Group.
- The Pilot User’s Directory Number (also explained in section *6 Trunking User Addresses*), which can optionally serve as a calling line identity for outbound calls from the PBX via the Trunk Group.

The Directory Number (DN) is integral to the billing framework. If a Pilot User has no DN, then a billing number is still required. Cisco BroadWorks can use the Group Calling Line ID (CLID) number as the billing number, provided the Pilot User has an Extension. Therefore, because of billing requirements, Cisco BroadWorks allows these two alternative configurations:

- The Pilot User has a DN.
- The Pilot User has an Extension and the Pilot User’s Group has a CLID number.

A pilot user has a service profile like any other Cisco BroadWorks user. A pilot user can make and receive calls and can use the same telephony services as any other Cisco BroadWorks user. The pilot user’s service profile, though, is also special, in that it is the default profile for the Trunk Group. Cisco BroadWorks executes call processing services according to the default profile when executing services for an “unscreened” origination (explained in section *9.3.3 Unscreened Originations*). These services typically include screening services, such as Outgoing Calling Plan or Communication Barring.

Cisco BroadWorks does not require every Trunk Group to have a pilot user assigned. However, if a Trunk Group has no Pilot User, then it is subject to certain limitations. For example, if a Trunk Group has no pilot user, then it cannot be assigned to an Enterprise Trunk. Furthermore, it is not possible to assign an AoR to that Trunk Group, which is required to permit a single SIP registration for all PBX users, as in the GIN registration described in *RFC 6140*. In addition, if a Trunk Group does not have a Pilot User, then the “Forward to Phone Number/SIP-URI” action is ignored when configured and the “None” action is selected instead. This action can be selected when configuring unconditional forwarding, when a Trunk Group’s incoming capacity is exceeded, and when a destination is unreachable.

Best Practice

An enterprise can designate a special role for a Pilot User, for example, by provisioning an Auto Attendant or Call Center on the PBX as the Pilot User. To support this role, Cisco provides a Trunk Group configuration option to optimize the Pilot User's service profile for high call volume. This option, labeled *Pilot User Call Optimization Policy* on the web interface, is described in section *19.1 Trunk Group Attributes*.

5.3 Enterprise Trunk User

When an Enterprise Trunk is provisioned to provide connectivity to a PBX, the users hosted on that PBX can be provisioned as Enterprise Trunk Users on Cisco BroadWorks. An Enterprise Trunk User is a Cisco BroadWorks trunking user assigned directly to an Enterprise Trunk and not assigned to a specific Trunk Group.

One unique advantage of an Enterprise Trunk User is simplicity for addressing. An administrator can assign a single phone number to an Enterprise Trunk User, which is sufficient to provision a PBX user with a Direct Inward Dialing (DID) number and allow the user both to make outbound calls and to receive inbound calls.

While an Enterprise Trunk User is not statically assigned to a Trunk Group at provisioning time, Cisco BroadWorks dynamically assigns the user to a Trunk Group at call setup time. If the user is the call originator, then Cisco BroadWorks assigns the Trunk Group as identified in the INVITE request from the PBX. If the user is the call terminator, then Cisco BroadWorks selects and assigns one of the Trunk Groups in the Enterprise Trunk, based on the outcome of the Enterprise Trunk's routing policy. This assignment exists only in the context of the call and lasts only for the duration of the call.

NOTE: A dynamic Trunk Group assignment is valid only within the context of a specific call. This means that if an Enterprise Trunk User has more than one simultaneous call, the user can have more than one dynamic Trunk Group assignment, that is, each call can result in a different Trunk Group assignment.

Because an Enterprise Trunk User is not assigned to a Trunk Group via provisioning, the user has neither a Device Endpoint assignment nor a Line/Port. This status has the following consequences:

- Because the user does not have a Line/Port, the user cannot have an explicit contact URI, either via SIP registration or provisioning. In short, the user cannot register.
- For Cisco BroadWorks to access properties associated with an Access Device, at call setup time it dynamically creates a Device Endpoint for the Enterprise Trunk User with the same properties as the Pilot User's Device Endpoint (see section *6 Trunking User Addresses* for an explanation of these concepts).

The next section covers addressing in more detail. In terms that are explained later, an Enterprise Trunk User can be assigned a Directory Number, which Cisco BroadWorks can use as both a network-side and access-side address.

Cisco recommends that customers provision trunking users as Enterprise Trunk Users, rather than Trunk Group Users (defined next), in most cases.

5.4 Trunk Group User

Cisco BroadWorks supports a deployment option in which a Trunk Group is provisioned as a static route to a PBX with no association to an Enterprise Trunk. Because there is no Enterprise Trunk, it is not possible to provision a user hosted on that PBX as an Enterprise Trunk User. The alternative in this case is to assign the PBX user directly to the Trunk Group. A trunking user provisioned in this way is a Trunk Group User.

A Trunk Group User has a Device Endpoint assignment and a Line/Port. This status has the following consequences:

- Cisco BroadWorks supports the user's DN as a network-side address only. This is a consequence of the fact that the Line/Port has precedence over the DN on the access side. (User addresses are explained in the next section.)
- Users can have a contact URI bound to their Line/Port, either via a SIP registration or as a provisioned contact URI. If the Trunk Group has a Pilot User, the Trunk Group User's contact URI is optional, since the Pilot User's contact URI may be sufficient.

NOTE: It is possible for a trunking user to be assigned to both an Enterprise Trunk and a Trunk Group, essentially making this user a hybrid of an Enterprise Trunk User and a Trunk Group User. Such a user has characteristics of both an Enterprise Trunk User and a Trunk Group User. Because the characteristics of this user are difficult to understand, and because this hybrid type of user is unnecessary, Cisco strongly recommends that customers avoid it.

Note, however, that Pilot Users are an exception, in that they are often assigned to both an Enterprise Trunk and a Trunk Group.

5.5 Hosted PBX User

A Hosted PBX User is in nearly all respects the same as a Hosted User. However, a Hosted PBX User is associated with a Trunk Group and all calls to or from that user are counted against the capacity of the Trunk Group. The Hosted PBX User is typically a special-purpose device, such as a fax machine directly attached to the PBX.

From a licensing perspective, this user is both a hosted user and a trunking user. A Hosted PBX User requires a user license at provisioning time. In addition, when the user originates or terminates a call, the user seizes a BTLU for that call.

5.6 Route List User

A Route List User is an Enterprise Trunk User that has the Route List service assigned (see section *13.1 Route List*). An administrator can assign sets of Route List DNs to the Route List User via the Route List service. (A set of Route List DNs is defined by an Enterprise Trunk Number Prefix or an Enterprise Trunk Number Range. For more information, see section *6 Trunking User Addresses*.) The Application Server permits incoming calls and optionally outgoing calls for all of the phone numbers within a set of Route List DNs, performing the call processing services using the Route List User's service profile. The Route List User, therefore, represents a shared Cisco BroadWorks service profile for multiple users served by the PBX. This functionality simplifies the steps needed to provide basic incoming and outgoing calls for PBX users.

The Route List User is specifically designed to facilitate a large number of simultaneous calls efficiently. The Application Server processes each Route List User call in its own call processing session, rather than in the same session as for usual user calls. This one-call-per-session policy permits greater concurrency on multiprocessor/multicore systems, thereby increasing call throughput.

5.7 Direct Route User

A Direct Route User is a trunking user that has the Direct Route service assigned (see section *13.2 Direct Route*). An administrator can assign one or more direct route identifiers to the user via the Direct Route service. During network translations (see section *10.2.2 Network Translations*), the Application Server performs a direct route identifier lookup and can identify the Direct Route User as the terminating user. Thus, the Direct Route User becomes the terminating Cisco BroadWorks user for the call, allowing the Application Server to route the call to the PBX via a Trunk Group. Because the Application Server identifies the Direct Route User via the direct route identifier, rather than the called number, it can route a terminating call to the destination PBX for a called number that is not recognized by Cisco BroadWorks. In short, the Direct Route service provides a way for the Application Server to support what might be loosely considered unscreened terminations.

The Direct Route User is specially designed to facilitate a large number of simultaneous calls efficiently. The Application Server processes each Direct Route User call in its own call processing session, rather than in the same session as for usual user calls. This one-call-per-session policy permits greater concurrency on multiprocessor/multicore systems, thereby increasing call throughput.

6 Trunking User Addresses

Cisco BroadWorks makes a distinction between access-side addresses and network-side addresses. Generally, access-side addresses and network-side address exist in different "name spaces", which means that the Application Server always interprets an address in the context of the access side or the network side. The Application Server's interface that faces the enterprise (that is, the PBX) is the access side interface. The interface that faces the PSTN (or, generally, any network gateway) is the network side interface. The concepts of access side interface and network side interface are illustrated in *Figure 9*.

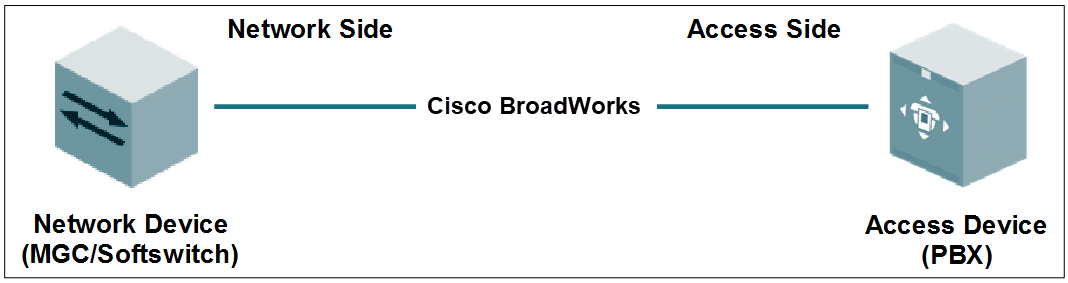

Figure 9 Network Side and Access Side Interfaces

NOTE: In IMS deployments, because the Application Server interfaces with the S-CSCF, the concept of access-side interface and network side interface is somewhat more abstract. For originating sessions, the Application Server receives the incoming INVITE request on the access side and sends the outgoing INVITE request on the network side. For terminating sessions, the Application Server receives the incoming INVITE request on the network side and sends the outgoing INVITE request on the access interface. (There are, of course, exceptions to these general rules, such as when the Application Server redirects a call.)

The access-side interface and network-side interface share the same physical interface, that is, they share the same transport addresses. For this reason, when the Application Server receives a SIP request, it cannot immediately determine, based on the physical interface on which it received the request, whether to process the request as an access-side or network-side request. Instead, the Application Server must examine the information in the request to make that determination.

When the Application Server receives a SIP INVITE request for a new call, it first tries to identify the calling party based on certain SIP header fields, searching for an access-side address in its database. If it finds a match, then it considers the call to be an origination from the access side and applies the service profile of the identified Cisco BroadWorks user for originating services. Otherwise, it tries to identify the called party based on the *Request-URI*, searching for a network-side address in its database. If it finds a match, then it considers the call to be a termination from the network side and applies the service profile of the identified Cisco BroadWorks user for terminating services. If the Application Server cannot identify a Cisco BroadWorks user for either the originating user of the terminating user, then it blocks the call.

There are special-case exceptions to the general rules explained in the preceding paragraph. These exceptions are explained elsewhere, as appropriate, in the context of the special cases in which they apply.

NOTE: At first, an extension-dialed call might not seem to agree with the two patterns described earlier, because the extension is neither an access-side address nor a network-side address. In fact, in an extension-dialed call, the Application Server first identifies the calling user, and then applies translations to the *Request-URI* (the extension) in the context of the calling user. The extension is not an access-side address, because the Application Server does not use it to identify an originating user. The extension is not a network-side address because the Application Server does not use it to identify the called user unless it is performing translations in the context of a known Cisco BroadWorks originating user. In short, the Application Server recognizes extensions in user translations. For more information, see section *10.2.1 User Translations*.

Every Cisco BroadWorks user can be provisioned with both access-side and network-side addresses.

The following are the access-side addresses that can be provisioned for a trunking user:

- Alternate Trunk Identity (Stand-alone only) – An Alternate Trunk Identity is an address that is recognized by Cisco BroadWorks only on the access interface. It has no specific syntax, but can be provisioned as a string of all digits and used as an access-side phone number.
- Alternate Trunk Identity (IMS only) – An Alternate Trunk Identity is an alternate address that is recognized by Cisco BroadWorks. It has a user part and a domain part, and the Application Server uses it as the user's primary identity if the user does not have a device and corresponding public identity.
- Line/Port – A Line/Port is an address that identifies a specific Device Endpoint in an Access Device. To the access device, the Line/Port is an AoR, as defined in *RFC 3261*. Thus, if a device registers, it registers against the Line/Port. A Line/Port must be provisioned for any Cisco BroadWorks user that has a Device Endpoint, which includes any Pilot User, Trunk Group User, or Hosted PBX User. An Enterprise Trunk User does not have an assigned Device Endpoint, and therefore cannot have a Line/Port.
- Directory Number – A DN is a phone number that Cisco BroadWorks recognizes on the network interface. Because of the special status of business trunking users, Cisco BroadWorks may also recognize a DN on the access side interface toward a PBX. This makes it easy to manage DID numbers in the SIP Trunking solution. Internally, Cisco BroadWorks stores a DN as a number in E.164 format.
- Route List Directory Number – A Route List DN is a DN that is assigned to a user indirectly, as part of a set of Route List DNs that match an Enterprise Trunk Number Prefix or an Enterprise Trunk Number Range. To assign a set of Route List DNs to a user, an administrator must first assign the Route List service to that user. Then, the administrator may assign one or more Enterprise Trunk Number Prefixes or Enterprise Trunk Number Ranges to the user via the user's Route List service configuration. When the administrator assigns an Enterprise Trunk Number Prefix, the administrator effectively assigns to that user all the phone numbers that match that prefix. Likewise, when the administrator assigns an Enterprise Trunk Number Range, the administrator effectively assigns to that user all the phone numbers that fall within that range.

The following are the network-side addresses that apply for a trunking user:

- Directory Number – A Directory Number is a phone number that Cisco BroadWorks recognizes on the network interface. Cisco BroadWorks stores the DN internally as an E.164 number. However, externally, as in SIP messages or provisioning interfaces, Cisco BroadWorks can present the DN in national format.
- Route List Directory Number – A Route List DN is a DN that is assigned to a user indirectly, as part of a set of Route List DNs that match an Enterprise Trunk Number Prefix or an Enterprise Trunk Number Range. To assign a set of Route List DNs to a user, an administrator must first assign the Route List service to that user. Then, the administrator may assign one or more Enterprise Trunk Number Prefixes or Enterprise Trunk Number Ranges to the user via the user's Route List service configuration. When the administrator assigns an Enterprise Trunk Number Prefix, the administrator effectively assigns to that user all the phone numbers that match that prefix. Likewise, when the administrator assigns an Enterprise Trunk Number Range, the administrator effectively assigns to that user all the phone numbers that fall within that range.
- Alternate Number – An alternate number has the same properties as the DN.
- Fax Number – A fax number is a special-purpose phone number that identifies a Fax Mailbox provided by Cisco BroadWorks.
- Alias – An Alias is a SIP URI that identifies a Cisco BroadWorks user on the network interface.
- Mobile DN – A Mobile DN is a special-purpose phone number used in the Cisco BroadWorks Mobility solution.

Provisioning and call processing on the access side involve a number of conceptual entities with defined relationships, as shown in *Figure 10*. The numbers in the diagram show the cardinality of the entity relationships. For example, the relationship between an Access Device Type and a Device Type is one-to-many.

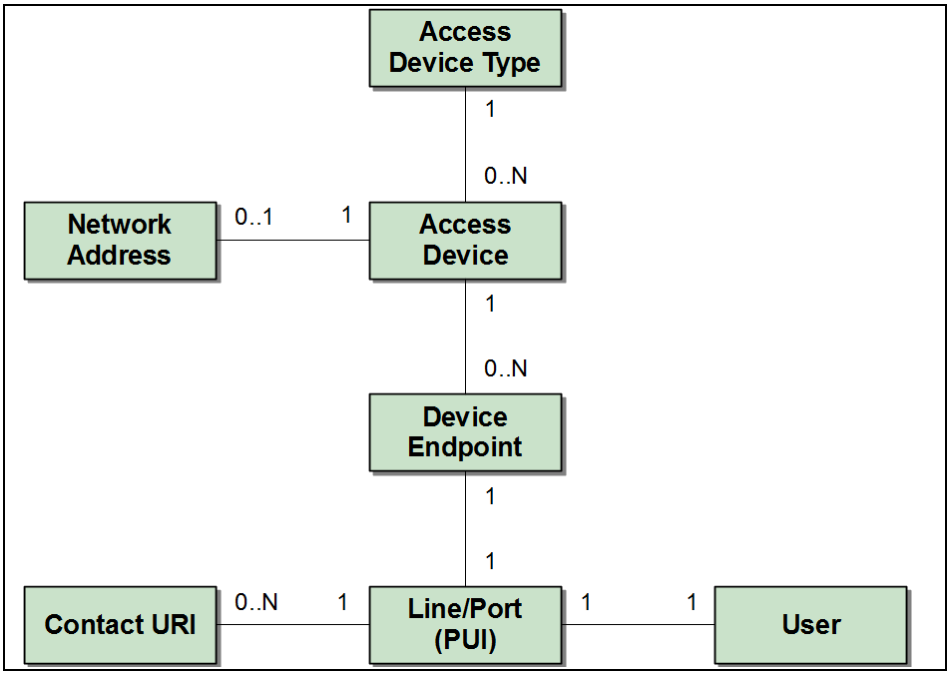

Figure 10 Access-side Entity Relationships

An **Access Device** is the logical representation in Cisco BroadWorks of a physical access device. In Cisco BroadWorks' provisioning interface, an Access Device is referred to as an *Identity/Device Profile*.

An **Access Device Type** defines the basic characteristics of an Access Device. In Cisco BroadWorks' provisioning interface, an Access Device Type is referred to as an *Identity/Device Profile Type*. Cisco BroadWorks supports a number of device options, which define the way in which Cisco BroadWorks interacts with an Access Device. These device options are configured for an Access Device Type and are inherited by the Access Device. For more information about the Access Device Type (Identity/Device Profile Type), see the *Cisco BroadWorks Device Management Configuration Guide* [5].

(Stand-alone deployment only) A **Network Address** can be assigned to an Access Device. The Network Address assignment is optional, and can be an IP address or a domain name. The same Network Address cannot be assigned to two different Access Devices.

A **Device Endpoint** is the logical representation in Cisco BroadWorks of a "port" or "line" in an Access Device. In Cisco BroadWorks provisioning interface, the Device Endpoint is referred to as an *Identity/Device Endpoint*. An Access Device can have zero or more Device Endpoints. Cisco BroadWorks creates a Device Endpoint instance when an administrator assigns a Line/Port to a Cisco BroadWorks user.

(Stand-alone deployment only) A **Line/Port** is the logical address of a Device Endpoint. The physical access device views the Line/Port as an AoR (in *RFC 3261* terminology) for the endpoint. In Cisco BroadWorks, the relationship between a Device Endpoint and a Line/Port is one-to-one.

(IMS deployment only) A **Line/Port** is a Public User Identity (PUI) of a subscriber in the IMS network. In Cisco BroadWorks, the relationship between a Device Endpoint and a Line/Port is one-to-one.

A **Contact URI** is a URI that identifies the endpoint location. If an access device registers, the Contact URI is the URI bound to the Line/Port (AoR). Cisco BroadWorks supports more than one Contact URI for a particular Line/Port, with some restrictions.

A **User** in the context of this diagram is a Cisco BroadWorks user who is assigned a Device Endpoint. Due to the one-to-one relationship between a Device Endpoint and a Line/Port, if a Cisco BroadWorks administrator assigns a Device Endpoint to a user, the administrator must also provision a Line/Port for that user. Note that Enterprise Trunk Users do not have a Device Endpoint assigned, and therefore do not have a Line/Port.

7 Registration (Stand-Alone Only)

7.1 Overview

The Cisco BroadWorks Application Server performs a function similar to the proxy server/registrar as described in *RFC 3261*. Specifically, the Application Server maintains a location database of contact address bindings, which it uses to determine the network address for routing an inbound call to an access device. Each address binding in the database binds a contact URI to an AoR, as explained in *RFC 3261*. In the Cisco BroadWorks SIP Trunking solution, the Application Server uses this location database to route inbound calls to the PBX within the enterprise via a Trunk Group.

Cisco BroadWorks provides two ways to add bindings to the location database. A device can send a SIP REGISTER request to add the binding, as described in *RFC 3261* and covered in more detail in *Cisco BroadWorks SIP Access Interface Interworking Guide* [1]. A binding added via a SIP REGISTER request is valid until it expires. Alternatively, a Cisco BroadWorks administrator can add a permanent binding via provisioning. This provisioned binding is sometimes referred to as a "static registration" to distinguish it from a SIP registration, which is similarly referred to as a "dynamic registration". A dynamic registration has precedence over a static registration. Therefore, if an AoR in the Cisco BroadWorks location database has both a static contact URI and an unexpired SIP-registered contact URI, Cisco BroadWorks uses the registered contact URI and ignores the static contact URI.

As explained in section *6 Trunking User Addresses*, a Line/Port is an access side AoR. Therefore, for a Cisco BroadWorks user to have an explicit binding in the location database, that user must have a Device Endpoint assigned and a Line/Port.

In the SIP Trunking solution, Cisco BroadWorks also supports implicit bindings in the location database, in accordance with *RFC 6140* [16]. These implicit bindings do not appear explicitly in any physical database. Rather, they are logical bindings that exist in connection with another explicit entry. The support of these logical bindings allows a Pilot User's SIP registration to cover all the trunking users reachable via a Trunk Group. This greatly simplifies provisioning and helps to facilitate a plug-and-play deployment model for small businesses. It is also a necessary facility for an Enterprise Trunk, because the Enterprise Trunk Users do not have a Line/Port.

Cisco BroadWorks supports at most one SIP-registered contact URI binding per Line/Port. If two devices register to the same Line/Port, the most recent unexpired registration is considered valid and any earlier registration is ignored. Similarly, if a Line/Port has an unexpired SIP registration and a provisioned contact URI, Cisco BroadWorks considers the SIP registration valid and ignores the provisioned contact URI.

A contact URI, whether it is established via SIP registration or static configuration, can contain an IP address or a Fully Qualified Domain Name (FQDN). If Cisco BroadWorks is configured to use IPv6, then an IPv6 address is also permitted.

7.2 Pilot User Registration

A Pilot User has a unique association with a Trunk Group and represents the Trunk Group as a whole in some important ways. This is especially true in relation to the location database. Every Pilot User has a Line/Port, which can be considered the AoR of the Trunk Group itself. A SIP registration for the Pilot User can therefore represent a registration for the Trunk Group.

The Pilot User's registration can be dynamic (a SIP registration) or static (a provisioned contact URI). If the Pilot User has both a dynamic registration and a static registration, Cisco BroadWorks uses the dynamic registration and ignores the static registration.

Cisco BroadWorks supports the GIN registration mechanism defined in *RFC 6140* [16] and included in the SIPconnect recommendation [15]. In this mechanism, a PBX registers with a registrar/proxy server once, according to what is referred to as "GIN" registration, and the registrar/proxy server applies that single registration to cover all users on the PBX. The registrar/proxy server essentially adds implicit bindings to its location database, based on E.164 numbers assigned to the users on the PBX. In the Cisco BroadWorks implementation of GIN, the PBX registers against the Line/Port of the Pilot User. Cisco BroadWorks then logically adds the implicit bindings for each trunking user reachable via that Trunk Group. Cisco BroadWorks supported a GIN-like mechanism before the publication of *RFC 6140*, and therefore the *bnc* parameter and the "gin" option tag specified in *RFC 6140* are optional.

A Trunk Group in Cisco BroadWorks has a Trunk Mode attribute that determines how Cisco BroadWorks populates the *Request-URI* in the INVITE requests it sends to the PBX via that Trunk Group. The GIN mechanism applies only if the Trunk Group has a Trunk Mode set to "User".

7.3 Trunk Group User Registration

A Trunk Group User has a Line/Port, and therefore the user can have a SIP registration or a provisioned contact URI. Any such explicit registration binding for a Trunk Group User has precedence over any implicit binding.

When a Trunk Group User is also assigned to an Enterprise Trunk (this is the "hybrid" user described in section *5.4 Trunk Group User*), the presence of a registration binding for that user, whether from SIP registration or static registration, prevents the Enterprise Trunk from running its route selection policy.

8 SIP Authentication

Cisco BroadWorks can be configured to authenticate SIP requests from the PBX. SIP authentication is configured independently for each Trunk Group. Therefore, authentication can be enabled or disabled independently for each Trunk Group, and each Trunk Group can have its own credentials. Cisco BroadWorks supports Digest authentication.

When authentication is enabled for a Trunk Group, Cisco BroadWorks authenticates all SIP REGISTER requests.

Cisco BroadWorks can be configured to authenticate INVITE requests as well. The authentication of INVITE requests is controlled by the SIP parameter *inviteAuthenticationRatio*. When this parameter has the value "0", Cisco BroadWorks does not challenge any INVITE requests. When it has the value "1", Cisco BroadWorks challenges all INVITE requests it receives outside an existing dialog (that is, new INVITE requests). When it has a value between "0" and "1", it defines the fraction of INVITE requests that Cisco BroadWorks should challenge. For example, if the value is "0.5", then Cisco BroadWorks challenges 50% of all new INVITE requests. In this case, if authentication fails, Cisco BroadWorks continues to challenge the access device until authentication succeeds.

For Trunk Groups, SIP authentication operates independently of the user Authentication service. However, for trunking users with a Shared Call Appearance (SCA) device endpoint, Cisco BroadWorks challenges the SCA device according to the user's Authentication service.

9 Outbound Calls

9.1 Overview

The term *outbound call* in this guide refers to a call that originates inside the enterprise and terminates outside the enterprise, such as a call from a PBX user that terminates to an endpoint in the PSTN.

To make an outbound call, the PBX sends an initial INVITE request to the Application Server. The address fields in the INVITE request must allow the Application Server to identify a user profile for originating services. This section provides the details of how the Application Server determines originating user's profile.

For simplicity, it is assumed that SIP messages are exchanged directly between the PBX and the Application Server, even though the SIP messages typically pass through intermediaries such as SBCs. Furthermore, the term "PBX" refers to the SIP signaling entity in the enterprise, and it could be, for example, an IAD that provides interworking with a legacy PBX.

Sometimes the requirements for the PBX are mentioned. An intermediary could satisfy these requirements on behalf of the PBX. For example, when the text describes a requirement for the PBX to add *tgrp* and *trunk-context* parameters in the *Contact* header, that requirement could be, and typically is, satisfied by an SBC.

The interface between the PBX and the Cisco BroadWorks Application Server is an access side interface. Therefore, in addition to the details provided in this guide, the guidelines described in the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1] also apply.

The processing of an outbound call begins when the Application Server receives a new INVITE request from the PBX. The processing follows distinct steps, which are explained in detail in the sections that follow. At a high level, the Application Server's processing steps are as follows:

1) Identify the originating Trunk Group.
2) Identify the originating trunking user.
3) Perform translations. During this step, the Application Server may send a query to the Network Server.
4) Check for an available BTLU and seize one unit for the call. During this step, the Application Server may optionally check Enterprise Trunk capacity.
5) Check for available Trunk Group capacity and increment the capacity counts for outgoing calls and for all calls.
6) Execute originating services for the originating user, including screening services.
7) Based on the results of translations, create a terminating session and pass control to it.
8) Create and send the outgoing INVITE request.

Variations of this sequence of steps are possible. For example, the Application Server could reject the call at any one of the processing steps. The steps are also different if the new INVITE request is discovered to be a request for a call redirection, such as a request for Call Forwarding initiated by the PBX. The processing for PBX redirections is covered in section *12 PBX Redirections*.

Some of these steps, namely, translations (step 3), originating services (step 6), and processing in the terminating session (step 7), are beyond the scope of this section.

9.2 Originating Trunk Group Identification

9.2.1 Originating Trunk Group Identification Processing Steps (Stand-Alone Only)

Upon receiving an INVITE request from the PBX, the Application Server commences a sequence of lookup steps to identify the originating Trunk Group, as described in this section. The Application Server completes the steps in the order presented here, and it completes only the steps necessary to identify the originating Trunk Group.

For most of the lookup steps, the Application Server can select a Trunk Group only if that Trunk Group has a Pilot User. If a Trunk Group does not have a Pilot User, then it can be selected only using the *Line/Port Lookup* policy (see step 6).

Best Practice

Each of the following steps indicates in square brackets the name of the policy applied by the Application Server. These are the same policy names the Application Server displays in its *Verify Translation and Routing (VTR)* output.

Cisco recommends that customers learn and use the VTR tool, which provides helpful information about Cisco BroadWorks' internal call processing activity.

1) [TGRP Lookup] If the INVITE request has *tgrp* and *trunk-context* parameters in the *Contact* header URI, then the Application Server tries to match these parameters' values to the Trunk Group identifier assigned to a Trunk Group.

   Example:

   Trunk Group Austin has the Trunk Group identifier "austin@initech.example" assigned.

   The Application Server receives a SIP INVITE request with the following Contact header:

   Contact:<sip:+12145550001;tgrp=austin;trunk-context=initech.example@192.0.2.20;user=phone>

   From the *tgrp* and *trunk-context* parameters, the Application Server forms the identity value "austin@initech.example", searches for a matching Trunk Group, and finds Trunk Group Austin. The Application Server continues its call processing with Trunk Group Austin as the identified Trunk Group.

2) [OTG Lookup (PAI)] If the *P-Asserted-Identity* header has a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group.

3) [OTG Lookup (From)] If the *From* header URI is a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group.

   Example:

   Trunk Group Austin has the OTG/DTG identifier "austin" assigned.

   The Application Server receives a SIP INVITE request with the following *From* header:

   From:<sip:+12142271001@initech.test;otg=austin;user=phone>;tag=34942

From the *otg* parameter in the *From* URI, the Application Server obtains the identity value “austin”, searches for a matching Trunk Group, and finds Trunk Group Austin. The Application Server continues its call processing with Trunk Group Austin as the identified Trunk Group.

4) [Pilot Lookup (P-Preferred-Identity)] If the INVITE request has a *P-Preferred-Identity* header that contains a SIP URI, then the Application Server tries to match this URI to the Line/Port of a Trunk Group Pilot User. If it finds a Pilot User match, then the identified Trunk Group is the one associated with the Pilot User.

5) [Pilot Lookup (P-Asserted-Identity)] If the INVITE request has a *P-Asserted-Identity* header that contains a SIP URI, then the Application Server tries to match this URI to the Line/Port of a Trunk Group Pilot User. If it finds a Pilot User, then the identified Trunk Group is the one associated with the Pilot User.

6) [Line/Port Lookup] The Application Server tries to find an originating Cisco BroadWorks user from the INVITE request’s originating identity headers, following the same steps it uses to identify a user for a non-trunking origination. These steps are described in detail in the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1]. In summary, the Application Server attempts to match the URI in the *P-Preferred-Identity*, the *P-Asserted-Identity*, the *Remote-Party-ID*, or the *From* header, in that order, to a Cisco BroadWorks user’s Line/Port.

   If the Application Server finds a matching user, then:

   – If user is assigned to a Trunk Group, the Application Server selects this user as the originating user and selects this Trunk Group as the originating Trunk Group. Note that because the Application Server identified the originating user during this step, it does not execute a separate procedure to look up the originating user.

   – If the user is *not* assigned to a Trunk Group, the Application Server proceeds to process the call as a non-Trunk Group call. (This is the normal processing path for originating calls from hosted (non-trunking) Cisco BroadWorks users.)

   If the Application Server does not find a matching user at this step, then it continues with the following step.

7) [Source Address Lookup] As a final step, the Application Server can attempt to identify the originating Trunk Group by looking up the IP address. The idea behind this step is straightforward: the Application Server gets the source IP address from the INIVITE request’s *Via* header and matches it to the IP address of a Trunk Group. The implementation, however, is more complex. To accommodate routing through proxy servers, SBCs, or other intermediaries, the Application Server attempts a lookup of the network address from every *Via* header. For each *Via* header, the Application Server obtains the IP address from the received parameter, if present, or the *sent-by* field, and then it combines the IP address with the UDP or TCP port number. To obtain the IP address of the Trunk Group, the Application Server uses, in order, (1) the host part from the Pilot User’s SIP registration, (2) the host part from the Pilot User’s static contact URI, (3) the provisioned IP address of the Access Device (Identity/Device Profile). The IP address can be an IPv4 address or an IPv6 address.

   In this step, a Trunk Group is included in the search only if it has the *Enable Network Address Identity* attribute enabled.

Warning: An administrator must use caution when enabling the Trunk Group attribute *Enable Network Address Identity*, because it could lead to unexpected results when the administrator does not have an adequate understanding of the network architecture. Before deciding to rely on the *SourceAddressBasedTrunkGroupLookup* policy, the administrator must have a complete understanding of the policy's functionality and the network architecture, particularly, the SBCs or other intermediaries that are deployed.

Note the following additional points:

- By default, the Application Server attempts a case-sensitive match for the *tgrp* parameter value and a case-insensitive match for the *trunk-context* value. However, an administrator can change this behavior via the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity*. (See the following note.)
- The Application Server attempts a case-insensitive match for the OTG/DTG identifier.

NOTE: By default, the Application Server performs a case-sensitive lookup for the *tgrp* parameter. It is possible to change this behavior via the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity*. If this option is set to "false", then the Application Server performs a case-insensitive lookup.

A related container option is the provisioning container option *bw.sip.useMixedCaseTrunkGroupIdentity*. By default, the Application Server stores the Trunk Group identifier "user" part exactly as entered. However, if this container option is set to "false", then the Application Server stores the Trunk Group identifier in its database as lowercase letters, converting to lowercase first if necessary.

The Application Server stores the Trunk Group identifier "host" part in lowercase. Therefore, it always performs a case-insensitive match of the *trunk-context* parameter. This behavior is not configurable.

If the deployment depends on the Network Server for originator redirection, then an administrator may need to set similar container options on the Network Server. These container options include the nsExecution container option *bw.sip.useMixedCaseTrunkGroupIdentity* and the nsProvisioning container option *bw.sip.useMixedCaseTrunkGroupIdentity*. For a description of these container options, see the *Cisco BroadWorks Container Options Guide* [8].

Best Practice

Popular SBCs have the capability to add the *tgrp* and *trunk-context* parameters or the *otg* parameter. Cisco recommends that service providers use this capability to add the originating trunk group identity.

If the Application Server has not identified an originating Trunk Group after performing all the steps for the originating Trunk Group identification, then it processes the call as a non-trunking originating call. If the originator is a hosted (non-trunking) Cisco BroadWorks user, then the Application Server should have identified that user by a Line/Port lookup (this is step 6 in the previous procedure), and it processes the call as an originating call from that user. However, if the Application Server cannot identify a Cisco BroadWorks originator, then it processes the call as an originating call from a network user.

9.2.2 Originating Trunk Group Identification Processing Steps (IMS Only)

Upon receiving an INVITE request from the PBX, the Application Server commences a sequence of lookup steps to identify the originating Trunk Group, as described in this section. The Application Server completes the steps in the order presented here, and it completes only the steps necessary to identify the originating Trunk Group.

For most of the lookup steps, the Application Server can select a Trunk Group only if that Trunk Group has a Pilot User. If a Trunk Group does not have a Pilot User, then it can be selected only using the *Line/Port Lookup* policy (step 5).

Best Practice

Each of the following steps indicate in square brackets the name of the policy applied by the Application Server. These are the same policy names the Application Server displays in its VTR output.

Cisco recommends that customers learn and use the VTR tool, which provides helpful information about Cisco BroadWorks' internal call processing activity.

1) [TGRP Lookup] If the INVITE request has *tgrp* and *trunk-context* parameters in the *Contact* header URI, then the Application Server tries to match these parameters' values to the Trunk Group identifier assigned to a Trunk Group.

   Example:

   Trunk Group Austin has the Trunk Group identifier "austin@initech.example" assigned.

   The Application Server receives a SIP INVITE request with the following *Contact* header:

   Contact:<sip:+12145550001;tgrp=austin;trunk-context=initech.example@192.0.2.20;user=phone>

   From the *tgrp* and *trunk-context* parameters, the Application Server forms the identity value "austin@initech.example", searches for a matching Trunk Group, and finds Trunk Group Austin. The Application Server continues its call processing with Trunk Group Austin as the identified Trunk Group.

2) [OTG Lookup (PAI)] If the *P-Asserted-Identity* header has a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group.

3) [OTG Lookup (From)] If the *From* header URI is a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group

Example:

Trunk Group Austin has the OTG/DTG identifier “austin” assigned.

The Application Server receives a SIP INVITE request with the following *From* header:

From:<sip:+12142271001@initech.test;otg=austin;user=phone>;tag=34942

From the *otg* parameter in the *From* URI, the Application Server obtains the identity value “austin”, searches for a matching Trunk Group, and finds Trunk Group Austin. The Application Server continues its call processing with Trunk Group Austin as the identified Trunk Group.

4) [Pilot Lookup (P-Asserted-Identity)] If the INVITE request has a *P-Asserted-Identity* header, then the Application Server tries to match the URI in that header to the identity of a Trunk Group Pilot User. More precisely:

   – If the *P-Asserted-Identity* header has a SIP URI with a *user=phone* parameter, then the Application Server tries to match this URI to the primary DN of a Pilot User.

   – If the *P-Asserted-Identity* header has a SIP URI, then the Application Server tries to match it to a Pilot User’s primary SIP Public User Identity.

   – If the *P-Asserted-Identity* header has a tel URI, then the Application Server tries to match this URI to the primary DN of a Pilot User.

   If the Application Server finds a Pilot User, then the identified Trunk Group is the one associated with the Pilot User.

5) [Line/Port Lookup] The Application Server tries to find an originating Cisco BroadWorks user from the INVITE request’s originating identity headers, following the same steps it uses to identify a user for a non-trunking origination. These steps are described in detail in the *Cisco BroadWorks AS Mode ISC Interface Specification* [3]. In summary, the Application Server attempts to match the URI in the *P-Asserted-Identity* or the *From* header, in that order, to a Cisco BroadWorks user’s DN or Public User Identity.

   If the Application Server finds a matching user, then:

   – If the user is assigned to a Trunk Group, the Application Server selects this user as the originating user and selects this Trunk Group as the originating Trunk Group. Note that because the Application Server identified the originating user during this step, it does not execute a separate procedure to look up the originating user.

   – If the user is *not* assigned to a Trunk Group, the Application Server proceeds to process the call as a non-Trunk Group call. (This is the normal processing path for originating calls from hosted [non-trunking] Cisco BroadWorks users.)

If the Application Server does not find a matching user at this step, then it continues with the following step.

6) [Source Address Lookup] As a final step, the Application Server can attempt to identify the originating Trunk Group by looking up the IP address. The idea behind this step is fairly straightforward: the Application Server gets the source IP address from the INIVITE request's *Via* header and matches it to the IP address of a Trunk Group. The implementation, however, is more complex. To accommodate routing through proxy servers, SBCs, or other intermediaries, the Application Server tries the network address from every *Via* header. For each *Via* header, the Application Server obtains the IP address from the received parameter, if present, or the sent-by field, and then it combines the IP address with the UDP or TCP port number. To obtain the IP address of the Trunk Group, the Application Server uses the provisioned IP address of the Access Device (Identity/Device Profile). The IP address can be an IPv4 address or an IPv6 address.

   In this step, a Trunk Group is included in the search only if it has the *Enable Network Address Identity* attribute enabled.

Warning: An administrator must use caution when enabling the Trunk Group attribute *Enable Network Address Identity*, because it could lead to unexpected results when the administrator does not have an adequate understanding of the network architecture. Before deciding to rely on the *SourceAddressBasedTrunkGroupLookup* policy, the administrator must have a complete understanding of the policy's functionality and the network architecture, particularly, the SBCs or other intermediaries that are deployed.

Note the following additional points:

- By default, the Application Server attempts a case-sensitive match for the *tgrp* parameter value and a case-insensitive match for the *trunk-context* value. However, an administrator can change this behavior via the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity*. (See the note below.)
- The Application Server attempts a case-insensitive match for the OTG/DTG identifier.

NOTE: By default, the Application Server performs a case-sensitive lookup for the *tgrp* parameter. It is possible to change this behavior via the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity*. If this option is set to "false", then the Application Server performs a case-insensitive lookup.

A related container option is the provisioning container option *bw.sip.useMixedCaseTrunkGroupIdentity*. By default, the Application Server stores the Trunk Group identifier "user" part exactly as entered. However, if this container option is set to "false", then the Application Server stores the Trunk Group identifier in its database as lowercase letters, converting to lowercase first if necessary.

The Application Server stores the Trunk Group identifier "host" part in lowercase. Therefore, it always performs a case-insensitive match of the *trunk-context* parameter. This behavior is not configurable.

Best Practice

Popular SBCs have the capability to add the *tgrp* and *trunk-context* parameters or the *otg* parameter. Cisco recommends that service providers use this capability to add the originating trunk group identity.

If the Application Server identifies the originating Trunk Group after performing these steps, then it examines the attributes of the identified Trunk Group and enforces the following restrictions:

- If the Application Server identified a Trunk Group using a policy other than the Line/Port Lookup policy (step 4 in the previous section), then:
  - The Trunk Mode must be "Pilot" or "Proxy". If the Trunk Mode is "User", then the Application Server rejects the INVITE request with a *403 Forbidden* response.

If the Application Server cannot identify an originating Trunk Group after performing all the steps for the originating Trunk Group identification, then it processes the call as a non-trunking originating call. If the originator is a hosted (non-trunking) Cisco BroadWorks user, then the Application Server should have identified that user by a Line/Port lookup (this is step 5 in the previous section), and it processes the call as an originating call from that user. However, if the Application Server cannot identify a Cisco BroadWorks originator, then it processes the call as an originating call from a network user.

9.3 Originating User Identification

9.3.1 Originating User Identification Processing Steps (Stand-Alone Only)

After the Application Server identifies the originating Trunk Group, it tries to identify a business trunking user as the originating user. If the Application Server already identified the originating trunking user when it identified the originating Trunk Group (step 6 [*Line/Port Lookup*] in the procedure to identify the Trunk Group), then it skips the steps described in this section. Otherwise, it commences a sequence of lookup steps to identify the originating trunking user. The precise sequence depends on the configuration of the originating Trunk Group, which can be configured for basic lookup, basic lookup with *From* preferred, or extended lookup.

The following tables list the processing steps for originating user identification according to the Trunk Group configuration. Each table lists the processing steps in order. For each step, the *SIP Header* column indicates the SIP header in the INVITE request that the Application Server examines, while the *User Address* column indicates the user address type that the Application Server tries to match. "ATI" in the table refers to the user's Alternate Trunk Identity, while "DN" refers to the user's directory number. The Application Server completes only as many steps as necessary to identify the originating user. After it identifies the originating user, it stops processing and does not execute the remaining steps.

As shown in the tables, the Application Server may conditionally perform or skip some steps.

- Some steps may be performed only if the caller requested privacy. Specifically, this means the INVITE request contained a *Privacy* header with the value of "user" or "id".
- Some steps may be skipped if the Application Server previously identified the originating Trunk Group by matching the URI in the *P-Asserted-Identity* header to a Pilot User's identity (step 5 [Pilot Lookup (*P-Asserted-Identity*)] in the procedure to identify the Trunk Group).

Best Practice

In the following tables, the column labeled *Policy Name* provides the name of the policy applied by the Application Server. These are the same policy names the Application Server displays in its VTR output.

Cisco recommends that customers learn and use the VTR tool, which provides helpful information about the Cisco BroadWorks internal call processing activity.

The following table summarizes the lookup steps when the Trunk Group is configured for basic lookup.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*P-Asserted-Identity*	ATI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 2	DN Lookup	*P-Asserted-Identity*	DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 3	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 4	ATI Lookup	*From*	ATI	
Step 5	DN Lookup	*From*	DN	
Step 6	Route List DN Lookup	*From*	Route List DN	

The following table summarizes the steps when the Trunk Group is configured for basic lookup with *From* preferred.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*From*	ATI	
Step 2	DN Lookup	*From*	DN	
Step 3	Route List DN Lookup	*From*	Route List DN	
Step 4	ATI Lookup	*P-Asserted-Identity*	ATI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 5	DN Lookup	*P-Asserted-Identity*	DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 6	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.

The following table summarizes the steps when the Trunk Group is configured for extended lookup.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*P-Preferred-Identity*	ATI	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 2	DN Lookup	*P-Preferred-Identity*	DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 3	Route List DN Lookup	*P-Preferred-Identity*	Route List DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 4	ATI Lookup	*P-Asserted-Identity*	ATI	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 5	DN Lookup	*P-Asserted-Identity*	DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 6	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 7	ATI Lookup	*Remote-Party-ID*	ATI	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 8	DN Lookup	*Remote-Party-ID*	DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 9	Route List DN Lookup	*Remote-Party-ID*	Route List DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 10	ATI Lookup	*From*	ATI	
Step 11	DN Lookup	*From*	DN	
Step 12	Route List DN Lookup	*From*	Route List DN	

The following additional rules apply:

- If the specified header is missing from the INVITE request, then the Application Server skips that step and continues to the next. For example, if a step requires the Application Server to examine the *P-Asserted-Identity* header and the INVITE request has no *P-Asserted-Identity* header, then the Application Server skips the step.
- When the Application Server attempts an ATI lookup, it extracts the user part of the SIP URI and removes any parameters (delimited by a semicolon), then tries to match the provisioned Alternate Trunk Identity exactly. For example, if the SIP URI is *sip:101;foo@initech.example*, then the Application Server attempts an exact match of "101". The Application Server does not attempt to match a tel URI to an Alternate Trunk Identity.

- When the Application Server attempts a DN lookup or a Route List DN lookup, it extracts the number from a SIP URI, a tel URI, or both. Note the following:
  - The *From* header and *Remote-Party-ID* header can have either a SIP URI or a tel URI, but not both. If the header does, in fact, have both a SIP URI and a tel URI, the Application Server ignores the tel URI.
  - The *P-Preferred-Identity* header and *P-Asserted-Identity* header can have a SIP URI, a tel URI, or both. If the header has both a SIP URI and a tel URI, the Application Server checks the SIP URI first, and then checks the tel URI.
- To parse a phone number from a SIP URI (to match a DN or Route List DN), the Application Server proceeds as follows:
  - If the URI has a *user=phone* parameter, then the Application Server treats the user part of the URI as the *telephone-subscriber* part of a tel URI. This means the Application Server removes any *telephone-subscriber* parameters before attempting to match the DN or Route List DN.
  - Otherwise, if the user part of the SIP URI is all digits, and if the domain part of the URI is an Application Server domain or alias, then the Application Server uses these digits as the phone number. In addition to the literal digits, the Application Server allows the characters "*" and "#" as digits and allows the character "+" as the first digit.
- After the Application Server parses a phone number, either from a SIP URI or a tel URI, it normalizes the phone number before attempting a DN lookup or Route List DN lookup.
  - If the Application Server is configured to support the *phone-context* parameter and the URI has a *phone-context* parameter that starts with a plus sign ("+"), then Application Server prepends the value of the *phone-context* parameter to the phone number. For example:

    The SIP URI is

    sip:5125550103;phone-context=+1@initech.com;user=phone

    The Application Server attempts a lookup of the number

    +15125550103
  - If the phone number does not begin with a plus sign (after prepending the *phone-context* parameter value, if any), then the Application Server prepends a plus sign and the Pilot User's country code. For example:

    The SIP URI is

    sip:5125550103@initech.com;user=phone

    and the Pilot User's country code is 1, the Application Server attempts a lookup of the number

    +15125550103
- The scope of an ATI lookup, DN lookup, or Route List DN lookup is the Enterprise (Enterprise model) or Group (Service Provider model) that contains the identified Trunk Group. Furthermore, the lookup can match only a trunking user.

If the Application Server completes all of the steps of the user lookup and is unable to identify the originating user, then it creates an originating session based on the Pilot User's service profile and marks the call as a candidate for an unscreened origination (as described in section *9.3.3 Unscreened Originations*). Later, when the Application Server performs translations, it checks to see if the identified Trunk Group allows unscreened originations. If the Trunk Group allows unscreened originations, the Application Server allows the call to continue as an unscreened origination. Otherwise, the Application Server blocks the call and applies the *Forbidden* treatment. By default, when the Application Server applies the *Forbidden* treatment, it plays a call failure announcement to the caller before releasing the call.

9.3.2 Originating User Identification Processing Steps (IMS Only)

After the Application Server identifies the originating Trunk Group, it tries to identify a business trunking user as the originating user. If the Application Server already identified the originating trunking user when it identified the originating Trunk Group (step 5 [Line/Port Lookup] in the procedure to identify the Trunk Group), then it skips the steps described in this section. Otherwise, it commences a sequence of lookup steps to identify the originating trunking user. The precise sequence depends on the configuration of the originating Trunk Group, which may be configured for basic lookup, basic lookup with *From* preferred, or extended lookup.

The following tables list the processing steps for originating user identification according to the Trunk Group configuration. Each table lists the processing steps in order. For each step, the *SIP Header* column indicates the SIP header in the INVITE request that the Application Server examines, while the *User Address* column indicates the user address type that the Application Server tries to match. "ATI" in the table refers to the user's Alternate Trunk Identity, while "DN" refers to the user's directory number. The Application Server completes only as many steps as necessary to identify the originating user. After it identifies the originating user, it stops processing and does not execute the remaining steps.

As shown in the following tables, the Application Server may conditionally perform or skip some steps.

- Some steps may be performed only if the caller requested privacy. Specifically, this means the INVITE request contained a *Privacy* header with the value of "user" or "id".
- Some steps may be skipped if the Application Server previously identified the originating Trunk Group by matching the URI in the *P-Asserted-Identity* header to a Pilot User's identity (step 4 [Pilot Lookup (*P-Asserted-Identity*)] in the procedure to identify the Trunk Group).

Best Practice

In the following tables, the column labeled *Policy Name* provides the name of the policy applied by the Application Server. These are the same policy names the Application Server displays in its VTR output.

Cisco recommends that customers learn and use the VTR tool, which provides helpful information about Cisco BroadWorks' internal call processing activity.

The following table summarizes the steps for originating user identification when the Trunk Group is configured for basic lookup.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*P-Asserted-Identity*	ATI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 2	DN Lookup	*P-Asserted-Identity*	DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 3	PUI Lookup	*P-Asserted-Identity*	Primary SIP PUI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 4	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 5	ATI Lookup	*From*	ATI	
Step 6	DN Lookup	*From*	DN	
Step 7	PUI Lookup	*From*	Primary SIP PUI	
Step 8	Route List DN Lookup	*From*	Route List DN	

The following table summarizes the steps for originating user identification when the Trunk Group is configured for “basic lookup with *From* preferred”.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*From*	ATI	
Step 2	DN Lookup	*From*	DN	
Step 3	PUI Lookup	*From*	Primary SIP PUI	
Step 4	Route List DN Lookup	*From*	Route List DN	
Step 5	ATI Lookup	*P-Asserted-Identity*	ATI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 6	DN Lookup	*P-Asserted-Identity*	DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 7	PUI Lookup	*P-Asserted-Identity*	Primary SIP PUI	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 8	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Only if the caller requested privacy. Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.

The following table summarizes the steps for originating user identification when the Trunk Group is configured for “extended lookup”.

Order	Policy Name	SIP Header	User Address	Conditions/Comments
Step 1	ATI Lookup	*P-Asserted-Identity*	ATI	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 2	DN Lookup	*P-Asserted-Identity*	DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 3	PUI Lookup	*P-Asserted-Identity*	Primary SIP PUI	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 4	Route List DN Lookup	*P-Asserted-Identity*	Route List DN	Skipped if *P-Asserted-Identity* was used to identify the Trunk Group.
Step 5	ATI Lookup	*From*	ATI	
Step 6	DN Lookup	*From*	DN	
Step 7	PUI Lookup	*From*	Primary SIP PUI	
Step 8	Route List DN Lookup	*From*	Route List DN	

The following additional rules apply:

- If the specified header is missing from the INVITE request, then the Application Server skips that step and continues to the next. For example, if a step requires the Application Server to examine the *P-Asserted-Identity* header and the INVITE request has no *P-Asserted-Identity* header, then the Application Server skips that step.
- When the Application Server attempts an ATI lookup, it extracts the user part of the SIP URI and removes any parameters (delimited by a semicolon), then tries to match the provisioned Alternate Trunk Identity exactly. For example, if the SIP URI is sip:101;foo@initech.example, then the Application Server attempts an exact match of “101”. The Application Server does not attempt to match a tel URI to an Alternate Trunk Identity.
- When the Application Server attempts a DN lookup or Route List DN lookup, it extracts the number from a SIP URI, a tel URI, or both. Note the following:
  - The *From* header may have either a SIP URI or a tel URI, but not both. (If the header does, in fact, have both a SIP URI and a tel URI, the Application Server ignores the tel URI.)
  - The *P-Asserted-Identity* header may have a SIP URI, a tel URI, or both. If the header has both a SIP URI and a tel URI, the Application Server checks the SIP URI first.

- To parse a phone number from a SIP URI (to match a DN or Route List DN), the Application Server proceeds as follows:
  - If the URI has a *user=phone* parameter, then the Application Server treats the user part of the URI as the *telephone-subscriber* part of a tel URI. This means the Application Server removes any *telephone-subscriber* parameters before attempting to match the DN or Route List DN.
  - Otherwise, if the URI does *not* have a *user=phone* parameter, the Application Server can still parse a phone number if the following conditions are met:
    - The user part of the SIP URI consists of only digits. In addition to the literal digits, the Application Server allows the characters "*" and "#" as digits and allows the character "+" as the first digit.
  - The system parameter *userPhoneErrorCorrection* is set to "identityDomain" (the default), "full", or "fullEnforceUserPhone".
- After the Application Server parses a phone number, either from a SIP URI or a tel URI, it normalizes the phone number before attempting a DN lookup or Route List DN lookup.
  - If the Application Server is configured to support the *phone-context* parameter and the URI has a *phone-context* parameter that starts with a plus sign ("+"), then Application Server prepends the value of the *phone-context* parameter to the phone number. For example:

    The SIP URI is

    sip:5125550103;phone-context=+1@initech.com;user=phone

    The Application Server attempts a lookup of the number

    +15125550103
  - If the phone number does not begin with a plus sign (after prepending the *phone-context* parameter value, if any), then the Application Server prepends a plus sign and the Pilot User's country code. For example:

    The SIP URI is

    sip:5125550103@initech.com;user=phone

    and the Pilot User's country code is 1, the Application Server attempts a lookup of the number

    +15125550103
- The scope of an ATI lookup, DN lookup, or Route List DN lookup is the Enterprise (Enterprise model) or Group (Service Provider model) that contains the identified Trunk Group. Furthermore, the lookup can match only a trunking user.

If the Application Server completes all of the steps of the user lookup and is unable to identify the originating user, then it creates an originating call half session based on the Pilot User's service profile and marks the call as a candidate for an unscreened origination (as described in section *9.3.3 Unscreened Originations*). Later, when the Application Server performs translations, it checks to see if the identified Trunk Group allows unscreened originations. If the Trunk Group allows unscreened originations, the Application Server allows the call to continue as an unscreened origination. Otherwise, the Application Server blocks the call and applies the *Forbidden* treatment. By default, when the Application Server applies the *Forbidden* treatment, it plays a call failure announcement to the caller before releasing the call.

9.3.3 Unscreened Originations

An unscreened origination is an originating call from a Trunk Group with an originating party or redirecting party that the Application Server does not recognize. When the Application Server is configured to allow these unscreened originations, it allows an enterprise to route outbound calls via the service provider's network, without requiring the provisioning of additional trunking users. In a typical use case, unscreened originations result when a multiple-site enterprise experiences a partial loss of connectivity at one site and must temporarily route outbound calls via an alternate site.

When the Application Server processes an unscreened origination, it uses the service profile of the Trunk Group's Pilot User. This permits the Application Server to apply call screening services, calling line identification options, translations, and so on, according to the Pilot User's service profile. Note, however, that some Cisco BroadWorks services, particularly services such as Three-Way Calling that involve multiple calls, do not work for unscreened originating calls.

Each Trunk Group provisioned in the Application Server has configuration options to allow or to block unscreened originations. When the Application Server processes an originating call, which it has determined to be a candidate for an unscreened origination, it checks the configuration of the originating Trunk Group. If the Trunk Group permits unscreened originations, then the Application Server allows the call to continue. Otherwise, it applies the *Forbidden* treatment, which by default causes the Application Server to play a call failure announcement to the caller before releasing the call.

The Trunk Group's configuration has separate unscreened origination policies for emergency and non-emergency calls. Therefore, it is possible to configure a Trunk Group to allow unscreened emergency calls and to block unscreened non-emergency calls, or vice versa.

9.4 Business Trunking License Check

After the Application Server identifies the originating Trunk Group and the originating trunking user, it tries to seize a BTLU for the call. If the originating user is in an Enterprise, then the Application Server tries to seize a license unit from the pool allocated to the user's Enterprise. Otherwise, if the user is in a Group within a Service Provider, then the Application Server tries to seize a license unit from the pool allocated to the user's Group. If it successfully seizes a license unit, then allows the call to continue.

If all license units in the relevant pool are already seized, then the Application Server's attempt to seize a license unit fails. The Application Server blocks the outgoing call with a *Forbidden* treatment, which by default causes the Application Server to play a call failure announcement to the caller before releasing the call. Additionally, the Application Server triggers an SNMP notification (*bwTrunkingLicensedCapacityExceeded*) and indicates the failure condition in the *btluExceeded* field in the CDR.

If the originating user is assigned to an Enterprise Trunk and that Enterprise Trunk has call capacity management enabled, then the Application Server performs an additional license-related check for Enterprise Trunk capacity. When Enterprise Trunk capacity management is enabled, the Application Server maintains a count of all the license units that are seized by the users assigned to that Enterprise Trunk. For the new incoming call, the Application Server checks that the license count has not reached the limit. If the current count is under the limit, then the Application Server increments the count for this call and allows the call to continue.

Cisco BroadWorks permits flexibility in Trunk Group originations, such that the originating Trunk Group can be any Trunk Group in the originating user's Enterprise or Group. If the originating user is assigned to an Enterprise Trunk, the originating Trunk Group does not have to be a constituent Trunk Group of that Enterprise Trunk. In fact, the originating Trunk Group could be a constituent of a different Enterprise Trunk or no Enterprise Trunk at all. However, the Application Server counts the call against the Enterprise Trunk assigned to the originating user; it does not consider the originating Trunk Group when applying Enterprise Trunk call capacity management.

If the check for Enterprise Trunk capacity fails, then the Application Server takes actions similar those for the system-level license failure. The Application Server blocks the outgoing call with a *Forbidden* treatment, which by default causes the Application Server to play a call failure announcement to the caller before releasing the call. Additionally, the Application Server triggers an SNMP notification (*bwEnterpriseTrunkCapacityExceeded*) and indicates the failure condition in the *enterpriseTrunkCapacityExceeded* field in the CDR.

9.5 Originating Trunk Group Capacity Check

If the Application Server is able to seize a license unit for the call, then it checks the Trunk Group's capacity. Every Trunk Group in Cisco BroadWorks has a capacity limit for the total of outbound and inbound calls and optionally a capacity limit for outbound calls. When processing an outbound call, the Application Server checks for available capacity, checking the limit for total calls, and, if a limit for outbound calls is provisioned, checking that limit as well. If the Application Server determines that the Trunk Group has sufficient capacity for a new outbound call, it increments the capacity count for outbound calls and allows the call to continue.

If the Application Server determines that the call is an emergency call, then it allows the call continue, even if there is insufficient capacity. In this case, the Application Server still increments the count of outbound calls, which could cause the call count to temporarily exceed the capacity limits.

If the capacity is exceeded and the call is not an emergency call, then the Application Server blocks the outgoing call with a *Forbidden* treatment, which by default causes the Application Server to play a call failure announcement to the caller before releasing the call. Additionally, the Application Server performs these actions:

- Triggers an SNMP notification (*bwTrunkGroupCapacityExceeded*), which could be suppressed according to the configured throttling parameters.
- Increments PM counters for the system (*bwTrunkOriginationBlocked*), the originating user's Service Provider or Enterprise (*bwTrunkSPOriginationBlocked*), and the originating user's Group (*bwTrunkGroupOriginationBlocked*).
- Increments PM counters for the Trunk Group itself (*bwTrunkGroupPerTGOriginationBlocked*).
- Generates an originating CDR with an indication that the call was blocked because of a capacity-exceeded condition.

9.6 Outgoing INVITE Request

After the Application Server completes the call processing for the outbound call, it normally sends an outgoing INVITE request to the destination network gateway or access device. Cisco BroadWorks provides several configuration options for SIP trunking originations that affect the information in the outgoing INVITE request. This section describes these configuration options.

It is important to note that the Trunk Group's policies described here apply to the call processing in the originating session. Further call processing in the terminating session may perform services or apply other policies that affect the outgoing INVITE request. For example, if the SIP parameter *sendCallerNameInfoForNetworkCalls* is set to "false", then the Application Server sends an outgoing INVITE request to the network without a calling name.

NOTE: The Application Server can apply certain attributes of the Trunk Group or the Pilot User to determine the information in the outgoing INVITE request, as described in this section. This includes such information as the calling line identity, the charge number, and so on. Other information in the outgoing INVITE request is taken from the attributes of the originating trunking user. This information includes all information not explicitly mentioned in this section, such as information about preferred carriers.

9.6.1 Caller Identity

By default, Cisco BroadWorks supports dual caller identity signaling, in which the caller has both a presentation identity and an asserted identity, and it treats these identities as distinct identities. Accordingly, the Trunk Group configuration has some options that apply to the presentation identity and other options that apply to the asserted identity. However, if the Application Server is configured to support only a single caller identity, then the options that apply to the presentation identity affect the single caller identity, while the options that apply to the asserted identity have no effect. The default is for Cisco BroadWorks to support the dual caller identity, but an administrator can set the SIP parameter *enableTS29163Compliance* to "false" to enable single caller identity.

When the Application Server sends an outgoing INVITE request, it populates the *From* header with the presentation identity. The presentation identity comprises both a calling name and a calling number, added to the *From* header as the display name and the user part of the SIP URI, respectively. If dual caller identity is enabled, the Application Server populates the *P-Asserted-Identity* header with the caller's asserted identity. Again, the asserted identity comprises both an asserted name and an asserted number in the *P-Asserted-Identity* header, populated in similar fashion to the *From* header.

9.6.1.1 Trunking User Originations

By default, when the Application Server processes an outbound call for a recognized trunking user (that is, a "screened" origination), it sets the caller's presentation identity according to that user's provisioned profile information. This presentation identity includes both the calling name and the calling number of the originating user. Thus, regardless of the content of the *From* header in the incoming INVITE request, the Application Server populates the *From* header of the outgoing INVITE request with the provisioned presentation identity.

The Application Server also supports Trunk Group configuration options to change the way the Application Server selects the presentation identity. The Trunk Group attribute *Calling Line Identity Source for Screened Trunk Group Calls Policy* provides options that allow the PBX to provide some elements of the caller's presentation identity. Depending on the option chosen for this policy, the Application Server can accept the calling name or the calling number from the *From* header in the INVITE request from the PBX. The allowed options for this attribute are as follows:

- *Profile Name and Profile Number* – When this option is selected, the Application Server ignores the content of the received *From* header and instead selects the provisioned calling name and calling number. This is the default option.
- *Received Name and Profile Numbe*r – When this option is selected, the Application Server selects the calling name from the display name of the received *From* header and selects the calling number the provisioned user profile.
- *Received Name and Received Number* – When this option is selected, the Application Server selects both the calling name and the calling number from the received *From* header.

The Application Server allows each Trunk Group to have its own option selected for the *Calling Line Identity Source for Screened Trunk Group Calls Policy*. Alternatively, a Trunk Group can defer to the system wide default setting, controlled by the system parameter *clidSourceForScreenedCallsPolicy*.

Under certain conditions, the Application Server ignores the *Calling Line Identity Source for Screened Trunk Group Calls Policy* and selects the calling user's profile name and number. These conditions include the following:

- The call is an emergency call.
- Or, the Application Server determines that the calling identity is unavailable (for example, the *From* URI has no user part).
- Or, the Application Server determines that the calling identity matches the identity associated with the user's primary device (for example, the URI matches the user's primary Line/Port).

There is one special exception to the preceding rules: if the *Calling Line Identity Source for Screened Trunk Group Calls Policy* is set to "Received Name and Profile Number" and the Application Server determines that the calling identity matches the identity associated with the user's primary device (for example, the URI matches the user's primary Line/Port), then the Application Server selects the *received* name and profile number. (The preceding rules suggest that the Application Server would select the *profile* name.)

The Trunk Group attribute *Pilot User Calling Line Identity for External Calls Usage Policy* provides options to override the presentation identity with the provisioned identity of the Trunk Group's Pilot User. When this policy is set to "All Originating Calls", the Application Server selects the Pilot User's provisioned calling name and number, overriding any other selection. This policy has precedence over the *Calling Line Identity Source for Screened Trunk Group Calls Policy*.

The *Pilot User Calling Line Identity for External Calls Usage Policy* applies only for non-emergency calls. For emergency calls, the Application Server provides a similar Trunk Group attribute *Pilot User Calling Line Identity Usage for Emergency Calls Policy*.

Lastly, the *Pilot User Calling Line Asserted Identity Usage Policy* provides the option to select the Pilot User's asserted identity. If the policy is set to "All Originating Calls", the Application Server selects the Pilot User's asserted identity instead of the originating user's asserted identity. The Application Server allows each Trunk Group to have its own option selected for the *Pilot User Calling Line Asserted Identity Usage Policy*. Alternatively, a Trunk Group can defer to the system wide default setting, controlled by the system parameter *pilotUserCallingLineAssertedIdentityPolicy*.

9.6.1.2 Unscreened Originations

When the Application Server processes an unscreened origination, it applies the service profile of the Pilot User. By default, it also selects the provisioned calling name and calling number from the Pilot User's profile for the presentation identity, and selects the Pilot User's asserted identity.

If *Pilot User Calling Line Identity for External Calls Usage Policy*, is set to "No Calls", then the Application Server accepts the content of the *From* header in the received INVITE request for the calling name and number.

The *Pilot User Calling Line Identity for External Calls Usage Policy* applies only for non-emergency calls. For emergency calls, the Application Server provides a similar Trunk Group attribute *Pilot User Calling Line Identity Usage for Emergency Calls Policy*.

Regardless of configuration, if the Application Server considers the received calling identity to be "unavailable", then it selects the calling name and calling number from the Pilot User's profile for the presentation identity.

9.6.1.3 Route List Originations

If the Application Server identified the originating user by a Route List DN lookup, then it may treat the origination as a normal trunking user origination (that is, a "screened" origination) or as an unscreened origination, depending on the Route List user configuration. If the *Treat Originations and PBX Redirections as Screened* policy is enabled for the Route List service, then the Application Server treats these Route List originations as screened originations. This means the Application Server applies policies as it does for normal trunking user originations, as described in section *9.6.1.1 Trunking User Originations*. Otherwise, the Application Server treats the Route List originations as unscreened originations and applies the policies as described in section *9.6.1.2* Unscreened Originations. The *Treat Originations and PBX Redirections as Screened* policy is enabled by default.

> **NOTE**: The *Treat Originations and PBX Redirections as Screened* policy affects outbound calls but not inbound calls. If this policy is disabled, then Route List originations are not permitted, but Route List terminations are. In other words, this policy can be used to allow only Route List terminations. Route List originations are an alternative to unscreened originations. If *Treat Originations and PBX Redirections as Screened* is disabled, then outbound calls from a Route List number could be permitted as unscreened originations (or blocked as unscreened originations).

The *Use Route List Identity for Non-Emergency Calls* policy also affects the calling identity. If this policy is enabled for the Route List service, then the Application Server uses the received Route List DN instead of the Route List user's primary DN, but only in situations where it would otherwise use the primary DN. For example, if the Trunk Group is configured to select the calling user's profile identity for the CLID, then it would normally select the user's primary DN. However, if the user is a Route List user and the Application Server identified the user via a Route List DN, then the Application Server can use that Route List DN for the CLID in the outgoing INVITE request.

For emergency calls, the Application Server applies the *Use Route List Identity for Emergency Calls* policy in the same way.

9.6.2 Originating Trunk Group Identity

If the Trunk Group attribute *Include Trunk Identity for Calls from Trunk Group* is enabled, then the Application Server adds the Trunk Group identifier to the outgoing INVITE request as *tgrp* and *trunk-context* parameters in the *Contact* URI. This follows the syntax of *RFC 4904* [17] for identifying the originating Trunk Group.

Similarly, if the Trunk Group attribute *Include OTG Identity for Calls from Trunk Group* is enabled, then the Application Server adds the OTG/DTG Identity to the outgoing INVITE request as an *otg* parameter in the *From* URI.

9.6.3 Charge Number

The Application Server can be configured to add an additional number, called a *charge number*, to an INVITE request sent to the network. The Trunk Group attribute *Pilot User Charge Number Usage Policy* determines whether the Application Server should add the Pilot User's charge number to the outgoing INVITE request for an outbound SIP trunking call. The allowed options for this policy are as follows:

- *No Calls* – The Application Server does not use the Pilot User's charge number (except for a call from the Pilot User). This is the default option.
- *Unscreened Originating Calls* – The Application Server uses the Pilot User's charge number for unscreened originations from the Trunk Group.
- *All Originating Calls* – The Application Server uses the Pilot User's charge number for all originating calls from the Trunk Group.

10 Inbound Calls

10.1 Overview

The term *inbound call* in this guide refers to a call that originates outside the enterprise and terminates inside the enterprise, such as a call from the PSTN that terminates at a trunking user's desk phone via the PBX.

The Application Server processes an inbound call differently depending on whether the terminating user is assigned to an Enterprise Trunk or not. If the user is assigned to an Enterprise Trunk, then the Application Server runs the Enterprise Trunk's routing policy to select a Trunk Group for the outgoing INVITE request. However, if the user is not assigned to an Enterprise Trunk but is assigned to a Trunk Group, then the Application Server selects the assigned Trunk Group for the outgoing INVITE request.

The processing for an inbound call begins when the Application Server receives an initial INVITE request from an originating endpoint. During originating session processing, the Application Server identifies the called user from the *Request-URI* of the INVITE request. After originating session processing, the Application Server creates a terminating session and executes terminating services in the context of the called user's service profile. Ultimately, the Application Server creates and sends an outgoing INVITE request to the PBX.

This section provides the details of the Application Server's processing for an inbound call. At a high level, the Application Server's processing steps are as follows:

1) Identify the called user.
2) Create a terminating session for the called user.
3) Select an initial Trunk Group for the call.
4) Execute terminating services for the called user.
5) Check for an available BTLU and seize one unit for the call. During this step, the Application Server may optionally check Enterprise Trunk capacity.
6) Check for available Trunk Group capacity and increment the capacity counts for incoming calls and for all calls.
7) Create and send the outgoing INVITE request.

At each step in the processing, events are possible that could alter the processing. For example, when the Application Server executes terminating services in step 4, it could forward the call and thereby avoid an attempt to route to the PBX. Moreover, at each step the Application Server might detect failure conditions, which it could handle in various ways. In short, the sequence of steps listed here is the straight success processing path. The following subsections cover the details of these steps, including a description of failure conditions and how the Application Server handles them.

Some of these steps, namely, session creation (step 2) and terminating services (step 4), are beyond the scope of this section.

10.2 Terminating User Identification

When the Application Server processes a basic call, it creates both an originating session and a terminating session. The Application Server creates the originating session after it receives the initial INVITE request and identifies the calling user (the originating user). Within the context of the originating session, the Application Server runs translations on the called address to identify the called user (the terminating user). After the Application Server executes services in the originating session, it creates a terminating session for the terminating user and passes service control to that session.

Independently of whether a session is an originating session or a terminating session, a session can be characterized by the type of user that controls the session. If the controlling user is a Cisco BroadWorks user, then the session is a *BroadWorks user* session (or just a *user* session). Alternatively, if the controlling user is not a BroadWorks user, then the session is a *network user* session. Within Cisco/BroadSoft's technical circles, the latter is commonly referred to as a *PSTN* session. (Note that technically speaking, the Application Server creates a PSTN session if it fails to identify a Cisco BroadWorks user. Therefore, it may be more correct to say that a PSTN session has no controlling user.)

A user session and a PSTN session are fundamentally different. Most importantly, a user session is controlled by a Cisco BroadWorks user service profile, while a PSTN session is not. A user session is also associated with a Group, as well as a Service Provider or Enterprise.

The additional context available in a user session affects how the Application Server performs translations. In a user session, the Application Server performs translations in the context of a specific Cisco BroadWorks user, Group, and Service Provider or Enterprise. In a PSTN session, such context is missing. Just as a session can be characterized as a user session or a PSTN session, translations can also be characterized as user translations, which are performed in the context of a user session, and network translations, which are performed in the context of a PSTN session. The steps the Application Server takes to identify the called user are different for user translations and for network translations.

The following subsections describe user translations and network translations in more detail.

10.2.1 User Translations

The Application Server performs user translations within an originating user session. A full description of user translations would be lengthy and not entirely relevant. Therefore, this section provides a description of only those steps most relevant to inbound calls for SIP trunking.

The purpose of user translations, as applied to inbound calls, is to identify the called Cisco BroadWorks user. There are two main parts to the processing: processing on the Application Server and processing on the Network Server. Processing on the Application Server takes place first. Processing on the Network Server takes place during a query from the Application Server to the Network Server and is skipped for a call within the Group.

On the Application Server, the basic processing steps include:

- Identify the called address from the received *Request-URI*.
- Look up the called user from the called address.

The first processing step is necessary because the *Request-URI* can contain information such as feature access codes (FACs) or URI parameters that should not be interpreted as a part of the called address. For example, the following URI has a diversion inhibitor FAC ("*80"), a location code ("6"), an extension ("1337"), and a telephone-subscriber parameter ("phone-context=initech.com"):

sip:*8061337;phone-context=initech.com@broadworks.net;user=phone

When the Application Server performs user translations on this URI, it must identify the digits "61337" as the called address.

The Application Server must also determine whether it should treat the *Request-URI* as a URI that contains a phone number or as an e-mail-like URI. An example of the former is the following:

sip:+15125550000@broadworks.net

An example of the latter is the following:

sip:bill.lumbergh@initech.com

When the Application Server processes the URI, it looks for specific indications that the URI contains a phone number. If it does not find any of these indications, then it assumes the URI is an e-mail-like URI. If any one of the following conditions is true, then the Application Server processes the URI as a phone number URI:

- The URI has a user=phone parameter.

  Example: sip:+15125550001@broadworks.net;user=phone

- The URI is a TEL URI.

  Example: tel:+15125550001;npdi

- (Stand-alone mode only) The domain part of the URI is a recognized Cisco BroadWorks domain and the user part matches a phone number pattern. The pattern allows an optional initial plus sign ("+") followed by digits.

  Example: sip:+15125550001@broadworks.net

- (IMS mode only) The domain part of the URI is a recognized Cisco BroadWorks domain, user=phone error correction is enabled, and the user part matches a phone number pattern. The pattern allows an optional initial plus sign ("+") followed by digits.

  Example: sip:5125550001@broadworks.net

If the Application Server processes a SIP URI as a phone number URI, then it processes the URI user part according to the syntax of telephone-subscriber in *RFC 3966*. This syntax allows the user part to contain parameters, such as *phone-context*, *rn*, *npdi*, and so on. The Application Server identifies these parameters and removes them from the called address before attempting to look up a user.

If the Application Server interprets the URI as a phone number, then it attempts to look up the called user by one of these addresses:

- Extension (same Group or Enterprise)
- Location Code + Extension (same Group or Enterprise)
- Directory Number (DN)
- Route List DN

The Application Server stores all DNs in E.164 format. Therefore, before the Application Server attempts a DN lookup, it must convert the called number to E.164 format if it is not already in that format.

If the Application Server interprets the URI as an e-mail-like URI, then it attempts to look up the called user by one of these addresses:

- Alias
- SIP PUI (IMS only)

10.2.2 Network Translations

The Application Server performs network translations within a PSTN session. Network translations are simpler than user translations, because the PSTN session has no Cisco BroadWorks user context. The following points highlight key differences between user translations and network translations:

- Since there is no Cisco BroadWorks user, Group, or Service Provider/Enterprise context, the Application Server does not translate extensions.
- The Application Server does not translate FACs or similar service-related address information.
- The Application Server does not send a query to the Network Server, since the network element that sent the initial INVITE should have already sent a Network Server query.
- Though there are some limited, specific exceptions, as a general rule network translations must identify a Cisco BroadWorks user as the terminating user. If the translations do not identify a Cisco BroadWorks user, then the Application Server blocks the call and applies the *User Not Found* treatment, which by default results in the Application Server sending a SIP *404* response to the INVITE request.

Similar to user translations, the basic processing steps for network translations include:

- Identify the called address from the received *Request-URI*.
- Look up the called user from the called address.

If the Application Server interprets the URI as a phone number, then it attempts to look up the called user by one of these addresses:

- Direct Route identifier
- Directory Number (DN)
- Route List DN

If the Application Server interprets the URI as an e-mail-like URI, then it attempts to look up the called user by one of these addresses:

- Alias
- SIP PUI (IMS only)

10.2.3 Direct Route Termination

Direct route termination is a SIP trunking capability that can be loosely considered support for unscreened terminations. The Application Server can accept and route a call from a network device to a PBX without identifying a Cisco BroadWorks user from a lookup of the terminating number. To allow such a termination, the Application Server must identify the terminating enterprise trunk or trunk group and the configuration must allow it.

Unlike unscreened originations, there is no trunk group configuration option to allow unscreened terminations. Instead, to allow an unscreened termination, the Application Server looks up the destination trunk group identifier and identifies a trunking user to whom the identifier is assigned. If the Application Server finds such a user, then it routes the call to that user's enterprise trunk or trunk group. In this way, the Application Server can apply call processing services according to the user's service profile and can use the usual SIP trunking routing policies.

Cisco BroadWorks supports a user service named Direct Route. An administrator can assign the Direct Route service to a user and then assign direct route identifiers to the service. When the Application Server runs network translations, it attempts to match the *tgrp* and *trunk-context* parameters or the *dtg* parameter to an identifier assigned to the Direct Route service. If this lookup succeeds, then the Application Server applies the routing policies of that user's enterprise trunk or trunk group, and routes the call to the destination PBX.

10.3 Trunk Group Selection

When the Application Server prepares to send a new INVITE request to a trunking user, its first action is to select a Trunk Group to use for the termination. If the user is assigned to an Enterprise Trunk, then the Application Server applies the routing policy of the Enterprise Trunk to select one of the Trunk Groups assigned to that Enterprise Trunk.

Cisco BroadWorks supports five different Enterprise Trunk routing policies, which are in the following list:

- **Ordered Load Balancing**: The Trunk Groups are ordered and the Application Server selects each Trunk Group in turn following a round-robin algorithm.
- **Overflow**: The Trunk Groups are ordered and the Application Server selects the first Trunk Group that is reachable and has available capacity.
- **Most Idle**: The Application Server selects the Trunk Group that has the fewest number of current active calls.
- **Least Idle**: The Application Server selects the Trunk Group that has the greatest number of current active calls.
- **Weighted Overflow**: Each Trunk Group has a priority and a weight. Starting with the Trunk Groups that have the highest priority (the lowest numerical value), the Application Server selects a Trunk Group at that priority according to a weighted random pick.

When the Application Server applies a routing policy, it applies the policy only to the Trunk Groups that are available at that time. The Application Server considers a Trunk Group unavailable if it has reached its maximum capacity; therefore, it excludes Trunk Groups with no capacity available. The exclusion of unavailable Trunk Groups is an essential factor in the behavior of routing policies such as the Overflow policy. The Overflow policy selects the first *available* Trunk Group; therefore, if the first Trunk Group is at full capacity, the Application Server excludes it and can select the second Trunk Group.

The Application Server applies the Enterprise Trunk routing policy when it first processes a new inbound call. It can apply the policy again, if it discovers that the selected Trunk Group is unavailable for any reason and needs to reroute to a different Trunk Group. When the Application Server reroutes, it applies the routing policy again with the unavailable Trunk Groups excluded.

Example of Weighted Overflow Routing Policy

The Enterprise Trunk has Trunk Groups assigned with the following priorities and weights:

- Trunk Group A, Priority 1, Weight 10
- Trunk Group B, Priority 1, Weight 50
- Trunk Group C, Priority 1, Weight 20
- Trunk Group D, Priority 2, Weight 30

The selection algorithm begins with dividing the Trunk Groups by priority, so A, B, and C are in one group (Priority 1) and D is in a second group (Priority 2). Priority 1 is higher, so the Application Server considers the Priority 1 group first. If A, B, and C all have available capacity, then the Application Server picks a Trunk Group randomly according to the following probabilities:

- Trunk Group A, Probability 10/(10+50+20) = 0.125
- Trunk Group B, Probability 50/(10+50+20) = 0.625
- Trunk Group C, Probability 20/(10+50+20) = 0.25

10.4 Business Trunking License Check

After the Application Server executes terminating services, it tries to seize a BTLU for the call. If the terminating user is in an Enterprise, then the Application Server tries to seize a license unit from the pool allocated to the user's Enterprise. Otherwise, if the user is in a Group within a Service Provider, then the Application Server tries to seize a license unit from the pool allocated to the user's Group. If it successfully seizes a license unit, then allows the call to continue.

If all license units in the relevant pool are already seized, then the Application Server's attempt to seize a license unit fails. If the Enterprise Trunk has a route exhaustion action configured, then the Application Server takes that action. If the route exhaustion action is set to "None", then the Application Server blocks the incoming call with a *Busy* treatment. Additionally, the Application Server triggers an SNMP notification (*bwTrunkingLicensedCapacityExceeded*) and indicates the failure condition in the *btluExceeded* field in the CDR.

If the terminating user is assigned to an Enterprise Trunk and that Enterprise Trunk has call capacity management enabled, then the Application Server performs an additional license-related check for Enterprise Trunk capacity. When Enterprise Trunk capacity management is enabled, the Application Server maintains a count of all the license units that are seized by the users assigned to that Enterprise Trunk. For the new incoming call, the Application Server checks that the license count has not reached the limit. If the current count is under the limit, then the Application Server increments the count for this call and allows the call to continue.

If the check for Enterprise Trunk capacity fails, then the Application Server takes actions similar those for the system-level license failure. If the Enterprise Trunk has a route exhaustion action configured, then the Application Server takes that action. If the route exhaustion action is set to "None", then the Application Server blocks the incoming call with a *Busy* treatment. Additionally, the Application Server triggers an SNMP notification (*bwEnterpriseTrunkCapacityExceeded*) and indicates the failure condition in the *enterpriseTrunkCapacityExceeded* field in the CDR.

10.5 Terminating Trunk Group Capacity Check (Enterprise Trunking)

If the Application Server is able to seize a BTLU for the call, then it checks the initial Trunk Group's capacity. Every Trunk Group in Cisco BroadWorks has a capacity limit for the total of outgoing and incoming calls and optionally a capacity limit for incoming calls. When processing an incoming call, the Application Server checks for available capacity in the selected Trunk Group, checking the limit for total calls, and, if a limit for incoming calls is provisioned, checking that limit as well. If the Application Server determines that the Trunk Group has sufficient capacity for a new incoming call, it increments the capacity count for incoming calls and allows the call to continue.

If the capacity is exceeded, then the Application Server executes the Enterprise Trunk routing policy to select another Trunk Group. The Application Server then checks the capacity of this Trunk Group. If the newly selected Trunk Group has available capacity, then the Application Server allows the call to continue. Otherwise, it continues to execute the Enterprise Trunk routing policy until it finds a Trunk Group with available capacity or it reaches the end of the Enterprise Trunk's route list. The latter condition is the "route exhaustion" condition.

If the Application Server detects the route exhaustion condition, then the Application Server performs the *Route Exhaustion Action* configured for the Enterprise Trunk (see section *11.4 Enterprise Trunk Route Exhaustion*).

Additionally, the Application Server performs these actions for each Trunk Group that it rejected because of unavailable capacity:

- Sends an SNMP notification (*bwTrunkGroupCapacityExceeded*) subject to throttling.
- Increments PM counters for the Trunk Group (*bwTrunkGroupPerTGTerminationBlocked*).
- Adds an indication in the terminating CDR that the Trunk Group was evaluated and rejected because of a capacity-exceeded condition.

10.6 Outgoing INVITE Request

10.6.1 Addressing for Inbound Calls (Stand-Alone Only)

After the Application Server selects a Trunk Group, it generates the address fields of the INVITE request based on:

- The address configuration of the destination trunking user and the Pilot User.
- The Trunk Mode of the Trunk Group's Identity/Device Profile (inherited from the Identity/Device Profile Type).
- The attributes of the Trunk Group.

10.6.1.1 Destination User Address Configuration

User addressing is explained in section *6 Trunking User Addresses*. In that section, it is explained that a trunking user can have the following access-side addresses:

- Alternate Trunk Identity
- Line/Port
- Directory Number (DN)
- Route List DN

When the Application Server prepares to send an INVITE request to the PBX for that trunking user, it can form two SIP URIs, one with the properties of an AoR and the other with the properties of a contact URI. The Application Server places the AoR in the INVITE request's *To* header. Depending on the Identity/Device Profile options (described next), it can also place the contact URI in the INVITE request's *Request-URI*.

When the Application Server forms either the AoR or the contact URI, it takes the URI's user part from the user's Alternate Trunk Identity, the user part of the user's Line/Port, the called Route List DN, or the user's primary DN, in that precedence order. When it forms the AoR, it takes the domain part from the domain part of the user's Line/Port or the domain part of the Pilot User's Line/Port. When it forms the contact URI, it takes the domain part from the user's registration contact if available, or from the Pilot User's registration contact if not.

If the Application Server identified the terminating user by a Route List DN lookup, then it sends that Route List DN to the PBX unless the terminating user – in this case, a Route List user – has an Alternate Trunk Identity or a Line/Port. This is the only scenario in which the Application Server can send a Route List DN as the called number. A Route List DN is a "passive" address, meaning that the Application Server can only use it if an external network element selects it. For example, a network element can send an INVITE request to the Application Server with a Route List DN in the *Request-URI.*

10.6.1.2 Trunk Mode

The Trunk Mode option of the Identity/Device Profile Type affects the addressing fields of the initial INVITE request to the PBX in a fundamental way.

Note that in all modes, if the destination trunking user has an explicit contact URI, either from a SIP registration or from provisioning, then the Application Server uses that contact URI as the *Request-URI* for the INVITE request to the PBX. The only exception to this rule is when the destination trunking user is a Pilot User, since the contact URI of a Pilot User is considered a contact URI for the Trunk Group the Pilot User is assigned to, and not necessarily a contact URI for the Pilot User itself.

Also note that after the Application Server formats the *Request-URI* according to the Trunk Mode, it can later modify the *Request-URI* based on other attributes of the Trunk Group, as described in the section that follows this one.

10.6.1.2.1 Trunk Mode User

Trunk Mode User is appropriate when routing to the PBX device depends on the called number being in the *Request-URI*, and when the Application Server should simulate the role of a proxy/registrar, that is, the Application Server retarget the request based on a binding of a contact URI to an AoR.

If the Identity/Device Profile has its Trunk Mode set to "User", then the Application Server populates the *Request-URI* of the INVITE request as follows:

- If the destination trunking user has a contact URI, obtained either from a SIP registration or from provisioning, then the Application Server uses this contact URI.
- Otherwise, the Application Server forms the *Request-URI* by taking the user part from the destination user's address, in order of precedence, the user's Alternate Trunk Identity, the user part of the user's Line/Port, the called Route List DN, or the user's primary DN and the host part from the Pilot User's contact URI. If the Pilot User does not have a contact URI, then the Application Server can instead take the host part from the Device Endpoint's configured network address.

Note that the *Request-URI*, in this case, has properties similar to a registered contact URI (rather than an AoR). This is because the host part is taken from the Pilot User's contact URI. This means, for example, that the host part is typically an IP address.

Based on the example configuration described above, the INVITE request would have the following address fields:

Request-URI: sip:+15125550006@10.16.145.10

To URI: sip:+15125550006@initech.example

10.6.1.2.2 Trunk Mode Pilot

Trunk Mode Pilot is appropriate when routing to the PBX device requires a *Request-URI* that is a contact URI for the Pilot User. (The Pilot User's AoR and registered contact URI are assumed to be representative of the PBX device itself).

If the Identity/Device Profile has its Trunk Mode set to "Pilot", then the Application Server populates the *Request-URI* of the INVITE request as follows:

- If the destination trunking user has a contact URI, obtained either from a SIP registration or from provisioning, then the Application Server uses this contact URI.
- Otherwise, the Application Server uses the Pilot User's contact URI. The Application Server obtains the contact URI either from a SIP registration or from a provisioned contact URI.

The *To* header URI is important when the Trunk Mode is Pilot, because the *To* URI identifies the called PBX user. Some PBXs always identify the called user from the *To* URI. Other PBXs can identify the called user from the *Request-URI*. For these PBXs, it is necessary for an SBC or other network element to copy the *To* URI into the *Request-URI* before sending the INVITE request to the PBX.

10.6.1.2.3 Trunk Mode Proxy

Trunk Mode Proxy is appropriate when the Application Server knows a route to the PBX, but does not simulate the role of an inbound proxy server/registrar, that is, it does not simulate a proxy server that resolves an AoR to a contact URI for retargeting. In this mode, the INVITE request has an AoR in the *Request-URI*, and a *Route* header with a URI to direct the INVITE request to the PBX.

When the Identity/Device Profile has its Trunk Mode set to "Proxy", then the Application Server populates the *Request-URI* of the INVITE request as follows:

- If the destination trunking user has a contact URI, obtained either from a SIP registration or from provisioning, then the Application Server uses this contact URI.
- Otherwise, the Application Server forms the *Request-URI* by taking the user part from the destination user's address, in order of precedence, the user's Alternate Trunk Identity, the user part of the user's Line/Port, the called Route List DN, or the user's primary DN, and the host part from the Pilot User's Line/Port.

The Application Server then adds a Route header with the Pilot User's contact URI.

10.6.1.2.4 Example

This section provides an example to show how the Trunk Mode affects the destination address fields in the INVITE request from the Application Server to the PBX. For this example, the addresses of the called user and the Pilot User for the selected Trunk Group are configured as follows.

Called User

Alternate Trunk Identity: (None)

Line/Port: (None, because the user is an Enterprise Trunk User.)

Directory Number: +1-512-555-0006

Contact URI: (None. Not possible because the user has no Line/Port)

Pilot User

Alternate Trunk Identity: (None)

Line/Port: sip:5125550000@initech.example

Directory Number: +1-512-555-0000

Contact URI: sip:5125550000@10.16.145.10

Address Fields for Trunk Mode User

When the Trunk Mode is "User", the Application Server simulates a proxy server/registrar, in that it simulates the retargeting of the called user's AoR to a contact URI. In this case, the called user's AoR and contact URI are implicit, in accordance with *RFC 6140*. The implicit AoR is sip:+15125550006@initech.example. The implicit contact URI is sip:+15125550006@10.16.145.10. Therefore, the destination address fields in the INVITE request are the following:

Request-URI: sip:+15125550006@10.16.145.10

To URI: sip:+15125550006@initech.example

Address Fields for Trunk Mode Pilot

When the Trunk Mode is "Pilot", the Application Server sets the Pilot User's contact URI as the *Request-URI* and the called user's implicit AoR as the *To* URI. The destination address fields in the INVITE request are the following:

Request-URI: sip:+15125550000@10.16.145.10

To URI: sip:+15125550006@initech.example

Address Fields for Trunk Mode Proxy

When the Trunk Mode is "Proxy", the Application Server acts in the role of a routing agent, and does not perform any retargeting. The destination address fields in the INVITE request are the following:

Request-URI: sip:+15125550006@initech.example

To URI: sip:+15125550006@initech.example

Route URI: sip:+15125550000@10.16.145.10

The following table summarizes the formation of the *Request-URI* based on the Trunk Mode.

Trunk Mode	Request-URI User Part	Request-URI Host Part
User	User's access-side address (Alternate Trunk Identity, Line/Port, Route List DN, DN)	Pilot User's contact URI
Proxy	User's access-side address (Alternate Trunk Identity, Line/Port, Route List DN, DN)	Pilot User's Line/Port
Pilot	Pilot User's contact URI	Pilot User's contact URI

10.6.1.3 Trunk Group Attributes

Certain Trunk Group attributes can affect how Cisco BroadWorks forms the *Request-URI*:

- If *Include DTG Identity for Calls to Trunk Group* is enabled for the Trunk Group, then the Application Server adds a *dtg* parameter with the value provisioned for that Trunk Group.
- If *Include Trunk Identity for Calls to Trunk Group* is enabled for the Trunk Group, then the Application Server adds a *tgrp* parameter with a value taken from the user part of the Trunk Group identity, and a *trunk-context* parameter with a value taken from the domain part of the Trunk Group identity.
- If *Route to Peering Domain* is enabled, then the Application Server overwrites the domain part of the *Request-URI* with the provisioned Peering Domain.

10.6.2 Addressing for Inbound Calls (IMS Only)

After the Application Server selects the destination Trunk Group, the attributes of that Trunk Group influence the way the Application Server forms the outgoing INVITE request to the PBX.

In an IMS deployment, the Application Server is somewhat constrained by its role as a Telephony Application Server in the IMS architecture, and therefore is constrained in its ability to manipulate destination address fields. The effect of these constraints is that the Application Server generally "proxies" the *Request-URI* between the incoming INVITE request from the network and the outgoing INVITE request to the PBX. The exception to this general statement is when the IMS network is configured to route requests to the Application Server based on a PSI. The PSI makes the Application Server itself a destination for the incoming INVITE from the network and allows the Application Server more freedom to set the destination address fields in the outgoing INVITE to the PBX, which it sends as an Out-of-the-Blue request.

The behavior of the Application Server in the larger IMS context is described in detail in the appendix. The basics "rules" concerning the Application Server's behavior are covered in this section. The way the Application Server forms the outgoing INVITE request to the PBX is affected by the following:

- Trunk Mode of the Trunk Group's Identity/Device Profile (inherited from the Identity/Device Profile Type)
- Trunk Group's attributes
- (Trunk Mode Pilot only) The called user's address configuration and the Pilot User's address configuration

10.6.2.1 Trunk Mode

10.6.2.1.1 Trunk Mode User

If the Trunk Group's Identity/Device Profile has the Trunk Mode set to "User", then the Application Server "proxies" the *Request-URI* received from the incoming INVITE request to the outgoing INVITE request sent to the PBX. The Application Server also copies the *Request-URI* to the *To* header URI.

> **NOTE**: Trunk Mode User is not compatible with Enterprise Trunking. The Application Server cannot route to a Trunk Group if the Trunk Mode is "User" and the Trunk Group was selected via an Enterprise Trunk routing policy.

10.6.2.1.2 Trunk Mode Pilot

If the Trunk Group's Identity/Device Profile has the Trunk Mode set to "Pilot", then the Application Server sets the Pilot User's Public User Identity as the Request-URI of the outgoing INVITE request sent to the PBX. Additionally, the Application Server sets the *To* header URI to identify the called user. The Application Server forms the *To* header URI as follows:

- If the called user has an Alternate Trunk Identity, then the Application server forms the *To* header URI as a SIP URI, setting the user part from the called user's Alternate Trunk Identity and setting the host part to match the host part of the Pilot User's Public Identity.
- Otherwise, if the called user has a Public Identity, then the Application Server uses this SIP URI for the *To* header URI.
- Otherwise, if the called user has a Directory Number, then the Application Server forms the *To* header URI as a SIP URI, setting the user part from the called user's DN and setting the host part to match the host part of the Pilot User's Public Identity.

The Application Server sends this request as an Out-of-the-Blue terminating request.

10.6.2.1.3 Trunk Mode Proxy

If the Trunk Group's Identity/Device Profile has the Trunk Mode set to "Proxy", then the Application Server "proxies" the *Request-URI* received from the incoming INVITE request to the outgoing INVITE request sent to the PBX. The Application Server also copies the *Request-URI* to the *To* header URI.

10.6.2.2 Trunk Group Attributes

Certain Trunk Group attributes can affect how Cisco BroadWorks forms the *Request-URI*:

- If *Include DTG Identity for Calls to Trunk Group* is enabled for the Trunk Group, then the Application Server adds a *dtg* parameter with the value provisioned for that Trunk Group.
- If *Include Trunk Identity for Calls to Trunk Group* is enabled for the Trunk Group, then the Application Server adds a *tgrp* parameter with a value taken from the user part of the Trunk Group identity, and a *trunk-context* parameter with a value taken from the domain part of the Trunk Group identity.
- If *Route to Peering Domain* is enabled, then the Application Server overwrites the domain part of the *Request-URI* with the provisioned Peering Domain.

10.6.2.3 Caller Preferences (IMS only)

In the Cisco BroadWorks SIP Trunking solution, a Trunk Group is understood to be a route between the Application Server and the PBX. Thus, when an Enterprise Trunk selects a Trunk Group, it is effectively selecting the routing path to the PBX. In an IMS deployment, Cisco BroadWorks must work together with the other IMS network element to control the routing path. Cisco BroadWorks supports a few different ways to affect the routing path. The recommended method is to use the caller preferences mechanism defined in *RFC 3841*. When the Application Server has caller preferences enabled, it adds a feature tag in the *Accept-Contact* header of the INVITE request to indicate the selected Trunk Group. The Application Server sends this INVITE request to the S-CSCF, which uses the feature tag to identify the P-CSCF and routes the INVITE request to that P-CSCF. The caller preferences mechanism integrates well with an IMS network in which all PBX users are included in the same implicit registration set.

Figure 11 shows dual routing paths for an IMS deployment. Each routing path is represented in Cisco BroadWorks as a Trunk Group. The two paths between the IMS network and the enterprise are two different physical paths, designed to protect business continuity in the event that one of the physical paths fails. For outgoing calls from the enterprise, the route selection depends on routing logic within the enterprise. For incoming calls to the enterprise, the routing depends on the Trunk Group selection in the Enterprise Trunk routing policy on the Application Server. E-SBCs in the enterprise register with the IMS network using SIP registration, for example, following the TISPAN Business Trunking Specification [18]. Even though the registrations occur through separate P-CSCFs, the same S-CSCF handles the registrations and becomes the serving CSCF.

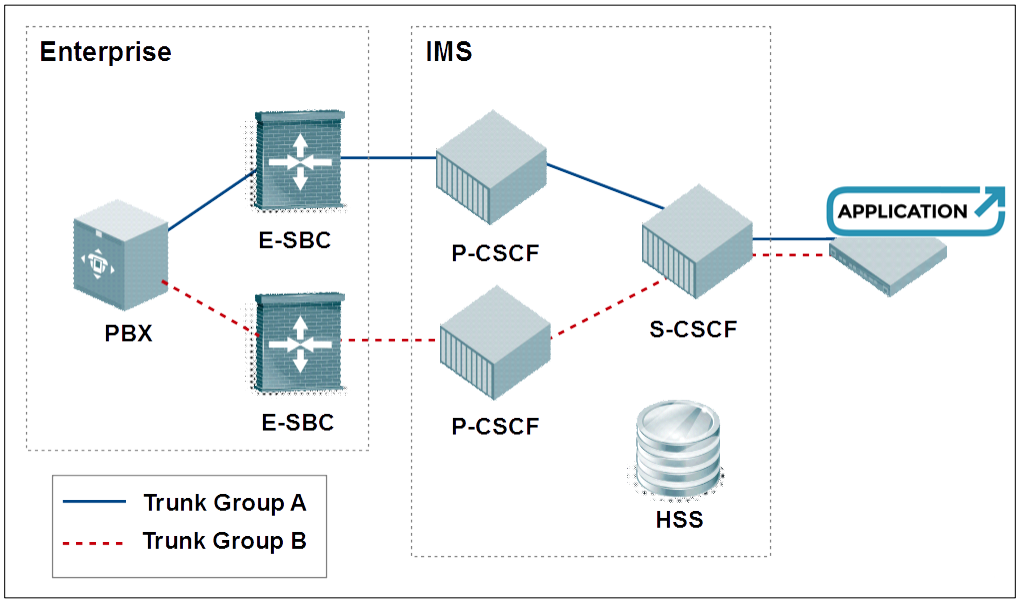

Figure 11 SIP Trunking Routing in IMS

If the S-CSCF supports SIP caller preferences, then the Application Server can make use of that capability to control the route selection. To use caller preferences, the identities and service profiles in the IMS network are set up as shown in *Figure 12*. All PBX users have service profiles and identities configured on the PBX in the enterprise. In the IMS, all PBX users are covered by a wildcarded public user identity, labeled as User X in the diagram. The IMS also has public user identities for pilot users: one for Trunk Group A and one for Trunk Group B. These pilot user identities are provisioned in an implicit registration set with the wildcarded public user identity. Because of this implicit registration set, any pilot user SIP registration implicitly registers all the PBX users via the wildcarded public user identity. PBX users also have service profiles and identities provisioned in Cisco BroadWorks. The pilot users in IMS are associated with trunk group pilot users in Cisco BroadWorks. Note that this diagram shows a Route List user provisioned in Cisco BroadWorks. The Route List user is optional, but is added here to show that this capability is useful in an IMS deployment.

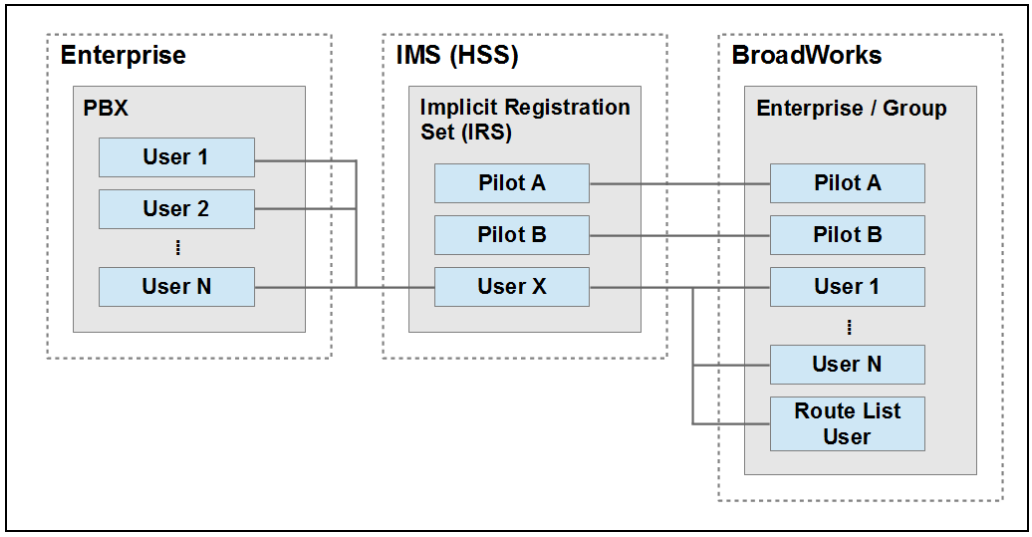

Figure 12 Service Profiles and Identities for IMS-based SIP Trunking

To understand how the S-CSCF uses caller preferences to route an incoming call to the enterprise, suppose that Pilot A and Pilot B are both registered so that the location database available to the S-CSCF contains the data in the following table.

Public Identity (AoR)	Device URI	Path	Implicitly Registered Identities
sip:pilot-a@enterprise	sip:pilot-a@device	sip:P-CSCF-A	sip:pilot-b@enterprise sip:user-*@enterprise
sip:pilot-b@enterprise	sip:pilot-b@device	sip:P-CSCF-B	sip:pilot-a@enterprise sip:user-*@enterprise

The following figure shows the call flow for an incoming call to the enterprise. The Application Server receives the incoming INVITE request, runs the routing policy of the Enterprise Trunk, and selects Trunk Group A. In the outgoing INVITE request, the Application Server adds the *Accept-Contact* header with a sip.description feature tag. The value of this feature tag is the public identity of Pilot A, indicating that Trunk Group A is selected. When the S-CSCF receives this INVITE request, it knows that it should route using the registration of Pilot A, and it routes the INVITE request toward the P-CSCF for that registration entry.

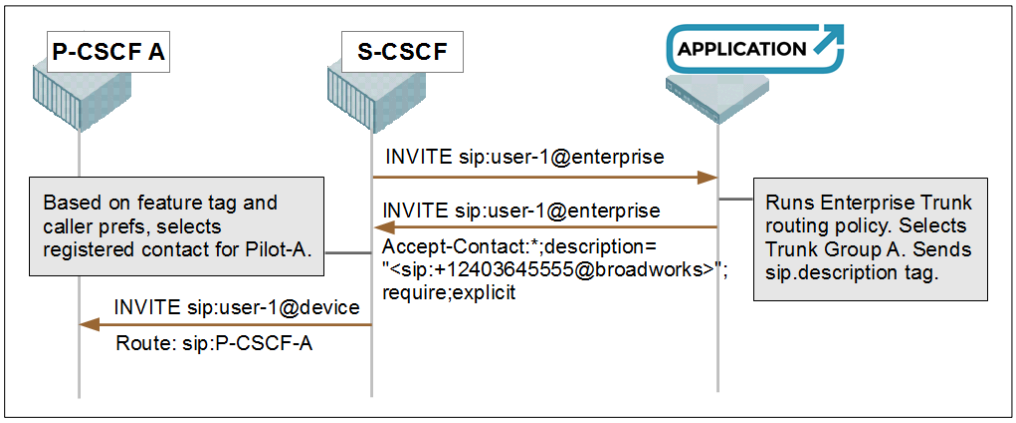

Figure 13 IMS Routing for Incoming SIP Trunking Call

The caller preferences mechanism is enabled or disabled by a policy setting on the Trunk Group. An administrator can enable the *Implicit Registration Set Support Policy* for a Trunk Group. Alternatively, an administrator can configure a Trunk Group to use the system-wide policy setting, which is controlled by the *implicitRegistrationSetSupport* system parameter.

When the selected Trunk Group has the policy enabled, the Application Server adds an *Accept-Contact* header entry to the INVITE request for trunking terminations. The *Accept-Contact* header entry added for the trunk group uses the "sip.description" feature tag with the following format.

```
Accept-Contact:*;description="<Trunk Group pilot PUI>";require;explicit
```

The trunk group pilot PUI value in the *Accept-Contact* header entry is the SIP PUI of the pilot user for the terminating trunk group. For example, if the trunk group's pilot user has a SIP PUI of "sip:+12403645555@broadworks", then the *Accept-Contact* header entry for the trunk group is as follows.

```
Accept-Contact:*;description="<sip:+12403645555@broadworks>";require;
explicit
```

10.7 Connected Identity

The connected identity is the identity of the connected remote party, taking into consideration any redirections that may have occurred. Cisco BroadWorks supports the connected identity, subject to configuration options and policies.

The *Support Connected Identity Policy* for a Trunk Group controls how the Application Server processes the connected identity for trunk group calls. By default, the *Support Connected Identity Policy* option is disabled, and the Application Server does not accept connected identity from the PBX.

The *Support Connected Identity Policy* affects the Application Server behavior in two ways. First, if the policy is enabled for a Trunk Group, then the Application Server can accept the connected identity from the PBX in SIP *18x* and *200* responses to the initial INVITE request. Note, however, that although the Application Server may initially accept the connected identity from the PBX, it may later override that update as it applies other identity policies. Second, if the policy is enabled for a Trunk Group, then the Application Server applies the trunk group's calling line ID (CLID) selection policies when selecting the connected identity. Depending on the settings of the Trunk Group's CLID policies, the Application Server can then select the connected identity received from the PBX, which is a more accurate connected identity when the PBX redirects a terminating call. For example, if the Application Server routes an inbound call to User A on the PBX and if User A forwards the call to User B (also on the PBX), then the PBX can provide User B's identity as the connected identity for the call. In general, when the *Support Connected Identity Policy* option is enabled, the Application Server selects a connected identity that is more consistent with the CLID. For example, if the trunk group's CLID policies are configured to use the pilot user's identity for the CLID, then the Application Server also uses the pilot user's identity consistently for the connected identity.

The Application Server does not accept connected identity updates from SIP re-INVITE or UPDATE requests from a trunk group. This means the Application Server supports neither connected identity updates after answer nor updates before answer from an UPDATE request.

If the *Support Connected Identity Policy* is enabled, then the Application Server applies the trunk group CLID policies when selecting the connected identity. The following rules describe how the Application Server selects the connected identity based on the CLID policies. The rules are listed in order of decreasing precedence.

- If the *Pilot User Calling Line Identity for External Calls Usage Policy* option is set to "All Originating Calls", then the Application Server selects the pilot user's identity as the connected identity for all calls to that Trunk Group.
- If the *Calling Line Identity Source for Screened Trunk Group Calls Policy* option is set to "Received Name and Received Number", then the Application Server selects the connected name and connected number received from the PBX.
- If the *Calling Line Identity Source for Screened Trunk Group Calls Policy* option is set to "Received Name and Profile Number", then the Application Server selects the connected name received from the PBX and the connected number from user's profile.
- If the *Calling Line Identity Source for Screened Trunk Group Calls Policy* option is set to "Profile Name and Profile Number", then the Application Server selects the connected name and the connected number from the user's profile.

If the *Support Connected Identity Policy* is enabled and the *Calling Line Identity Source for Screened Trunk Group Calls Policy* option is set to "Received Name and Received Number" or "Received Name and Profile Number", then the Application Server receives the connected identity from the trunk group in SIP *18x* and *200* responses to the initial INVITE request. This is the only possibility for the Application Server to receive the connected identity from the PBX. The Application Server does not accept the connected identity in re-INVITE or UPDATE requests. This means the Application Server cannot accept a connected identity update after answer or before answer via an UPDATE request.

If the Application Server receives an *18x* or *200* response with no connected identity, then the connected identity in effect at that time remains in effect. For example, if the PBX sends an *18x* response with a *P-Asserted-Identity* header followed by a *200* response without a *P-Asserted-Identity* header, then the Application Server retains the connected identity from the *18x* response rather than revert back to the profile identity.

The Application Server does not accept an "unavailable" identity from an access device. If the PBX sends a connected identity that the Application Server interprets as an unavailable identity, then the Application Server ignores that connected identity entirely, including the identity name, identity number, and presentation indicator. An example of an unavailable identity is a SIP URI that has no user part. For a complete explanation of the rules the Application Server applies to interpret an identity as unavailable, see the *Calling Line Identity Compliance Enhancements Feature Description, Release 18.0* [14].

One additional special case applies. If the connected identity matches the user's primary Line/port (primary SIP PUI in IMS mode), then the Application Server selects the user's profile identity for the connected identity.

10.7.1 Connected Identity Privacy

The Application Server supports connected identity privacy, both through the Connected Line Identification Restriction (COLR) service as well as through the SIP signaling. COLR is a user service that can be enabled or disabled by the user via the web interface, as well as through OCI-P and other provisioning interfaces. A SIP message can indicate privacy in the *Privacy*, *RPID-Privacy*, *Remote-Party-ID*, or *Anonymity* headers.

When the Application Server receives a SIP response with connected identity from a Trunk Group and that Trunk Group is configured to support connected identity, then the Application Server considers both the COLR setting and the SIP message headers to determine whether to apply privacy protection. The following is the process taken by the Application Server to determine the privacy status:

- If the SIP system parameter, *supportPrivacyNone*, is set to "true", then connected identity privacy can be controlled completely by the *Privacy* header.
  - If the *Privacy* header is present and has the "user" or "id" value, then the Application Server applies privacy protection.
  - If the *Privacy* header is present and has the "none" value, then the Application Server applies no privacy protection, even if COLR is enabled.
  - If the *Privacy* header is not present, then the privacy status is determined by the COLR setting. The Application Server provides privacy protection if and only if COLR is enabled.
- If the SIP system parameter, *supportPrivacyNone*, is set to "false", then connected identity privacy is controlled by both the COLR setting and the *Privacy* header.
  - If COLR is enabled, then the Application Server provides privacy protection.
  - If the SIP message requests privacy (for example, it has a *Privacy* header with the "user" or "id" value), then the Application Server provides privacy protection.

  If neither one of the two preceding conditions is true, the Application Server omits privacy protection.

10.7.2 Asserted Identity Selection

If the Multiple Calling Line Identity Model is enabled in the Application Server (that is, the *enableTS29163Compliance* SIP parameter is set to "true"), then the connected identity is the *presentation* identity, which is distinct from the *asserted* identity. In this model, the asserted identity selection is also affected when the *Support Connected Identity Policy* option is enabled for a Trunk Group. Specifically, if a Trunk Group has the *Support Connected Identity Policy* option enabled, then the Application Server can select the pilot user's asserted identity for a redirected call in accordance with the Trunk Group's *Pilot User Calling Line Asserted Identity Usage Policy* option. As an example scenario, if the following conditions are all true, then the Application Server uses the identity of the Trunk Group's pilot user for the asserted identity sent to the redirection target:

- The redirected user is a trunking user.
- The call to the trunking user was initially established as a terminating call.
- The connected Trunk Group has the *Support Connected Identity Policy* option enabled.
- The connected Trunk Group has the *Pilot User Calling Line Asserted Identity Usage Policy* option set to "All Originating Calls".

11 Route Advancing

11.1 Route Advancing and Timing

Route advancing is a key aspect of Cisco BroadWorks support for network resiliency through redundancy. The Application Server can be configured to communicate with redundant network elements. Then, if the Application Server detects that a particular network element is unreachable or unresponsive, it can route advance to an alternate network element. This route advancing can enable a call to succeed that would otherwise fail.

Timing is a key aspect of a route advancing strategy. The Application Server allows a network element a definite amount of time to respond before it considers the element unresponsive. If the time limit is too short, it could lead to a false positive, deciding the element is unreachable when it is merely slow to respond. However, if the time limit is too long, it limits the actions that the Application Server can take before the caller abandons the call attempt. Accordingly, the Application Server provides a number of timing related parameters, which administrative staff can tweak to control the route advance timing.

Cisco BroadWorks supports route advancing through several mechanisms, operating at different levels. At the lowest level, the Application Server can resolve a domain name in the DNS and attempt to reach different network elements via the transport addresses returned from the name server queries. At this level, the Application Server behavior follows the mechanism of *RFC 3263*, and is able to resolve NAPTR, SRV, and A/AAAA records. At the next level, the Application Server can carry out a route advance strategy defined at the Trunk Group level. In the recommended configuration, this means the Application Server applies the routing policy of the Enterprise Trunk to try different Trunk Groups in succession. Finally, at the highest level, the Application Server can take action at a services level. At this level, the Application Server can perform an action according to the called user's service profile, such as Call Forwarding Not Reachable, or it can perform an action according to the Enterprise Trunk or Trunk Group configuration, such as applying a *Busy* treatment.

11.2 Transport Address Route Advancing

Cisco BroadWorks supports the *RFC 3263* procedures for locating SIP servers using the DNS. Compared to the other procedures Cisco BroadWorks supports for route advancing, such as Enterprise Trunk routing, the DNS-based procedures are typically not the best choice. The reason is that the DNS-based procedure offers a minimal degree of control. Using a more advanced mechanism such as Enterprise Trunk routing allows finer control over route advance timers and alternate route selection. Nevertheless, DNS-based routing can be useful in some deployments, and it is one option available to the service provider.

Although Cisco BroadWorks supports NAPTR and SRV DNS lookups, this support is not enabled by default. To enable SRV lookups, an administrator must set the SIP parameter *supportDnsSrv* to "true".

```
AS_CLI/Interface/SIP> set supportDnsSrv true
...Done
```

Similarly, NAPTR lookups are not enabled by default. To enable NAPTR lookups, an administrator must the SIP parameter *supportTcp* to "true" and set the SIP parameter *supportDnsNaptr* to "true".

```
AS_CLI/Interface/SIP> set supportTcp true
```

```
SIP TCP support change will not take effect until a restart is performed

...Done

AS_CLI/Interface/SIP> set supportDnsNaptr true
...Done
```

The lookup of A or AAAA records depends on the IP versions that are enabled, according to the value of the SIP parameter *sipIpVersion*. If this parameter is set to "ipv4" (the default value), then the Application Server supports only IPv4 and performs only A record queries. If it is set to "ipv6", the Application Server supports only IPv6 and performs only AAAA queries. Finally, if the parameter is set to "both", then the Application Server supports IPv4 and IPv6 simultaneously and performs both A and AAAA queries.

Based on the settings of the SIP parameters, Cisco BroadWorks performs DNS queries as necessary. If a contact URI has a domain name for the host part, then Cisco BroadWorks queries for the NAPTR, SRV, A, or AAAA records, as appropriate for the configuration. As an optimization, the Application Server supports a local lookup database, which can contain statically configured entries. This facility uses a local file, */usr/local/broadworks /bw_base/conf/namedefs*, which is similar to the familiar */etc/hosts* file.

After Cisco BroadWorks has collected transport addresses from the DNS queries, it sends the first INVITE request to the first IP address. If Cisco BroadWorks has additional transport addresses to try, it attempts to detect quickly whether the network element at that transport address is reachable. Cisco BroadWorks follows the same procedure for each transport address until the last one, when it allows more time for the network element to respond.

There are three SIP interface parameters that control the timing of Cisco BroadWorks route advancing to the next IP address:

- *t1* – Equivalent to the value of T1 as defined in *RFC 3261*. Cisco BroadWorks uses this parameter to set the initial value of the retransmission timer for UDP. The default value is 500 (ms).
- *t2* – Equivalent to the value T2 as defined in *RFC 3261*. Cisco BroadWorks uses this parameter in calculating the route advance timer for TCP. The default value is 4000 (ms).
- *suspiciousAddressThreshold* – The maximum number of times Cisco BroadWorks can send the INVITE request with UDP when the transport address is not the last address. The default value is 3.

Cisco BroadWorks' route advance timer, when there is at least one additional transport address to try, depends on whether the transmission protocol is UDP or TCP.

For UDP destinations, Cisco BroadWorks uses a retransmission and route advance strategy as follows:

- Cisco BroadWorks sets the timer for the first retransmission to *t1*.
- Cisco BroadWorks doubles the length of the retransmission timer each time it retransmits the INVITE request. Thus it sets the timer for the n^{th} retransmission to 2^(n-1)**t1*.
- If Cisco BroadWorks has another transport address to try after the current one, it limits the number of times it sends the INVITE request to the current transport address to a value configured as the SIP parameter *suspiciousAddressThreshold*.

- After Cisco BroadWorks sends an INVITE request for the final time to a transport address, it sets the retransmission timer again, using the value 2^(n-1)**t1*. When the timer again expires, Cisco BroadWorks route advances to the next transport address.
- When Cisco BroadWorks tries the last transport address, it sets the maximum number of retransmissions to 7, ignoring the value of *suspiciousAddressThreshold*.

UDP Route Advance Example:

In this example, the values of the SIP interface parameters are:

t1 = 500 (ms)

suspiciousAddressThreshold = 3

supportDnsSrv = true

supportTcp = false

Cisco BroadWorks needs to send an INVITE request to the contact URI sip:+12142270001@initech.com. Cisco BroadWorks makes SRV and A queries to the DNS and obtains two IP addresses, IP1 and IP2. Cisco BroadWorks sends an INVITE request first to IP1. The host at that address is unreachable, so Cisco BroadWorks retransmits the INVITE request. After the maximum number of attempts to IP1, Cisco BroadWorks route advances and sends the INVITE request to IP2. The following table shows the events and actions, along with the timing.

Time (Seconds)	Event	Action(s)	Comment
0.0	INVITE ready to send	INVITE to IP1 / Timer set to 0.5s	Initial INVITE to IP1. Retransmission timer set to the value of the parameter *t1* (default value is 0.5s).
0.5	Timer expires	INVITE to IP1 / Timer set to 1.0s	Timer set to double the previous value.
1.5	Timer expires	INVITE to IP1 / Timer set to 2.0s	Timer set to double the previous value.
3.5	Timer expires	INVITE to IP2 / Timer set to 0.5s	Maximum number of transmissions to IP1 reached, as determined by the *suspiciousAddressThreshold* parameter, causing a route advance. Timer set again to the value of the parameter *t1*.
3.5+delta	Response from IP2	Timer stopped	

For TCP destinations, Cisco BroadWorks does not retransmit INVITE requests. However, Cisco BroadWorks does employ a route advance strategy as follows:

- If the current transport address is not the last one, Cisco BroadWorks sets a route advance timer based on the values of t1, t2, and *suspiciousAddressThreshold*.

  If the *suspiciousAddressThreshold* parameter has the value n, then Cisco BroadWorks calculates the value of the route advance timer by applying the following recursive formula:

  – timer(n) = timer(n-1) + min(t2, 2^{n-1}*t1)

  – timer(1) = t1

Applying this formula, the route advance timer takes the values shown in the following table for default values of t1 (500 ms) and t2 (4000 ms).

Suspicious Address Threshold	Route Advance Timer (seconds)
1	0.5s
2	1.5s
3	3.5s
4	7.5s
5	11.5s
6	15.5s

- When the route advance timer expires, Cisco BroadWorks performs a route advance, sending the INVITE request to the next transport address, which then becomes the current transport address.
- If the current transport address is the last one, then Cisco BroadWorks sets a timer for 64*t1. If this timer expires before Cisco BroadWorks receives any response, Cisco BroadWorks considers the remote host unreachable.

TCP Route Advance Example

In this example, the values of the SIP interface parameters are:

t1 = 500 (ms)

t2 = 4000 (ms)

suspiciousAddressThreshold = 3

supportDnsSrv = true

supportTcp = true

supportDnsNaptr = true

Cisco BroadWorks needs to send an INVITE request to the contact URI sip:+12142270001@initech.com. Cisco BroadWorks makes NAPTR, SRV, and A queries for the domain name initech.com and obtains two IP addresses, IP1 and IP2, both reachable via TCP. Cisco BroadWorks sends an INVITE request first to IP1. Cisco BroadWorks calculates the value of the route advance timer as t1 + min(2*t1, t2) + min(4*t1, t2) = 3.5s. After receiving no response from IP1, the route advance timer expires and Cisco BroadWorks sets IP2 as the current transport address. Cisco BroadWorks sends the INVITE request to IP2 and sets a timer for 64*t1 = 32s. The following table shows the events and actions, along with the timing:

Time (Seconds)	Event	Action or Event	Comment
0.0	INVITE ready to send	INVITE to IP1 / Timer set to 3.5s	Initial INVITE to IP1. Route advance timer set according to the values of the parameters *t1*, *t2*, and *suspiciousAddressThreshold*.
3.5	Timer expires	INVITE to IP2 / Timer set to 32s	Route advance timer expires, causing a route advance. Because IP2 is the last transport address, the timer is set to 64**t1*.
3.5+delta	Response from IP2	Timer stopped	

11.3 Enterprise Trunk Route Advancing

In Cisco BroadWorks SIP Trunking, a Trunk Group is a logical route to a PBX. For reliability, a typical deployment consists of redundant Trunk Groups, which provide alternate routes in the case of a failure. If Cisco BroadWorks detects that a PBX is unreachable via a particular Trunk Group, then it can route advance to try a different Trunk Group.

Compared to route advancing at the level of transport addresses, route advancing at the Trunk Group level offers far greater control. Cisco BroadWorks supports configurations where both levels of route advancing can be used for the same inbound call. However, Cisco recommends that operators avoid the DNS-based route advancing at the transport address level and fully use the route advancing at the Trunk Group level, as provided by the Enterprise Trunk routing policies.

Every Enterprise Trunk in Cisco BroadWorks has a number of constituent Trunk Groups and a routing policy to select a Trunk Group for an inbound call. When Cisco BroadWorks handles a new inbound call, it applies the Enterprise Trunk's routing policy to select an initial Trunk Group and prepares to send an INVITE request to the PBX via that Trunk Group. If an event occurs to indicate a failure or to otherwise block a termination via that Trunk Group, then the Application Server can perform a route advance and select an alternate Trunk Group. To select the alternate Trunk Group, the Application Server applies the Enterprise Trunk's routing policy again, this time excluding the unusable Trunk Group. If the Application Server finds a newly selected Trunk Group to also be unacceptable, it can again perform a route advance, up to the maximum number of reroute attempts as configured for the Enterprise Trunk. Each time the Application Server route advances, it applies the routing policy, excluding those Trunk Groups that it determined to be unusable.

When the Application Server selects a Trunk Group to route to, several conditions can cause the Application Server to reject that Trunk Group and perform a route advance. In some cases, the Application Server can detect such a condition before it actually sends an INVITE request via that Trunk Group. These conditions include:

- The Application Server determines that the Trunk Group does not have capacity to allow the call.
- Cisco BroadWorks Session Admission Control determines that a new terminating session is not allowed.
- The Application Server has no transport address to which to route. This can occur because of a failure to resolve a domain name, an unregistered Pilot User, or other similar conditions.

When the Application Server sends an INVITE request via a Trunk Group, it sets an *invitation timer* to the value set in the Trunk Group's *Unreachable Destination Timeout* attribute. If the invitation timer expires, the Application Server aborts the termination attempt with a REQUEST_TIMEOUT release cause, which causes the Application Server to route advance.

The following table lists events that are possible after the Application Server sends the INVITE request. For each event, the table describes how the event affects the Application Server's processing. For more information about release causes and treatments, see the *Cisco BroadWorks Treatment Guide* [9].

Event	Comments
100 response received	If the Application Server is communicating via UDP, it stops the retransmission timer. If the Application Server route advances later due to the invitation timer, it sends a CANCEL request at that time to terminate the SIP transaction.
18x response received	If the Application Server is communicating via UDP, it stops the retransmission timer. The Application Server stops the invitation timer.
3xx response received	The Application Server interprets this response as a request from the PBX to forward the call. Under certain conditions, the Application Server can also process the response as a PBX Redirection. For more information about such redirections, see section *12.1 In-Dialog PBX Redirection*.
Invitation timer expires	The Application Server aborts the termination attempt with a REQUEST_TIMEOUT release cause, which causes the Application Server to attempt a route advance. If the Application Server received any 1xx response, it sends a CANCEL request to cancel the SIP transaction.
REQUEST_TIMEOUT release cause	The Application Server performs a route advance.
REQUEST_FAILURE release cause	The Application Server performs a route advance.
SERVER_FAILURE release cause	The Application Server performs a route advance.
TEMPORARILY_UNAVAILABLE release cause	If the Application Server did not receive an *18x* response previously, then it performs a route advance. If the Application Server did receive an *18x* response, then it may or may not perform a route advance, depending on the Cisco BroadWorks system configuration. Specifically, if the system parameter *terminateUnreachableTriggerDetectionOnReceiptOf18x* is "true", then the Application Server does not attempt a route advance. (That is, the Application Server assumes that it is the PBX itself that has rejected the INVITE request, so that using a different Trunk Group to reach the PBX would be ineffective.)
Configurable treatment	If the treatment has "route advance" enabled, then this causes the Application Server to perform a route advance.
Other release cause (for example, BUSY, USER_NOT_FOUND)	The Application Server does not perform a route advance.

Cisco BroadWorks supports configurable treatments, as described in the *Cisco BroadWorks Treatment Guide* [9]. This facility allows an administrator to map a SIP response code to a system-defined release cause, such as REQUEST_FAILURE, or to a customer-defined treatment (called a "configurable treatment"). The following table shows the default mapping of SIP status codes to the release causes that trigger a route advance.

Incoming SIP Status Code	Release Cause
401, 407, 480, 606	TEMPORARILY_UNAVAILABLE
408	REQUEST_TIMEOUT
400, 402, 405, 406, 409, 411, 414, 415, 420, 422, 481, 482, 483, 485, 487, 488	REQUEST_FAILURE
All 5xx	SERVER_FAILURE

Other system-defined release causes do not trigger a route advance.

NOTE: For the most up-to-date information about treatments, including the default mapping of SIP status codes, see the *Cisco BroadWorks Treatment Guide* [9].

If Cisco BroadWorks detects a failure for every Trunk Group in the Enterprise Trunk, or if it reaches the configured limit for route advance attempts, then it considers the PBX unreachable, and it proceeds according to the route exhaustion policy of the Enterprise Trunk.

11.4 Enterprise Trunk Route Exhaustion

If the Application Server exhausts all routes within the Enterprise Trunk, either by reaching the maximum number of reroute attempts or by unsuccessfully trying each Trunk Group in the route list, then the Application Server performs the *Route Exhaustion Action* configured for the Enterprise Trunk. The choices for the *Route Exhaustion Action* are as follows:

- When the action is set to "Forward", the Application Server forwards the call to the configured destination.
- When the action is set to "None", the Application Server applies the *Temporarily Unavailable* treatment by default. An administrator can change this default behavior via Cisco BroadWorks' configurable treatments facility.

When the Application Server applies a treatment for Enterprise Trunk route exhaustion, the default is to apply the *Temporarily Unavailable* treatment. However, this behavior is configurable via the Application Server's configurable treatments facility, which is described in the *Cisco BroadWorks Treatment Guide* [9]. Depending on the scenario conditions, the Application Server can provide either of the following two call blocking service events:

- If the Application Server determines at least one Trunk Group in the routing list to be "unreachable", then the Application Server applies a configurable treatment mapped to the *ETRouteExhaustUnreachable* call blocking service event.
- Otherwise, the Application Server applies a configurable treatment mapped to the *ETRouteExhaust* call blocking service event.

The Application Server determines a Trunk Group to be "unreachable" if the termination attempt fails for a reason other than status or capacity. In other words, if the Trunk Group has the "available" status and sufficient capacity, and the Application Server tries unsuccessfully to terminate to it, then that Trunk Group is unreachable. The following are examples of unreachable Trunk Group scenarios:

- The Application Server sends an INVITE request and the PBX sends a *480* (*Temporarily Unavailable*) response.
- The Application Server sends an INVITE request which times out before the PBX sends a response.
- The pilot user has an expired SIP registration, so the Application Server has no address to terminate to.

For clarity, the following are two scenarios where the Trunk Group is *not* considered unreachable:

- The Trunk Group has reached its capacity and the Application Server will not allow any more terminating calls to the Trunk Group.
- The Trunk Group is configured for Stateful Trunk Group routing and the Application Server has determined that it is "unavailable". For more information about Stateful Trunk Group Routing, see section *19.6 Stateful Trunk Group Routing Configuration*.

When the Application Server applies the treatment, it may invoke services in response, such as Call Forwarding Unreachable or Call Forwarding No Answer, based on the terminating user's service profile.

Note that an administrator can provision a forward or reroute action directly on a Trunk Group for an unreachable or capacity-exceeded condition. These actions provisioned for a Trunk Group take precedence over the *Route Exhaustion Action* provisioned for an Enterprise Trunk.

11.5 Trunk Group Rerouting and Forwarding

If Cisco BroadWorks detects that a Trunk Group has failed, meaning that the PBX is not reachable via that Trunk Group, then it can execute an unreachable action provisioned specifically for that Trunk Group.

If a Trunk Group is part of an Enterprise Trunk, then the unreachable action provisioned for the Trunk Group has precedence over the Enterprise Trunk's routing policy. This means that if Cisco BroadWorks detects that the Trunk Group has failed, it takes the action provisioned for the Trunk Group and stops executing the Enterprise Trunk routing policy. This feature interaction is typically not what was intended. Therefore, it is recommended to set the Unreachable Destination Action to None for each Trunk Group that is part of an Enterprise Trunk, and instead configure the Route Exhaustion Action at the Enterprise Trunk level.

If a Trunk Group is not part of an Enterprise Trunk, then it makes sense to configure the Unreachable Destination Action for the Trunk Group. The allowed actions are as follows:

- *None* – Cisco BroadWorks applies *Busy* treatment. If the called user has services that trigger on busy, such as Call Forwarding Busy or Voice Mail Deposit, then these services are executed.
- *Forward to Phone Number/SIP-URI* – Cisco BroadWorks forwards the call to the configured destination.
- *Reroute to Trunk Group* – Cisco BroadWorks reroutes the call to an alternate Trunk Group. The alternate Trunk Group must have a Pilot User.

Several events trigger an unreachable condition. These events are the following:

- The invitation timer expires.
- The Application Server receives a SIP failure response, and the response code maps to one of these internal release causes: REQUEST_TIMEOUT, REQUEST_FAILURE, and SERVER_FAILURE.
- The Application Server receives a SIP failure response, the response code maps to the TEMPORARILY_UNAVAILABLE internal release cause, *and* the Application Server did not previously receive an *18x* response.
- The Application Server receives a SIP failure response, the response code maps to the TEMPORARILY_UNAVAILABLE internal release cause, the Application Server previously received an *18x* response, and the value of the system parameter *terminateUnreachableTriggerDetectionOnReceiptOf18x* is "false".
- The Application Server receives a SIP failure response, the response code maps to a configurable treatment, and the configurable treatment has the *routeAdvance* indicator set to "true".
- The Session Admission Control processing determined that it could not allow a new terminating session.

For more information about internal release causes and configurable treatments, see the *Cisco BroadWorks Treatment Guide* [9].

NOTE: (Stand-alone only) If the called user is not a Pilot User and has an explicit contact URI (from a SIP registration or a provisioned "static" contact URI), then the Application Server attempts to route directly to the contact URI. If that attempt fails, the Application Server applies TEMPORARILY_UNAVAILABLE treatment, ignoring any Trunk Group reroute action.

12 PBX Redirections

Although Cisco BroadWorks considers the PBX an access device, Cisco BroadWorks also recognizes the PBX as a call control platform, capable of call processing actions that go beyond the capabilities of basic access devices such as SIP phones. Because Cisco BroadWorks is also a call control platform, Cisco BroadWorks and the PBX must coordinate call processing activities in some cases to avoid undesirable feature interactions. For example, both Cisco BroadWorks and the PBX are able to perform a Call Forwarding or Call Transfer operation. When the PBX performs a Call Forwarding or Call Transfer, generally, a "redirection", that operation can have an impact on Cisco BroadWorks in areas such as screening services and accounting.

Figure 14 shows a general PBX redirection scenario. User X in the PSTN calls User A, who is provisioned as a trunking user in Cisco BroadWorks and has service profiles on both Cisco BroadWorks and the PBX. Cisco BroadWorks runs terminating services for User A and routes the call to the PBX. The PBX also runs terminating services for User A and redirects the call to User B, who is also a trunking user with service profiles on both Cisco BroadWorks and the PBX. User B's profile on the PBX redirects the call to PSTN User Y, causing the PBX to route the call through Cisco BroadWorks. When Cisco BroadWorks processes the SIP message from the PBX, it interprets the message as indicating a call redirection caused by User B in the PBX. Therefore, Cisco BroadWorks runs redirecting services, including screening services using User B's service profile, before routing the call out to the PSTN.

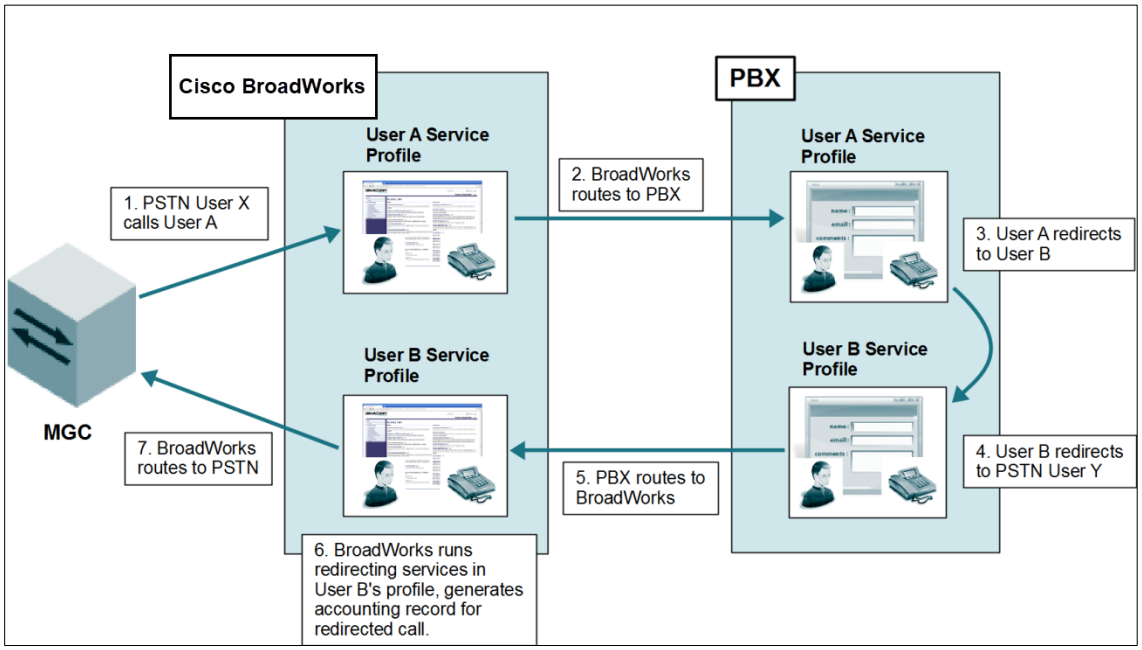

Figure 14 Cisco BroadWorks and PBX Interaction for Redirection behind the PBX

NOTE: To enable the PBX access device as an access-side call control platform, the Identify/Device Profile Type in Cisco BroadWorks for the PBX must have the *PBX Integration* option enabled.

The way Cisco BroadWorks handles the PBX redirection is intended to emulate the way Cisco BroadWorks handles an internal redirection. *Figure 15* shows a redirection scenario that is similar to the redirection scenario in *Figure 14*, except that the redirection occurs completely within Cisco BroadWorks. In some key aspects, the way Cisco BroadWorks performs User B's redirecting services and generates accounting records in these two scenarios is largely the same.

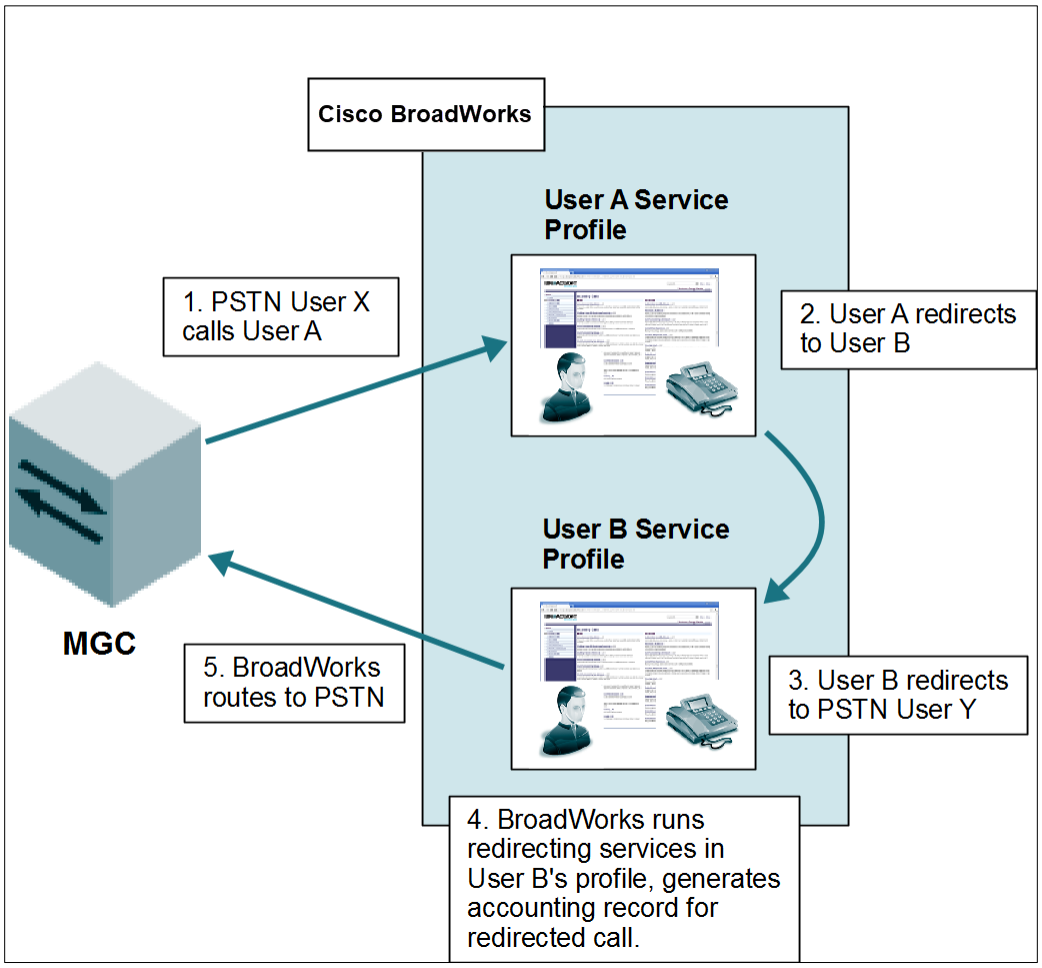

Figure 15 Redirection Internal to Cisco BroadWorks.

The diagram in *Figure 14* depicts the general PBX redirection scenario and illustrates the need for coordination between Cisco BroadWorks and the PBX for call redirections. The most important aspect of this coordination is how Cisco BroadWorks processes the SIP message from the PBX. Depending on the particular scenario, this SIP message can be a 302 response, a REFER request, or an INVITE request. The following subsections cover the details of these specific scenarios.

12.1 In-Dialog PBX Redirection

12.1.1 Overview

A typical in-dialog PBX redirection scenario begins with the Application Server sending an INVITE request to the PBX for a new call. The call processing on the PBX results in the PBX redirecting the call back through the Application Server. In the specific case of an in-dialog PBX redirection, the PBX sends the Application Server a SIP message in the same dialog as the original INVITE request. If the call is unanswered, which means the PBX has not yet sent a final response to the INVITE request, then the PBX sends a *302* response to indicate that the Application Server should redirect the call. If the call is answered, then the PBX sends a REFER request in the same dialog as the original INVITE request. Note that the case of a *302* response is a Call Forwarding scenario, while the case of a REFER request is a Blind Transfer scenario.

NOTE: In a third possible scenario, the PBX sends a REFER request after the call is alerting but before it is answered. Although this scenario is less common than the *302* response scenario, the Application Server supports it.

12.1.1.1 SIP 302 Response (Call Forward)

If the PBX has not yet sent a final response to the INVITE request, then it can send a *302* response to the Application Server to redirect the call. (Although a *302* response is typical, any 3xx response is allowed and has the same effect.) If the redirecting user and the terminating user are different, as in the scenario shown in *Figure 16*, then the PBX must add the necessary redirection information to the *302* response in the form of a *History-Info* header or a *Diversion* header. The Application Server inspects these headers to determine the redirecting party, and uses that information to execute redirecting services and generate accounting records.

The Application Server supports both *History-Info* and *Diversion* headers. Normally, the PBX sends only a *History-Info* header or only a *Diversion* header, but not both. If the PBX sends both headers, then the Application Server can process the headers in three different ways, depending on configuration:

- The Application Server can merge the *History-Info* and *Diversion* headers, following the recommendations in *RFC 6044*.
- The Application Server can process the *History-Info* header and ignore the *Diversion* header.
- The Application Server can process the *Diversion* header and ignore the *History-Info* header.

For details on the Application Server's processing of the *History-Info* header and *Diversion* header, including the related configuration, see the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1].

A call flow diagram depicting the before answer in-dialog PBX redirection scenario is provided in the following figure.

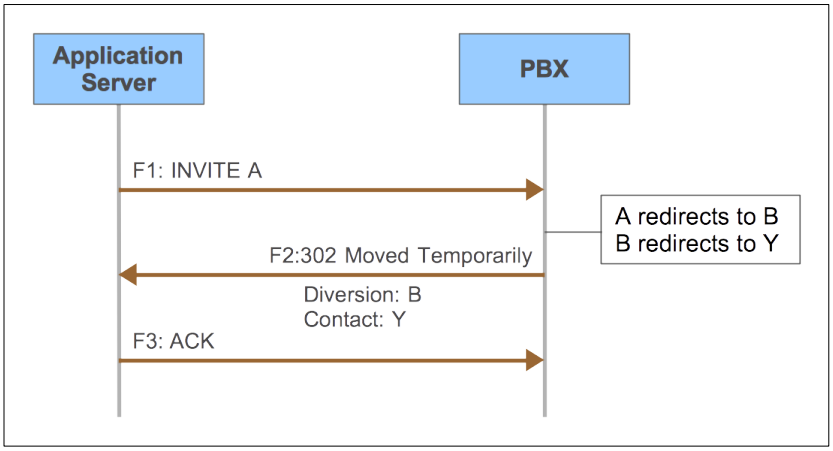

Figure 16 In-Dialog PBX Redirection Using 302 Response

If the *302* response contains a *History-Info* header, it must indicate that User B is the last redirecting party. An example *History-Info* header for this scenario is the following:

```
History-Info: <sip:+12142271001@10.16.145.5;user=phone>;index=1,
 <sip:+12142271002@initech.example;user=phone>;index=1.1
```

In the example, the first *History-Info* URI is for User A (+1-214-227-1001). This URI is the *Request-URI* from the original INVITE request (F1). The second URI is for User B (+1-214-227-1002), and reflects the internal redirection from User A to User B within the PBX.

If the *302* response contains a *Diversion* header instead of a *History-Info* header, it too must indicate that User B is the last redirecting user. An example *Diversion* header for this scenario is the following.

```
Diversion: <sip:+12142271002@initech.example;user=phone>;reason=unknown,
 <sip:+12142271001@10.16.145.5;user=phone>;reason=user-busy
```

Note that if the Application Server were to receive the *302* response without the required redirection information – that is, either the *History-Info* header or the *Diversion* header – then it would assume that User A is the redirecting user, because the response is in the same dialog as the INVITE request to User A, and it would perform the redirecting services of User A. This behavior is likely to yield undesirable consequences if in fact User B is the redirecting user. For example, if User B redirected to their Voice Mail (in the call flow diagram, User Y is an external Voice Mail server), then the Voice Mail Deposit would be for User A instead of User B.

12.1.1.2 SIP REFER request (Blind Transfer)

If the PBX has already sent a *200* response to the INVITE request, then it can send a REFER request to the Application Server to redirect the call. The PBX must send the REFER request in the same dialog as the established call. (The Application Server does not accept an out-of-dialog REFER request.) To indicate the last redirecting user, the PBX must add a *Referred-By* header to the REFER request. The Application Server inspects the *Referred-By* header to identify the redirecting user.

A call flow diagram depicting this scenario is provided in the following figure.

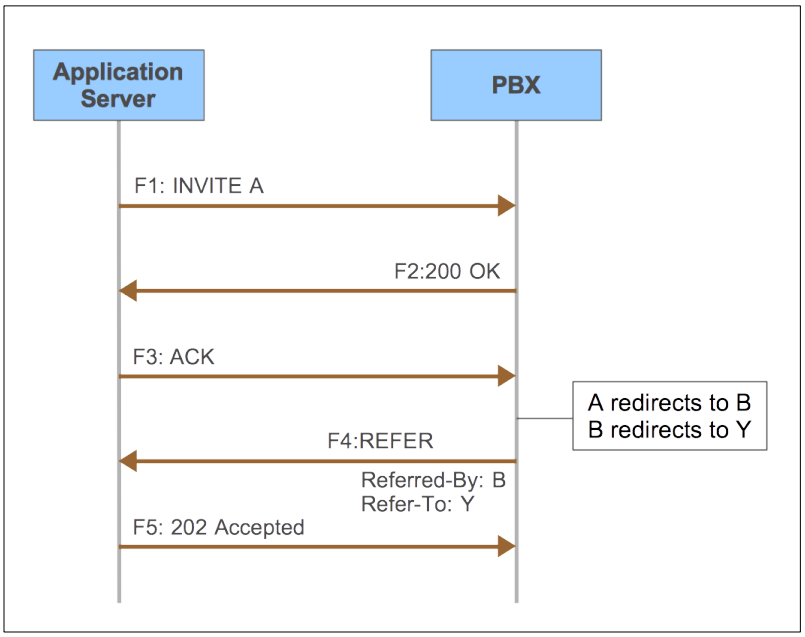

Figure 17 In-Dialog PBX Redirection Using REFER Request

Referring again to the scenario shown in *Figure 14,* the *Referred-By* header should contain User B's identity. The following is an example of the *Referred-By* header.

```
Referred-By: <sip:+12142271002@initech.example;user=phone>
```

In this example, +1-214-227-1002 is the directory number of User B.

An in-dialog PBX redirection using a REFER request is possible for any established call, even one that originated from the PBX. The following figure shows a call flow diagram for an alternative scenario in which the PBX originates a call before initiating a blind transfer.

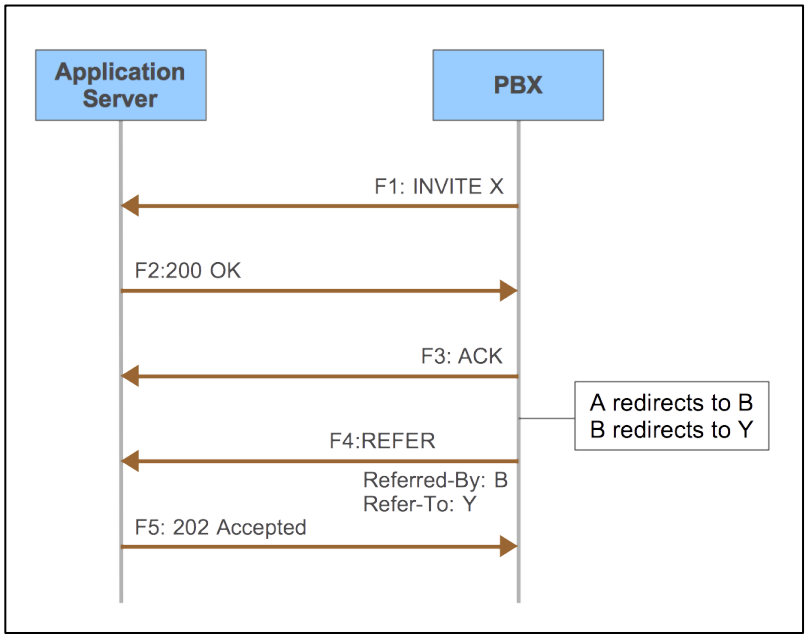

Figure 18 In-Dialog PBX Redirection Using REFER Request, Outbound Call

12.1.1.3 Call Processing

Although an in-dialog PBX redirection may occur before answer, via the *302* response, or after answer, via the REFER request, the Application Server performs similar call processing steps for either type of in-dialog redirection.

At a high level, the Application Server's processing steps are as follows:

1) Identify the redirecting trunking user.
2) Perform translations. During this step, the Application Server may send a query to the Network Server.
3) Execute redirecting services for the redirecting user, including screening services.
4) Based on the results of translations, create a terminating session and pass control to it.
5) Create and send the outgoing INVITE request.

Some of these steps are explained in more detail in the following sections.

12.1.2 Redirecting User Identification

12.1.2.1 Redirecting User Identification Processing Steps (Stand-Alone Only)

When Cisco BroadWorks receives the SIP message for the redirection, it inspects the relevant URI in the *History-Info* header, the *Diversion* header, or the *Referred-By* header to identify a Cisco BroadWorks user who is the redirecting user. Since the Application Server received the SIP message in an existing dialog, it inspects these headers in the context of a known user and a known Trunk Group, namely, the user and the Trunk Group associated with the dialog. To identify the redirecting user, the Application Server proceeds with the following steps:

1) The Application Server tries to match the user part of the URI to the Alternate Trunk Identity of a trunking user in the same Group or Enterprise as the Trunk Group. If it finds a match, then it selects the matched user.
2) Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to the directory number of a business trunking user in the same Group or Enterprise as the Trunk Group. If it finds a match, then it selects the matched user.
3) Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to Route List DN assigned to a Route List user in the same Group or Enterprise as the Trunk Group. If the Application Server finds a match, then it checks the *Treat Originations and PBX Redirections as Screened* option for the user's Route List service. The Application Server selects the Route List user if, and only if, the option is enabled.

To parse a phone number from a SIP URI, as required in steps 2 and 3, the Application Server proceeds as follows:

- If the URI has a user=phone parameter, then it treats the user part of the URI as the telephone-subscriber part of a tel URI.
- Otherwise, if the user part of the SIP URI is all digits, and if the domain part of the URI is an Application Server domain, then the Application Server uses these digits as the phone number. In addition to the literal digits, the Application Server allows the characters "*" and "#" as digits and allows the character "+" as the first digit.

If the redirecting user lookup fails, then the Application Server proceeds with one of the following alternatives:

- If the Trunk Group has a pilot user and allows unscreened originations, then the Application Server can substitute the Trunk Group's pilot user for the redirecting user. This is similar to the way the Application Server uses the pilot user's service profile for an unscreened origination.
- If the Trunk Group does not have a pilot user or does not allow unscreened originations, then the Application Server can substitute the call's local user for the redirecting user.

  The local user is the trunking user that owns the SIP dialog. For example, referring to *Figure 16*, *Figure 17*, or *Figure 18*, the local user is User A, who is either the originating or terminating user for the call being transferred.

12.1.2.2 Redirecting User Identification Processing Steps (IMS Only)

When Cisco BroadWorks receives the SIP message for the redirection, it inspects the relevant URI in the *History-Info* header, the *Diversion* header, or the *Referred-By* header to identify a Cisco BroadWorks user who is the redirecting user. Since the Application Server received the SIP message in an existing dialog, it inspects these headers in the context of a known user and a known Trunk Group, namely, the user and the Trunk Group associated with the dialog. To identify the redirecting user, the Application Server proceeds with the following steps:

1) The Application Server tries to match the URI to the Alternate Trunk Identity of a trunking user in the same Group or Enterprise as the Trunk Group. If it finds a match, then it selects the matched user.
2) Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to the directory number of a business trunking user in the same Group or Enterprise as the Trunk Group. If it finds a match, then it selects the matched user.
3) Otherwise, the Application Server tries to match the SIP URI to the Public User Identity of a trunking user in the same Group or Enterprise as the Trunk Group. If it finds a match, then it selects the matched user.
4) Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to a Route List DN assigned to a Route List user in the same Group or Enterprise as the Trunk Group. If the Application Server finds a match, then it checks the *Treat Originations and PBX Redirections as Screened* option for the user's Route List service. The Application Server selects the Route List user if, and only if, the option is enabled.

To parse a phone number from a SIP URI, as required in steps 2 and 4, the Application Server proceeds as follows:

- If the URI has a user=phone parameter, then it treats the user part of the URI as the telephone-subscriber part of a tel URI.
- Otherwise, if the user part of the SIP URI is all digits, and if the Application Server is configured to apply the user=phone error correction, then the Application Server uses these digits as the phone number. In addition to the literal digits, the Application Server allows the characters "*" and "#" as digits and allows the character "+" as the first digit. (For details on the user=phone error correction, see the *Cisco BroadWorks AS Mode IP Multimedia Subsystem Solution Guide* [4].)

If the redirecting user lookup fails, then the Application Server proceeds with one of the following alternatives:

- If the Trunk Group has a pilot user and allows unscreened originations, then the Application Server can substitute the Trunk Group's pilot user for the redirecting user. This is similar to the way the Application Server uses the pilot user's service profile for an unscreened origination.
- If the Trunk Group does not have a pilot user or does not allow unscreened originations, then the Application Server can substitute the call's local user for the redirecting user.

  The local user is the trunking user that owns the SIP dialog. For example, referring to *Figure 16*, *Figure 17*, or *Figure 18*, the local user is User A, who is either the originating or terminating user for the call being transferred.

12.1.3 Service Execution

12.1.3.1 Screening services

The Application Server provides screening services, which implement policies that control redirections. These policies support basic actions, such as allowing or blocking the redirected call, as well as more advanced actions such as placing a time limit on the redirected call. Following is a list of the most frequently used screening services:

- Communication Barring – Fixed – This service allows a system-level administrator to define communication barring profiles and associate them to Network Classes of Service. The profiles define the policies that the Application Server applies to outgoing, redirected, and incoming calls. For more information, see *Cisco BroadWorks Communication Barring – Fixed Guide* [11].
- Hierarchical Communication Barring – This service is similar to Communication Barring – Fixed, but it allows an enterprise administrator to configure policies.
- Outgoing Calling Plan – This service allows a Group or Enterprise administrator to configure basic screening policies for outgoing or redirected calls.

12.1.3.2 Calling Line Identification Restriction

As explained in the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1], the Application Server creates a list of internal diversion entries for a redirected call. Each internal entry contains a URI and a privacy indicator, as well as other information.

If the redirecting user for the call has Calling Line Identification Restriction[1] (CLIR) enabled, then the Application Server sets the privacy indicator to "anonymous" for that user's internal diversion entry. Later, when the Application Server creates a *History-Info* header or *Diversion* header in the outgoing INVITE request, it provides privacy protection to that entry.

The Application Server supports per-call CLIR activation and deactivation via FACs. When the Application Server processes an in-dialog PBX redirection, it checks the destination address for a per-call CLIR FAC. If it finds such a FAC, it activates or deactivates the CLIR service for the redirecting user accordingly.

How the Application Server applies privacy protection depends on whether it trusts the destination endpoint. If the destination endpoint is untrusted, then the Application Server anonymizes the URI for that diversion entry. For details on how the Application Server applies privacy protection to the *History-Info* header or the *Diversion* header, see the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1].

12.1.4 Outgoing INVITE Request

12.1.4.1 Redirecting User Identity

As described in section *12.1.2 Redirecting User Identification*, the Application Server processes the incoming SIP message to identify the redirecting user. When the Application Server sends the outgoing INVITE request, it adds a corresponding *History-Info* header entry or *Diversion* header entry that contains the identity of the identified redirecting user.

[1] The BroadWorks name for this service is Calling Line ID Delivery Blocking.

If the Application Server identified a Cisco BroadWorks user as the redirecting user, then by default it selects that user's profile identity for the redirecting user identity in the outgoing INVITE request. However, depending on configuration options, it may select a different redirecting identity.

- If the redirecting Trunk Group's *Pilot User Calling Line Identity for External Calls Usage Policy* is set to *All Originating Calls*, then the Application Server selects the pilot user's identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
  - If the pilot user's CLIR service is enabled, then the Application Server also applies privacy protection for the pilot's identity, which is selected for the redirecting identity.
  - If the pilot user's CLIR service is *disabled* and the redirecting user's CLIR service is *enabled*, then the Application Server provides privacy protection for the redirecting identity because the redirecting user requires it.
- Otherwise, if the redirecting user is a Route List user, and if the redirecting identity in the incoming INVITE request is a Route List DN, then the Application Server may select that Route List DN. This behavior is enabled if the Route List option *Use Route List Identity for Non-Emergency Calls* is enabled.
- Otherwise, the Application Server selects the redirecting user's profile identity.

If the Application Server did not identify a Cisco BroadWorks user as the redirecting user, then it selects the redirecting user identity as follows:

- If the redirecting Trunk Group's *Pilot User Calling Line Identity for External Calls Usage Policy* is set to *All Originating Calls* or *Unscreened Originating Calls*, then the Application Server selects the pilot user's identity. If the pilot user's CLIR service is enabled, then the Application Server applies privacy protection to the redirecting identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
- Otherwise, the Application Server selects the received redirecting identity.

12.2 Out-of-Dialog PBX Redirection

12.2.1 Overview

In the out-of-dialog PBX redirection scenario, the PBX sends a new INVITE request to the Application Server to establish a call leg for the redirection. Normally, the Application Server would interpret a new INVITE request from the PBX as a new originating call. In the PBX redirection scenario, however, the Application Server interprets the new INVITE request as a redirection. To achieve this interpretation, the PBX must add the required redirection information to the INVITE request in a *History-Info* header or a *Diversion* header.

There are a few variations of the out-of-dialog PBX redirection scenario. In each of these scenarios, the PBX sends a new INVITE request to the Application Server with the redirection information in the *History-Info* header or the *Diversion* header.

In one scenario as shown in *Figure 19*, PBX User A calls PBX User B and the call is handled entirely within the PBX. User B redirects the call, either before answer (Call Forward) or after answer (Blind Transfer) to PSTN User Y. The PBX routes the B-to-Y call leg through Cisco BroadWorks.

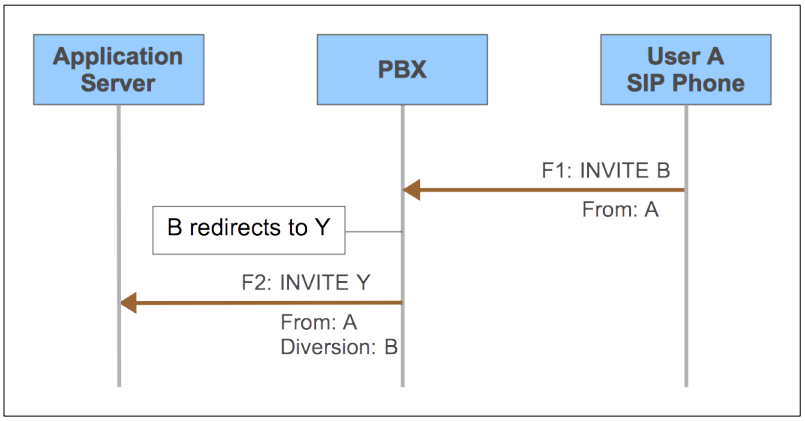

Figure 19 Out-of-Dialog PBX Redirection with Originator in the Enterprise

In another scenario, shown in *Figure 20*, PSTN User X calls PBX User A. User A redirects the call, after answer, to PSTN User Y. The PBX routes the A-to-Y call leg through Cisco BroadWorks. The call flow diagram shows the redirection after answer (Blind Transfer); however, the PBX redirection can also occur before answer (Call Forward).

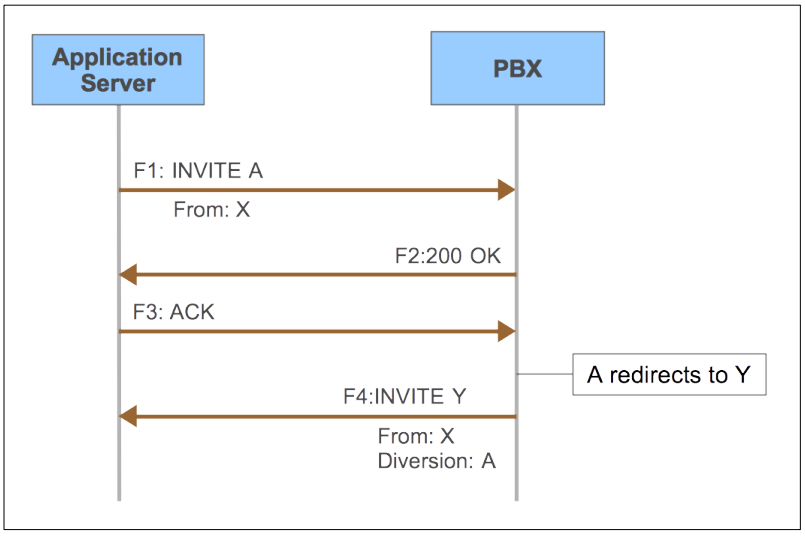

Figure 20 Out-of-Dialog PBX Redirection with Originator in the PSTN

Note that in this latter scenario, Cisco BroadWorks should recognize User A as the chargeable entity for the call leg to User Y. The INVITE request has User X in the *From* header, because User X is the actual originating party. Without a *History-Info* or *Diversion* header, Cisco BroadWorks would be unable to interpret the INVITE request as a redirected call with User A as the chargeable entity, and depending on the Trunk Group configuration, the Application Server could reject the call.

The processing for an out-of-dialog PBX redirection follows distinct steps, which are explained in detail in the sections that follow. At a high level, the Application Server's processing steps are as follows:

1) Identify the redirecting Trunk Group.

2) Identify the redirecting trunking user.

3) Identify the calling user.

4) Perform translations. During this step, the Application Server may send a query to the Network Server.

5) Check for an available BTLU and seize one unit for the call.

6) (Optional) Check for available Trunk Group capacity and increment the capacity counts for outgoing calls and for all calls.

7) Execute redirecting services for the redirecting user, including screening services.

8) Based on the results of translations, create a terminating session and pass control to it.

9) Create and send the outgoing INVITE request.

The Application Server performs these steps whenever it receives an out-of-dialog INVITE request that contains a *History-Info* header or a *Diversion* header. If the Application Server fails to identify the redirecting Trunk Group (step 1) then it does not process the call as an out-of-dialog PBX redirection. In such case, the Application Server may allow the call to continue as an originating call or terminating call, depending on configuration and other address headers in the INVITE request. For more details, see section *12.2.2.3 Failure Scenarios*. If the Application Server identifies the redirecting Trunk Group, but fails to identify the redirecting user (step 2), then it may allow the call to continue as an unscreened redirection or as an origination, depending on configuration. See section *12.2.3.3 Unscreened PBX Redirection*.

NOTE: The Application Server creates an originating PSTN session for an out-of-dialog PBX redirection (as well as a Cisco BroadWorks user session for the redirecting user). In many ways, this PSTN session is like any other PSTN session for a call origination from a network user. However, in the case of a PBX redirection, the Application Server modifies the session to use the Device Profile of the Trunk Group's Access Device. The Application Server must make this modification so that it can correctly apply the device policies for features such as Connected Line Identification Presentation, Call Correlation Identifier, and so on.

NOTE: If the PBX places an outbound call as an out-of-dialog PBX redirection, then it is not possible to transfer that call via a REFER request. If the PBX sends a REFER request within the dialog associated with that call, then the Application Server rejects the REFER with a 403 (Forbidden) response. Alternatively, if the PBX attempts an Attended Transfer by sending a REFER request within an unrelated dialog, but with a Replaces header referencing the PBX redirection dialog, then the Application Server rejects that REFER with a 403 (Forbidden) response.

The Application Server's rejection of the REFER request is a known limitation.

12.2.2 Redirecting Trunk Group Identification

12.2.2.1 Redirecting Trunk Group Identification Processing Steps (Stand-Alone Only)

In the case of the in-dialog PBX redirection, Cisco BroadWorks processes the *302* response or REFER request in the context of an existing dialog and session. The out-of-dialog redirection is different, though, since Cisco BroadWorks has no existing dialog context in which to process the new INVITE request. As in the case of an outbound originating call, Cisco BroadWorks first tries to identify the originating Trunk Group. To identify the originating Trunk Group, the Application Server performs the following steps:

1) [TGRP Lookup] If the *Contact* header URI has *tgrp* and *trunk-context* parameters, then the Application Server tries to match the parameters' values to the Trunk Group identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

> **NOTE**: The *tgrp* and *trunk-context* parameters are telephone-subscriber parameters, which means they are included in the user part of the SIP URI.

2) [OTG Lookup (PAI)] If the *P-Asserted-Identity* header has a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

3) [OTG Lookup (From)] If the *From* header URI is a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

4) [OTG Lookup (Redirecting URI)] If the most recent diversion entry in the *History-Info* or *Diversion* header has a SIP URI and the URI has an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

5) [Pilot Lookup (P-Preferred-Identity)] If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "true" and the INVITE request has a *P-Preferred-Identity* header that contains a SIP URI, then the Application Server tries to match the URI to the Line/Port of a pilot user. If the Application Server finds a match, then it selects the Trunk Group assigned to that pilot user as the redirecting Trunk Group. If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "false", then the Application Server skips this step.

6) [Pilot Lookup (P-Asserted-Identity)] If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "true" and the INVITE request has a *P-Asserted-Identity* header that contains a SIP URI, then the Application Server tries to match the URI to the Line/Port of a pilot user. If the Application Server finds a match, then it selects the Trunk Group assigned to that pilot user as the redirecting Trunk Group. If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "false", then the Application Server skips this step.

7) [Line/Port Lookup (Redirecting URI)] If the most recent diversion entry in the *History-Info* or *Diversion* header has a SIP URI, then the Application Server tries to match the URI to the Line/Port of a Cisco BroadWorks user. If it finds a match, and if the matched user is assigned to a Trunk Group, then the Application Server selects the Trunk Group to which the user is assigned.

8) [Source Address Lookup] The Application Server tries to match the source address to the network address of a Trunk Group device. The Application Server obtains the "source address" from the *Via* headers of the SIP INVITE request. For details on the source address lookup, see section *9.2.1 Originating Trunk Group Identification Processing Steps (Stand-Alone Only)*.

Note the following additional points:

- By default, the Application Server attempts a case-sensitive match for the *tgrp* parameter value and a case-insensitive match for the *trunk-context* value. However, if the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity* is set to "false", then the Application Server attempts a case-insensitive match for the *tgrp* value. See the note in section *9.2.1 Originating Trunk Group Identification Processing Steps (Stand-Alone Only)* for details.
- The Application Server attempts a case-insensitive match for the OTG/DTG identifier.

12.2.2.2 Redirecting Trunk Group Identification Processing Steps (IMS Only)

In the case of the in-dialog PBX redirection, Cisco BroadWorks processes the 302 response or REFER request in the context of an existing dialog and session. The out-of-dialog redirection is different, though, since Cisco BroadWorks has no existing dialog context in which to process the new INVITE request. As in the case of an outbound originating call, Cisco BroadWorks first tries to identify the originating Trunk Group. To identify the originating Trunk Group, the Application Server performs the following steps:

1) [TGRP Lookup] If the *Contact* header URI has *tgrp* and *trunk-context* parameters, then the Application Server tries to match the parameters' values to the Trunk Group identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

> **NOTE**: The *tgrp* and *trunk-context* parameters are telephone-subscriber parameters, which means they are included in the user part of the SIP URI.

2) [OTG Lookup (PAI)] If the *P-Asserted-Identity* header has a SIP URI that contains an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

3) [OTG Lookup (From)] If the *From* header URI is a SIP URI and has an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

4) [OTG Lookup (Redirecting URI)] If the most recent diversion entry in the *History-Info* or *Diversion* header has an *otg* parameter, then the Application Server tries to match the parameter's value to the OTG/DTG identifier assigned to a Trunk Group. If the Application Server finds a match, and if the matched Trunk Group has a pilot user, then the Application Server selects the matched Trunk Group as the redirecting Trunk Group.

5) [Pilot Lookup (P-Asserted-Identity)] If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "true" and the INVITE request has a *P-Asserted-Identity* header, then the Application Server tries to match the URI in that header to the identity of a Pilot User.

   – If the *P-Asserted-Identity* header has a SIP URI with a *user=phone* parameter, then the Application Server tries to match this URI to the primary DN of a Pilot User.

   – If the *P-Asserted-Identity* header has a SIP URI, then the Application Server tries to match it to a Pilot User's primary SIP Public User Identity.

   – If the *P-Asserted-Identity* header has a tel URI, then the Application Server tries to match this URI to the primary DN of a Pilot User.

   If the Application Server finds a match, then it selects the Trunk Group assigned to that pilot user as the redirecting Trunk Group.

   If the system parameter *allowPAILookupForOutOfDialogPBXRedirection* is set to "false", then the Application Server skips this step.

6) [Line/Port Lookup (Redirecting URI)] If the most recent diversion entry in the *History-Info* or *Diversion* header has a SIP URI, then the Application Server tries to match the URI to the Public User Identity of a Cisco BroadWorks user. If it finds a match, and if the matched user is assigned to a Trunk Group, then the Application Server selects the Trunk Group to which the user is assigned.

7) [Source Address Lookup] The Application Server tries to match the source address to the network address of a Trunk Group device. The Application Server obtains the "source address" from the *Via* headers of the SIP INVITE request. For details on the source address lookup, see section *9.2.2 Originating Trunk Group Identification Processing Steps (IMS Only)*.

Note the following additional points:

- By default, the Application Server attempts a case-sensitive match for the *tgrp* parameter value and a case-insensitive match for the *trunk-context* value. However, if the execution container option *bw.sip.useMixedCaseTrunkGroupIdentity* is set to "false", then the Application Server attempts a case-insensitive match for the *tgrp* value. See the note in section *9.2.2 Originating Trunk Group Identification Processing Steps (IMS Only)* for details
- The Application Server attempts a case-insensitive match for the OTG/DTG identifier.

12.2.2.3 Failure Scenarios

When the Application Server receives an out-of-dialog INVITE request that contains a *History-Info* header or *Diversion* header, it attempts to identify a redirecting Trunk Group following the steps described above. If it cannot identify a redirecting Trunk Group, then it does not process the call as an out-of-dialog PBX redirection. In such case, the Application Server continues to process the call, and the following alternatives are possible:

- If the Application Server identifies the originating Trunk Group (see section *9.2 Originating Trunk Group Identification*), then further processing depends on the value of the system parameter *unscreenedRedirectionHandling*. If *unscreenedRedirectionHandling* is set to "ignore" or "ignoreIfUnscreenedCallsDisallowed", then the Application Server continues to process the call as an outbound trunking call (section *9 Outbound Calls*). If the option is set to "reject" or "rejectIfUnscreenedCallsDisallowed", then the Application Server blocks the call with Forbidden treatment.
- If the Application Server fails to identify an originating Trunk Group but identifies a non-trunking Cisco BroadWorks user as the originating user, then it allows the call to continue as a user origination.
- The Application Server creates a PSTN originating session and performs network translations. If it identifies a Cisco BroadWorks user as a terminating user, then it allows the call to continue as a user termination. If it fails to identify a terminating user, then it rejects the call with User Not Found treatment.

12.2.3 Redirecting User Identification

To identify the redirecting trunking user, the Application Server processes the received *History-Info* header or *Diversion* header. Cisco BroadWorks supports both *History-Info* and *Diversion* headers. Normally, the PBX sends only a *History-Info* header or only a *Diversion* header, but not both. If the PBX sends both headers, then the Application Server can process the headers in three different ways, depending on configuration:

- The Application Server can merge the *History-Info* and *Diversion* headers, following the recommendations in *RFC 6044*.
- The Application Server can process the *History-Info* header and ignore the *Diversion* header.
- The Application Server can process the *Diversion* header and ignore the *History-Info* header.

For details on the Application Server's processing of the *History-Info* header and *Diversion* header, including the related configuration, see the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1].

12.2.3.1 Redirecting User Identification Processing Steps (Stand-Alone Only)

If the Application Server identifies a redirecting Trunk Group, then it performs additional steps to identify the redirecting user from the *History-Info* header or the *Diversion* header. The Application Server obtains the URI from the most recent diversion entry of the *History-Info* header or *Diversion* header, and then performs the following lookup steps:

1) [Line/Port Lookup (Redirecting URI)] If the Application Server identified the redirecting Trunk Group in the preceding steps by a Line/Port lookup, then it selects the user identified by the Line/Port lookup.
2) [ATI Lookup] Otherwise, if the URI is a SIP URI, then the Application Server tries to match the user part of the URI to the Alternate Trunk Identity of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.
3) [DN Lookup] Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to the directory number of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.

4) [Route List DN Lookup] Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to a Route List DN assigned to a Route List user in the same Group or Enterprise as the Trunk Group. If the Application Server finds a match, then it checks the *Treat Originations and PBX Redirections as Screened* option for the user's Route List service. The Application Server only selects the Route List user if the option is enabled.

12.2.3.2 Redirecting User Identification Processing Steps (IMS Only)

If Cisco BroadWorks identifies an originating Trunk Group, then it performs additional steps to identify the redirecting user from the *History-Info* header or the *Diversion* header. The Application Server obtains the URI from the most recent diversion entry of the *History-Info* header or *Diversion* header, and then performs the following lookup steps:

1) [Line/Port Lookup (Redirecting URI)] If the Application Server identified the redirecting Trunk Group in the preceding steps by a PUI lookup, then it selects the user identified by the PUI lookup.

2) [ATI Lookup] Otherwise, if the URI is SIP URI, then the Application Server tries to match the user part of the SIP URI to the Alternate Trunk Identity of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.

3) [DN Lookup] Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to the directory number of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.

4) [PUI Lookup] Otherwise, if the URI is SIP URI, then the Application Server tries to match the URI to the primary SIP PUI of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.

5) [Route List DN Lookup] Otherwise, if the URI is a tel URI or a SIP URI that contains a phone number, then the Application Server tries to match the phone number to a Route List DN assigned to a Route List user in the same Group or Enterprise as the Trunk Group. If the Application Server finds a match, then it checks the *Treat Originations and PBX Redirections as Screened* option for the user's Route List service. The Application Server only selects the Route List user if the option is enabled.

12.2.3.3 Unscreened PBX Redirection

If the Application Server cannot identify a trunking user as the redirecting user, then it may block the call or allow it to continue, depending on system configuration and the configuration of the redirecting Trunk Group. The system configuration depends on the value of the system parameter *unscreenedRedirectionHandling*, which is accessible from the CLI at the */Service/TrunkGroup* level.

- If *unscreenedRedirectionHandling* is set to "reject", then the Application Server blocks the redirected call.
- If *unscreenedRedirectionHandling* is set to "ignore", then the Application Server proceeds to process the call as an originating call instead of a PBX redirection. The Application Server may block the call at a later time if it cannot allow the call to continue as an origination.

- If *unscreenedRedirectionHandling* is set to “rejectIfUnscreenedCallsDisallowed”, then the disposition depends on the configuration of the redirecting Trunk Group.
  - If the Trunk Group allows unscreened originations, then the Application Server allows the call to continue as an out-of-dialog PBX redirection with the Trunk Group pilot user as the redirecting user.
  - Otherwise, the Application Server blocks the call.
- If *unscreenedRedirectionHandling* is set to “ignoreIfUnscreenedCallsDisallowed”, then the disposition depends on the configuration of the redirecting Trunk Group.
  - If the Trunk Group allows unscreened originations, then the Application Server allows the call to continue as an out-of-dialog PBX redirection with the Trunk Group pilot user as the redirecting user.
  - Otherwise, the Application Server proceeds to process the call as an originating call instead of a PBX redirection. The Application Server may block the call at a later time if it cannot allow the call to continue as an origination.

Note that the last two options (“rejectIfUnscreenedCallsDisallowed” and “ignoreIfUnscreenedCallsDisallowed”) could both be interpreted as “allow if unscreened calls allowed”. These two values are different only when the Application Server does not allow unscreened calls.

12.2.4 Originating User Identification

After the Application Server identifies the redirecting user, it attempts to identify the originating user. For an out-of-dialog PBX redirection, the Application Server does not execute originating services for the originating user. However, if the Application Server identifies a Cisco BroadWorks trunking user as the originating user, then it does apply CLID policies configured for the user and may optionally apply CLID policies configured for the redirecting Trunk Group. If the Application Server fails to identify a Cisco BroadWorks user, then it treats the originating user as a network user and may optionally apply CLID policies configured for the redirecting Trunk Group.

12.2.4.1 Originating User Identification Processing Steps

The Application Server attempts to identity a Cisco BroadWorks user as the originating user, performing steps similar to the originating user lookup for an outbound call. This procedure is needed so that the Application Server can apply CLID policies.

To identify the originating user, the Application Server first performs the following steps to select a URI to use for the user lookup:

1) (Stand-alone only) If the INVITE request has a *P-Preferred-Identity* header, then the Application Server selects the URI from this header. If the *P-Preferred-Identity* header has both a SIP URI and a tel URI, then the Application Server selects the tel URI. The Application Server skips this step if it identified the redirecting Trunk Group by matching the Pilot User’s identity to the *P-Asserted-Identity* header (Pilot Lookup).
2) If the INVITE request has a *P-Asserted-Identity* header, then the Application Server selects the URI from this header. If the *P-Asserted-Identity* header has both a SIP URI and a tel URI, then the Application Server selects the tel URI. The Application Server skips this step if it identified the redirecting Trunk Group by matching the Pilot User’s identity to the *P-Asserted-Identity* header (Pilot Lookup).

3) (Stand-alone only) If the INVITE request has a *Remote-Party-ID* header, then the Application Server selects the URI from this header. The Application Server skips this step if it identified the redirecting Trunk Group by matching the Pilot User's identity to the *P-Asserted-Identity* header (Pilot Lookup).

4) The Application Server selects the URI from the *From* header.

NOTE: If the system parameter *outOfDialogPBXRedirectionOriginatorLookupPolicy* is set to "presentation", then the Application Server selects the URI from the *From* header and ignores the *P-Preferred-Identity*, *P-Asserted-Identity*, and *Remote-Party-ID* headers. That is, the Application Server skips steps 1), 2), and 3) in the previous list of steps.

If the system parameter *outOfDialogPBXRedirectionOriginatorLookupPolicy* is set to "asserted", then the Application Server selects the URI from the *P-Preferred-Identity*, *P-Asserted-Identity*, or *Remote-Party-ID* header and ignores the *From* header. That is, the Application Server skips step 4) in the previous list of steps.

Next, the Application Server performs the following lookup steps on the URI:

1) If the URI is a SIP URI, then the Application Server tries to match the URI to the Alternate Trunk Identity of a trunking user in the same Group or Enterprise as the redirecting Trunk Group. If it finds a match, then it selects the matched user.

2) Otherwise, if the URI contains a phone number, then the Application Server performs user translations on the number. The Application Server performs these translations in the context of the redirecting user. This means it can identify the originating user by the user's extension (see section *10.2.1 User Translations*). If it identifies a Cisco BroadWorks user, then it selects that user. As a special case, if the Application Server identifies a Cisco BroadWorks user via a Route List DN (that is, by matching an Enterprise Trunk Number Prefix or an Enterprise Trunk Number Range), then it remembers this result, but continues processing the following steps, which have a higher precedence that a Route List DN.

3) (Stand-alone only) Otherwise, if the URI is a SIP URI, then the Application Server tries to match the URI to the primary Line/Port or a user in the same Group or Enterprise as the redirecting user. If it finds a match, then it selects the matched user.

4) (IMS only) Otherwise, if the URI is a SIP URI, then the Application Server tries to match the URI to the primary SIP PUI of a user in the same Group or Enterprise as the redirecting user. If it finds a match, then it selects the matched user.

5) Otherwise, if the Application Server identified a user via a Route List DN when performing user translations (step 2), and if the user's Route List service has *Treat Originations and PBX Redirections as Screened* enabled, then it selects that user.

Note the following additional point:

- A user's primary Line/Port or primary SIP PUI is associated with a Device Endpoint, an Access Device, and an Access Device Type (see section *6 Trunking User Addresses*). For the Application Server to identify the calling user by a Line/Port lookup (step 3 in the previous list of steps) or a PUI lookup (step 4 in the previous list of steps), the associated Access Device Type must have the PBX Integration option enabled.

12.2.4.2 CLID Mapping

If the Application Server did not identify a Cisco BroadWorks user as the originating user, then it can optionally perform additional steps to screen the received CLID against a list of numbers it temporarily stored from inbound calls. The Application Server performs these steps when *CLID mapping* is enabled.

To enable CLID mapping, a system administrator must set the system parameter *enforceOutOfDialogPBXRedirectionPolicies* to "true" and set the system parameter *outOfDialogPBXRedirectionCLIDMapping* to "enabledAndIgnorePolicies" or "enabledAndApplyPolicies". These system parameters are accessible at the CLI */Service/TrunkGroup* level.

When CLID mapping is enabled, the Application Server remembers the phone numbers it sends to the PBX for inbound calls so that it has them available to match against the CLID received from the PBX. This functionality can be used in conjunction with other CLID policies to protect against CLID spoofing from the enterprise. *Figure 20* shows a scenario in which CLID mapping is useful. In this scenario, the Application Server receives an incoming call from the PSTN and routes it to the PBX. Before the Application Server sends the INVITE request to the PBX, however, it stores the CLID in a cache associated with the Enterprise or Group of the terminating Trunk Group. The PBX redirects the call back to the Application Server and sends a new INVITE request to the Application Server for an out-of-dialog PBX redirection. When the Application Server processes the redirection, it looks for and finds the CLID in the cache. This cache lookup provides assurance that the PBX has not spoofed the CLID. When the cache lookup succeeds, the Application Server marks the CLID as a screened CLID. However, if the cache lookup fails, then the Application Server marks the CLID as an unscreened CLID. As described in section *12.2.8.1 Caller Identity*, the Application Server supports policies that may prevent it from sending an unscreened CLID to the called party. If CLID mapping is disabled, then the Application Server does not maintain the CLID cache, and it marks any unrecognized CLID as an unscreened CLID.

The Application Server stores numbers in the CLID mapping cache temporarily. It adds a new number to the cache when it processes a new incoming call, and it associates the number with that call. When the Application Server releases the associated call, it also removes the number from the cache.

12.2.5 Business Trunking License Check

After the Application Server identifies the redirecting Trunk Group, the redirecting trunking user, and possibly the calling user, it tries to seize a BTLU for the call. This procedure is similar to the procedure to seize a license for an originating call (section *9.4 Business Trunking License Check*), except that the Application Server seizes a license unit for the redirecting user instead of the calling user. If it successfully seizes a license unit, then allows the call to continue.

If the Application Server cannot seize a license unit, then it blocks the call with a *Forbidden* treatment, which by default causes the Application Server to send a 603 (Decline) response to the INVITE request. Additionally, the Application Server triggers an SNMP notification (*bwTrunkingLicensedCapacityExceeded*) and indicates the failure condition in the *btluExceeded* field in the CDR.

If the redirecting user is assigned to an Enterprise Trunk and that Enterprise Trunk has call capacity management enabled, then the Application Server performs an additional license-related check for Enterprise Trunk capacity. For the new call, the Application Server checks that the license count for the Enterprise Trunk has not reached the limit. If the current count is under the limit, then the Application Server increments the count for this call and allows the call to continue.

If the check for Enterprise Trunk capacity fails, then the Application Server takes actions similar those for the system-level license failure. The Application Server blocks the outgoing call with a *Forbidden* treatment, which by default causes the Application Server to send a 603 (Decline) response to the INVITE request. Additionally, the Application Server triggers an SNMP notification (*bwEnterpriseTrunkCapacityExceeded*) and indicates the failure condition in the *enterpriseTrunkCapacityExceeded* field in the CDR.

12.2.6 Trunk Group Capacity Check

The Application Server can optionally count out-of-dialog PBX redirections against the outgoing call capacity of the redirecting Trunk Group. This functionality is controlled by the system parameter *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity*, which is available at the CLI */Service/TrunkGroup* level. If *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* is set to "true", then such redirections are counted against the Trunk Group's outgoing call capacity.

If the redirection causes the capacity count to exceed the capacity limit for outgoing calls or for total (outgoing + incoming) calls, then the Application Server blocks the call with a *Forbidden* treatment, which by default causes the Application Server to send a 603 (Decline) response to the INVITE request. Additionally, the Application Server triggers an SNMP notification (*bwTrunkGroupCapacityExceeded*) and updates the CDR field *trunkGroupInfo* with the value "CapacityExceeded".

Best Practice

As a general rule, you should set *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* to "true" so that out-of-dialog PBX redirections are counted against the Trunk Group capacity. However, there may be some situations where you set it to "false".

Regarding *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity*, there are two distinct scenarios to consider. If one communicating endpoint is in the enterprise network and the other in the PSTN, as shown in the scenario in *Figure 19*, then the redirection sets up a media session between the enterprise network and the service provider's network. If *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* is set to "true", then the Application Server accurately accounts for this media session in the Trunk Group's capacity. In contrast, if both communicating endpoints are in the PSTN, as shown in the scenario in *Figure 20*, then the redirection typically sets up a "hairpin" media session that does not route through the enterprise network (even though the signaling path still does). If *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* is set to "true", then the Application Server counts this redirection against the Trunk Group's capacity even though there are no associated media streams traversing the link to the enterprise network. Therefore, if these "hairpin" redirections are common, or if only loose bandwidth constraints are required, then it might make sense to set *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* to "false".

Another possibility is to configure the PBX to use in-dialog PBX redirections whenever possible. Instead sending an INVITE request, which results in an out-of-dialog PBX redirection and a "hairpin" media session (*Figure 20*), the PBX can send a 302 response for a Call Forward (*Figure 16*) or a REFER request for a Call Transfer (*Figure 17*). When the Application Server processes an in-dialog PBX redirection for a "hairpin" scenario, it releases both media and signaling paths to the PBX as well as any Trunk Group capacity. If you configure the PBX to avoid the "hairpin" out-of-dialog PBX redirections and you set *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* to "true", then you can expect the Trunk Group's capacity to accurately account for the media sessions.

12.2.7 Service Execution

For an out-of-dialog PBX redirection, the Application Server executes redirecting services using the service profile of a Cisco BroadWorks user. In the typical case, the Application Server identifies a trunking user as the redirecting user and selects that user's service profile. In another possible case, the Application Server cannot identify a trunking user as the redirecting user, and it selects the service profile of the Trunk Group's pilot user. (If the Application Server cannot identify a trunking user as the redirecting user, then it may instead block the call, depending on configuration. See section *12.2.3.3 Unscreened PBX Redirection*.

Redirecting services in Cisco BroadWorks are similar to originating services, but not identical. For example, for some originating services the Application Server connects the caller to an IVR (interactive voice response) system. For redirecting services, the Application Server avoids this kind of interaction with the caller.

The Application Server may identify a Cisco BroadWorks user as the originating user. However, it does not execute any originating services from that user's service profile. For example, the originating user may have enabled CLIR to block their CLID. The Application Server however does not execute that user's originating services, and therefore it may not block the user's CLID.

12.2.7.1 Screening services

The Application Server provides a few different screening services, which implement policies that control redirections. These policies support basic actions, such as allowing or blocking the redirected call, as well as more advanced actions such as placing a time limit on the redirected call. Following is a list of the most frequently used screening services:

- Communication Barring – Fixed – This service allows a system-level administrator to define communication barring profiles and associate them to Network Classes of Service. The profiles define the policies that the Application Server applies to outgoing, redirected, and incoming calls. For more information, see the *Cisco BroadWorks Communication Barring – Fixed Guide* [11].
- Hierarchical Communication Barring – This service is similar to Communication Barring – Fixed, but it allows an enterprise administrator to configure policies.
- Outgoing Calling Plan – This service allows a Group or Enterprise administrator to configure basic screening policies for outgoing or redirected calls.

12.2.7.2 Calling Line Identification Restriction

When the Application Server receives a *History-Info* header or a *Diversion* header, it converts the information in the header to a list of internal diversion entries, as explained in the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1]. Each internal entry contains a URI and a privacy indicator, as well as other information.

If the redirecting user for the call has CLIR[2] enabled, then the Application Server sets the privacy indicator to "anonymous" for that user's internal diversion entry. Later, when the Application Server creates a *History-Info* header or *Diversion* header in the outgoing INVITE request, it provides privacy protection to that entry.

The Application Server supports per-call CLIR activation and deactivation via FACs. When the Application Server processes an out-of-dialog PBX redirection, it checks the destination address for a per-call CLIR FAC. If it finds such a FAC, it activates or deactivates the CLIR service for the redirecting user accordingly.

[2] The Cisco BroadWorks name for this service is Calling Line ID Delivery Blocking.

How the Application Server applies privacy protection depends on whether it trusts the destination endpoint. If the destination endpoint is untrusted, then the Application Server anonymizes the URI for that diversion entry. For details on how the Application Server applies privacy protection to the *History-Info* header or the *Diversion* header, see the *Cisco BroadWorks SIP Access Interface Interworking Guide* [1].

12.2.8 Outgoing INVITE Request

12.2.8.1 Caller Identity

In the outgoing INVITE request, the Application Server adds a presentation identity and optionally a separate asserted identity (when the system parameter *enableTS29163-Compliance* is "true"). The Application Server selects these identities while applying policies to information from the incoming INVITE request as well as provisioned data. For more information, see the *Cisco BroadWorks Application Server Identity Guide* [5].

If the Application Server identifies a Cisco BroadWorks user as the originating user (section *12.2.4.1 Originating User Identification Processing Steps*), then it selects the presentation identity and asserted identity as usual for a Cisco BroadWorks user origination. Additionally, if the system parameter *enforceOutOfDialogPBXRedirectionPolicies* is "true", then it also applies the identity selection policies of the redirecting Trunk Group, as described in section *9.6.1.1 Trunking User Originations*. If *enforceOutOfDialogPBXRedirectionPolicies* is "false", then the Application Server ignores the identity selection policies of the redirecting Trunk Group.

If the Application Server did not identify a Cisco BroadWorks user, then it selects the presentation identity and asserted identity according to the value of the system parameter *enforceOutOfDialogPBXRedirectionPolicies*. If this parameter is "false", then the Application Server selects the received presentation identity and (optionally) the received asserted identity. However, if the parameter is "true", then the identity selection depends on whether the Application Server previously marked the received CLID as screened or unscreened, as described section *12.2.4.2 CLID Mapping*. If CLID mapping is disabled, then the Application Server considers every received CLID to be unscreened.

If *enforceOutOfDialogPBXRedirectionPolicies* is "true" and the CLID is unscreened, then the Application Server applies the identity policies of the redirecting Trunk Group as follows:

- The Application Server selects the presentation identity according to the *Pilot User Calling Line Identity for External Calls Usage Policy*. If the policy is set to "All Originating Calls" or "Unscreened Originating Calls", then the Application Server selects the pilot user's identity for the presentation identity. If the policy is set to "No Calls", then the Application Server selects the received presentation identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
- If the Application Server is configured to support a separate asserted identity, then it selects the pilot user's identity for the asserted identity[3]. (This selection results because the Application Server applies the *Pilot User Calling Line Asserted Identity Usage Policy* for the redirecting Trunk Group.)

[3] If the execution container option *bw.trunkGroup.keepAssertedIdForUnscreened-OutOfDialogPbxRedirection* is set to "true" and the *Pilot User Calling Line Asserted Identity Usage Policy* for the redirecting Trunk Group is set to "Unscreened Originating Calls", then the Application Server selects the received asserted identity.

If *enforceOutOfDialogPBXRedirectionPolicies* is "true" and the CLID is screened, then the Application Server selects the presentation identity and asserted identity as follows:

- If *outOfDialogPBXRedirectionCLIDMapping* is set to "enabledAndIgnorePolicies", then the Application Server ignores the identity policies of the redirecting Trunk Group and selects the received presentation identity and (optionally) the received asserted identity.
- Otherwise, if *outOfDialogPBXRedirectionCLIDMapping* is set to "enabledAndApplyPolicies", then the Application Server applies the identity policies of the redirecting Trunk Group as follows:
  - The Application Server selects the presentation identity according to the *Pilot User Calling Line Identity for External Calls Usage Policy*. If the policy is set to "All Originating Calls", then the Application Server selects the pilot user's identity for the presentation identity. If the policy is set to "No Calls" or "Unscreened Originating Calls", then the Application Server selects the received presentation identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
  - If the Application Server is configured to support a separate asserted identity, then it selects the asserted identity according to the *Pilot User Calling Line Asserted Identity Usage Policy*. If the policy is set to "All Originating Calls", then the Application Server selects the pilot user's identity for the asserted identity. If the policy is set to "Unscreened Originating Calls", then the Application Server selects the received asserted identity.

12.2.8.2 Redirecting User Identity

As described in section 12.2.3 Redirecting User Identification, the Application Server processes the History-Info header or Diversion header of the incoming INVITE request to identify the redirecting user. When the Application Server sends the outgoing INVITE request, it adds a History-Info header or Diversion header, including an entry that contains the identity of the identified redirecting user. Depending on the outcome of the redirecting user identification, the Application Server may modify the History-Info or Diversion header entry for the redirecting user accordingly.

If the Application Server identified a Cisco BroadWorks user as the redirecting user, then by default it selects that user's profile identity for the redirecting user identity in the outgoing INVITE request. However, the identity selection depends on configuration options.

- If the redirecting Trunk Group's *Pilot User Calling Line Identity for External Calls Usage Policy* is set to "All Originating Calls", then the Application Server selects the pilot user's identity. If the pilot user's CLIR service is enabled, then the Application Server applies privacy protection to the redirecting identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
- Otherwise, if the redirecting user is a Route List user, and if the redirecting identity in the incoming INVITE request is a Route List DN, then the Application Server selects that Route List DN.
- Otherwise, the Application Server selects the redirecting user's profile identity.

If the Application Server did not identify a Cisco BroadWorks user as the redirecting user, then it selects the redirecting user identity as follows:

- If the redirecting Trunk Group's *Pilot User Calling Line Identity for External Calls Usage Policy* is set to "All Originating Calls" or "Unscreened Originating Calls", then the Application Server selects the pilot user's identity. If the pilot user's CLIR service is enabled, then the Application Server applies privacy protection to the redirecting identity. (The Application Server applies the *Pilot User Calling Line Identity Usage for Emergency Calls Policy* similarly for emergency calls.)
- Otherwise, the Application Server selects the received redirecting identity.

13 Services

Cisco BroadWorks supports a vast number of services. In general, Cisco BroadWorks supports services for both trunking users and non-trunking users. However, there are a few services that are designed specifically in support of SIP trunking. Such services are described in the following subsections.

13.1 Route List

The Route List services allows an administrator to provide basic connectivity to a large number of PBX users with minimal provisioning.

Configure a range of directory numbers for users hosted on the PBX.

An administrator can assign the Route List service to a trunking user and assign Enterprise Trunk Number Ranges and/or Enterprise Trunk Number Prefixes to a user account. When the Route List service is assigned to a user, that user is considered to be a Route List user.

A Route List user is used as a conduit to handle trunking calls for all the DNs in the Enterprise Trunk Number Ranges assigned to the user's Route List service that are not assigned to a Cisco BroadWorks user as a real DN (such as a user's primary DN). These DNs represent trunking users without their own Cisco BroadWorks user profile. Using the Route List service, ranges of DNs (that is, trunking users without their own Cisco BroadWorks user profiles) can be assigned to and handled by a single Route List user profile instead of requiring an individual Cisco BroadWorks user profile for each DN.

By design, a DN lookup has a higher precedence than a Route List DN lookup. Therefore, if a user's assigned DN matches an Enterprise Trunk Number Prefix/Range, then the Application Server identifies that user by the user's DN and processes that call using that user's service profile. This precedence order makes it simple for an administrator to migrate a PBX user from the shared profile of the Route List User to an individual user service profile. The administrator can create the new profile and assign the DN, and no action is needed to modify the Enterprise Trunk Number Prefix/Range. For more information about the user service, see the *Enterprise Trunk Enhancements Feature Description* [19].

13.2 Direct Route

An administrator can assign the Direct Route service to a trunking user and provision direct route identifiers to the Direct Route service. There are two types of direct route identifiers. They are distinguished by how the direct route identifier is used within the SIP signaling.

- The trunk identity type has a label component and a domain component, and these are used as the values of the *tgrp* and *trunk-context* parameters, respectively.
- The DTG type has only a single component, and this is used as the value of the *dtg* parameter.

A trunk identity type direct route identifier is similar to a Trunk Group Identity that is provisioned for a trunk group, in that both of these identities may appear as values of the *tgrp* and *trunk-context* parameters. Similarly, the DTG-type direct route identifier is similar to the OTG/DTG Identity in that both may appear as the value of the *dtg* parameter.

The Direct Route service enables the Application Server to identify a route to a destination PBX. Upon receiving a call from network, the Application Server parses the trunk group identifier in the *Request-URI* of an incoming INVITE request and tries to match it to a direct route identifier. If it finds a match, then it selects the user to whom the direct route identifier is assigned and routes the call using that user's routing profile. The user must be a trunking user, and the Application Server routes the call as a trunk group call. For more information about the user service, see the *Direct Route Service Feature Description* [20].

13.3 Terminating Alternate Trunk Identity

An administrator can assign the Terminating Alternate Trunk Identity service to a trunking user and provision a terminating trunk identity to the service. The terminating trunk identity is similar to that of an alternate trunk identity, but is used for terminating calls only. The terminating trunk identities are not required to be unique within the system.

When the Application Server terminates a call to a trunking user with a provisioned terminating trunk identity, the terminating trunk identity is used to form the *Request-URI* and *To* header in the SIP request depending on the trunking mode in use.

The terminating trunk identity has a higher precedence than the alternate trunk identity. When both the alternate trunk identity and the terminating trunk identity are provisioned, the terminating trunk identity is used in places where the alternate trunk identity is usually used. For more information about the user service, see the *Terminating Alternate Trunk Identity Feature Description* [21].

14 Trunk Group Capacity Management

The term *Trunk Group Capacity Management* refers the Application Server's ability to keep track of active incoming and outgoing calls for a Trunk Group, to enforce limits on those calls, and to execute actions on calls that exceed the limits. In a sense, capacity management assumes a model analogous to the physical capacity that occurs in TDM lines.

Capacity management is applied only to Trunk Groups. There is no concept of capacity management for Enterprise Trunks. This makes sense, because an Enterprise Trunk aggregates Trunk Groups and distributes terminating calls to them. Capacity management therefore, is configured individually on each Trunk Group in the Enterprise Trunk.

Capacity management for Trunk Groups is distinct from the capacity management via Group Call Capacity Management, which Cisco BroadWorks also provides. A business trunking user cannot be assigned to a Capacity Management Group, which means the trunking user cannot be included in Group Call Capacity Management. Thus Trunk Group Capacity Management is the capacity management facility Cisco BroadWorks provides for trunking users (non-trunking users cannot make or receive calls over a Trunk Group), while Group Call Capacity Management is the capacity management facility it provides for non-trunking users. Session Admission Control is yet another facility that Cisco BroadWorks provides for "capacity management", which is applicable for both trunking and non-trunking users and is independent of Trunk Group Capacity Management and Group Call Capacity Management.

To manage Trunk Group capacity, for each Trunk Group, the Application Server keeps separate counts for active incoming calls (calls that terminate to the Trunk Group device) and active outgoing calls (calls that originate from the Trunk Group device). Trunk Group Capacity Management (or just Capacity Management in the following description) allows the Application Server to place limits on active incoming calls, active outgoing calls, or all active calls (the sum of incoming and outgoing calls).

For each new outgoing call, the Application Server checks the capacity limits for all active calls and active outgoing calls. If the new call does not violate the capacity limits, then the Application Server allows the call to continue. However, if the new call exceeds the capacity limit for all calls or for outgoing calls, the Application Server blocks the call by sending a SIP 403 (Forbidden) response to the SIP INVITE request.

Similarly, for each new incoming call, the Application Server checks the capacity limits for all active calls and active incoming calls. If the new call would not violate the capacity limits, then the Application Server allows the call to continue. However, if the new call would exceed the capacity limit for all calls or for incoming calls, the Application Server can apply an action that is configured through provisioning. The allowed actions are:

- *Reroute* – This action causes the Application Server to reroute the call to an alternate Trunk Group. (The alternate Trunk Group must have a Pilot User.)

  This action is not recommended for a Trunk Group that is part of an Enterprise Trunk, because it could interfere with the execution of the Enterprise Trunk's routing policy.

- *Forward* – This action causes the Application Server to forward the call to a configured destination.

  This action is not recommended for a Trunk Group that is part of an Enterprise Trunk, because it could interfere with the execution of the Enterprise Trunk's routing policy.

If the Trunk Group is assigned to an Enterprise Trunk, then it is recommended to set the capacity-exceeded action to “No Action”, because this allows the Enterprise Trunk’s routing policy to continue routing. If the action is “Reroute” or “Forward”, then that action has precedence over the Enterprise Trunk’s routing policy.

The maximum value for Trunk Group capacity is limited by the number of BTLUs. This restriction is enforced at provisioning time, such that the provisioned value cannot exceed the number of trunking license units available in the appropriate pool. Moreover, the value can be further limited administratively through provisioning at the Group or Enterprise level. The way these limits are established is different for the Service Provider and Enterprise models.

In the Enterprise model:

- For a Group within the Enterprise, an administrator can set a value for the maximum capacity of any Trunk Group within that Group. This value cannot exceed the number of BTLUs allocated to the Enterprise.
- For a Trunk Group within the Group, an administrator can set a capacity limit for all active calls, and, optionally, for incoming calls or outgoing calls. These capacity limits cannot exceed the limit set for the Group, described in the preceding paragraph.

In the Service Provider model:

- For a Trunk Group within any Group within the Service Provider, an administrator can set a capacity limit for active calls, and, optionally, for incoming and outgoing calls. These capacity limits cannot exceed the number of BTLUs allocated to the Group.

Emergency Calls

Call capacity management actions cannot block emergency calls. The Application Server allows an emergency call to proceed as usual even if the call exceeds a capacity limit. An emergency call always counts toward capacity, though, even if the call exceeds the capacity limit.

15 Performance Measurements

While the accounting records provide a basic facility for tracking the usage of Trunk Group capacity, Cisco BroadWorks also provides direct SNMP gauges that can provide more immediate information on capacity utilization and license utilization. The gauges are available in a table indexed by each Trunk Group in the system, allowing the information to be gathered in real time independently for each Trunk Group. The information provided by these gauges includes:

- Maximum total calls allowed
- Maximum incoming calls allowed
- Maximum outgoing calls allowed
- High-water mark for all calls
- High-water mark for incoming calls
- High-water mark for outgoing calls

To collect the utilization information, the operator requires a network management console capable of reading the SNMP table. The way the Network Management System (NMS) interacts with Cisco BroadWorks depends on the mode of operation. Cisco BroadWorks supports two modes of operation, hold-over mode, and immediate mode.

Hold-over Mode

At regular intervals, Cisco BroadWorks records a snapshot of the current high-water mark, then resets the current high-water mark. When Cisco BroadWorks resets the current high-water mark, it saves the previous high-water mark as a “hold-over” high-water mark. At any time, the network management system can read the value of the hold-over high-water mark, which contains a snapshot of the current high-water mark at the time Cisco BroadWorks last reset it.

Immediate Mode

In this mode, Cisco BroadWorks does not automatically reset the high-water mark and the hold-over high-water mark is not available. Instead, the external network management system is permitted to control the high-water mark sampling and resets. For example, a network management system can poll for a sample of the high-water mark every 20 minutes and reset the high-water mark immediately after taking the sample.

Although these performance measurements are made available via SNMP to an external network management system, Cisco BroadWorks also allows access to them via the CLI. The following is a sample of the CLI output for the Trunk Group Performance Measurements.

```
AS_CLI/Monitoring/PM/Execution> get
------------------------------------------------------------------------------
executionServer/services/trunkGroup/
------------------------------------------------------------------------------
             *bwTrunkOriginationAttempt           0
             *bwTrunkOriginationBlocked           0
             *bwTrunkTerminationAttempt           0
             *bwTrunkTerminationBlocked           0
bwTrunkSPTable:

  (1) bwTrunkSPIndex
  (2) bwTrunkSPID
  (3) bwTrunkSPOriginationAttempt
  (4) bwTrunkSPOriginationBlocked
  (5) bwTrunkSPTerminationAttempt
  (6) bwTrunkSPTerminationBlocked
```

```
  (7) bwTrunkGroupOodPbxRedirectionAttempt
  (8) bwTrunkGroupOodPbxRedirectionBlocked

        (1)     (2)     (3)     (4)     (5)     (6)     (7)     (8)
  138096051     en1       0       0       0       0       0       0
  154517250     sp1       0       0       0       0       0       0

bwTrunkGroupTable:

  (1) bwTrunkGroupIndex
  (2) bwTrunkGroupID
  (3) bwTrunkGroupOriginationAttempt
  (4) bwTrunkGroupOriginationBlocked
  (5) bwTrunkGroupTerminationAttempt
  (6) bwTrunkGroupTerminationBlocked
  (7) bwTrunkGroupOodPbxRedirectionAttempt
  (8) bwTrunkGroupOodPbxRedirectionBlocked

        (1)       (2)     (3)     (4)     (5)     (6)     (7)     (8)
  146119650   initech       0       0       0       0       0       0

bwTrunkGroupPerTGTable:

  (1) bwTrunkGroupPerTGIndex
  (2) bwTrunkGroupPerTGName
  (3) bwTrunkGroupPerTGCapacityExceeded
  (4) bwTrunkGroupPerTGUnreachableDestination
  (5) bwTrunkGroupPerTGMaxActiveCalls
  (6) bwTrunkGroupPerTGMaxOutgoingActiveCalls
  (7) bwTrunkGroupPerTGMaxIncomingActiveCalls
  (8) bwTrunkGroupPerTGCapacityExceededInitialValue
  (9) bwTrunkGroupPerTGCapacityExceededOffsetValue
 (10) bwTrunkGroupPerTGBursting
 (11) bwTrunkGroupPerTGBurstingMaxActiveCalls
 (12) bwTrunkGroupPerTGBurstingMaxOutgoingActiveCalls
 (13) bwTrunkGroupPerTGBurstingMaxIncomingActiveCalls
 (14) bwTrunkGroupPerTGGroupID
 (15) bwTrunkGroupPerTGTotalActiveCalls
 (16) bwTrunkGroupPerTGOutgoingActiveCalls
 (17) bwTrunkGroupPerTGIncomingActiveCalls
 (18) bwTrunkGroupPerTGTotalCallHighWaterMark
 (19) bwTrunkGroupPerTGOutgoingCallHighWaterMark
 (20) bwTrunkGroupPerTGIncomingCallHighWaterMark
 (21) bwTrunkGroupPerTGCallHighWaterMarkReset
 (22) bwTrunkGroupPerTGHoldingTotalCallHighWaterMark
 (23) bwTrunkGroupPerTGHoldingOutgoingCallHighWaterMark
 (24) bwTrunkGroupPerTGHoldingIncomingCallHighWaterMark
 (25) bwTrunkGroupPerTGOriginationAttempt
 (26) bwTrunkGroupPerTGOriginationBlocked
 (27) bwTrunkGroupPerTGTerminationAttempt
 (28) bwTrunkGroupPerTGTerminationBlocked
 (29) bwTrunkGroupPerTGTerminationFailure
 (30) bwTrunkGroupPerTGOodPbxRedirectionAttempt
 (31) bwTrunkGroupPerTGOodPbxRedirectionBlocked

    (1)     (2)     (3)     (4)     (5)     (6)     (7)     (8)     (9)    (10)    (11)
(12)    (13)      (14)    (15)    (16)    (17)    (18)    (19)    (20)    (21)    (22)    (23)
(24)    (25)    (26)    (27)    (28)    (29)    (30)    (31)
      1  Alpha      0       0      20      15      15       0       0  false       0
0       0  initech       0       0       0       0       0       0       0       0       0
0       0       0       0       0       0       0       0
      2  Bravo      0       0      24      16      24       0       0  false       0
0       0  initech       0       0       0       0       0       0       0       0       0
0       0       0       0       0       0       0       0

    *bwTrunkGroupCallHighWaterMarkReset           0
    *bwTrunkOodPbxRedirectionAttempt              0
    *bwTrunkOodPbxRedirectionBlocked              0
```

16 Business Trunking License Unit Allocation

16.1 Business Trunking License Unit Allocation Procedure

In a Cisco BroadWorks deployment, a certain number of BTLUs are licensed for the entire system. These license units must be further allocated to Enterprises (in the Enterprise model) or to Groups (in the Service Provider model).

To allocate BTLUs to an Enterprise in the Enterprise model, follow these steps:

1) From the *Profile* web page for the Enterprise, click the **Resources** link in the left navigation menu. This link takes you to the *Resources* web page for the Enterprise.

2) From the *Resources* web page, click the **Trunking Call Capacity** link. This link takes you to the *Trunking Call Capacity* web page for the Enterprise.

3) On the *Trunking Call Capacity* web page, enter a value in the field labeled *Number of Business Trunking License Units for this Enterprise*. The value you enter determines how many BTLUs are allocated to this Enterprise's license pool.

4) Click the **Apply** or **OK** button.

The *Trunking Call Capacity* web page for an Enterprise is shown in *Figure 21*.

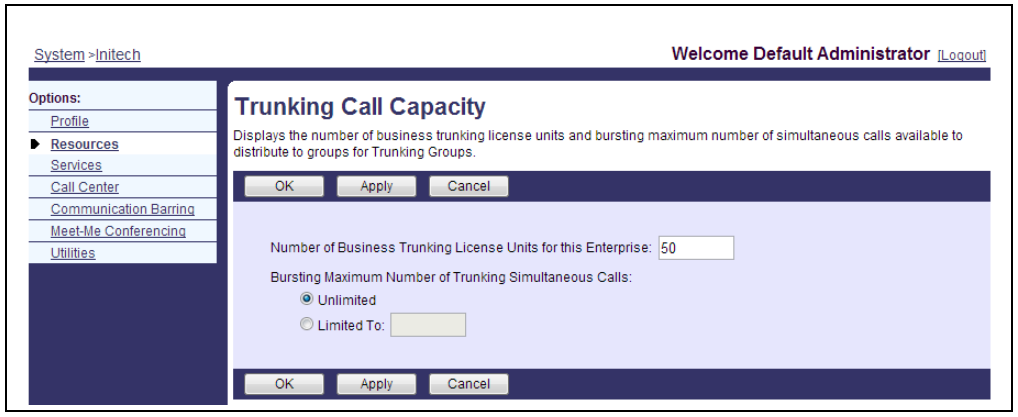

Figure 21 Trunking Call Capacity Web Page for Enterprise

In the Service Provider model, BTLUs must be allocated to the Groups within a Service Provider. Optionally, an administrator can create a pool of reserved license units for the Server Provider. If a Service Provider has such a pool, then the Groups within that Service Provider take their allocated license units from the Service Provider's reserved pool. Otherwise, the Groups take their allocated license units directly from the system-wide license unit stock, which includes all the trunking license units granted to the system that are not otherwise allocated or reserved.

To manage the BTLUs for a Service Provider, follow these steps:

1) From the *Profile* web page for the Service Provider, click the **Resources** link in the left navigation menu. This link takes you to the *Resources* web page for the service provider.

2) From the *Resources* web page, click the **Trunking Call Capacity** link. This link takes you to the *Trunking Call Capacity* web page for the Service Provider.

3) In the *Trunking Call Capacity* web page, below the label *Number of Business Trunking License Units Reserved for the Service Provider* either:

   – Select the *No Reservation* button. (If you select *No Reservation*, no license units are reserved for this Service Provider. This also allows license units to be allocated to the Groups directly from the stock of trunking licenses in the System.)

   – Or, select the *Reserved License Units* button and enter a value into the adjacent field. The value you enter determines how many BTLUs are allocated to this Service Provider.

4) Click the **Apply** or **OK** button.

The *Trunking Call Capacity* web page for a Service Provider is shown in *Figure 22.*

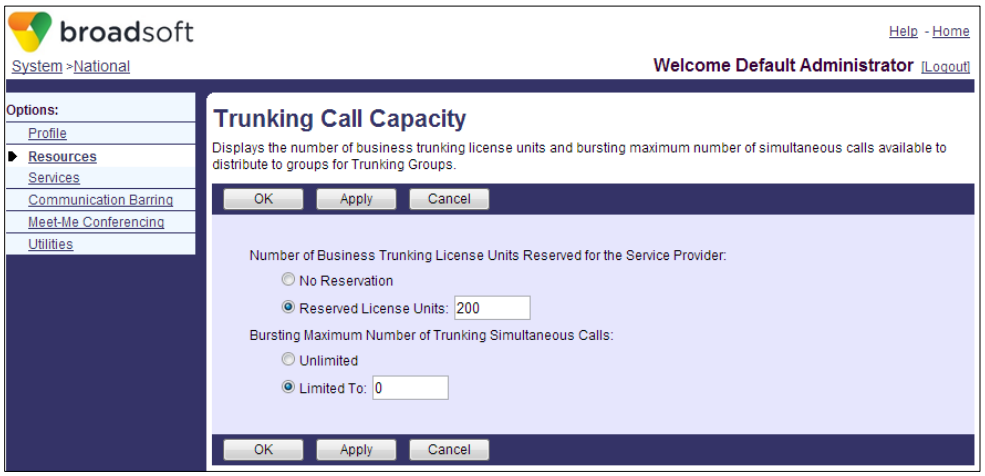

Figure 22 Trunking Call Capacity Web Page for Service Provider

To allocate BTLUs to a Group within a Service Provider, follow these steps:

1) From the *Profile* web page for the Group, click the **Resources** link in the left navigation menu. This link takes you to the *Resources* web page for the Group.

2) From the *Resources* web page, click the **Trunking Call Capacity** link. This link takes you to the *Trunking Call Capacity* web page for the Group.

3) In the field labeled *Number of Business Trunking License Units for this Group*, enter the number of BTLUs to allocate to this Group's license pool. Note that the web page shows the maximum value for this field. This maximum value depends on how many license units are currently reserved for the Service Provider and the number of license units currently allocated to other Groups in the Service Provider.

The *Trunking Call Capacity* web page for a Group is shown in *Figure 23.*

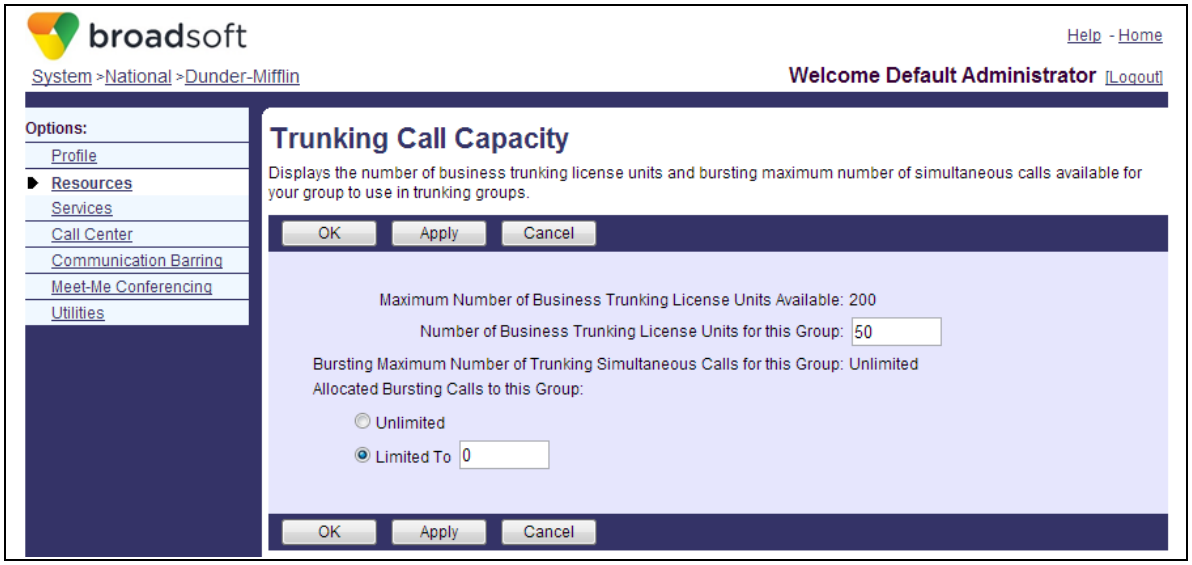

Figure 23 Trunking Call Capacity Web Page for Group in Service Provider

17 System-Wide SIP Trunking Configuration

System wide options that affect SIP trunking are configured in the CLI at the */Service/TrunkGroup* level.

- *enforceCLIDServiceAssignmentForPilotUser* – If the value of this parameter is "false", then the Application Server provides CLID delivery for a Pilot User, even if that Pilot User does not have any CLID delivery services assigned and enabled. If the value is "true", then a Pilot User is treated no differently than any other user in regards to CLID delivery. This means the Application Server provides CLID delivery to a Pilot User only if that Pilot User has the relevant CLID delivery service assigned and enabled. (CLID delivery services include Internal Calling Line ID Delivery, External Calling Line ID Delivery, Calling Name Delivery, and Calling Number Delivery).
- *terminateUnreachableTriggerDetectionOnReceiptOf18x* – If the value of this parameter is "true", then the Application Server considers a Trunk Group device to be reachable when it receives an 18x provisional response to a SIP INVITE request. If the Trunk Group device subsequently sends a failure response and the response code maps to Cisco BroadWorks TEMPORARILY_UNAVAILABLE internal release cause, then Cisco BroadWorks does not perform a route advance. For more information, see section *11.3 Enterprise Trunk Route Advancing.*
- *pilotUserCallingLineAssertedIdentityPolicy* – This parameter sets the system-wide default policy for the asserted identity for originating calls from a Trunk Group. If the value is "allOriginatingCalls", then the Application Server asserts the Pilot User's identity for all originating calls made via the Trunk Group. If the value is "unscreenedOriginatingCalls", then the Application Server asserts the Pilot User's identity only for unscreened originating calls made from the Trunk Group.

  Each Trunk Group can defer to this system-wide default setting or have its own setting for this policy.
- *enforceOutOfDialogPBXRedirectionPolicies* – This parameter controls how the Application Server processes an out-of-dialog PBX redirection with respect to capacity and calling line identity. For a detailed description of this policy, see section *12.2.8.1 Caller Identity*.
- *unscreenedRedirectionHandling* – This parameter controls how the Application Server processes an out-of-dialog PBX redirection with an unscreened redirecting identity. For a detailed description of this policy, see section *12.2.3.3 Unscreened PBX Redirection*.
- *enableHoldoverOfHighwaterCallCounts* – When this parameter is set to "true", the Application Server periodically records license utilization high-water marks as hold-over high-water marks and resets the current high-water marks. When the parameter is set to "false", the Application Server does not record hold-over high-water marks and does not automatically reset the current high-water marks.
- *holdoverPeriodMinutes* – This parameter establishes the period for the Application Server's periodic recording of hold-over high-water marks.
- *timeZoneOffsetMinutes* – This parameter can be used to adjust for a time zone difference between the primary and secondary Application Servers, so that license utilization high-water marks between the servers can be synchronized. (This parameter should be used only for servers that are on time zones with 30 or 45 minute offsets from the hour.)

- *clidSourceForScreenedCallsPolicy* – This parameter sets the system-wide default policy for calling line ID selection. The choices are “profileNameProfileNumber”, “receivedNameProfileNumber”, and “receivedNameReceivedNumber”. For more information, see section *9.6.1 Caller Identity*.

  Each Trunk Group can defer to this system-wide default setting or have its own setting for this policy.

- *userLookupPolicy* – This parameter sets the system-wide default policy for originating user lookups. The choices are “basic”, to enable basic lookups, and “extended”, to enable extended lookups. For more information, see section *9.3 Originating User Identification*.

  Each Trunk Group can defer to this system-wide default setting or have its own setting for this policy.

- *outOfDialogPBXRedirectionCLIDMapping* – This parameter controls whether the Application Server supports CLID mapping. For a detailed description of this policy, see section *12.2.4.2 CLID Mapping*.

- *enforceOutOfDialogPBXRedirectionTrunkGroupCapacity* – This parameter controls whether the Application Server counts out-of-dialog PBX redirections against the capacity of the redirecting Trunk Group. For a detailed description of this policy, see section *12.2.6 Trunk Group Capacity Check*.

- *implicitRegistrationSetSupport* (IMS only) – This parameter is the system-wide setting for enabling caller preferences for routing inbound calls to the PBX. For a detailed description of this parameter, see section *10.6.2.3 Caller Preferences (IMS only)*.

- *sipIdentityForPilotAndProxyTrunkModes* (IMS only) – This parameter controls how the Application Server selects the identity for the *P-Asserted-Identity* header or *P-Served-User* header (alternatively, the *P-Served-User-Identity* header) for certain trunking originations or redirections. If the parameter is set to the default value “user”, then the Application Server selects the originating or redirecting user’s own identity. Otherwise, if the parameter is set to “pilotUser”, then it selects the identity of the pilot user of the originating or redirecting Trunk Group. This parameter is effective only if the originating or redirecting Trunk Group has the Trunk Mode device option set to “Pilot” or “Proxy”. Moreover, this parameter controls only the system-wide setting, which may be overridden by a similar setting on the Trunk Group.

- *supportConnectedIdentityPolicy* – This parameter is the system-wide setting for enabling connected identity for inbound calls. For a detailed description of this parameter, see section *10.7 Connected Identity*.

- *useUnmappedSessionsForTrunkUsers* – This parameter controls whether Cisco BroadWorks processes calls for non-pilot trunking users via unmapped sessions.

- *allowPAILookupForOutOfDialogPBXRedirection* – This parameter controls how the Application Server identifies the redirecting trunk group for an out-of-dialog PBX redirection. If the parameter is set to “true”, then the Application Server examines the *P-Preferred-Identity* header (stand-alone mode only) or the *P-Asserted-Identity* header when it attempts to identify the redirecting trunk group. If the parameter is set to “false”, then the Application Server ignores those headers.

- *outOfDialogPBXRedirectionOriginatorLookupPolicy* – This parameter controls how the Application Server identifies the originating user for an out-of-dialog PBX redirection. If the parameter is set to “asserted”, then the Application Server uses the originator’s asserted identity for the user lookup. If the parameter is set to “presentation”, then the Application Server uses the originator’s presentation identity. If the parameter is set to “assertedOrPresentation”, then the Application Server uses the originator’s asserted identity if it is present, or the originator’s presentation identity if it is not.
- *allowTrunkIdentityForAllOriginations* – This parameter controls whether the Application Server sends originating trunk group information to the network for all trunking user originations. If the parameter is set to “false”, then the Application Server may send originating trunk group information only for calls that originated from an identified trunk group. If the parameter is set to “true”, then the Application Server may send originating trunk group information for all trunking user calls, even for calls that did not originate from a trunk group.

The system-wide list of “success” status code patterns is configured at the */Service/TrunkGroup/OptionsMessageResponseStatusCode* level. For an explanation of the purpose of this list, see section *19.6 Stateful Trunk Group Routing Configuration*.

18 SIP Trunking Device Configuration

18.1 Identity/Device Profile Type Configuration

Cisco BroadWorks supports a number of device configuration options, which shape the SIP interface that Cisco BroadWorks presents to that device. These options are configured as part of an Identity/Device Profile Type. *Figure 24* shows the *Identity/Device Profile Add* web page, where these options can be configured.

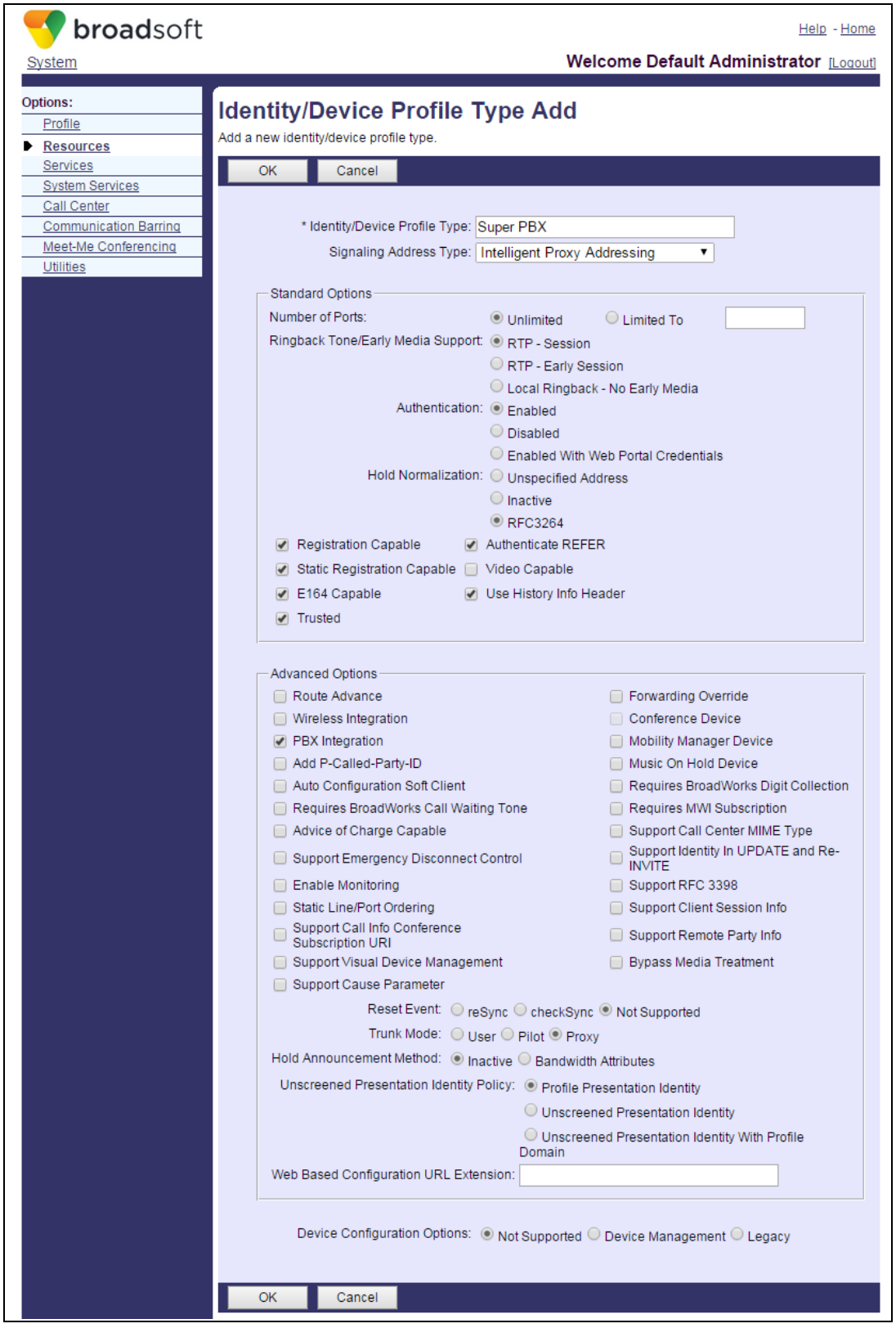

Figure 24 Identity/Device Profile Type Add Web Page

A complete description of all device configuration options is available in the *Cisco BroadWorks Device Management Configuration Guide* [5]. This section summarizes some of the options that are especially relevant to configuring business trunking.

- **Identity/Device Profile Type** – This field provides the name for the Identity/Device Profile Type. This name is used to select the Identity/Device Profile Type when creating an Identity/Device Profile.
- **Signaling Address Type** – The signaling address type of an Identity/Device Profile Type indicates the addressing characteristics of the Trunk Group device. For SIP Trunking, the device should always support intelligent addressing.
- **Number of Ports** – This field determines the number of Line/Ports that can be assigned to the device. In the common configuration case where only the Pilot User has a Line/Port or SIP PUI, a single port can be sufficient. Many generic devices have the number of ports set to unlimited.
- **Registration Capable** – If this policy is enabled, then the Application Server allows a device with this type to perform a SIP registration. A registration is allowed for each port.
- **Static Registration Capable** – Static registration is an alternative to normal SIP registration. When static registration is enabled, an administrator can provision a contact URI binding (a "static registration"), which the Application Server treats much like a contact URI binding from a SIP REGISTER request (a "SIP registration" or "dynamic registration"). This device option is especially useful if the device does not support SIP registration or if it is configured not to register.
- **E.164 Capable** – When this policy is enabled, the Application Server uses E.164 format for phone numbers in the addressing fields. When it is disabled, it normally uses the national format for phone numbers. E.164 format addresses are required by the SIPconnect recommendation. Therefore, for SIPconnect-compliant devices, this policy should be enabled.
- **Trusted** – If this policy is enabled, then the Application Server can send sensitive identity information to the device. Specifically, the Application Server includes *P-Asserted-Identity* and *Privacy* headers in the INVITE requests.
- **PBX Integration** – If this policy is enabled, as it should be for any PBX-like device, then the Application Server correctly handles redirections that take place within the device and outside of Cisco BroadWorks.
- **Trunk Mode** – Depending on the value set, this device policy has an impact on the way terminating requests are routed to the trunking device. For more information on the trunk mode, see section *10 Inbound Calls*. The possible values are:
  - User
    - (Stand-alone only) Typically, terminating requests are routed using the user's registered contact.
    - (IMS only) Typically, terminating requests are routed back to the CSCF without modifying the *Request-URI*.

- Pilot
  - (Stand-alone only) Typically, terminating requests are formatted as using the Pilot User's registered contact for the Request-URI and the terminating user's AoR in the *To* header. When using the Pilot trunk mode, there is usually a single contact address for the device, rather than a contact address for each user on the device. If the device is a registering device, then the device registers only for the Pilot User and not for other users reachable through that device (if the device requires a statically configured contact URI, then the contact address is the Pilot User's URI).
  - (IMS only) The Application Server and the IMS core are configured to use a "wildcarded" PSI for business trunking users. Typically, terminating requests sent back to the CSCF are using a retargeted *Request-URI* containing the Pilot User's Public User Identity and are treated as out-of-the-blue (OOTB) calls.
- Proxy
  - (Stand-alone only) Typically, terminating requests are routed using the *Route* header added by Cisco BroadWorks that contains the Pilot User's registered contact.
  - (IMS only) Typically, terminating requests are routed back to the CSCF without modifying the *Request-URI* and by reusing the *Route* header to make sure the termination is not treated as OOTB.

18.2 Identity/Device Profile Type Configuration Procedure

A new Cisco BroadWorks installation typically offers a number of pre-configured Identity/Device Profile Types, covering both generic types and popular vendor products. A System Administrator can add additional Identity/Device Profile Types by following these steps:

1) Log in to the Cisco BroadWorks web configuration interface as a system administrator.
2) Under the *Resources* tab in the left-side navigation, select the **Identity/Device Profile Types** link.
3) Click **Add**.
4) Enter the Identity/Device Profile name.
5) Select the appropriate Signaling Address type.
6) Configure the device options.
7) Click **OK**.

18.3 Identity/Device Profile Attributes Configuration

Each Trunk Group must have a device that is configured in Cisco BroadWorks as an Identity/Device Profile. The configuration of an Identity/Device Profile is fully documented in *Cisco BroadWorks Application Server Group Web Interface Administration Guide – Part 1* [6]. This section provides information on selected device attributes that are especially relevant to SIP Trunking configuration.

- **Name** – The Identity/Device Profile name is used to identify the Identity/Device Profile within Cisco BroadWorks provisioning interfaces. For example, this name is used to identify the Identity/Device Profile that is assigned to a Trunk Group.

- **Host name/IP address** (Stand-alone only) – The host name or IP address is optional for certain deployments. However, in these specific situations, the host name or IP address is required:
  - Source-based Trunk Group identification, if the device does not use SIP registration and does not have a provisioned contact URI.
  - Access control list screening, if the access control list (ACL) is enabled.
  - SIP signaling if the signal addressing type for the device is Device.
- **Transport** – Cisco BroadWorks supports UDP and TCP transports. Set this to "Unspecified" if you want to allow either UDP (preferred) or TCP.
- **Physical Location** – The Physical Location field can be used to add the *P-Access-Network-Info* header when it is not added by the device, which can be important for emergency calls. It can also be used for screening calls based on the received *P-Access-Network-Info* header.

18.4 Identity/Device Profile Attributes Configuration Procedure

The following procedure shows how to create an Identity/Device Profile at the Group to use for the Trunk Group.

1) Log in to the Cisco BroadWorks web configuration interface as an administrator.
2) Navigate to the *Group* page where the Trunk Group belongs.
3) Under the *Resources* tab in the left-side navigation, select the **Identity/Device Profiles** link.
4) Click **Add**.
5) Enter a unique Identity/Device Profile name (for example, PBX1).
6) Select the appropriate Identity/Device Profile Type from the drop-down list for the PBX classification.
7) Complete the remaining fields, as necessary.
8) Click **OK**.

Figure 25 shows an example *Identity/Device Profile Add* web page used to add the Identity/Device Profile for use with the Trunk Group configuration on Cisco BroadWorks.

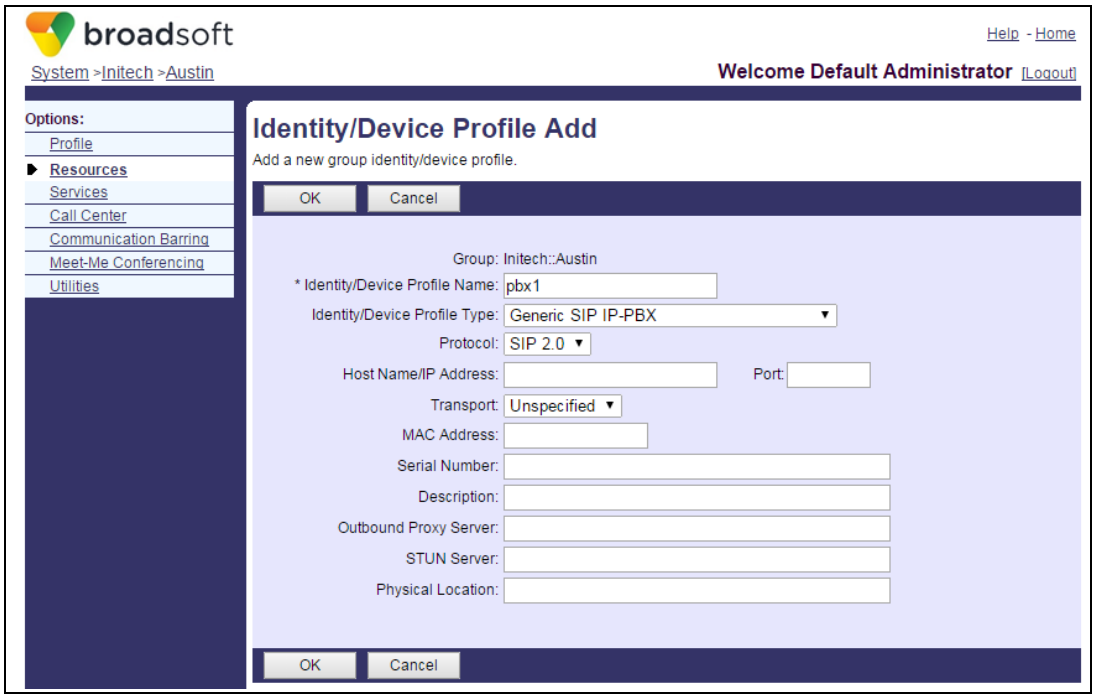

Figure 25 Identity/Device Profile Add Page in Web Portal

19 Trunk Group Configuration

19.1 Trunk Group Attributes

This section describes the attributes that can be configured for each Trunk Group.

- *Name* – This required attribute defines the name of the Trunk Group. Every Trunk Group must have a name that is unique within the Group. The Application Server uses this name to identify the Trunk Group in provisioning interfaces, as well as in log files, billing records, and so on.
- *Department* – This optional attribute defines the department to which the Trunk Group belongs. If a Trunk Group is assigned to a department, then the department administrators for that department can be authorized to make changes to that Trunk Group.
- *Maximum Active Calls Allowed* –This required attribute determines the maximum number of simultaneous calls allowed for the Trunk Group, including both incoming and outgoing calls. For more information about Trunk Group capacity management, see section *14 Trunk Group Capacity Management*.
- *Maximum Active Incoming Calls Allowed* – This optional attribute determines the maximum number of simultaneous incoming calls that are allowed for the Trunk Group. If this attribute is not set, then the Application Server enforces no explicit limit on incoming calls, although it still enforces the limit on the total of incoming and outgoing calls determined by *Maximum Active Calls Allowed*. If the value is set to "0", then the Application Server blocks incoming calls for this Trunk Group. This value cannot exceed the value of *Maximum Active Calls Allowed*.
- *Maximum Active Outgoing Calls Allowed* – This optional attribute determines the maximum number of simultaneous outgoing calls that are allowed through the Trunk Group. If this attribute is not set, then the Application Server enforces no explicit limit on outgoing calls. However, it still enforces the limit on the total of incoming and outgoing calls determined by *Maximum Active Calls Allowed*. If the value is set to "0", then the Application Server blocks outgoing calls for this Trunk Group. This value cannot exceed the value of *Maximum Active Calls Allowed*.
- *Enable Authentication* – If this attribute is enabled, then the Application Server requires authentication for any SIP REGISTER requests it receives from the Trunk Group. The Trunk Group has its own SIP credentials. For more information about authentication, see section *8 SIP Authentication*.
- *Authentication User Name* – This attribute defines the user name for SIP authentication for the Trunk Group.
- *Authentication Password* – This attribute defines the password for SIP authentication for the Trunk Group.
- *Trunk Group Identity* – This optional attribute defines the Trunk Group's identity, which may be used to identify the Trunk Group in SIP INVITE requests in accordance with *RFC 4904* [17]. In the provisioning interface, it has the form of user@host. However, in the SIP signaling, the user part is the value of the *tgrp* parameter and the host part is the value of the *trunking-context* parameter. The value of this attribute must be unique system wide.
- *OTG/DTG Identity* – This optional attribute defines an alternate Trunk Group identity, which may be used to identify the Trunk Group in SIP INVITE requests via an *otg* (originating trunk group) parameter or *dtg* (destination trunk group) parameter. The value of this attribute must be unique system wide.

- *Enable Trunk Group Prefix* – When this option is enabled, the Application Server adds a prefix to the *Request-URI* for initial INVITE requests it sends to the Trunk Group. If the option is enabled, then the prefix must be entered in the adjacent text field.
- *Allow calls directly to trunk group with Trunk Identity* – If the Application Server receives an INVITE request from the network interface and the *Request-URI* in that request has *tgrp* and *trunking-context* parameters that match this Trunk Group, then the Application Server can apply translations in the context of this Trunk Group's Group. To enable the behavior, this attribute must be enabled.
- *Allow calls directly to trunk group with DTG Identity* – If the Application Server receives an INVITE request from the network interface and the *Request-URI* in that request has a *dtg* parameter that matches this Trunk Group, then the Application Server can apply translations in the context of this Trunk Group's Group. To enable the behavior, this attribute must be enabled.
- *Include Trunk Identity for Calls to Trunk Group* -- If this attribute is enabled, then the Application Server adds the *tgrp* and *trunk-context* parameters to the *Request-URI* of the SIP INVITE requests it sends to the Trunk Group device. When this attribute is enabled, the *Trunk Group Identity* attribute must have a valid value. Note that it is not recommended to activate this attribute if the *tgrp* and *trunk-context* were provided at registration time. The result would be to have two sets of *tgrp* / *trunk-context* pairs in the outgoing INVITE.
- *Include DTG Identity for Calls to Trunk Group* – If this attribute is enabled, then the Application Server adds the *dtg* parameter to the *Request-URI* of the SIP INVITE requests it sends to the Trunk Group device. When this attribute is enabled, the *OTG/DTG Identity* attribute must have a valid value.
- *Include Trunk Identity for Calls from Trunk Group* – If this attribute is enabled, Trunk Group-originated calls terminating to the network side include the *tgrp* and *trunk-context* parameters in the *Contact* URI using the provisioned data from the *Trunk Group Identity* field. The *tgrp* value is taken from the *Trunk Group Identity* user part and the *trunk-context* is taken from the *Trunk Group Identity* domain.
- *Include OTG Identity for Calls from Trunk Group* -- If this attribute is enabled, Trunk Group-originated calls terminating to the network side include the *otg* parameter in the *From* header using the provisioned data from the *OTG/DTG Identity* field.
- *Enable Network Address Identity* – The Application Server can identify the Trunk Group for a SIP request from the source IP address of the Trunk Group device. This capability in the Application Server can be enabled or disabled, and it is recommended to disable it unless it is specifically needed. To disable the capability, this policy in the Trunk Group should be disabled. The Application Server can avoid IP address lookups altogether if all Trunk Groups in the Application Server have this policy disabled. Note that when using this configuration option, all Trunk Group devices need to have unique static or dynamic contact addresses. Multiple trunk devices that register through a single contact SBC must not be identified with the source IP address mechanism.

- *Allow Unscreened Calls* – Usually, the Application Server blocks originating calls on the access side when it cannot identify a Cisco BroadWorks user as the originator. For Trunk Groups, however, it can be configured to allow originating calls even if the originator is not a Cisco BroadWorks user, provided the originating Trunk Group can be identified via available signaling. Such a call is called an "unscreened call". If this policy is enabled, the Application Server allows these unscreened calls through a Trunk Group. Note, however, that the concept of "unscreened calls" does not apply when the originating user can be identified as a Cisco BroadWorks subscriber and this latter belongs to a Group or Enterprise outside the scope of the Trunk Group. The previous note is true for simple originations only and cannot be true for some PBX redirection scenarios where a more complex scheme applies to identify the parties involved.
- *Allow Unscreened Emergency Calls* – This attribute is similar to the *Allow Unscreened Calls* attribute, but it applies to emergency calls.
- *Route to Peering Domain* – If this attribute is enabled, then the Application Server overwrites the host part of the *Request-URI* with the *Peering Domain* for terminating INVITE requests to the Trunk Group.
- *Peering Domain* – A peering domain can be specified for a given Trunk Group to help routing the terminating requests to the proper location. The peering domain is used to overwrite the host part of the *Request-URI* for terminating requests destined to the trunking device.
  - The peering domain can be configured on a per Trunk Group basis.
  - The route to peering domain functionality can be enabled or disabled altogether on a per Trunk Group basis using a flag.
- *Pilot User Call Optimization Policy* – This attribute affects the way that the Application Server processes incoming and outgoing calls for the Pilot User. If the policy is set to "Optimize for User Services", then the Application Server supports the same services for the Pilot User as it does for other trunking users. If the policy is set to "Optimize for High Call Volume", then the Application Server places some restrictions on the Pilot User's services to process basic calls more efficiently. For example, if the policy is set to "Optimize for High Call Volume", then services such as Three-Way Calling do not work for the Pilot User.
- *Trunk Group User Lookup Policy* – This policy controls the steps the Application Server takes to identify the originating user after it has identified the originating Trunk Group. If "Use default System Policy" is selected, then the Application Server applies the policy *userLookupPolicy* defined at the system level (see section *17 System-Wide SIP Trunking Configuration*). If "Use this Trunk Group Policy" is selected, then the policy for this Trunk Group can be defined independently from the system-wide policy. The policy choices are:
  - "Basic Lookup" – The Application Server identifies the originating user from the *From* header, or the *P-Asserted-Identity* header if the caller requested privacy.
  - "Extended Lookup" – In addition to the *From* header, the Application Server examines additional headers, such as *Remote-Party-ID*, to identify the originating user.
  - "Basic Lookup Prefer From" – The Application Server performs user lookups like "Basic Lookup" except that it consistently examines the *From* URI before examining the *P-Asserted-Identity* URI.

  For more information, see section *9.3 Originating User Identification*.

- *Calling Line Identity Source for Screened Trunk Group Calls Policy* – This policy controls how the Application Server selects the calling line identity for a call from the Trunk Group. It does not apply to unscreened originations. If "Use default System Policy" is selected, then the Application Server applies the policy *clidSourceForScreenedCallsPolicy* defined at the system level (see section *17 System-Wide SIP Trunking Configuration*). If "Use this Trunk Group Policy" is selected, then the policy for this Trunk Group can be defined independently from the system-wide policy. The policy choices are:
  - "Profile Name and Profile Number" – The Application Server selects the calling name and calling number as provisioned for the originating user.
  - "Received Name and Profile Number" – The Application Server selects the calling name from the received *From* header and the calling number as provisioned for the originating user.
  - "Received Name and Received Number" – The Application Server selects the calling name and the calling number from the received *From* header.

  For more information, see section *9.6.1 Caller Identity*.

  If *Support Connected Identity Policy* is enabled, then the *Calling Line Identity Source for Screened Trunk Group Calls Policy* also affects the connected identity. See section *10.7 Connected Identity*.
- *Pilot User Calling Line Asserted Identity Usage Policy* – This attribute selects the policy the Application Server applies to determine the asserted identity for calls that originate from the Trunk Group. If "Use default System Policy" is selected, then the Application Server applies the policy *pilotUserCallingLineAssertedIdentityPolicy* defined at the system level (see section *17 System-Wide SIP Trunking Configuration*). If "Use this Trunk Group Policy" is selected, then the policy for this Trunk Group can be defined independently from the system-wide policy. The policy choices are:
  - "Unscreened Originating Calls" – When the Application Server applies this policy, it asserts the Pilot User's identity for all unscreened originating calls, which are defined as calls that originate from the Trunk Group for which the Application Server cannot identify a Cisco BroadWorks user as the originator.
  - "All Originating Calls" – When the Application Server applies this policy, it asserts the Pilot User's identity for all calls that originate from the Trunk Group.
- *Support Connected Identity Policy* – When this policy is enabled, the Application Server applies CLID configuration options to the connected identity. In particular, the Application Server can be further configured to allow the PBX to provide the connected identity. See section *10.7 Connected Identity*.
- *Pilot User Calling Line Identity for External Calls Usage Policy* – The Application Server can be configured to use the Pilot User's CLID for originations from the Trunk Group. This policy determines how the Application Server uses the Pilot User's CLID.
  - If the value is "All Originating Calls", then the Application Server uses the Pilot User's CLID for all originations from the Trunk Group.
  - If the value is "All Unscreened Originating Calls", then the Application Server uses the Pilot User's CLID for the Pilot User and for non-Cisco BroadWorks users.
  - If the value is "No Calls", then the Application Server uses the Pilot User's CLID only for the Pilot User.

- *Pilot User Calling Line Identity for Emergency Calls Usage Policy* – This policy is similar to the *Pilot User Calling Line Identity for External Calls Usage Policy*, but it applies to emergency calls.
- *Pilot User Charge Number Usage Policy* – If the Pilot User is assigned the Charge Number feature and has a configured charge number, then the Application Server can use the Pilot User's charge number for originating calls through the Trunk Group. This policy determines how the Application Server uses the Pilot User's charge number.
  - If the value is "All Originating Calls", then it uses the Pilot User's charge number for all originating calls, unless the originating user is a Cisco BroadWorks business trunking user with their own charge number. In the latter case, the Application Server uses the Cisco BroadWorks user's own charge number instead of the Pilot User's charge number.
  - If the value is "Unscreened Originating Calls", then it uses the Pilot User's charge number for the Pilot User and for non-Cisco BroadWorks users.
  - If the value is "No Calls", then it uses the Pilot User's charge number for the Pilot User only.

19.2 Trunk Group Configuration Procedure

After the Identity/Device Profile is created, the Trunk Group configuration can be started. The following procedure shows how to provision the Trunk Group on Cisco BroadWorks.

1) Log in to the Cisco BroadWorks web configuration interface as an administrator.
2) Navigate to the Group page where the Trunk Group is to be added.
3) Under the *Services* tab in the left-side navigation, select the **Trunk Group** link.
4) Click **Add**.
5) Enter a unique Trunk Group name for the Trunk Group (for example, PBX).
6) Complete the fields for the various Trunk Group attributes. For the descriptions of the various attributes, see section *19.1 Trunk Group Attributes*.
7) Select Identity/Device Profile for the device category. From the drop-down list, select the name of the Identity/Device Profile for the Trunk Group.
8) Click **OK**.

NOTE: It is possible to create a Pilot User from the Trunk Group Add web page. The following sections describe the Pilot User and explain how to assign the Pilot User after the Trunk Group is created. Administrators who have already configured one or more Trunk Groups may find the ability to create a Pilot User at this point in the procedure to be a convenient shortcut.

Figure 26 shows the *Trunk Group Add* web page.

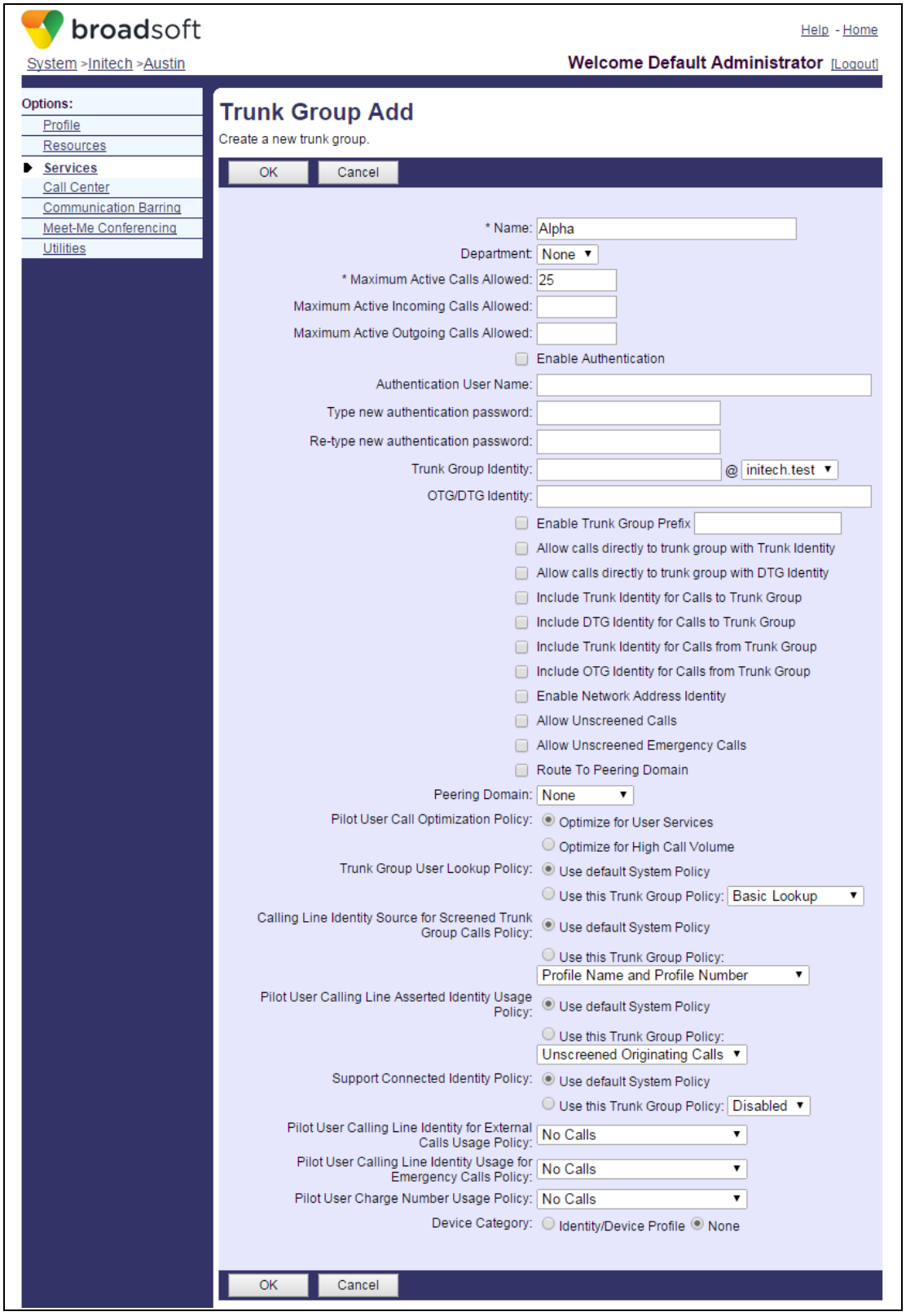

Figure 26 Trunk Group Add Web Page

19.3 Trunk Group Capacity Configuration

Trunk Group capacity limits are configured as properties of a Trunk Group. However, when provisioning within an Enterprise, a separate provisioning step at the Group level is required to establish the maximum capacity allowed for any Trunk Group within that Group. This step is not available when provisioning within a Service Provider.

To set the maximum capacity allowed for any Trunk Group within the Group (Enterprise model only):

1) From the *Profile* web page for the Group, click the **Resources** link in the left navigation menu. This link takes you to the *Resources* web page for the Group.

2) From the *Resources* web page, click the **Trunking Call Capacity** link. This link takes you to the *Trunking Call Capacity* web page for the Group.

3) In the field labeled *Maximum Number of Trunking Simultaneous Calls*, enter the value for the maximum call capacity limit for any Trunk Group within the Group. This value cannot exceed the number of BTLUs allocated to the Enterprise.

The *Trunking Call Capacity* web page for a Group in an Enterprise is shown in *Figure 27*.

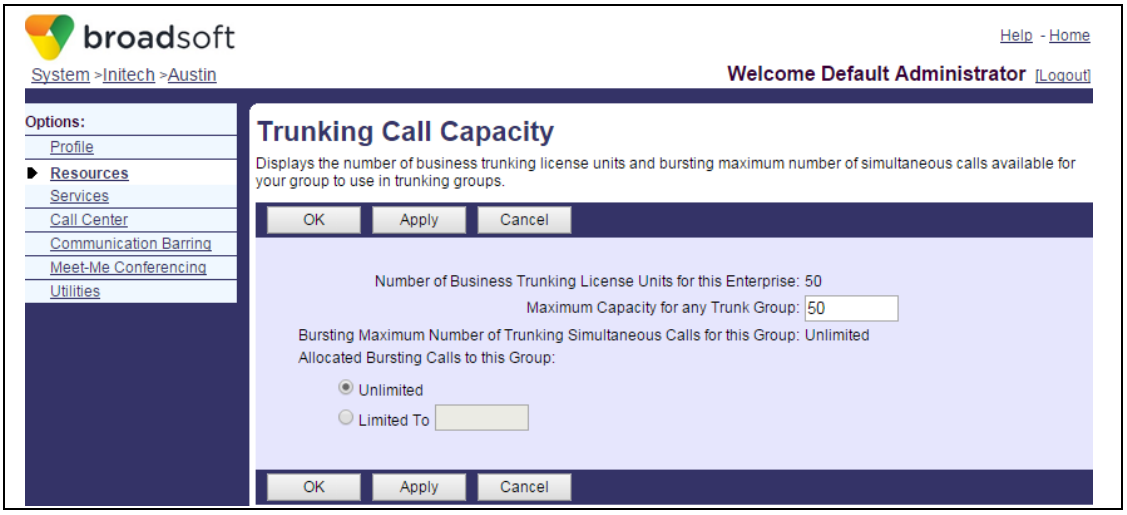

Figure 27 Trunking Call Capacity Web Page for Group in Enterprise

To configure the capacity management for a Trunk Group:

1) From the *Profile* web page for the Group, click the **Services** link in the left navigation menu. This link takes you to the *Services* web page for the Group.

2) From the *Services* web page for the Group, click the **Trunk Group** link. This link takes you to the *Trunk Group* web page for the Group.

3) From the *Trunk Group* web page, click the **Edit** link next to the Trunk Group you want to configure. This link takes you to the *Profile* web page for the Trunk Group.

4) From the *Profile* page, click the **Capacity Management** link. This link takes you to the *Capacity Management* web page for the Trunk Group.

5) Enter the capacity limits in the labeled fields for *Total Calls*, *Incoming Calls*, and *Outgoing Calls*. Note that incoming calls are calls that terminate to the Trunk Group device, and outgoing calls are calls that originate from the Trunk Group device.

6) Select a button for the *Incoming Capacity Exceeded Action*. Note that if this Trunk Group is assigned to an Enterprise Trunk, it is recommended to set this action to "None" to allow the Enterprise Trunk to reroute on the capacity-exceeded condition.

The *Capacity Management* web page for a Trunk Group is shown in *Figure 28*.

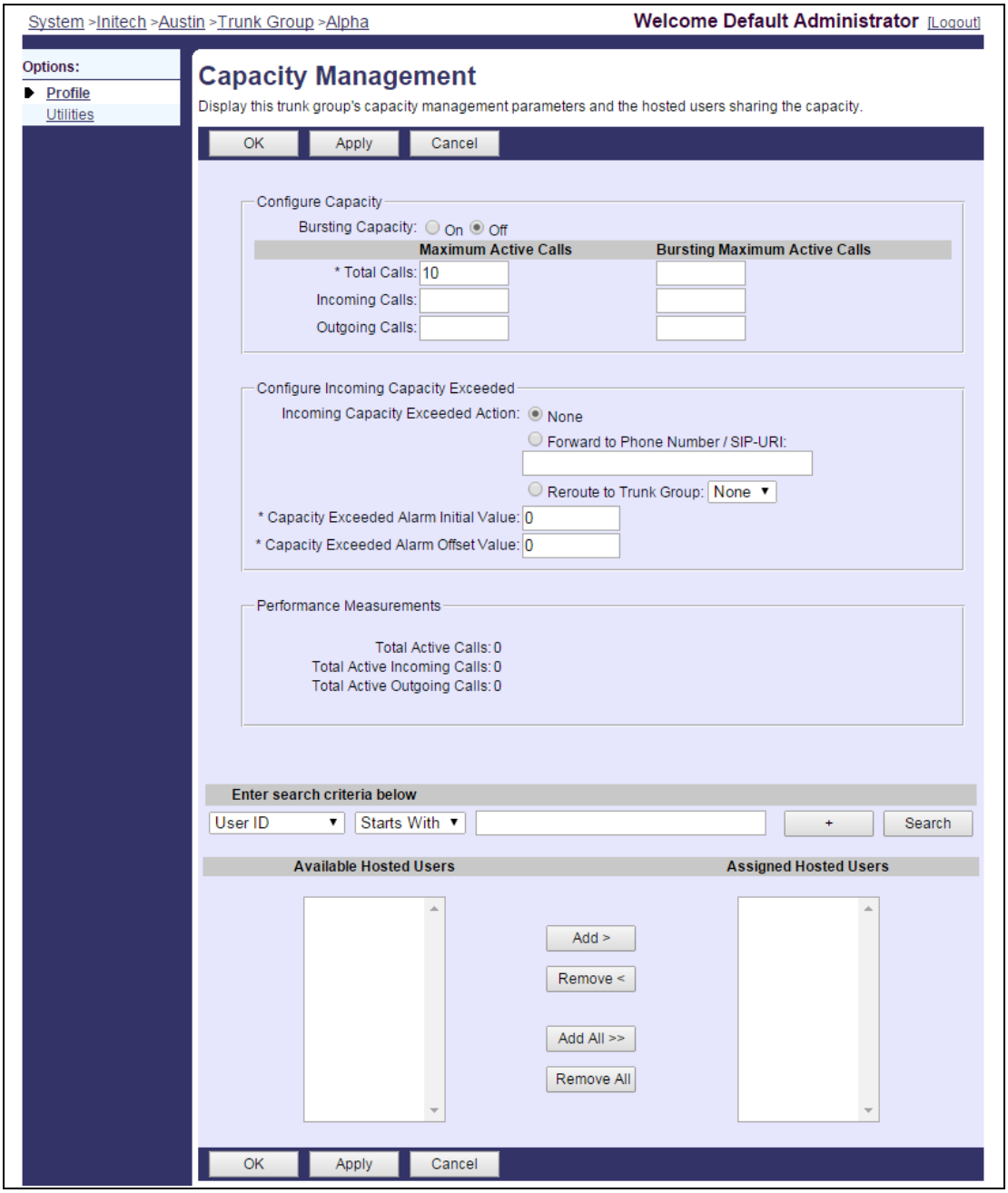

Figure 28 Capacity Management Web Page for Trunk Group

19.4 Capacity-Exceeded Threshold Configuration

Trunk Groups can be configured to generate SNMP alarms when capacity thresholds are crossed. The configurable settings of initial and offset values are used to determine the frequency with which the alarms are generated.

- *Capacity Exceeded Alarm Initial Value* – Whenever the capacity is exceeded for a Trunk Group, the corresponding capacity counter is incremented by one. When the value of the counter crosses the initial value, the *bwTrunkGroupCapacityExceeded* SNMP alarm is generated. The alarm is never generated when the value is "0".
- *Capacity Exceeded Alarm Offset Value* – When the initial value of the capacity-exceeded counter has been reached, the *bwTrunkGroupCapacityExceeded* SNMP alarm is generated every time the counter reaches an exact multiple of the offset value. The alarm is never generated after the initial time when the value is "0".

Example:

- Capacity Exceeded Initial Value is set to "20".
- Capacity Exceeded Offset Value is set to "5".

The *bwTrunkGroupCapacityExceeded* SNMP alarm is generated when the counter reaches, 21, 26, 31, and so on.

19.5 Trunk Group Forwarding and Rerouting Configuration Procedure

19.5.1 Unconditional Forwarding or Rerouting

To configure unconditional forwarding or rerouting for a Trunk Group, follow these steps:

1) From the *Profile* page for the Group, click the **Service** link in the left navigation menu. This link takes you to the *Service* web page for the Group.
2) From the *Service* web page, click the **Trunk Group** link. This link takes you to the *Trunk Group* web page.
3) From the *Trunk Group* web page, click the **Edit** link next to the Trunk Group you want to configure. This link takes you to the *Profile* web page for the Trunk Group.
4) From the *Profile* page for the Trunk Group, click the **Call Forwarding Always** link. This link takes you to the *Call Forwarding Always* web page for the Trunk Group.
5) Select the button for the *Call Forwarding Always Action*.
   - If you select "Forward to Phone Number / SIP-URI", then enter the phone number of the SIP URI for the forwarding destination. This action is only executed if the Trunk Group has a Pilot User.
   - If you select "Reroute to Trunk Group", then select the destination Trunk Group from the drop-down list.
6) Click the **Apply** or **OK** button to save the changes.

The *Call Forwarding Always* web page for the Trunk Group is shown in *Figure 29*.

Figure 29 Call Forwarding Always Web Page for Trunk Group

19.5.2 Forwarding or Rerouting on Capacity-Exceeded Condition

To configure forwarding or rerouting for Trunk Group, for a capacity-exceeded condition, follow these steps:

1) From the *Profile* page for the Group, click the **Service** link in the left navigation menu. This link takes you to the *Service* web page for the Group.
2) From *Service* web page, click the **Trunk Group** link. This link takes you to the *Trunk Group* web page.
3) From the *Trunk Group* web page, click the **Edit** link next to the Trunk Group you want to configure. This link takes you to the *Profile* web page for the Trunk Group.
4) From the *Profile* page for the Trunk Group, click the **Capacity Management** link. This link takes you to the *Capacity Management* web page for the Trunk Group.
5) Select the button for the *Incoming Capacity Exceeded Action*.
   - If you select “Forward to Phone Number / SIP-URI”, then enter the phone number of the SIP URI for the forwarding destination. This action is only executed if the Trunk Group has a Pilot User.
   - If you select “Reroute to Trunk Group”, then select the destination Trunk Group from the drop-down list.
6) Click the **Apply** or **OK** button to save the changes.

The *Capacity Management* web page for a Trunk Group is shown in *Figure 28*.

19.5.3 Forwarding or Rerouting on Unreachable Destination Condition

To configure forwarding or rerouting for Trunk Group, for an unreachable destination condition, follow these steps:

1) From the *Profile* page for the Group, click the **Service** link in the left navigation menu. This link takes you to the *Service* web page for the Group.
2) From the *Service* web page, click the **Trunk Group** link. This link takes you to the *Trunk Group* web page.
3) From the *Trunk Group* web page, click the **Edit** link next to the Trunk Group you want to configure. This link takes you to the *Profile* web page for the Trunk Group.
4) From the *Profile* page for the Trunk Group, click the **Unreachable Destination** link. This link takes you to the *Unreachable Destination* web page for the Trunk Group.
5) Enter a value for the *Unreachable Destination Timeout* field.
6) Select the button for the *Unreachable Destination Action*.
   - If you select "Forward to Phone Number / SIP-URI", then enter the phone number of the SIP URI for the forwarding destination. This action is only executed if the Trunk Group has a Pilot User.
   - If you select "Reroute to Trunk Group", then select the destination Trunk Group from the drop-down list.
7) Click the **Apply** or **OK** button to save the changes.

The *Unreachable Destination* web page for a Trunk Group is shown in *Figure 30*.

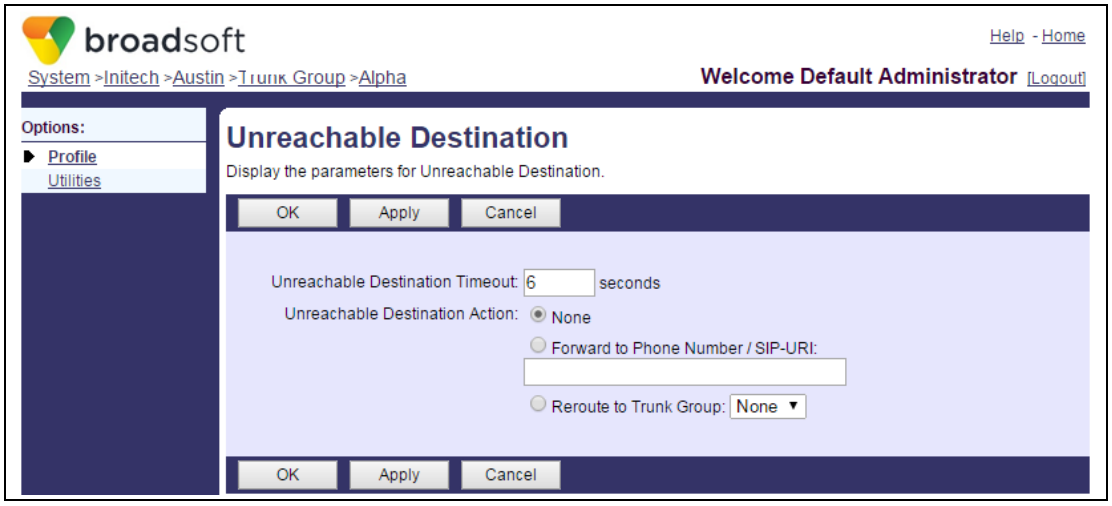

Figure 30 Unreachable Destination Web Page for Trunk Group

19.6 Stateful Trunk Group Routing Configuration

Internally, the Application Server tracks the state of every Trunk Group. The state can be either “available” or “unavailable”. When the state is “unavailable”, the Application Server does not attempt to route calls to that Trunk Group.

The “available” state is the default state, and the Application Server considers a Trunk Group to be available unless it discovers through some means that the Trunk Group is unavailable. There are two ways the Application Server can discover that the Trunk Group is unavailable. First, it can track the failure rate of INVITE requests it sends to that Trunk Group and change the Trunk Group’s state to “unavailable” when the failure rate is too high. Second, it can regularly send a SIP OPTIONS request to the Trunk Group and change the Trunk Group’s state to “unavailable” when the PBX does not respond to the OPTIONS requests. The Application Server sends the OPTIONS requests to the address of the Trunk Group’s Pilot User; therefore, the Pilot User is required. If a Trunk Group does not have a Pilot User, the Application Server does not send OPTIONS requests to that Trunk Group.

When a Trunk Group is in the “unavailable” state, the Application Server sends periodic SIP OPTIONS requests to that Trunk Group to discover when the Trunk Group becomes available again. As long as these OPTIONS requests fail, the Trunk Group remains in the “unavailable” state. When the Trunk Group begins responding to the OPTIONS requests, the Application Server changes the Trunk Group’s state to “available”. The Application Server sends these OPTIONS requests to the Trunk Group’s Pilot User; therefore, a Pilot User is required.

NOTE 1: Because a Pilot User is required for the Application Server to send OPTIONS requests, a Pilot User is required for the stateful Trunk Group functionality. If a Trunk Group does not have a Pilot User, then the Application Server considers that Trunk Group available always.

NOTE 2: If the address for the OPTIONS request is a DNS name, then the Application Server performs DNS queries (NAPTR, SRV, AAAA, or A) according to the DNS configuration. The Application Server then sends the OPTIONS request to the first transport address (that is, the IP address and port number). However, if the Application Server does not receive a response to the OPTIONS request, it does not advance to the next transport address. This is special behavior that applies only to the OPTIONS request. For INVITE requests, the Application Server does advance to the next transport address, as described in section *11.2 Transport Address Route Advancing*.

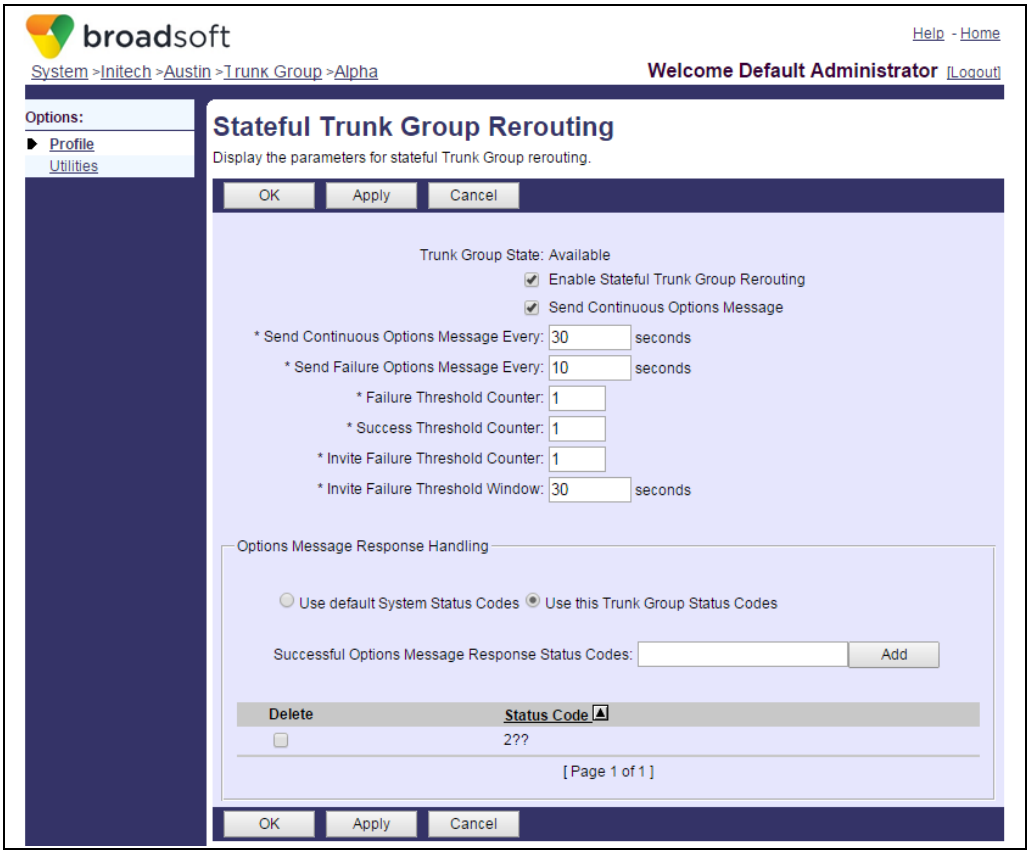

Figure 31 Stateful Trunk Group Rerouting Web Page for Trunk Group

Figure 31 shows the provisioning web page for configuring the stateful Trunk Group functionality. The fields on this page are described in the following list:

- *Trunk Group State* – This display-only field shows the current state of the Trunk Group, which can be "Available" or "Unavailable".
- *Enable Stateful Trunk Group Rerouting* – This option enables or disables the stateful Trunk Group functionality. If the value is "off", then the functionality is disabled and the Trunk Group's state is always "available".
- *Send Continuous Options Message* – This option enables or disables the behavior of the Application Server to send SIP OPTIONS requests to determine when the Trunk Group becomes unavailable. If the value is "off", the Application Server does not send OPTIONS requests when the Trunk Group is available.
- *Send Continuous Options Message Every ___ Seconds* -- If *Send Continuous Options Message* is "on", then the value entered here determines the interval between successive OPTIONS requests when the Trunk Group is available. To avoid undesired synchronization with any other Trunk Groups, the Application Server randomizes the actual time interval to +/- 20% of the configured value.
- *Send Failure Options Message Every ___ Seconds* – The value entered here determines the interval between successive OPTIONS requests when the Trunk Group is "unavailable". To avoid undesired synchronization with any other Trunk Groups, the Application Server randomizes the actual time interval to +/- 20% of the configured value.

- *Failure Threshold Counter* – The value entered here sets the threshold the Application Server applies for declaring the Trunk Group unavailable based on OPTIONS requests. If the value of this property is *N*, then the Application Server changes the Trunk Group's state to "unavailable" after it sends *N* consecutive OPTIONS requests for which it receives no response.
- *Success Threshold Counter* -- The value entered here sets the threshold the Application Server applies for declaring the Trunk Group available based on OPTIONS requests. If the value of this property is *N*, then the Application Server changes the Trunk Group's state to "available" after it sends *N* consecutive OPTIONS requests for which it receives a response.
- *Invite Failure Threshold Counter* – The value entered here sets the threshold the Application Server applies for declaring the Trunk Group unavailable based on INVITE requests. If the value of this property is *N* and the value of Invite Failure Threshold Window is *T*, then the Application Server changes the Trunk Group's state to "unavailable" if it detects an unreachable condition *N* times over an interval of *T* seconds. An unreachable condition occurs when the Application Server sends an INVITE request and receives no response, or receives certain specific error responses.
- *Invite Failure Threshold Window* -- The value entered here sets the time interval the Application Server applies for declaring the Trunk Group unavailable based on INVITE requests. Refer to the previous description of *Invite Failure Threshold Counter*.
- *Options Message Response Handling* – This panel contains fields that permit an administrator to define the "success" status codes, that is, the SIP response codes that indicate the Trunk Group is available. When the Application Server receives a response to the OPTIONS request, the Application Server checks the status code against this configuration. A success status code indicates that the Trunk Group is available. Any other status code or no response at all, indicates that the Trunk Group is unavailable.
  - *Use default System Status Codes* / *Use this Trunk Group Status Codes* – If *Use default System Status Codes* is selected, then the list of success codes for this Trunk Group is the system-wide list, which is configured at the CLI. If *Use this Trunk Group Status Codes* is selected, then this Trunk Group has its own list of success codes.
  - Status Code List – This list contains the patterns that define the success status codes. A pattern consists of three elements, which the Application Server matches against the three digits of a status code in a SIP response message. The allowed elements are the following.

Pattern Element	Example	Description
Single digit	2	A literal digit matches a digit exactly.
Wildcard	?	A question mark is a wildcard that matches any digit.
Set	[1,4-6]	Square brackets define a set of digits.

Examples:

404 – Matches the 404 status code.

2?? – Matches any 2xx status code.

1[1-9]? – Matches any status code in the range 110 to 199

20 Enterprise Trunk Configuration

Enterprise Trunks aggregate multiple Trunk Groups and implement a routing policy that determines how calls are routed to those Trunk Groups. The Application Server implements several routing policies, and the routing policy used by an Enterprise Trunk is a defining characteristic of the Enterprise Trunk.

- In the Service Provider model, Enterprise Trunks exist within a Group and can only include Trunk Groups that are within that Group.
- In the Enterprise model, Enterprise Trunks exist within an Enterprise and can include Trunk Groups that are within that Enterprise.

20.1 Routing Policies

When the Application Server processes an incoming call that terminates to an Enterprise Trunk User, it applies a routing policy to determine the Trunk Group to which to route the call. The Cisco BroadWorks Application Server supports several routing policies, which are described in this section.

- *Ordered Load Balancing* – This policy is a round-robin policy. The Application Server maintains an ordered list of the Trunk Groups in the Enterprise Trunk and remembers the last Trunk Group it selected for a terminating call. When routing a new terminating call, it selects the next available Trunk Group from the list. It advances in the list in a circular fashion, so that when it reaches the last Trunk Group in the list, it returns to the first Trunk Group. When routing, it considers a Trunk Group unavailable if that Trunk Group has reached its capacity or is found to be unreachable.

  This policy results in a fairly even distribution of terminating calls among all the Trunk Groups in the Enterprise Trunk. However, it does not take into consideration the current load on any Trunk Group, nor does it take into consideration calls originating from the Trunk Groups.

- *Overflow* – For this policy, the Application Server maintains an ordered list of Trunk Groups. When it applies the policy to a new terminating call, it selects the first available Trunk Group in the list. It considers a Trunk Group to be unavailable if that Trunk Group has reached its capacity or is found to be unreachable.

  This policy could be useful for a primary/secondary kind of arrangement, allowing the Application Server to use the secondary Trunk Group both for redundancy and for handling a temporary over-capacity condition of the primary Trunk Group.

- *Most Idle* – When the Application Server applies this policy for a new terminating call, it selects the Trunk Group that has the fewest active calls at the time. If there is a tie between two or more Trunk Groups, then the Application Server picks the Trunk Group that appears first on the list as displayed on the web page.

  This policy spreads the load fairly evenly over all Trunk Groups in the Enterprise Trunk, taking into consideration both incoming and outgoing calls.

- *Least Idle* – When the Application Server applies this policy for a new terminating call, it selects the Trunk Group that has the most active calls at the time. If there is a tie between two or more Trunk Groups, then the Application Server picks the Trunk Group that appears first on the list as displayed on the web page.

- *Weighted Overflow* – When this policy is configured, each constituent Trunk Group is assigned a priority and a weight. The Application Server selects a terminating Trunk Group based on these values. First, it considers all the Trunk Groups together that have the highest priority (for example, all those that have priority *N*). Next, it excludes any Trunk Groups that it considers to be unavailable. Finally, from the remaining Trunk Groups, it makes a random selection, using a probabilistic distribution according to the assigned weights. If a terminating call attempts to the selected Trunk Group fails, which could be because of a capacity-exceeded condition or an unreachable condition, then the Application Server excludes that Trunk Group from the routing policy and executes the policy again. In general, the Application Server tries all Trunk Groups at a priority level higher than *N* before it tries any Trunk Groups at priority level *N*. However, the configuration allows an administrator to limit the number of terminating call attempts at any particular priority level.

NOTE: An administrator can provision a *forwarding* or rerouting policy directly on a Trunk Group as part of that Trunk Group's configuration. Such a configuration is not recommended if that Trunk Group is assigned to an Enterprise Trunk, since it can interfere with the routing policy that is configured for the Enterprise Trunk. An Enterprise Trunk's routing policy can handle a capacity-exceeded or unreachable condition for any of its constituent Trunk Groups. Therefore, a forwarding or rerouting policy on any of the constituent Trunk Groups is unnecessary.

20.2 Enterprise Trunk Attributes

Further configuration of an Enterprise Trunk is possible by setting the value of various attributes, as described here.

- *Enterprise Trunk Name* – This value is the name of the Enterprise Trunk, which must be unique within the Enterprise (Enterprise model) or Group (Service Provider model). The name is used to refer to the Enterprise Trunk in other provisioning web pages.
- *Routing Algorithm* – This value determines the routing policy for terminating calls. If you select the Weighted Overflow policy when the Enterprise Trunk is created, then you cannot change it later to a different policy. Similarly, if you select a policy other than Weighted Overflow, then you cannot change it later to Weighted Overflow.
- *Maximum number of reroute attempts* – This value determines how many Trunk Groups the Application Server can try to route to before it performs the route exhaustion action. For example, if this attribute is set to "3", then the Application Server can try to route to four Trunk Groups, including the initial route attempt, then three reroute attempts. This parameter is useful if the Enterprise Trunk contains many Trunk Groups, since it can force the Application Server to perform the route exhaustion action in a timely manner.
- *Maximum number of reroute attempts within a priority* – (Weighted Routing policy only) This value determines how many Trunk Groups the Application Server can try to terminate to at priority *N* before it tries to terminate to Trunk Groups at priority *N*-1. The attribute can force the Application Server to try Trunk Groups at different priority levels.

- *Route Exhaustion Action* – When the Application Server cannot complete a termination to an Enterprise Trunk User because all Trunk Groups are unreachable or at capacity, it can perform a route exhaustion action. The allowed actions are as follows:
  - *None* – If the action is "*None*", then the Application Server applies the usual *Busy* treatment, which could mean transferring to Voice Mail Deposit, indicating a busy condition to the caller, or executing a user-configured busy action such as Call Forwarding Busy.
  - *Forward* – If the action is "*Forward*", then the Application Server forwards the call to a configured destination.
- *Capacity Management* – The fields in this panel control capacity management for the Enterprise Trunk. The Application Server enforces the capacity limit via license unit usage. For details, see section *4.2 Enterprise Trunk Capacity Management* .
  - *Enable* – If "On" is selected, then capacity management is enabled for this Enterprise Trunk.
  - *Maximum Active Calls Allowed* – The value for this attribute sets the maximum number calls allowed by users assigned to this Enterprise Trunk.
  - *Capacity Exceeded Alarm Initial Value* – The value for this attribute and the value for *Capacity Exceeded Alarm Offset Value* control alarm throttling for a capacity-exceeded condition. If the value of this attribute is set to *N*, then the Application Server sends the first alarm notification only after the condition occurs for the *Nth* time. If the value is "0", then the alarm is disabled.
  - *Capacity Exceeded Alarm Offset Value* – The value for this attribute and the value for *Capacity Exceeded Alarm Initial Value* control alarm throttling for a capacity-exceeded condition. If the value of this attribute is set to *N*, then the Application Server sends the alarm notification every *Nth* time the condition occurs, after it sends the initial alarm notification.

20.3 Enterprise Trunk Configuration Procedure

20.3.1 Create Enterprise Trunk

Before you create an Enterprise Trunk, you must decide if you want to choose the Weighted Overflow Routing policy or one of the other routing policies.

The following steps assume that you want to add the Enterprise Trunk to an Enterprise. This assumption simplifies the explanation. The procedure for adding an Enterprise Trunk to a Group (Service Provider model) is similar to the procedure for an Enterprise; however, you perform it in a Group context.

If you choose the Weighted Overflow Routing policy, then follow these steps to add a new Enterprise Trunk to an Enterprise:

1) From the *Profile* web page for the Enterprise, click the **Services** link in the left navigation menu. This link takes you to the *Services* web page.
2) From the *Services* web page, click the **Enterprise Trunk** link. This link takes you to the *Enterprise Trunk* web page.
3) Click the **Add By Weighted Routing** button.
4) Complete the form and click the **Apply** button. For the attributes that you can enter in the form, see Section 20.2 Enterprise Trunk Attributes.
5) Click the **OK** button to complete the procedure.

The *Add Enterprise Trunk using Weighted Routing* web page for an Enterprise is shown in *Figure 32*.

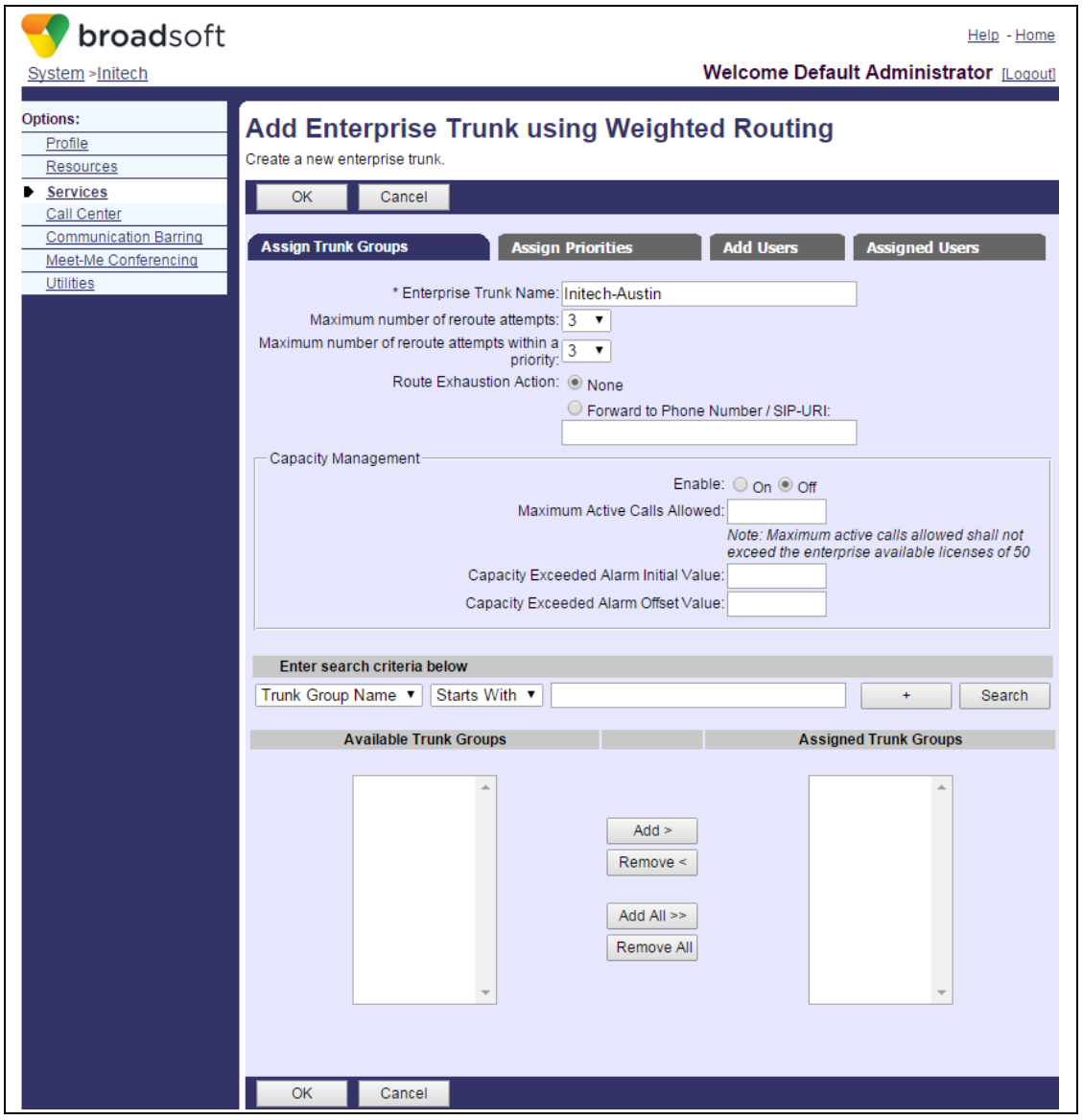

Figure 32 Add Enterprise Trunk using Weighted Routing Web Page for Enterprise

If you choose a routing policy other than Weighted Overflow, then follow these steps to add a new Enterprise Trunk to an Enterprise:

1) From the *Profile* web page for the Enterprise, click the **Services** link in the left navigation menu. This link takes you to the *Services* web page.
2) From the *Services* web page, click the **Enterprise Trunk** link. This link takes you to the *Enterprise Trunk* web page.
3) Click the **Add By Ordered Routing** button.
4) Complete the form and click the **Apply** button. For the attributes that you can enter in the form, see section *20.2 Enterprise Trunk Attributes*.
5) Click the **OK** button to complete the procedure.

The *Add Enterprise Trunk Using Ordered Routing* web page for an Enterprise is shown in *Figure 33*.

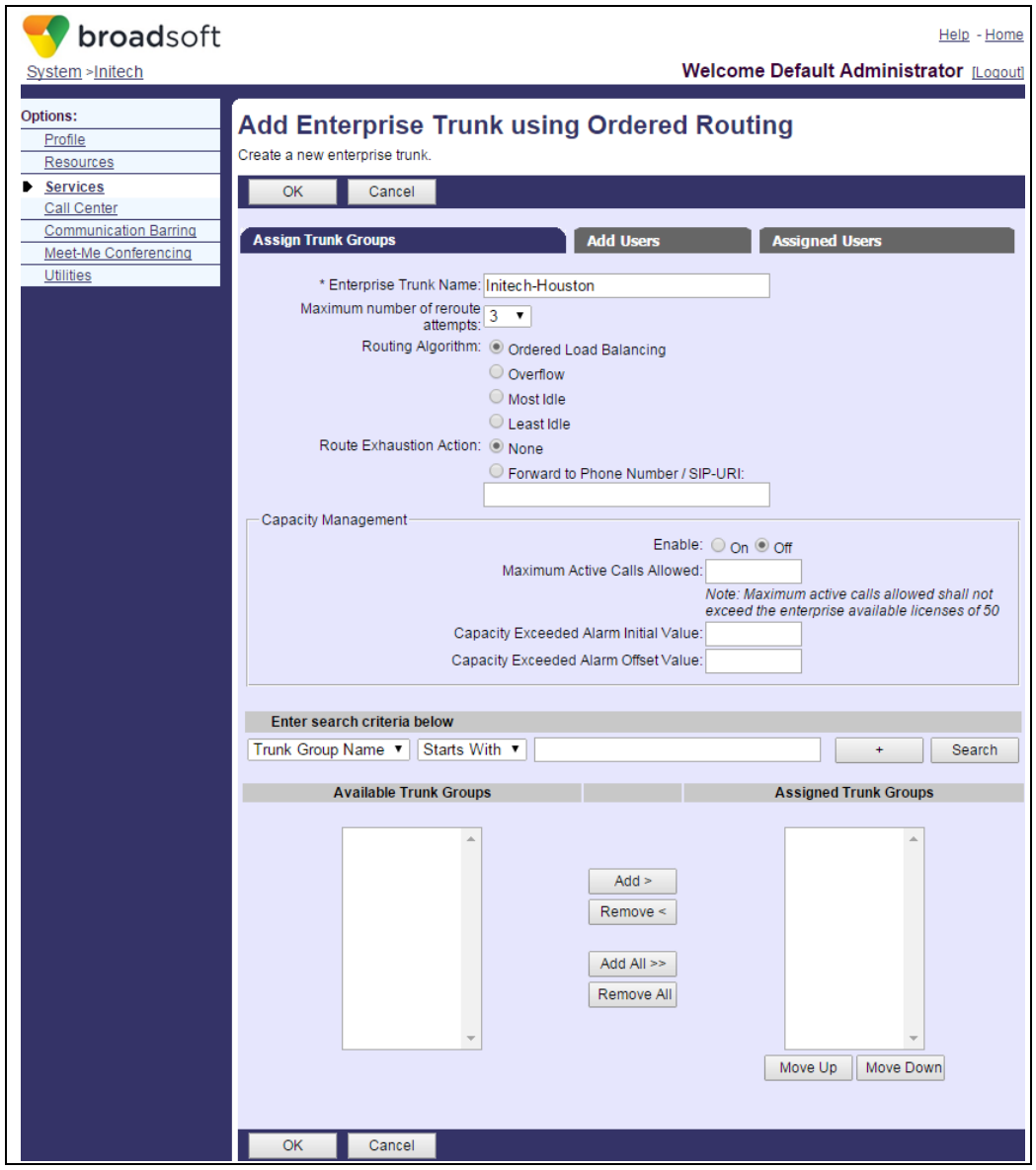

Figure 33 Add Enterprise Trunk using Ordered Routing Web Page for Enterprise

20.3.2 Add Trunk Groups

When you configure an Enterprise Trunk, you must add to it all the Trunk Groups to which the Enterprise Trunk can route.

A Trunk Group must meet certain criteria before you can add it to an Enterprise Trunk:

- If the Enterprise Trunk is assigned to an Enterprise, then the Trunk Group must be in that Enterprise.
- If the Enterprise Trunk is assigned to a Group (Service Provider model), then the Trunk Group must be in that Group.

- The Trunk Group must have an Identity/Device Profile assigned and it must have a Pilot User assigned.

To add one or more Trunk Groups to an Enterprise Trunk, follow these steps:

1) If the Enterprise Trunk is assigned to an Enterprise, go to the *Profile* page for that Enterprise. If the Enterprise Trunk is assigned to a Group, go to the *Profile* page for that Group.
2) From the left navigation menu, click the **Services** link. This link takes you to the *Services* page for the Enterprise or Group.
3) From the *Services* page, click the **Enterprise Trunk** link. This link takes you to the *Enterprise Trunk* page for the Enterprise or Group.
4) From the *Enterprise Trunk* page, click the **Edit** link next to the Enterprise Trunk to which you want to add Trunk Groups. This link takes you to the *Modify Enterprise Trunk* web page. The *Assign Trunk Groups* tab should be the current tab. If it is not, then click the link in the tab.
5) Enter search criteria and click the **Search** button. This action causes the web page to fill the list box labeled *Available Trunk Groups* with all available Trunk Groups that match the search criteria.
6) Select the Trunk Group you want to add and click the **Add** button. Repeat this step for all Trunk Groups you want to add. Click the **OK** or **Apply** button to save the changes.
7) If the Enterprise Trunk uses weighted routing, then you must perform an additional step to assign weights and priorities to the Trunk Groups. To do this, click the link in the *Assign Priorities* tab in the *Enterprise Trunk Modify* web page. This link takes you to the *Assign Trunk Group Priorities* web page. On this page, enter the weights and priorities for each Trunk Group and click the **OK** or **Apply** button to save the changes.

The *Modify Enterprise Trunk using Weighted Routing* web page is shown in *Figure 34*.

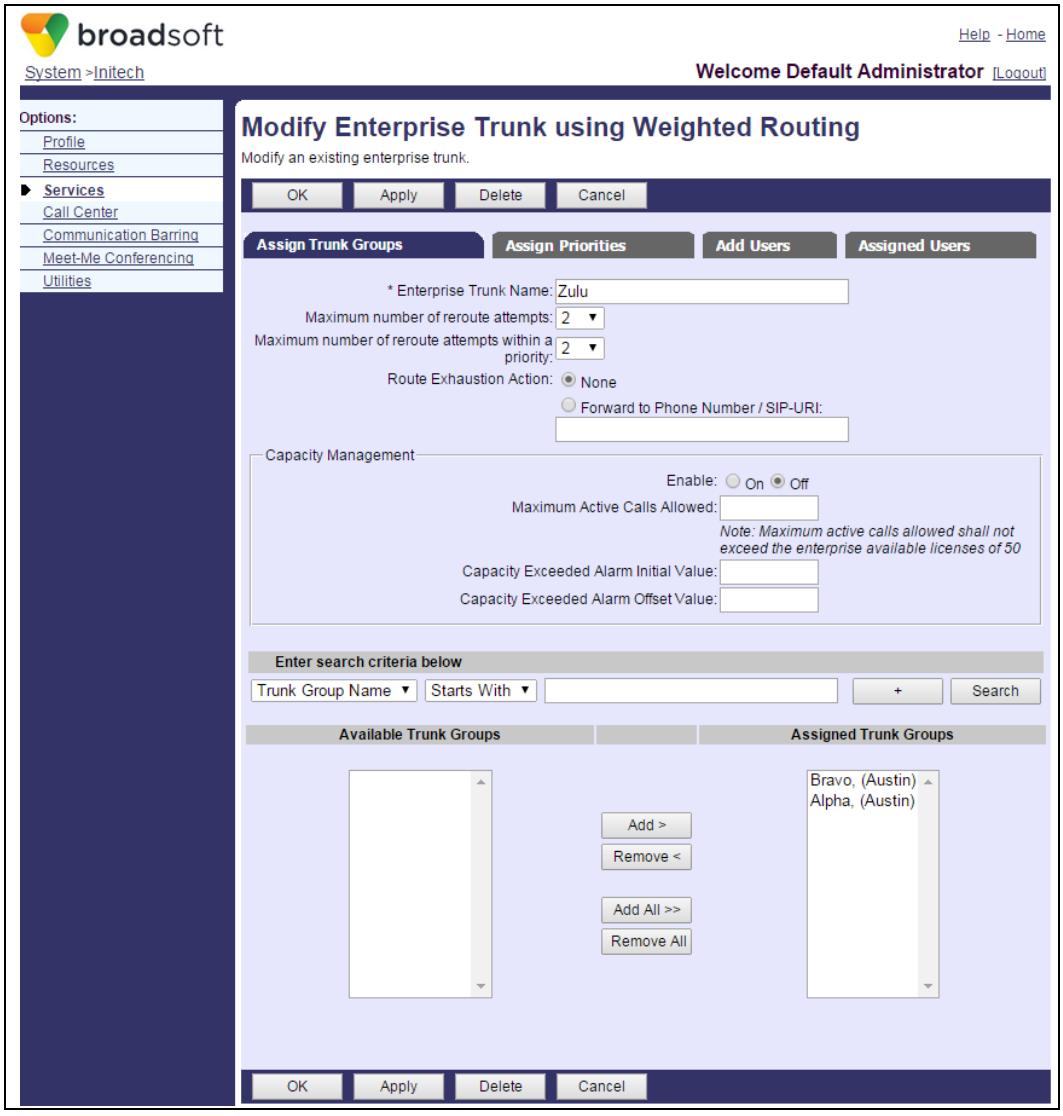

Figure 34 Modify Enterprise Trunk using Weighted Routing Web Page

The *Assign Trunk Group Priorities* web page is shown in *Figure 35*.

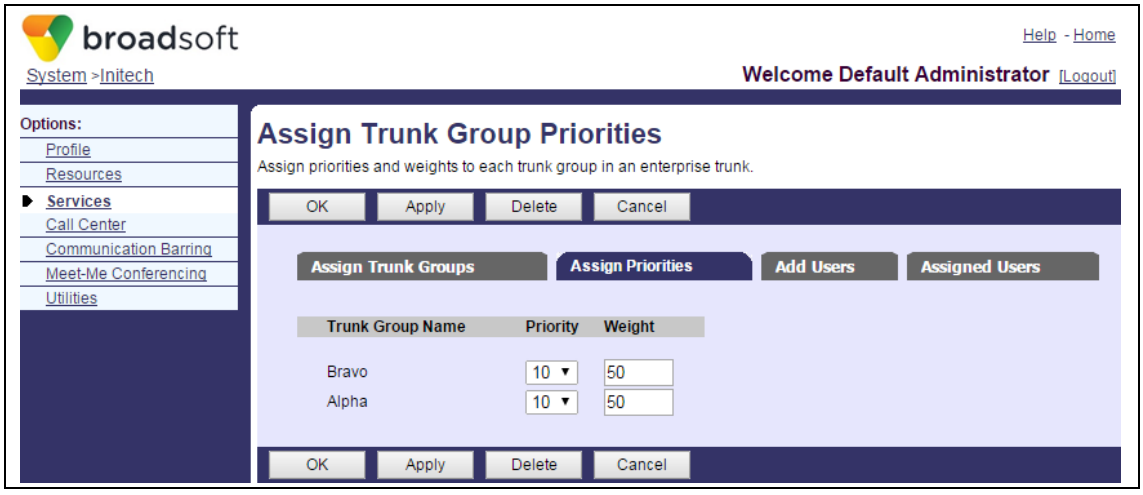

Figure 35 Assign Trunk Group Priorities Web Page

21 Business Trunking User Configuration

21.1 Business Trunking User Configuration

21.1.1 Business Trunking User Configuration

Assignment to trunk group – A business trunking user can be assigned to a specific Trunk Group. However, when Enterprise Trunking is in use, it is not a usual configuration to assign a business trunking, other than a Pilot User, user to a Trunk Group. Such a configuration could interfere with terminating calls to the user, particularly if the user has a SIP registration contact or a static contact. If it is expected that a business trunking user can make or receive calls over more than one Trunk Group, then the user should not be assigned to a specific Trunk Group.

Assignment to Enterprise Trunk – A business trunking user can be assigned to an Enterprise Trunk. This is the normal configuration for a business trunking user who can make or receive calls over more than one Trunk Group. The assignment of a user to an Enterprise Trunk means that when the Application Server receives a terminating call attempt for that user, it applies the routing policy for the Enterprise Trunk to select a Trunk Group for the termination.

It is allowed to provision a business trunking user who is not assigned to a Trunk Group or an Enterprise Trunk. Such a user can have a service profile and be able to place calls, but cannot receive any calls.

Line/Port (Stand-alone only) – A business trunking user who is not assigned to a specific Trunk Group cannot have a Line/Port. Therefore, as mentioned above, it is not a usual configuration for a business trunking user to have a Line/Port when Enterprise Trunking is in use.

SIP Public User Identity (IMS only) – A business trunking user who is not assigned to a specific Trunk Group cannot have a primary SIP Public User Identity. Therefore, as mentioned above, it is not a usual configuration for a business trunking user to have a primary SIP Public User Identity when Enterprise Trunking is in use.

Alternate trunk identity – The Alternate Trunk Identity is a private, access-side address that the Application Server and Trunk Group device can use on their shared SIP interface. The Trunk Group device can use the Alternate Trunk Identity in INVITE requests it sends to the Application Server for originating calls or redirected calls, and the Application Server can identify the originating or redirecting user from the Alternate Trunk Identity. Similarly, the Application Server can use the Alternate Trunk Identity in the INVITE requests it sends to the Trunk Group device for terminating calls, and the Trunk Group device can identify the terminating user from the Alternate Trunk Identity. In either case, the Alternate Trunk Identity appears as the user part of a SIP URI. The Alternate Trunk Identity can have any form that is allowed in the user part of a SIP URI. The Application Server does not parse the Alternate Trunk Identity, except that if the Alternate Trunk Identity is all digits, then the Application Server adds a user=phone parameter to the URI in the terminating INVITE request to identify the user part as a phone number.

Static contact – Depending on the particular Trunk Group device, the Static Contact field may or may not have a value. (The field is present in the provisioning web page only if the Identity/Device Profile Type supports it.) If the device has no active SIP registration, then the Application Server uses the static contact SIP URI as it would a SIP registration Contact URI.

SIP registration – In one common configuration, the Trunk Group device registers with a single SIP registration. (The field is present in the provisioning web page only if the Identity/Device Profile Type supports it.) In Cisco BroadWorks, this registration should be associated with the Pilot User for the Trunk Group. When the Trunk Group has an active registration, that is, when the Trunk Group's Pilot User has an active registration, then the Application Server uses the registered contact URI for terminations to that Trunk Group.

Phone number – The Application Server allows a business trunking user to have a phone number configured. This phone number, also referred to as a "Directory Number" is a DID number for the user. If the user is a member of an Enterprise Trunk, and if the user does not have an Alternate Trunk Identity configured, then the Application Server uses the user's phone number as the terminating address for terminating calls to that user.

Extension – A business trunking user can have an extension, which allows other users in the same Group or Enterprise to call that user via extension dialing. The extension is not exposed outside the Group or Enterprise.

Physical Location – A Trunking User's Physical Location configured against the user's trunking address. This user-assigned physical location has priority over a device-assigned physical location and applies to outgoing calls from a trunk group.

21.1.2 Business Trunking User Configuration Procedure

For the procedure to provision a Cisco BroadWorks user, see the *Cisco BroadWorks Application Server Group Web Interface Administration Guide – Part 1* [6]. The following procedure assumes that the user is already provisioned in Cisco BroadWorks and explains how to configure that user as a business trunking user.

To configure an existing Cisco BroadWorks user as a business trunking user, follow these steps:

1) From the *Profile* web page for the user, click the **Addresses** link. This link takes you to the *Addresses* web page for the user.
2) On the *Addresses* web page, select the "Trunking" button.
3) To add this user to an Enterprise Trunk, select the Enterprise Trunk from the drop-down list next to the *Enterprise Trunk* label. The user must be in the same Enterprise or Group as the Enterprise Trunk. If the user is already assigned to an Enterprise Trunk, you can unassign the user by selecting "None" from the drop-down list.
4) Optionally, add an Alternate Trunk Identity.
5) To assign this user to a Trunk Group, select the Trunk Group from the drop-down list next to the Trunk Group label. The user must be in the same Group as the Trunk Group. If the user is already assigned to a Trunk Group, you can unassign the user by selecting "None" from the drop-down list.
6) Optionally, assign a physical location descriptor for the user.

NOTE: If the user is assigned to an Enterprise Trunk, then it is not recommended to also add that user to a Trunk Group unless the user is the Trunk Group's Pilot User.

7) Click the **Apply** or **OK** button to save the changes.

The *Addresses* web page for a user is shown in *Figure 36*.

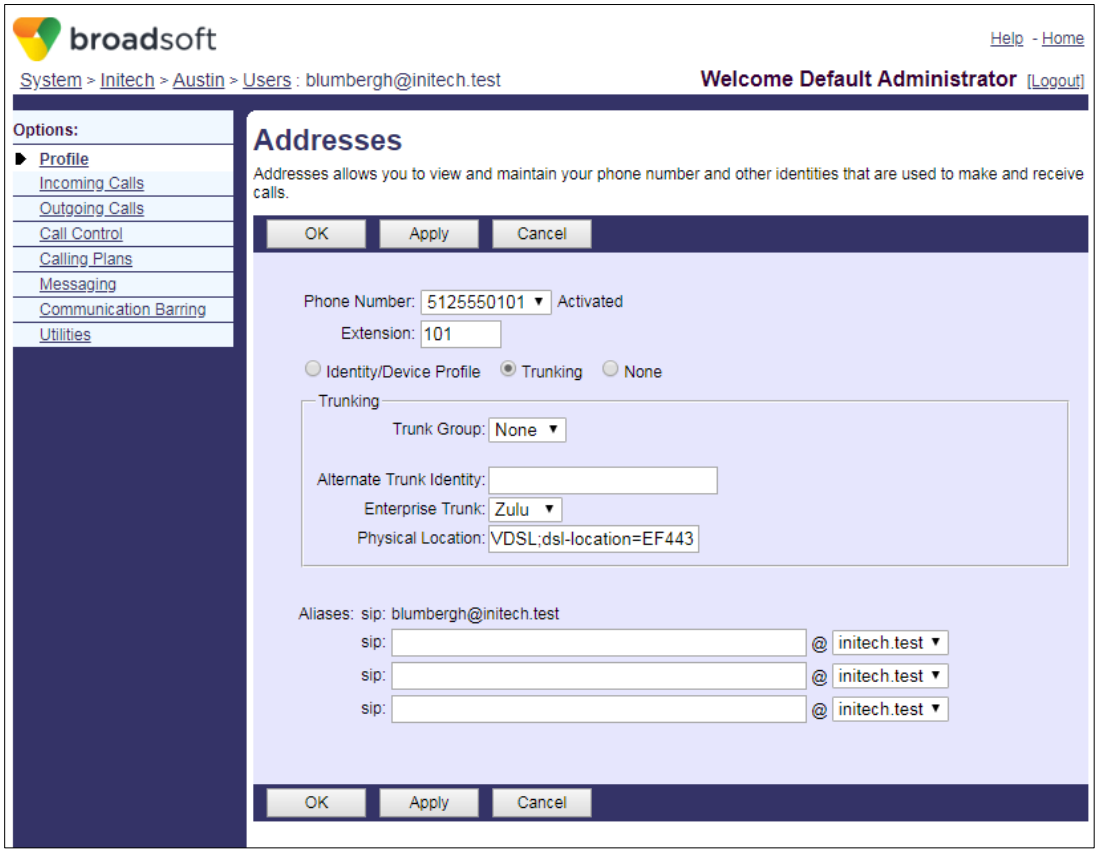

Figure 36 Addresses Web Page for User

21.1.3 Pilot User Configuration Procedure

The following steps describe how to assign the Pilot User.

1) Navigate to the main profile page of the Trunk Group.
2) Click the **Profile** link.
3) Enter (search) the search criteria to find the Trunk Group user who is selected as the Pilot User, and click the Search button.
4) Click the check box next to the Trunk Group user you want to assign as the Pilot User.
5) Click **Apply** or **OK**.

Figure 37 shows the *Trunk Group Modify* web portal page with a Pilot User selected.

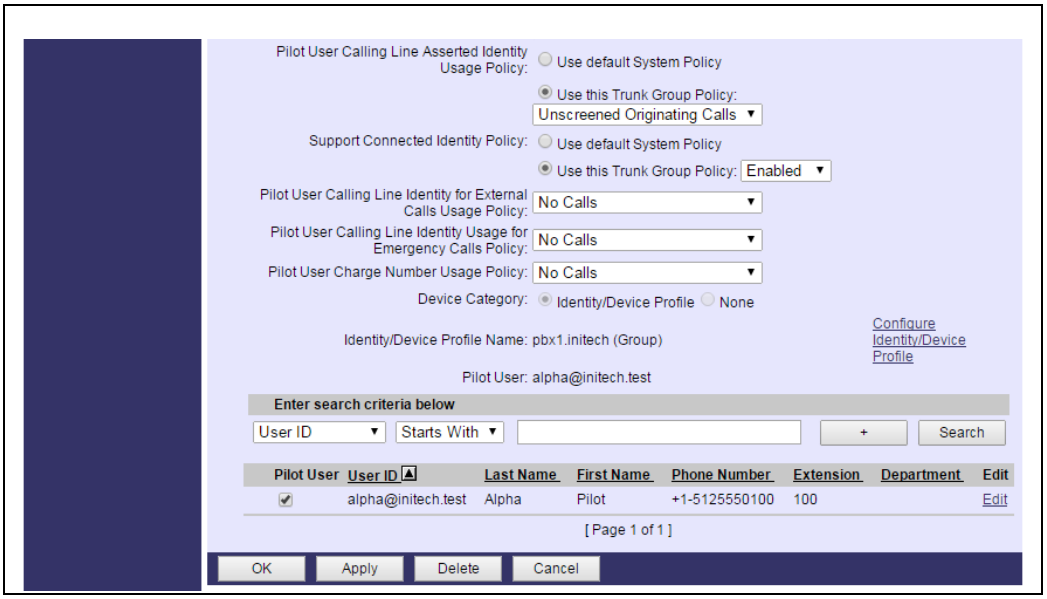

Figure 37 Trunk Group Modify Web Portal Page with Pilot User Selected

21.2 Hosted PBX User Configuration

21.2.1 Overview

The Application Server allows a regular Cisco BroadWorks user to be configured as a Hosted PBX User, that is, a regular user for whom originating and terminating calls are counted against the capacity of a particular Trunk Group. Such a user uses a regular user license at provisioning time, and additionally uses a BTLU when originating or terminating a call. A typical use for a Hosted PBX User is a fax machine that is plugged into the FXS port of a Trunk Group device.

An origination from a Hosted PBX User or a termination to a Hosted PBX User is otherwise identical to an origination or termination for any other regular Cisco BroadWorks user. Specifically, the Application Server does not apply an Enterprise Trunking routing policy for a terminating call, and it does not allow an originating call over a Trunk Group. Because an originating call over a Trunk Group is not allowed, the Application Server does not apply the Pilot User's CLID or charge number for an origination. Any terminating or originating call must use that user's own device and Line/Port.

The actions configured for the Trunk Group for handling capacity-exceeded or unreachable conditions do not apply to a Hosted PBX User. If an originating call from a Hosted PBX User causes a capacity-exceeded condition, then the Application Server blocks that call. If a terminating call to a Hosted PBX User causes a capacity-exceeded condition, then the Application Server applies a *Busy* treatment. The Application Server does not reroute or forward the call. Similarly, if a terminating call to a Hosted PBX User results in an unreachable condition, then the Application Server treats this as an unreachable condition to a regular user's device and not as an unreachable condition to a Trunk Group device.

To add a Cisco BroadWorks user to a Trunk Group as a Hosted PBX User, that user must be a regular (non-business-trunking) user in the same Group as the Trunk Group, must not already be assigned as a Hosted PBX User for another Trunk Group, and must not be a member of a capacity group.

21.2.2 Hosted PBX User Configuration Procedure

The following steps describe how to associate a Cisco BroadWorks user with a Trunk Group as a Hosted PBX User:

1) Navigate to the main profile page of the Trunk Group.
2) Click the **Capacity Management** link.
3) Enter (search) the search criteria to find the Cisco BroadWorks user who is associated with the Trunk Group capacity management as a hosted user.
4) Select one or more users from the list. Click the **Add** button. (Alternatively, click the **Add All** button to add all the users on the list.)
5) Click **Apply** or **OK**.

Figure 38 shows a section of the *Capacity Management* web page with a Hosted PBX User assigned.

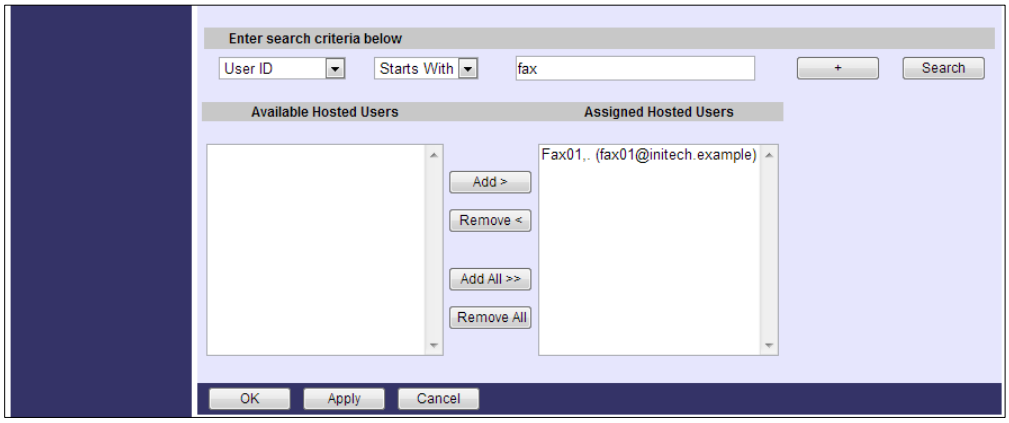

Figure 38 Capacity Management Web Portal Page with Hosted PBX User Assigned

22 Appendix A – Case Studies

To demonstrate the SIP trunking concepts and the specific Cisco BroadWorks SIP trunking features described earlier, this appendix develops use cases for two SIP Trunking deployment scenarios. The two deployment scenarios are based on the "TDM PBX with IAD" and "IP PBX" reference architectures, respectively. As with the reference architectures, real-world deployments are expected to be quite diverse and it is not practical to describe the full suite of the Cisco BroadWorks capabilities/features against all possible PBX deployment models. However, the two scenarios were selected to provide a framework to allow the capabilities of the Cisco BroadWorks SIP Trunking solution to be extracted and applied to different deployment models.

In addition to general SIP trunking concepts and specific Cisco BroadWorks SIP Trunking capabilities, the deployment scenarios also show how the Cisco' broader portfolio (BroadWorks Hosted PBX/Call Center, UC-One, and BroadCloud) can be used to differentiate your SIP Trunk solution and increase Average Revenue Per Unit (ARPU) associated with a SIP Trunk.

22.1 Scenario 1: Employee/Business Efficiency and Cost Reduction

In this scenario, a Small Medium Business (SMB), A1 Construction, is currently reviewing their communication infrastructure for cost reduction opportunities, as well as ways to increase overall efficiency. While their business is currently housed in a single site, recent contract wins in neighboring states are forcing A1 to consider opening additional facilities. The existing telecommunication infrastructure is based on a traditional TDM PBX, servicing 58 office employees. In addition to the 58 office employees, A1 has roughly 350 field employees. A1 offers a cell phone reimbursement policy for key office and field employees. A1 uses a single service provider for PSTN access (single PRI), cell phones, and Internet access.

As a SMB, A1 did not maintain a dedicated telecom staff and solicited both their existing PBX vendor and service providers for proposals. Based principally on up-front capital expenditures associated with the PBX vendor's options (full replacement of the TDM PBX or UC overlay), as well as desire not to lock into a single solution before a decision was made about an additional site, A1 has decided to go with their service provider's proposal.

The key value propositions offered by the service provider's SIP Trunking solution included:

- Cost reduction/avoidance:
  - Capacity offered on a per trunk basis with a fixed price (no requirement to purchase a full PRI)
  - Converged access (voice and data) on common access, optimizing bandwidth utilization
  - Cost control or reduced overhead in managing cell phone reimbursements
  - No up-front capital expenditures that is, keep existing PBX and desk phones
  - Flexibility associated with adding new site(s) – Hosted or Customer Premises Equipment (CPE)
- Enterprise/employee efficiency:
  - Self-provisioning (moves, adds, changes)
  - Overlay Services

- Auto Attendant
- MobileLink Client

- Reliability:
  - Business Continuity at user level
  - Carrier-grade reliability, that is, greater than five nines

To achieve the outlined value propositions, the service provider migrates A1 Construction's network as shown in *Figure 39*. The Cisco BroadWorks platform provides the basis for the connectivity and services to achieve the cost reduction/avoidance, enterprise/employee efficiencies, and reliability within their offering. The IAD, or business gateway, selected by the service provider provided the security functionality associated with a session border controller, as well as aggregating multiple channels of information including voice and data across a single shared access link.

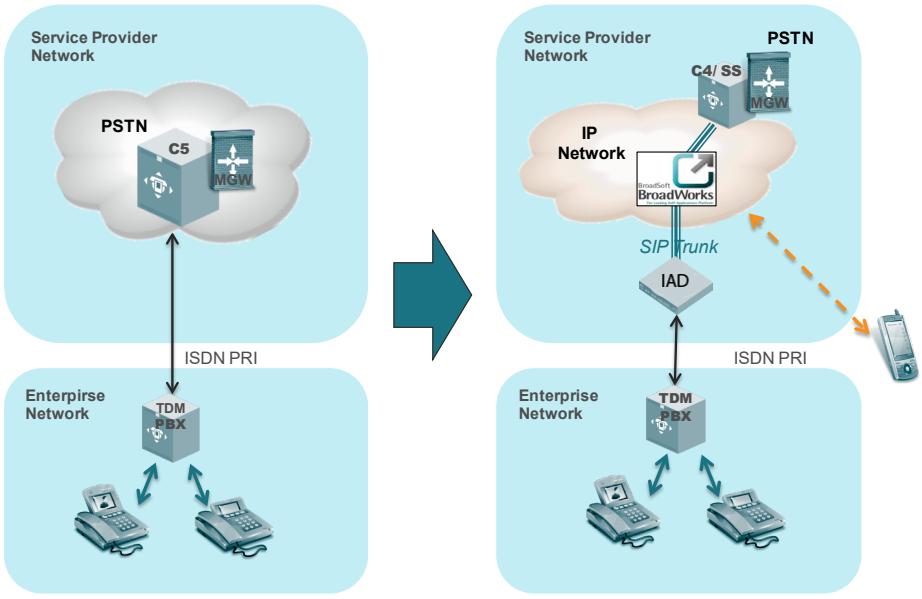

Figure 39 A1 Construction Network Migration

As an initial starting point for provisioning within Cisco BroadWorks, the service provider proposed the creation of three groups within an enterprise (A1Const). The groups would be built around the user types, and include a group for office personnel (A1ConstOffice), field personnel (A1ConstField) and a separate group for the Pilot User and associated trunk group (A1ConstTrunk). Cisco BroadWorks does not require a separate group to be established for the Pilot User/Trunk Group, however since the service provider also uses the Enterprise Trunking model business trunk users and trunk groups are not required to be in the same group, only the same enterprise. The only exception is the Pilot User, who is assigned to the Trunk Group and both the Trunk Group and Pilot User must be assigned to the same group.

Figure 40 shows the relationship of the groups within the enterprise.

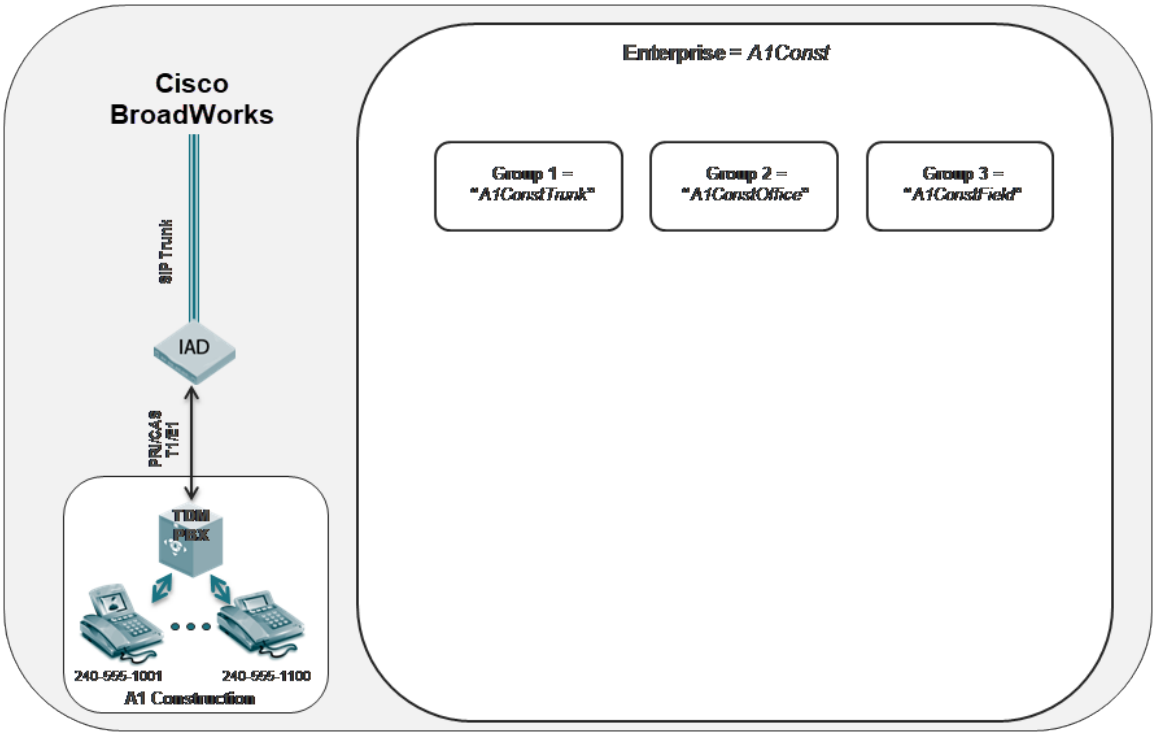

Figure 40 A1 Construction Group Structure

To implement the capacity management functionality of the SIP Trunking offering, the service provider leverages the Enterprise Trunking functionality and provisions an Enterprise Trunk (A1ConstEnttrk1) within the Cisco BroadWorks A1 Construction enterprise. Although the use of Enterprise Trunking is not required, the service provider has adopted the best practice of always deploying an Enterprise Trunking model, even if only one trunk group is required to meet the enterprise's requirements. Defaulting to the Enterprise Trunking model has the following benefits:

- Provides the greatest flexibility in achieving business continuity capability through the support of the five Enterprise Trunking routing policies.
- Reduces the cost of implementation by simplifying the service providers' internal provisioning system(s) and personnel training since a single deployment model can address all enterprise network configurations.
- Improves operational efficiency and customer satisfaction associated with the addition or removal of trunk groups as the enterprise's requirements change.

In this particular example, the service provider also positioned this as a selling point within their proposal, specifically showing how additional trunk groups could be added within the Enterprise Trunking model without impacting existing service if or when A1 Construction decided to expand the number of sites.

To establish the trunk group capacity to support the Service Level Agreement (SLA), the service provider used historical trunk utilization as a basis for the number of trunk groups to be provisioned.

Assuming the historical data shows a peak usage at ten trunks, with typical usage <8 trunks, the service provider would provision the number of business trunking licenses (maximum number of trunking simultaneous calls) for the A1 Construction enterprise to be 10. Additionally the service provider would provision two trunk groups with Total Calls = 10. Incoming and Outgoing Calls are set to 10, allowing full usage of the trunks for either inbound (to PBX) or outbound (from PBX) calls.

The trunk group (A1ConstTG1) is provisioned and assigned to the Enterprise Trunk (A1ConstEnttrk1). Although there is a single trunk group at this point and all incoming calls are routed against this trunk group, the routing policy for the Enterprise Trunk is set to "Weighted". Weighted routing policy was selected as it provides the most flexibility in structuring routes, and simplifies the addition of new trunk groups going forward. *Figure 41* shows the relationship of the Enterprise Trunk and Trunk Group within the Enterprise and Group structure.

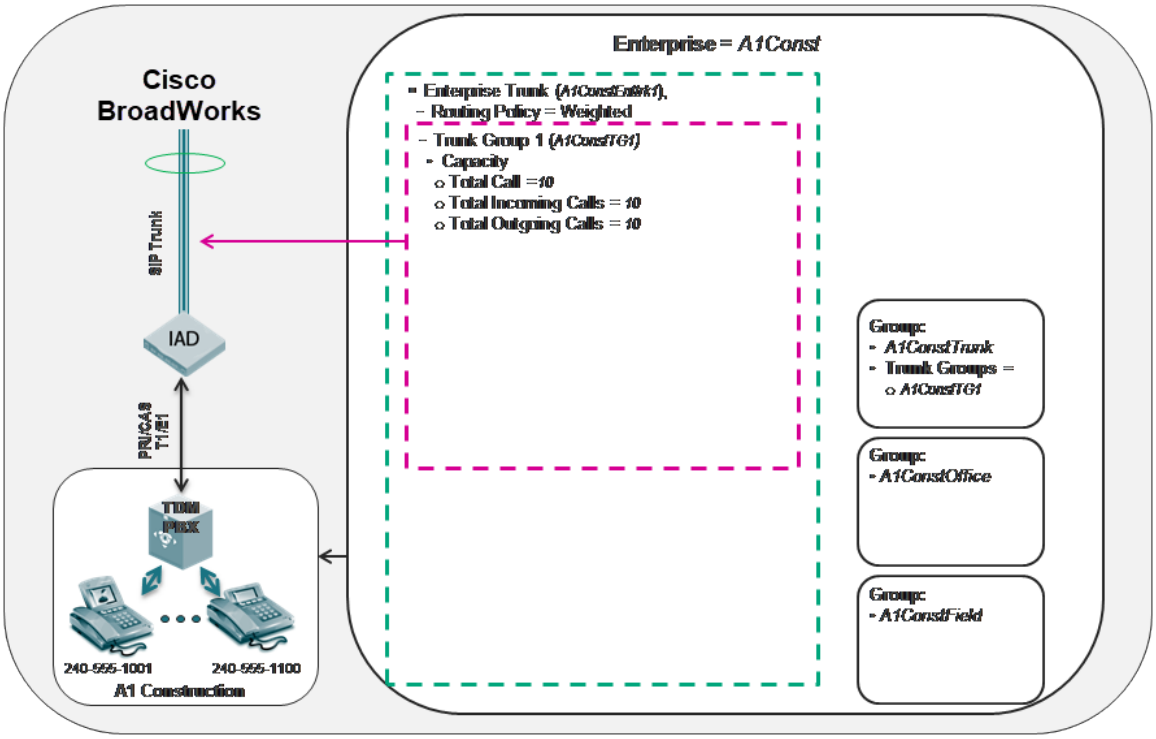

Figure 41 Enterprise Trunk to Trunk Group Mapping

In addition to the capacity management attributes associated with the trunk group, the service provider completes the provisioning process associated with the trunk group. This includes assigning a Pilot User and an Identity/Device Profile, as well as key attributes to support the TDM CPE configuration. For A1, this includes the following:

- Pilot User – As all trunk groups require a Pilot User, the service provider assigns the main number of the TDM switch to a user (Main User), and assigns this user to be the Pilot User for the trunk group (A1ConstTG1).

- Registration method – In this case, the IAD registers using the main number of the TDM PBX (240-555-1000) and all PBX users are associated with the main line registration. Therefore, the individual users (240-555-1000 through 1100) do not register separately. The service provider implements this by setting or validating the Trunk Mode = "Pilot" within the Identity/Device Profile associated with the Trunk Group. The Identity/Device Profile must be assigned to the trunk group (A1ConstTG1). The service provider has named the Identity/Device profile as "A1ConstIAD1".
- Authentication – For security purposes, the service provider has elected to enable authentication for registrations, by enabling authentication on the trunk group (A1ConstTG1), as well as the Identity/Device Profile (A1ConstIAD1). This includes defining both the authentication user name (A1ConstTG1un) and password (A1ConstITG1pswd).

Figure 42 shows the relationship of the Identity/Device Profile to the trunk group and pilot use to the trunk group and group.

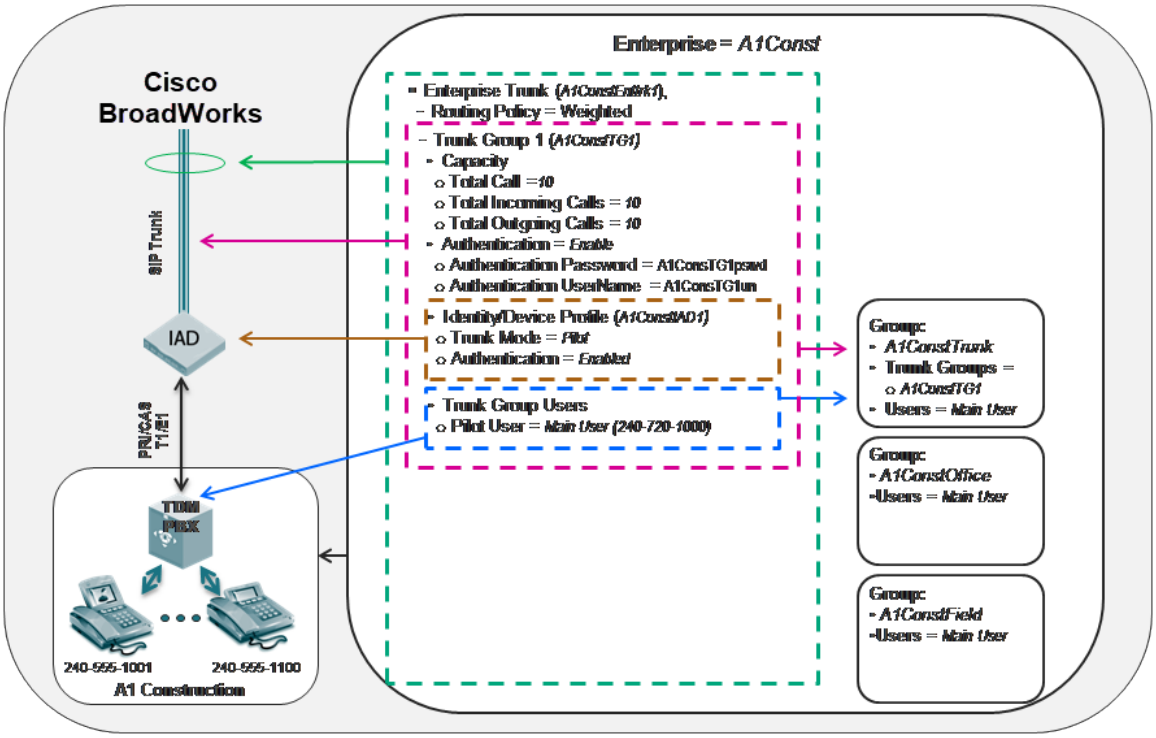

Figure 42 Identity/Device Profile Mapping

As noted above, the service provider leverages Enterprise Trunking for all deployments, therefore all users are assigned to the Enterprise Trunk, with the exception of the Pilot User. In this case, it includes all users associated with Group 2 (Office Personnel) and Group 3 (Field Personnel).

Figure 43 shows the relationship of the user (non-pilot) to the Enterprise Trunk and group.

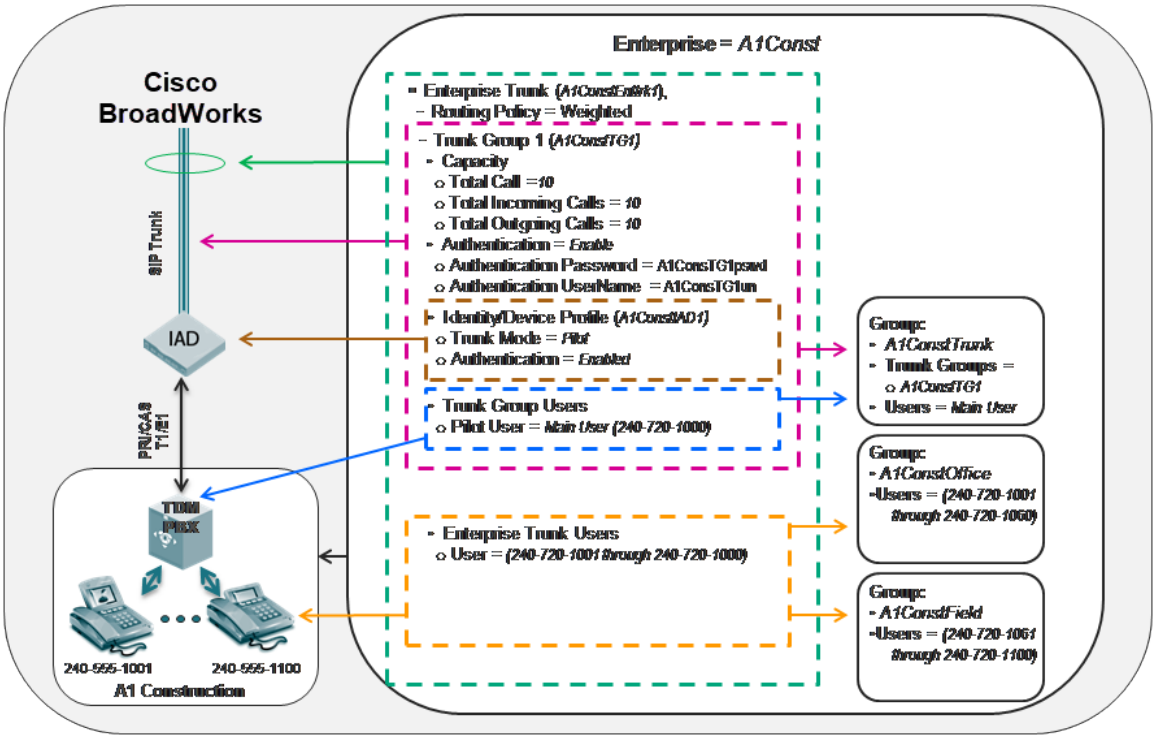

Figure 43 Business Trunk User Mapping

Part of the value proposition was to make sure A1 Construction had administrative capabilities, which allowed them to manage moves, adds, and changes associated with the services provided. To facilitate this, the service provider established an enterprise administrator account within Cisco BroadWorks linked to the Enterprise ID (A1Const) account. The enterprise administrator can execute tasks that affect all groups, one group, and/or user-related tasks for an Enterprise ID account and for capabilities. These tasks are executed via a web interfaces and include, but are not limited, to:

- Add and provision groups (and the initial group administrator for the group)
- Add and delete devices and service packs
- For existing groups, assign and authorize resources for which only an enterprise administrator has the authority, for example:
  - View, add, delete or modify Enterprise Trunks
  - View, modify, or delete Enterprise Trunk Users
  - View, add, delete or modify Trunk Groups
  - View, add, delete or modify Identity/Device Profiles
  - Configure Trunking Call Capacity
  - Assign service packs
  - Assign phone numbers
  - Authorize services

For a complete description of an Enterprise Administrator's roles and responsibilities, see the *Cisco BroadWorks Application Server Enterprise Web Interface Administration Guide* [7] and the *Cisco BroadWorks Application Server Group Web Interface Administration Guide – Part 1* [6].

In addition to creating the enterprise administrator account, the service provider's system administrators authorized the required services to support the SLA. Included within these services was Call Forwarding Not Reachable (CFNR) functionality used to support business continuity at the user level, BroadWorks Mobility to support the MobileLink Client functionality, and Auto Attendant to support the auto attendant functionality. By authorizing the CFNR functionality, A1 Construction's enterprise administrator can assign the service to specific, or all personnel ensuring in the event of catastrophic failure associated with the TDM PBX and/or the service provider connection calls are not missed.

To address both employee accessibility/efficiency, the service provider has leveraged the BroadWorks MobileLink client within the offering. With the MobileLink solution, A1 Construction benefits from increased control coupled with ease of use, by deploying the familiar "apps on a Smartphone". Since the MobileLink application allows the user to optionally select and display the business number for outbound calls, whether direct dial or click-to-dial, and texting, and then A1 can now structure their reimbursement policy for only those calls made using the business number. Another benefit is the automatic call back feature, which alleviates roaming charges when users are travelling outside of their calling area.

The final element of the service provider's value proposition enabled by Cisco BroadWorks is the deployment of an auto attendant. With the Cisco BroadWorks Automated Attendant, A1 is able to make sure callers receive a professional and consistent greeting and routing options that allow them to reach the correct destination, improving efficiency and customer satisfaction.

22.2 Scenario 2: Network Collapse Reduction

In this scenario, an Internet Service Provider (ISP), National ISP, has been retained by a national retailer, BigBox, to optimize their SIP Trunking service in support of BigBox's network collapse. In this phase of the project, BigBox has established four regional hubs all with inter-enterprise connectivity. Three of the four hubs are connected via BigBox's internal WAN network. At present, the fourth is not connected to the enterprise WAN. The following figure shows the current network topology.

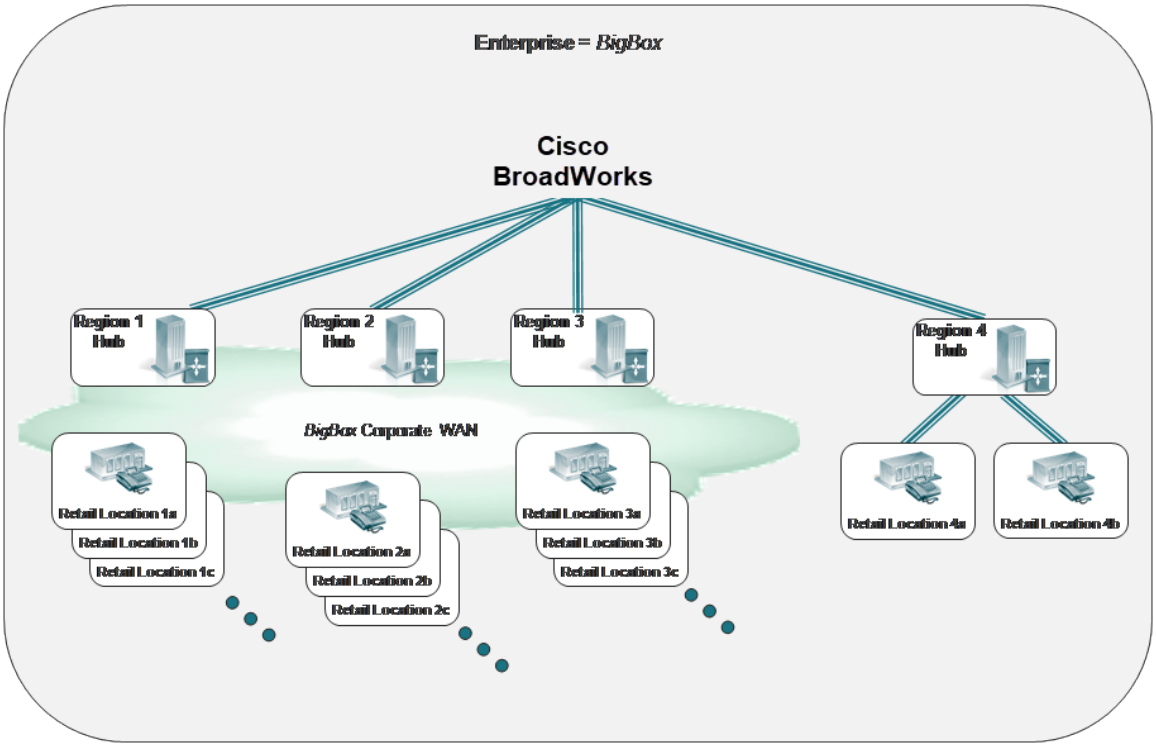

Figure 44 BigBox Network Topology

Based on the number of retail locations and bandwidth/proximity of the different hubs to retail locations, BigBox has requested different redundancy and load-balancing strategies associated with the hubs connected to the corporate WAN. To support these different strategies, National ISP has created Enterprise Trunks with the assigned Enterprise Trunk Users aligned by locations. This has resulted in three Enterprise Trunks with user assignment based on proximity of the retail location to the Hub, that is, retail location 1 users being assigned to the first Enterprise Trunk (Region1EntTrk), retail location 2 users being assigned to second Enterprise Trunk (Region2EntTrk), and retail location 3 users being assigned to a third Enterprise Trunk (Region3EntTrk).

Additionally, for retail locations reachable via Hub 4, the ISP has adopted the best practice of always deploying an Enterprise Trunking model. Therefore two additional enterprise trunks have been created, with the users in retail location 4a in one Enterprise Trunk (Region4aEntTrk) and the users in retail location 4b in another Enterprise Trunk (Region4bEntTrk).

For Region 1 and Region 2, the ISP has implemented an identical redundancy strategy. Leveraging the “Overflow” Enterprise Trunk routing policy the ISP assigns the same two trunk groups (Region1TrkGrp and Region2TrkGrp) to both enterprise trunks. However, the order in which the trunk groups have been provisioned within the Enterprise Trunk has been reversed. That is, for the Enterprise Trunk associated with retail location 1 users (Region1EntTrk), the trunk groups have been provisioned with Region1TrkGrp entered first and then Region2TrkGrp. Since the routing policy is set as “Overflow” this makes sure the first trunk group attempted for termination is Region1TrkGrp. Only in an unreachable or over-capacity scenario is Region2TrkGrp attempted.

For the Enterprise Trunk associated with retail location 2 users (Region2EntTrk), the trunk groups have been provisioned with Region2TrkGrp first and then Region1TrkGrp. Since the routing policy is set as “Overflow” this makes sure the first trunk group attempted for termination is Region2TrkGrp. Only if an unreachable or over-capacity scenario occurs is Region1TrkGrp attempted.

Since it is possible for outbound (PBX to PSTN) calls for retail locations to use any Regional Hub (that is, outbound calls from Retail Locations 1 can be routed via Region 2 Hub), the ISP has also enabled the ability to allow unscreened calls.

Additionally, for trunk group identification, both the ISP and BigBox have opted to include *tgrp/tgrp* context within the SIP signaling. For outbound calls (BigBox to ISP), the SBC located at the Regional Hub inserts the *tgrp/tgrp* context and for inbound (ISP to BigBox), Cisco BroadWorks insert the *tgrp/tgrp* context into the SIP signaling.

The structure of the Enterprise Trunk and associated trunk groups in shown in *Figure 45* and *Figure 46*, respectively.

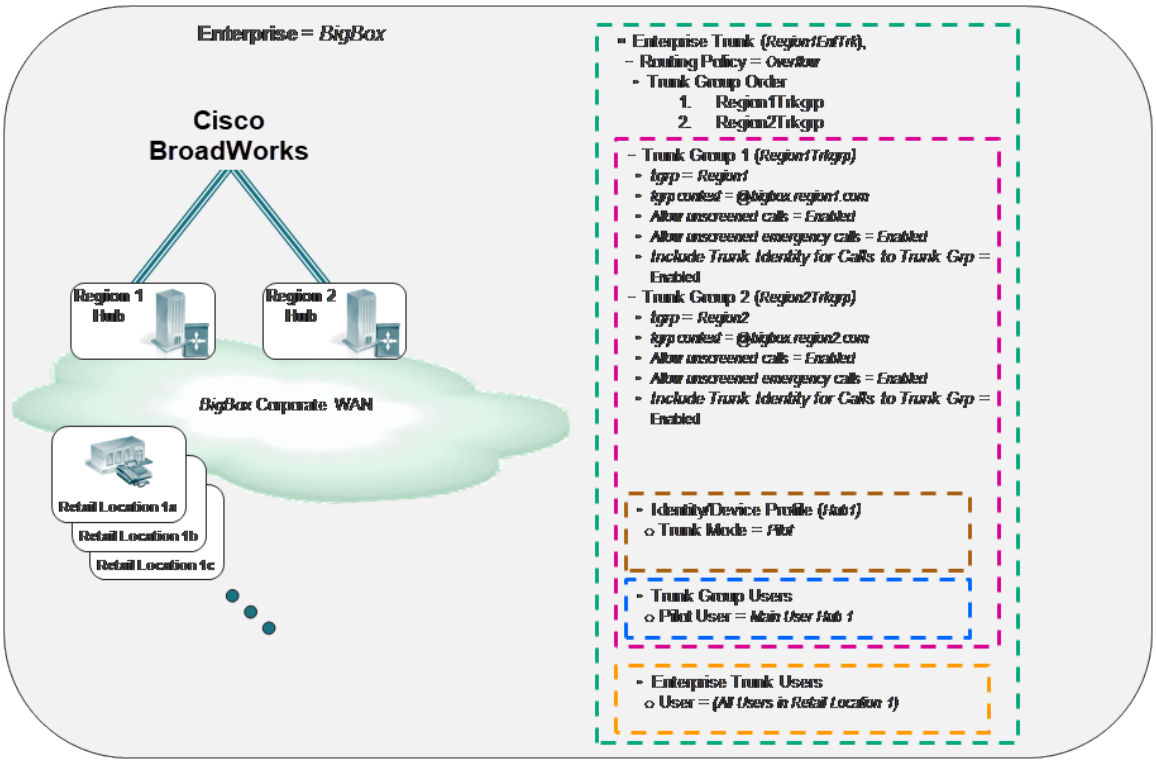

Figure 45 Retail Location 1 Enterprise Trunking/Trunk Group Mapping

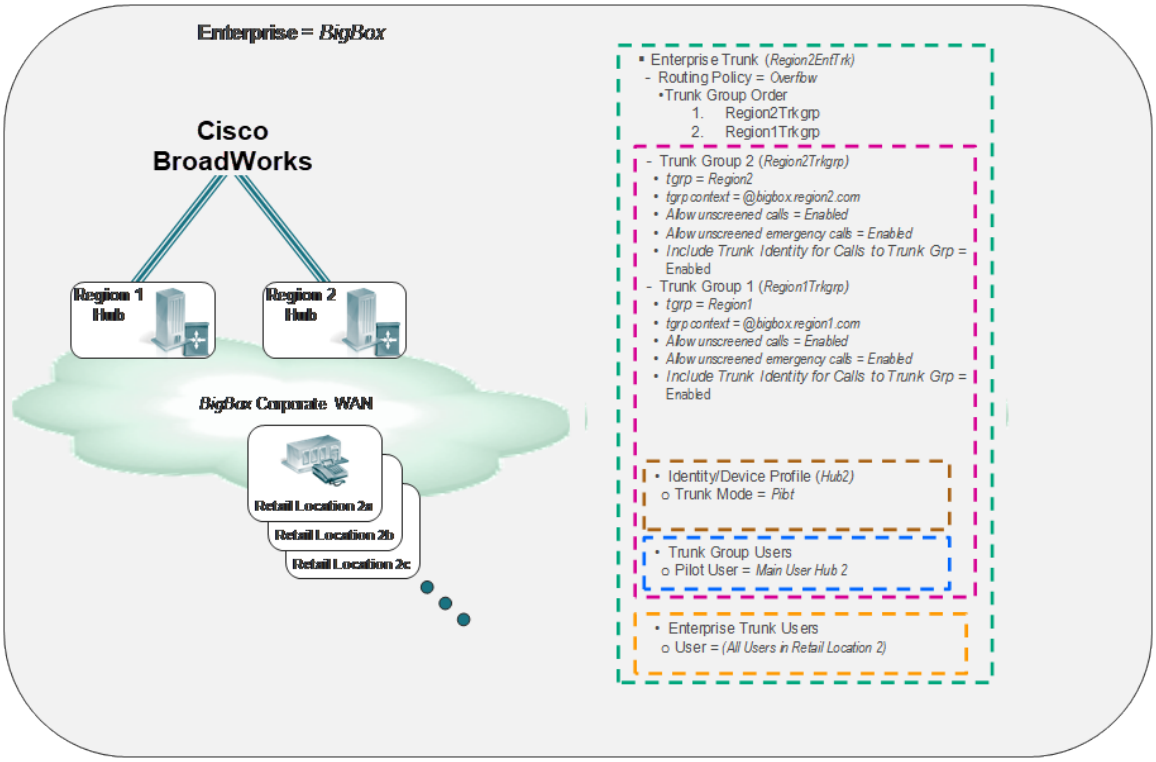

Figure 46 Retail location 2 Enterprise Trunking/Trunk Group Mapping

For Region 3, the ISP has opted to use “Weighted” Enterprise Trunk routing policy. Weighted was selected to allow calls to Retail Location 3 users to be routed via Region 3 Hub first and leverage both Region 1 and Region 2 Hubs for redundancy in a load-balancing scenario. This is accomplished by assigning the trunk group associated with Hub 3 (Region3TrkGrp) as the highest priority and assigning a lower priority value to the trunk groups associated with Hub 1 (Region1TrkGrp) and Hub 2 (Region2TrkGrp). Assigning the same priority and weight to Region1TrkGrp and Region2TrkGrp, establishes an equal probability of either trunk group being attempted. However, they are only attempted in the event Region3TrkGrp is unreachable or in an over-capacity scenario.

The structure of the Enterprise Trunk and associated trunk groups in shown in the following figure.

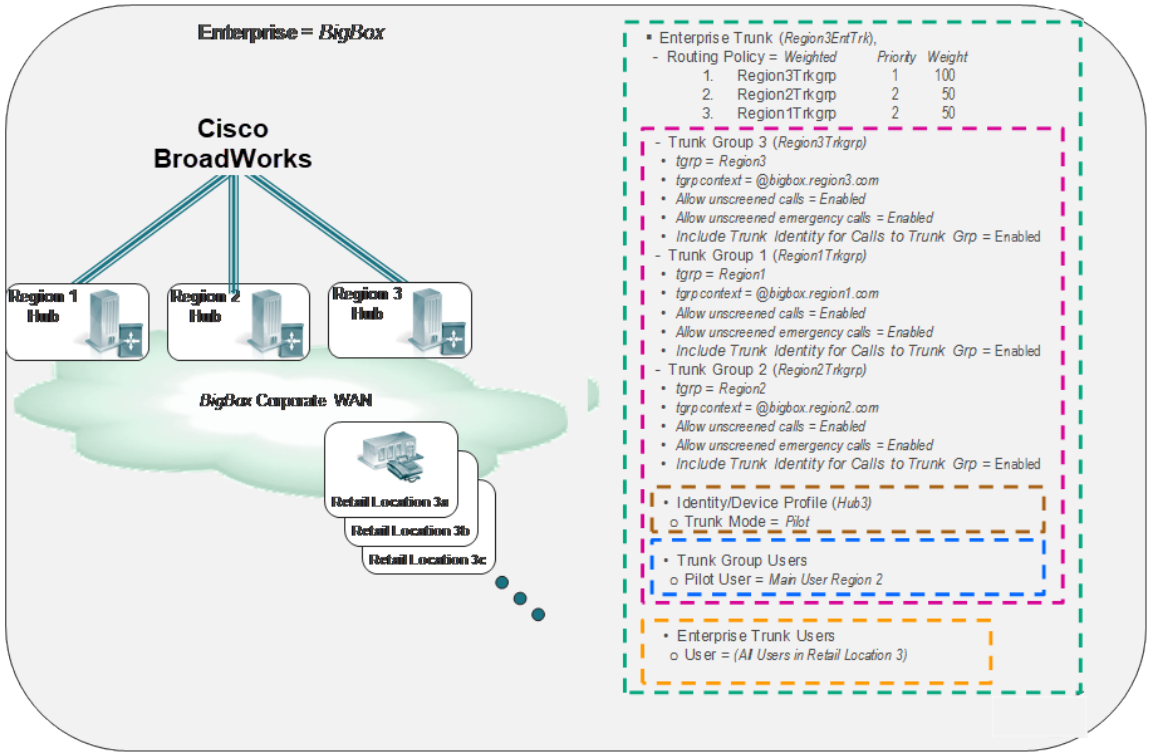

Figure 47 Retail location 3 Enterprise Trunking/Trunk Group Mapping

For Hub 4, BigBox would like to maintain separate trunk groups for the two retail locations supported. Once again, although the use of Enterprise Trunking is not required, the service provider has adopted the best practice of always deploying an Enterprise Trunking model, even if only one trunk group is required to meet the enterprise's requirements. The Enterprise Trunk and Trunk Group assignment for Hub 4 is shown in *Figure 48* and *Figure 49.*

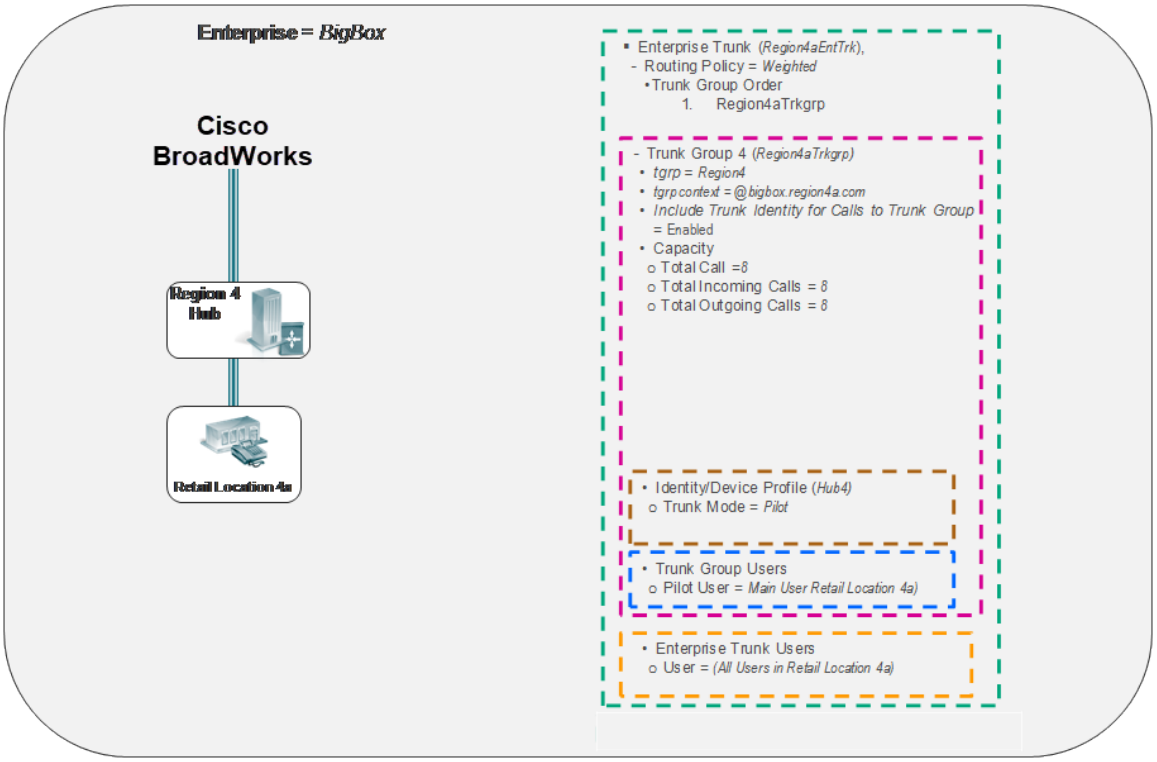

Figure 48 Retail location 4 Enterprise Trunking/Trunk Group Mapping

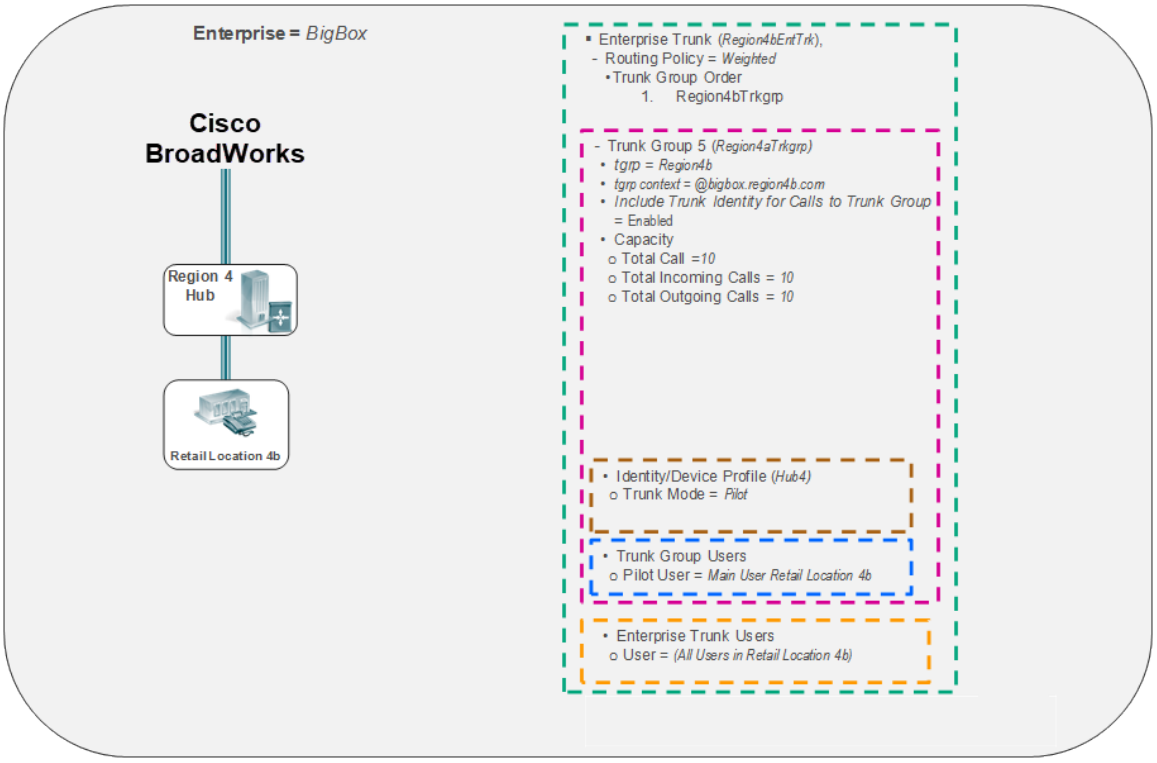

Figure 49 Retail Location 5 Enterprise Trunking/Trunk Group Mapping

23 Appendix B – IMS Deployment Examples

This section provides a high-level description of Cisco BroadWorks' support for SIP Trunking in an IMS deployment.

In an IMS deployment, the Cisco BroadWorks Application Server plays the role of a Telephony Application Server, providing important call processing services. Cisco BroadWorks provides the same services to hosted users and trunking users. Therefore, from the perspective of services offered, how those services are configured, Cisco BroadWorks SIP Trunking requires no special consideration.

However, when Cisco BroadWorks is deployed to provide services to business trunking users, who are reachable via a PBX, there are two issues that require special consideration. The first area is user provisioning. In a worst-case scenario, each user must be provisioned with three different services profiles: a profile on the PBX, a profile in the IMS network (Home Subscriber Server [HSS]), and a profile on Cisco BroadWorks. Cisco BroadWorks provides a few alternatives to simplify the provisioning by optimizing the provisioning of user service profiles in the IMS network. These alternatives are:

- "Wildcarded" Public User Identity to cover all users on the PBX
- "Wildcarded" Public Service Identity to cover all users on the PBX

The second area is routing to the PBX. An important element of Cisco BroadWorks SIP Trunking solution is the ability of Cisco BroadWorks to select the route to the PBX. In an IMS deployment, the issue to consider is how Cisco BroadWorks can influence the routing of requests in the IMS network to the PBX. Cisco BroadWorks provides these alternatives:

- Route Out-of-the-Blue using the Trunk Group Pilot User's Public User Identity
- Route to the PBX as a peering domain by selecting the domain

In the remainder of this section, example deployments are presented and how these issues are resolved is described.

23.1 Single-Site Enterprise: Subscription-Based Business Trunking With Wildcarded Public User Identity

In this example, the PBX serves a small business and resides in a single site. The service provider depends on the IMS network itself to provide reliability (for example, by deploying active and standby CSCF nodes), and does not use the advanced routing capability available via Cisco BroadWorks' Enterprise Trunk routing policies. However, to simplify user provisioning, the service provider does require an optimization to eliminate the need to create an IMS service profile for every user on the PBX. To satisfy this requirement, the service provider provisions a "wildcarded" Public User Identity to cover all users on the PBX.

The details of this deployment are as follows:

- Each PBX user is provisioned in Cisco BroadWorks as a trunking user and assigned a DN, which serves as the DID number for that user.
- One service profile is provisioned in the HSS. This service profile has a "wildcarded" Public User Identity, which covers all the DID numbers for the PBX users.
- One Trunk Group is provisioned in Cisco BroadWorks, with the following characteristics:

- The Trunk Group has a Pilot User. The Public Identity of the Pilot User matches the explicit Public User Identity of the provisioned IMS service profile.
- The Trunk Mode of the Identity/Device Profile is set to “Proxy”.

- One Enterprise Trunk is provisioned in Cisco BroadWorks. The Trunk Group is added to this Enterprise Trunk. All PBX users are assigned to this Enterprise Trunk. Because the Enterprise Trunk has only one Trunk Group, the routing policy could be chosen arbitrarily. (Note that the Overflow policy would be a good choice.)

23.1.1 Registration

In accordance with the subscription-based business trunking described in *ETSI TS 182 025*, the PBX registers with the P-CSCF. The AoR for this registration is the explicit Public User Identity of the IMS service profile. The registration is also valid as an implicit registration for the associated URIs, which are specified by the wildcard that covers the DID numbers.

23.1.2 Incoming Call from the PSTN to a PBX User

For inbound calls from the PSTN to the enterprise, the call flow is shown in the following figure.

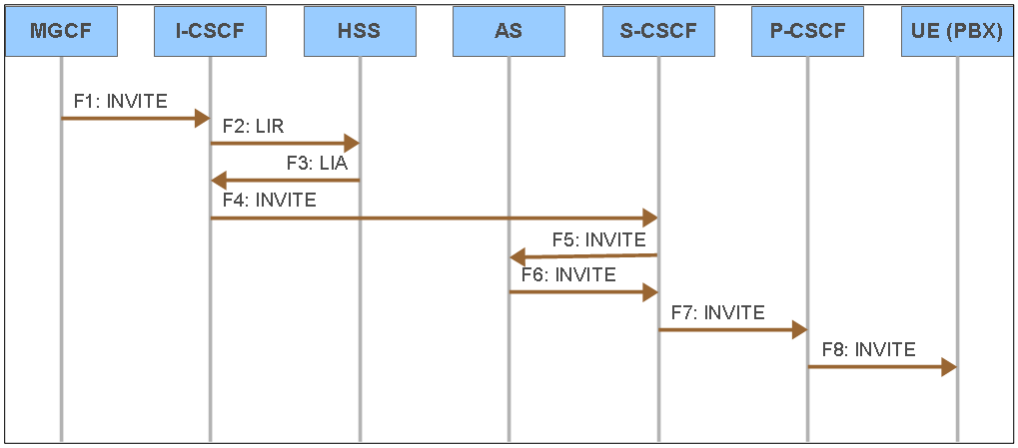

Figure 50 Inbound Call from PSTN to PBX

F1: INVITE from MGCF to I-CSCF

The MGCF provides the interface to the PSTN and translates the Integrated Services User Part (ISUP)/Bearer Independent Call Control (BICC) to SIP. The MGCF routes the SIP INVITE request to the I-CSCF, which serves as the entry point into the IMS core network.

F2: Location-Info-Request from I-CSCF to HSS

The I-CSCF sends a Location-Info-Request to the HSS to find the S-CSCF that processes sessions for the called user.

F3: Location-Info-Answer from HSS to I-CSCF

The HSS looks up the destination address (DID) and finds a match for a wildcarded Public User Identity for the Pilot User’s service profile. The HSS sends a Location-Info-Answer indicating that the Pilot User’s sessions are served on a particular S-CSCF.

F4: INVITE from I-CSCF to S-CSCF

Based on the information from the HSS, the I-CSCF routes the INVITE request to the S-CSCF that serves the Pilot User.

F5: INVITE from S-CSCF to AS

The S-CSCF runs initial filter criteria for the Pilot User's terminating session and decides it should route the INVITE request to the Application Server.

F6: INVITE from AS to S-CSCF

The Application Server identifies the PBX subscriber from the DID and executes terminating services for that subscriber. Then the Application Server sends the INVITE request back to the S-CSCF, based on the received Route header.

F7: INVITE from S-CSCF to P-CSCF

The S-CSCF forwards the INVITE request to the P-CSCF based on the registration information of the Pilot User identity.

F8: INVITE from P-CSCF to UE

The P-CSCF forwards the INVITE request to the enterprise's network, represented here as User Equipment. When the PBX receives the INVITE request, it alerts the station addressed by the DID in the *Request-URI*.

23.1.3 Outgoing Call from a PBX User to the PSTN

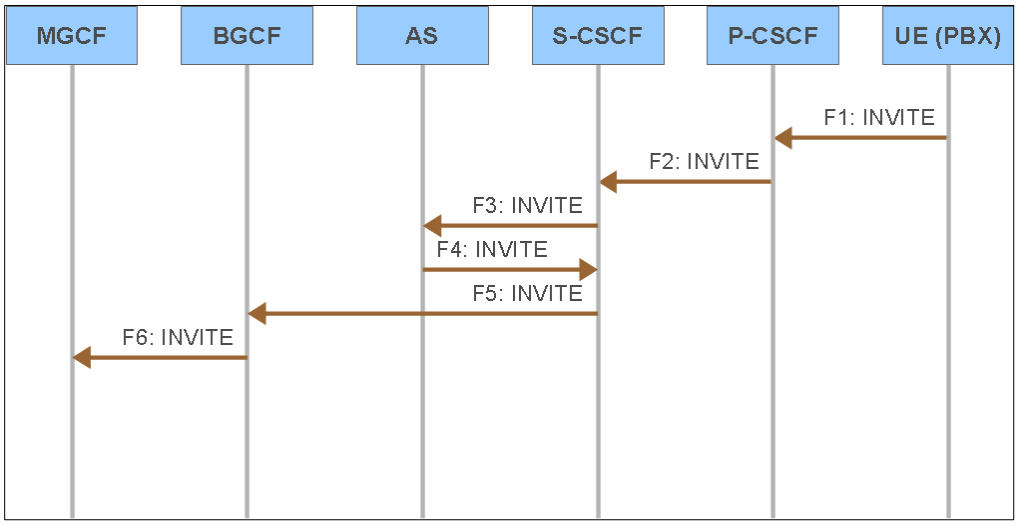

Figure 51 Outbound call from PBX to PSTN

F1: INVITE from UE to P-CSCF

The PBX, represented here as UE, sends an INVITE request to the P-CSCF. The INVITE has the PBX subscriber's DID as the asserted identity, which is associated with the Pilot User's service profile in the IMS. The *From* header has the DID of the PBX subscriber originating the call.

F2: INVITE from P-CSCF to S-CSCF

After examining the *P-Asserted-Identity* header, the P-CSCF routes the INVITE request to the S-CSCF that serves the Pilot User. This depends on the P-CSCF identifying the asserted identity as an associated identity of the Pilot User.

F3: INVITE from S-CSCF to AS

The S-CSCF runs initial filter criteria for the Pilot User's originating session and decides it should route the INVITE request to the Application Server.

F4: INVITE from AS to S-CSCF

The Application Server determines the calling subscriber from the *P-Asserted-Identity* and executes originating services for this subscriber. To continue the call routing, the Application Server routes the INVITE request back to the S-CSCF based on the received *Route* header.

F5: INVITE from S-CSCF to BGCF

The S-CSCF determines that it should route the call for termination to the PSTN. Based on this information, the S-CSCF routes the INVITE request to the BGCF.

F6: INVITE from BGCF to MGCF

The BGCF determines which MGCF should handle this call, and routes the INVITE request to that MGCF. The MGCF provides the entry point into the PSTN.

23.2 Multiple-Site Enterprise: Subscription-Based Business Trunking with Wildcarded Public Service Identity

In this example, the enterprise is a large business with employees in multiple sites. The users at each site are served by a PBX that resides at that site. The enterprise has its own internal network, which is integrated into the plan for survivability. Inbound calls are to be routed to the site where the PBX and the called user reside. If the site is unreachable, the plan is to route to an alternate site and allow the enterprise to route the call on its internal network to the PBX and to the called user. Therefore, the service provider relies on the advanced routing capabilities available via Cisco BroadWorks' Enterprise Trunk routing policies. Furthermore, to simplify user provisioning, the service provider requires an optimization to eliminate the need to create an IMS service profile for every user on the PBX. To satisfy this requirement, the service provider provisions a "wildcarded" PSI to cover all users on the PBX.

The details of this deployment are as follows:

- Each PBX user is provisioned in Cisco BroadWorks as a trunking user and assigned a DN, which serves as the DID number for that user.
- For each site, a "wildcarded" PSI is provisioned in the HSS. The "wildcarded" PSI covers all DID numbers for the PBX users at that site.
- For each site, a Pilot User is provisioned in Cisco BroadWorks. Each such Pilot User is associated with a service profile in the IMS (see the following item) and has a Public User Identity.
- For each site, a service profile is provisioned in the IMS. Each such service profile is associated with a Pilot User (see the preceding item). The service profile has a single Public User Identity.
- For each site, a Trunk Group is provisioned in Cisco BroadWorks, with the following characteristics:
  - The Trunk Mode of the Identity/Device Profile is set to "Pilot".
- For each site, an Enterprise Trunk is provisioned in Cisco BroadWorks, with the following characteristics:
  - Each user is assigned to the Enterprise Trunk for their site.

- The Trunk Group for that site is assigned to the Enterprise Trunk as the primary route. For example, if the Enterprise Trunk routing policy is Overflow, the Trunk Group is the first on the list.
- Additional Trunk Groups to other sites are assigned to the Enterprise Trunk as alternate routes.

This configuration is compatible with subscription-based business trunking, as described in *ETSI TS 182 025.* Each site is reachable via a different IMS service profile and corresponding Public User Identity. The Application Server is able to control the routing in the IMS network by setting the *Request-URI* in the INVITE request it sends to the enterprise for inbound calls. The connectivity of any particular site to the IMS network can also have redundant links, for example, each PBX can register to two different P-CSCFs. However, this level of redundancy is independent of the redundancy provided by Cisco BroadWorks via the Enterprise Trunk routing policy, which is able to route to an alternate site rather than an alternate P-CSCF for the same site.

Because the Trunk Mode for each Trunk Group is "Pilot", this deployment places a special requirement on the enterprise to correctly interpret the destination address fields of the incoming INVITE request. Specifically, the Application Server sets the Pilot User's Public User Identity as the *Request-URI* and sets the called user's address as the To URI. Therefore, the PBX must be able to identify the called user by parsing the *To* header. Alternatively, the enterprise can rely on an intermediary network element, such as an SBC, to "fix" the destination address fields so that the PBX can correctly identify the called user.

23.2.1 Registration

In accordance with the subscription-based business trunking described in *ETSI TS 182 025*, the PBX registers with the P-CSCF. The AoR for this registration is the explicit Public User Identity of the Pilot User for that site. For a large enterprise, it can also be possible to statically configure the contact URI as an alternative to a SIP registration, depending on the ability of the P-CSCF to support it.

23.2.2 Incoming Call from the PSTN to a PBX User

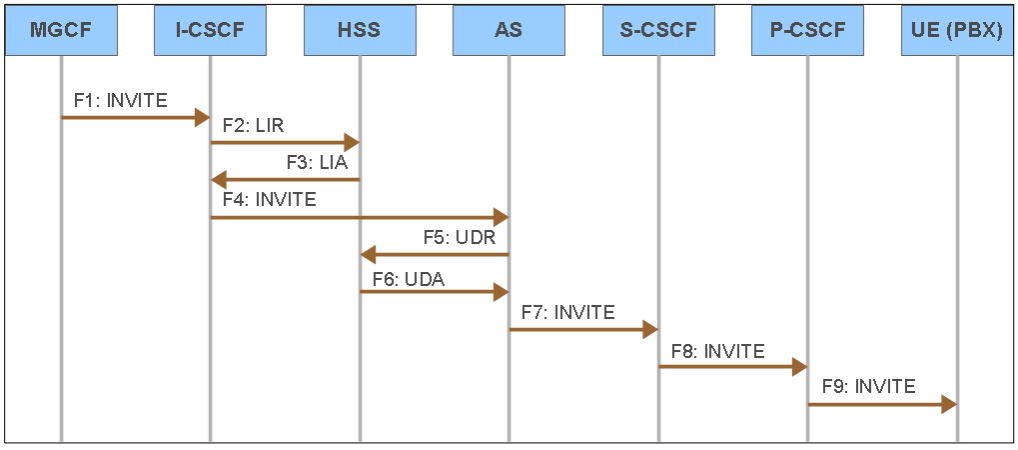

Figure 52 Inbound Call from PSTN to PBX

F1: INVITE from MGCF to I-CSCF

The MGCF provides the interface to the PSTN and translates the ISUP/BICC to SIP. The MGCF routes the SIP INVITE request to the I-CSCF, which serves as the entry point into the IMS core network.

F2: Location-Info-Request from I-CSCF to HSS

The I-CSCF sends a Location-Info-Request to the HSS to find the S-CSCF that processes sessions for the called user.

F3: Location-Info-Answer from HSS to I-CSCF

The HSS looks up the destination address (DID) and finds a match for a "wildcarded" PSI. The HSS sends a Location-Info-Answer indicating that the PSI is served on the Cisco BroadWorks Application Server.

F4: INVITE from I-CSCF to AS

Based on the information in the Location-Info-Answer message, the I-CSCF routes the INVITE request to the Cisco BroadWorks Application Server.

F5: User-Data-Request from AS to HSS

If the Application Server does not have up-to-date subscriber data from the HSS, it can send a *User-Data-Request* to the HSS to get the *CSCFName* value for the trunk group Pilot User.

Note, that the Application Server caches the *CSCFName* value, so that a UDR/UDA query to the HSS is not required for every incoming call. Furthermore, the Application Server can learn the *CSCFName* from a third-party registration from the S-CSCF, so that queries to the HSS are not required at all.

F6: User-Data-Answer from HSS to AS

The HSS sends a *User-Data-Answer* message to the Application Server. The answer message contains a *CSCFName* value that indicates which S-CSCF the Application Server should route requests to for the Pilot User.

F7: INVITE from AS to S-CSCF

Based on information from the HSS, the Application Server sends an OOTB terminating INVITE request to the S-CSCF that processes sessions for the Pilot User. To facilitate routing in the core network, the Application Server populates the *Request-URI* with the Pilot User's PUI. The *To* header contains the DID of the called PBX subscriber.

F8: INVITE from S-CSCF to P-CSCF

The S-CSCF forwards the INVITE request to the P-CSCF based on the registration information of the Pilot User identity.

F9: INVITE from the P-CSCF to the UE

The P-CSCF forwards the INVITE request to the enterprise's network, represented here as User Equipment. When the PBX receives the INVITE request, it alerts the station addressed by the DID in the *To* header field.

23.2.3 Outgoing Call from a PBX User to the PSTN

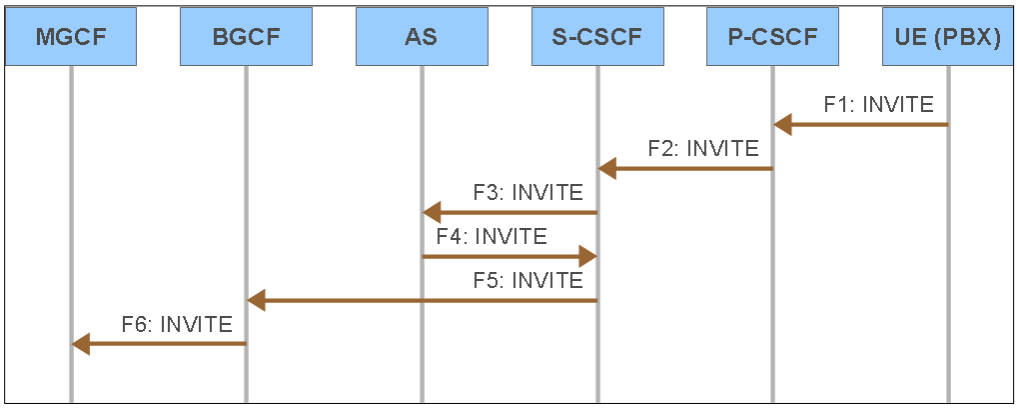

Figure 53 Outbound Call from PBX to PSTN

F1: INVITE from UE to P-CSCF

The PBX, represented here as UE, sends an INVITE request to the P-CSCF. The INVITE has the Pilot User's PUI as the asserted identity. The *From* header has the DID of the PBX subscriber originating the call.

F2: INVITE from the P-CSCF to the S-CSCF

After examining the P-Asserted-Identity header, the P-CSCF routes the INVITE request to the S-CSCF that serves the Pilot User.

F3: INVITE from the S-CSCF to the AS

The S-CSCF runs initial filter criteria for the Pilot User's originating session and decides it should route the INVITE request to the Application Server.

F4: INVITE from the AS to the S-CSCF

The Application Server determines the calling subscriber from the DID in the *From* header and executes originating services for this subscriber. To continue the call routing, the Application Server routes the INVITE request back to the S-CSCF based on the received *Route* header.

F5: INVITE from the S-CSCF to the BGCF

The S-CSCF determines that it should route the call for termination to the PSTN. Based on this information, the S-CSCF routes the INVITE request to the BGCF.

F6: INVITE from BGCF to MGCF

The BGCF determines which MGCF should handle this call, and routes the INVITE request to that MGCF. The MGCF provides the entry point into the PSTN.

23.3 Multiple-Site Enterprise: Peering-Based Business Trunking With Wildcarded Public User Identities

In this example, the enterprise is a large business with employees in multiple sites. The users at each site are served by a PBX that resides at that site. The enterprise has its own internal network, which is integrated into the survivability plan. Inbound calls are to be routed to the site where the PBX and the called user reside. If the site is unreachable, the plan is to route to an alternate site and allow the enterprise to route the call on its internal network to the PBX and to the called user. Therefore, the service provider relies on the advanced routing capabilities available via Cisco BroadWorks' Enterprise Trunk routing policies. Furthermore, to simplify user provisioning, the service provider requires an optimization to eliminate the need to create an IMS service profile for every user on the PBX. To satisfy this requirement, the service provider provisions a "wildcarded" Public User Identity to cover all users on the PBX.

The details of this deployment are as follows:

- Each PBX user is provisioned in Cisco BroadWorks as a trunking user and assigned a DN, which serves as the DID number for that user.
- For each site, a Pilot User is provisioned in Cisco BroadWorks. Each such Pilot User is associated with a service profile in the IMS (see the following item) and has a distinct Public User Identity.
- For each site, a service profile is provisioned in the IMS. Each such service profile is associated with a Pilot User in Cisco BroadWorks (see the preceding item). The service profile has a distinct Public User Identity, which identifies the Pilot User, as well as an associated "wildcarded" Public User Identity that covers all users at a site.
- For each site, a Trunk Group is provisioned in Cisco BroadWorks, with the following characteristics:
  - The Trunk Mode of the Identity/Device Profile is "Pilot".
- For each site, an Enterprise Trunk is provisioned in Cisco BroadWorks, with the following characteristics:
  - Each user is assigned to the Enterprise Trunk for their site.
  - The Trunk Group for that site is assigned to the Enterprise Trunk as the primary route (for example, if the Enterprise Trunk routing policy is Overflow, the Trunk Group is the first on the list).
  - Additional Trunk Groups to other sites are assigned to the Enterprise Trunk as alternate routes.

This configuration is compatible with peering-based business trunking described in *ETSI TS 182 025.* Each site is reachable via a different Trunk Group and peering domain. The Application Server is able to control the routing in the IMS network by setting the *Request-URI* domain name in the INVITE request it sends to the enterprise for inbound calls.

23.3.1 Registration

This deployment conforms to the peering-based business trunking of *ETSI TS 182 025.* Therefore, routing to the enterprise depends on resolving the destination domain, and registration is not used.

23.3.2 Incoming Call from the PSTN to a PBX User

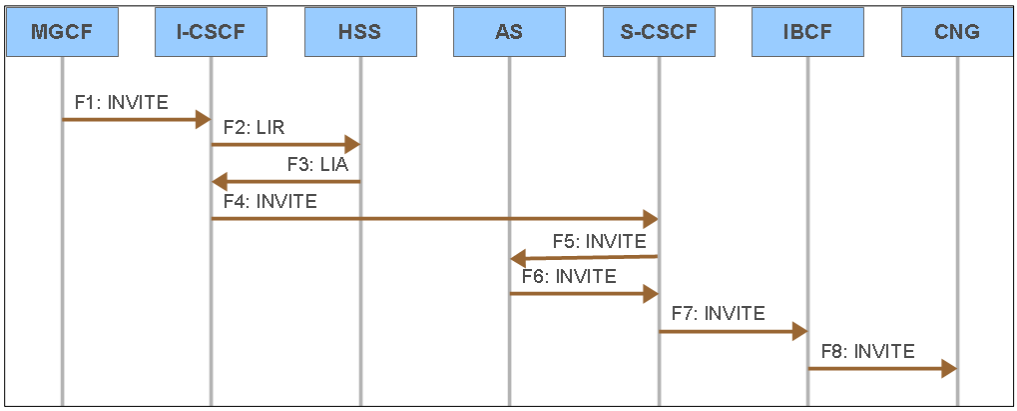

Figure 54 Inbound Call from PSTN to PBX

F1: INVITE from MGCF to I-CSCF

The MGCF provides the interface to the PSTN and translates the ISUP/BICC to SIP. The MGCF routes the SIP INVITE request to the I-CSCF, which serves as the entry point into the IMS core network.

F2: Location-Info-Request from I-CSCF to HSS

The I-CSCF sends a *Location-Info-Request* to the HSS to find the S-CSCF that processes sessions for the called user.

F3: Location-Info-Answer from HSS to I-CSCF

The HSS looks up the destination address (DID) and finds a match for a "wildcarded" PUI for the Pilot User's service profile. The HSS sends a *Location-Info-Answer* indicating that the Pilot User's sessions are served on a particular S-CSCF.

F4: INVITE from I-CSCF to S-CSCF

Based on the information from the HSS, the I-CSCF routes the INVITE request to the S-CSCF that serves the Pilot User.

F5: INVITE from S-CSCF to AS

The S-CSCF runs initial filter criteria for the Pilot User's terminating session and decides it should route the INVITE request to the Application Server.

F6: INVITE from AS to S-CSCF

The Application Server identifies the PBX user from the DID number and executes terminating services for that subscriber. Based on the identified terminating trunk group, the Application Server changes the domain in the *Request-URI* to that of the peering domain. Then the Application Server sends the INVITE request back to the S-CSCF, based on the received *Route* header.

F7: INVITE from S-CSCF to IBCF

The S-CSCF examines the domain of the *Request-URI* of the INVITE request and determines that the destination is in a peering domain. Consequently, the S-CSCF routes the INVITE request to the IBCF that represents the request to the peering network.

F8: INVITE from IBCF to CNG

The IBCF forwards the INVITE request to the Customer Network Gateway (CNG).

NOTE: The CNG is likely an SBC, which is the SIP entry point into the enterprise network and which routes the INVITE on to the IP PBX.

23.3.3 Outgoing Call from a PBX User to the PSTN

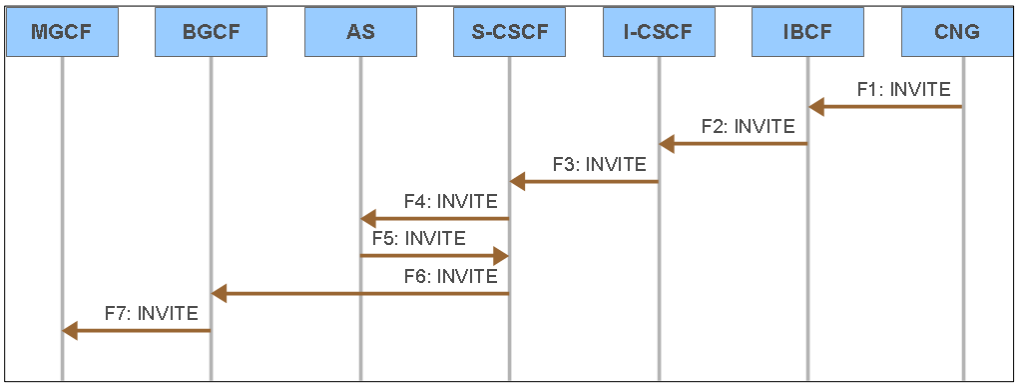

Figure 55 Outbound Call from PBX to PSTN

F1: INVITE from CNG to IBCF

The PBX, represented here as CNG, sends an INVITE request to the IBCF, which is the entry point to the service provider's IMS network. The INVITE has the calling user's PUI as the asserted identity. The *From* header has the calling user's presentation identity.

F2: INVITE from IBCF to I-CSCF

The IBCF adds a *Route* header with an *orig* parameter to the INVITE request and sends it to the I-CSCF.

F3: INVITE from I-CSCF to S-CSCF

The I-CSCF forwards the INVITE request to the S-CSCF.

F4: INVITE from S-CSCF to AS

The S-CSCF runs initial filter criteria decides it should route the INVITE request to the Application Server.

F5: INVITE from AS to S-CSCF

The Application Server determines the calling subscriber from the *P-Asserted-Identity* and executes originating services for this subscriber. To continue the call routing, the Application Server routes the INVITE request back to the S-CSCF based on the received *Route* header.

F6: INVITE from S-CSCF to BGCF

The S-CSCF determines that it should route the call for termination to the PSTN. Based on this information, the S-CSCF routes the INVITE request to the BGCF.

F7: INVITE from BGCF to MGCF

The BGCF determines which MGCF should handle this call, and routes the INVITE request to that MGCF. The MGCF provides the entry point into the PSTN.

24 Appendix C – Bursting Call Capacity

For non-emergency calls, the Application Server can be provisioned to allow a limited number of calls that exceed the configured capacity limits. This capability is called bursting.

Bursting capacity must be licensed and allocated to Service Providers, Enterprises, Groups, and Trunk Groups. The following restrictions apply:

- The total bursting capacity of all the Trunk Groups in a particular group cannot exceed the bursting capacity allocated to that group.
- The total bursting capacity of all the groups in a particular Service Provider or Enterprise cannot exceed the bursting capacity allocated to that Service Provider or Enterprise.
- The total bursting capacity of all the Service Providers or Enterprises in the system cannot exceed the bursting capacity licensed to the system.

When a call is attempted and the Trunk Group does not have sufficient regular capacity, it can continue the call attempt using any available bursting capacity. When a call uses the Trunk Group's bursting capacity, the event is recorded in the CDR for that call, thus allowing the bursting capacity usage to be reported. Additionally, the Application Server can send an SNMP notification to report the bursting event.

Bursting capacity is configured to apply to all call attempts, both incoming and outgoing. The bursting capacity that can be configured for a Trunk Group is limited by the remaining bursting capacity allocated to the group, and by licensed parameter, *burstingOverMaxPercentage*, which determines the maximum bursting capacity relative to the Trunk Group capacity. For example, if a group has 10 bursting capacity license units unallocated, the bursting capacity that can be allocated to a new Trunk Group is limited to 10. Moreover, if a new Trunk Group has capacity of 24, and the value of *burstingOverMaxPercentage* is 25%, then the bursting capacity is limited to 6. The parameter, *burstingOverMaxPercentage*, can take values from zero to unbound, the default value being 25%.

Bursting capacity can optionally be configured for incoming calls and outgoing calls as well. The bursting capacity for incoming calls cannot exceed the bursting capacity for all calls. Similarly, the bursting capacity for outgoing calls cannot exceed the bursting capacity for all calls.

The Application Server can occasionally tap, as needed, the bursting capacity of a Trunk Group that is part of an Enterprise Trunk. When it applies the Routing policy to select a Trunk Group, the Application Server usually considers only the regular capacity of each Trunk Group. However, if each constituent Trunk Group has reached the limit of its regular capacity, then the Application Server applies the policy using a bursting capacity instead of the regular capacity. Thus, it taps into the bursting capacity only when necessary.

Bursting Example 1

An Enterprise Trunk with the Weighted Overflow policy has Trunk Groups A and B, which have the same priority. Both A and B have a regular capacity of 100 terminating calls and a bursting capacity of 10 terminating calls. Assume A has 100 active terminating calls and B has 99 active terminating calls when the Enterprise Trunk processes another termination. In this case, it routes the call to B, which still has a regular capacity available. So now both A and B have 100 active terminating calls. When the Enterprise Trunk processes another termination under these conditions, it must tap into the bursting capacity. Both A and B have available bursting capacity; therefore, the Application Server uses the assigned weights to randomly select either A or B.

Bursting Example 2

An Enterprise has 200 BTLUs allocated. During a particularly busy time, the Enterprise reaches its limit of 200 simultaneous trunking calls, so that it has no available BTLUs. A user in the enterprise attempts to make a new outgoing call via one of the Enterprise's Trunk Groups. Even though the Enterprise has available bursting capacity, the Application Server blocks the call because no BTLUs are available.

Bursting Example 3

An Enterprise has 200 BTLUs allocated. Trunk Group A in the Enterprise is configured with a bursting capacity of 5. During a busy time, the Enterprise has 198 simultaneous active trunking calls. If Trunk Group A has reached its regular capacity, Cisco BroadWorks allows only two bursting calls to Trunk Group A, because there are only two BTLUs available.

25 Appendix D – PBX Classifications Examples

The information in this appendix was copied from the *BroadWorks Business Trunking Configuration Guide, Release 18.0*, which was absorbed into this guide in Release 19.0. The classifications described here are referenced in partner configuration guides and elsewhere. They are retained here for reference.

25.1 Cisco BroadWorks Business Trunking PBX Classifications for Stand-alone Deployments

Cisco BroadWorks supports both IP PBXs and TDM PBXs via an IAD or gateway, via a SIP interface. Cisco BroadWorks has configurable policies to support the vast variety of addressing models, which an IP PBX or IAD/gateway can use when interfacing with Cisco BroadWorks Business Trunking. Additionally, Cisco BroadWorks also supports configurable policies on handling a variety of mechanisms for call redirections within the PSTN; including redirections to external voice mail/unified messaging from the PBX.

To determine which policies to apply on Cisco BroadWorks to support the varying IP PBX and TDM PBX configurations, the IP PBX or TDM PBX via an IAD or gateway are placed into different classifications. These classifications are then mapped into configurations on Cisco BroadWorks.

The following classifications are used to characterize the interworking of the IP PBX or TDM PBX via an IAD or gateway with Cisco BroadWorks:

- Type A – SIP Registering PBX
- Type B – SIP Non-registering PBX
- Type C – SIP Registering PBX with modified *Request-URI* header
- Type D – SIP Non-registering PBX with modified *Request-URI* header
- Type E – Device Addressing PBX
- Type F – Subscriber Registering PBX
- Type G – SIP Registering PBX with pilot contact *Route* header
- Type H – SIP Non-registering PBX with pilot contact *Route* header

To simplify the description, in the following sections, the term “PBX” is used to mean either an IP PBX or a TDM PBX accessed via an IAD/gateway.

25.1.1 Type A – SIP Registering PBX Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP Registering PBX maps to a parent registration for the PBX covering all PBX subscribers.

In this classification, a PBX sends a single REGISTER with the contact of the PBX representing all of the subscribers served by the PBX. This method is referred to as a parent registration, in which the PBX is the parent registering on behalf of the children, that is, the PBX subscribers.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *To* header of the INVITE. Cisco BroadWorks populates the Request-URI with the registered contact of the PBX.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Cisco BroadWorks Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity*, and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The PBX IP address is used only in the *Contact* header of the REGISTER.

25.1.2 Type B – SIP Non-registering PBX Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP non-registering PBX maps to a static parent registration for the PBX covering all PBX subscribers.

In this classification, PBX does not register with Cisco BroadWorks. However, the PBX is statically configured on Cisco BroadWorks with the IP address of the PBX. The signaling for this classification is identical to that of a SIP Registering PBX classification except for the register.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *To* header of the INVITE. Cisco BroadWorks populates the Request-URI with the registered contact of the PBX.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity*, and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The PBX IP address is used only in the Request-URI of the INVITE populated by Cisco BroadWorks to send calls to the PBX.

25.1.3 Type C – SIP Registering PBX with Modified Request-URI Header Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP registering PBX with modified *Request-URI* header maps to a Per-Business Trunk Group configuration for the PBX covering all PBX subscribers. This classification is identical to the *Type A – SIP Registering PBX* classification except that the PBX routes calls from Cisco BroadWorks within the PBX using the *Request-URI* rather than the *To* header. Cisco BroadWorks must populate the user portion of the *Request-URI* with the identity of the PBX subscriber, and the host portion of the *Request-URI* with the host portion from the registered contact received from the PBX.

In this classification, a PBX sends a single REGISTER with the contact of the PBX representing all of the subscribers served by the PBX. This method is referred to as a parent registration, in which the PBX is the parent registering on behalf of the children, that is, the PBX subscribers.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Request-URI* with the registered contact of the PBX and Cisco BroadWorks modifies the user portion to contain the Business Trunking user identity. The PBX ignores the *To* header for call routing.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Cisco BroadWorks Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity,* and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The PBX IP address is used only in the *Contact* header of the REGISTER.

25.1.4 Type D – SIP Non-registering PBX with Modified Request-URI Header Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP non-registering PBX with modified *Request-URI* header maps to a Per-Business Trunk Group configuration for the PBX covering all PBX subscribers. This classification is identical to the *Type B – SIP Non-registering PBX* classification with the exception that the PBX routes calls from Cisco BroadWorks within the PBX using the *Request-URI* rather than the *To* header. Cisco BroadWorks must populate the user portion of the *Request-URI* with the identity of the PBX subscriber, and the host portion of the *Request-URI* with the host portion from the statically configured contact on Cisco BroadWorks.

In this classification, a PBX does not register with Cisco BroadWorks. However, the PBX is statically configured on Cisco BroadWorks with the IP address of the PBX. The signaling for this classification is identical to that of a SIP registering PBX classification except for the REGISTER.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Request-URI* with the statically configured contact of the PBX and Cisco BroadWorks modifies the user portion to contain the Business Trunking user identity. The PBX ignores the *To* header for call routing.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Cisco BroadWorks Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity*, and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The IP address is used only in the *Request-URI* of the INVITE populated by Cisco BroadWorks to send calls to the PBX.

25.1.5 Type E – Device Addressing PBX Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a device addressing PBX maps to a Per-Business Trunk Group configuration for the PBX covering all PBX subscribers. This classification is similar to the *Type D – SIP Non-Registering PBX with modified Request-URI Header* classification with the exception that the PBX uses device addressing rather than proxy addressing. Device addressing means that the PBX populates the host portion of the addressing headers (for example, *From, To, P-Asserted-Identity, Request-URI*) with the IP address of the device rather than a domain configured in Cisco BroadWorks for calls sent to Cisco BroadWorks.

In this classification, a PBX does not register with Cisco BroadWorks. However, the PBX device is statically configured on Cisco BroadWorks with the IP address of the PBX.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Request-URI* with the statically configured contact of the PBX, and Cisco BroadWorks modifies the user portion to contain the Business Trunking user identity. The PBX ignores the *To* header for call routing.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the device for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity,* and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is used by the PBX in populating all of the addressing headers.

25.1.6 Type F – Subscriber Registering PBX Classification

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a subscriber registering a PBX maps to an individual child (per the PBX subscriber) registration.

In this classification, a PBX sends a REGISTER with the contact of the PBX for each subscriber served by the PBX. This method is referred to as a child registration, where the PBX as the parent, registers the PBX contact for each of the children, that is, the PBX subscribers. The contact for each child registration can all have the same addresses or the contact can be unique for each child registration.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Request-URI* with the registered contact of the PBX subscriber.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity,* and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The IP address is used only in the *Contact* header of the register.

25.1.7 Type G – SIP Registering PBX with Pilot Contact Route Header

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP registering PBX with pilot contact *Route* header maps to a Per-Business Trunk Group configuration for the PBX covering all PBX subscribers. This classification is similar to the *Type C – SIP Registering PBX with Modified Request-URI Header* classification except that the Application Server uses the *Route* header to route terminating requests to the PBX. Cisco BroadWorks populates the user portion of the *Request-URI* with the identity of the PBX subscriber, and the host portion of the *Request-URI* with the host portion from the Pilot User line port (AoR) as provisioned.

In this classification, a PBX sends a single REGISTER with the contact of the PBX representing all of the subscribers served by the PBX. This method is referred to as a parent registration, in which the PBX is the parent registering on behalf of the children, that is, the PBX subscribers.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Route* header with the registered contact of the PBX and the request is routed from Cisco BroadWorks to the PBX using loose routing. The PBX ignores the *To* header for call routing.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Cisco BroadWorks Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity,* and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers. The PBX IP address is used only in the *Contact* header of the REGISTER.

25.1.8 Type H – SIP Non-registering PBX with Pilot Contact Route Header

From the *Cisco BroadWorks SIP Business Trunking Interworking Guide* [13], a SIP non-registering PBX with pilot contact *Route* header maps to a Per-Business Trunk Group configuration for the PBX covering all PBX subscribers. This classification is similar to the *Type D – SIP Non-Registering PBX with Modified Request-URI header* classification except that the Application Server uses the *Route* header to route terminating requests to the PBX. Cisco BroadWorks populates the user portion of the *Request-URI* with the identity of the PBX subscriber, and the host portion of the *Request-URI* with the host portion from the Pilot User line port (AoR) as provisioned.

In this classification, a PBX does not register with Cisco BroadWorks. However, the PBX is statically configured on Cisco BroadWorks with the IP address of the PBX. The signaling for this classification is identical to that of a SIP registering PBX classification except for the REGISTER.

The PBX routes calls from Cisco BroadWorks to the PBX subscribers using the *Request-URI* header of the INVITE. Cisco BroadWorks populates the *Route* header with the statically configured contact of the PBX (Pilot User) and the request is routed from Cisco BroadWorks to the PBX using loose routing. The PBX ignores the *To* header for call routing.

For calls originated within the PBX and sent to Cisco BroadWorks, the PBX populates the calling line identity of the PBX subscriber in the *From* or *P-Asserted-Identity* header.

The PBX uses the addressing/domain space of the Cisco BroadWorks Application Server for populating the host portion of the SIP URIs in the *From, To, P-Asserted-Identity,* and *Request-URI* headers for calls sent from the PBX to Cisco BroadWorks. The PBX IP address is not used by the PBX in any of the addressing headers.

25.2 Identity/Device Profile Type Configuration Procedure for Stand-alone Deployments

To configure a trunk group for a PBX in one of the defined PBX classifications, the Identity/Profile Type must either be selected or created in Cisco BroadWorks.

The following procedure can be used to determine if the Identity/Device Profile Type for the PBX classification exists in Cisco BroadWorks. If the Identity/Device Profile Type does not exist, the system administrator can create the Identity/Device Profile Type for the PBX classification using the following the instructions for the appropriate PBX classification.

Step	Details	Purpose
Step 1	Log into the Cisco BroadWorks web configuration interface as a system administrator.	You must be logged into Cisco BroadWorks as a system administrator to view the attributes of an Identity/Profile Type in the system.
Step 2	Under the *Resources* tab in the left-side navigation, select the **Identity/Device Profile Types** link.	This is the search page for all of the Identity/Device Profile Types defined in the system.
Step 3	In the search criteria, enter the name of the Identity/Device Profile Type for the appropriate PBX classification and click on the Search button.	Search for the Identity/Device Profile Type in the system.

Step	Details	Purpose
Step 4	Determine if an entry is found. If an entry is found, the Identity/Device Profile Type exists for the PBX classification. Otherwise, an Identity/Device Profile Type must be created for the PBX classification.	Determine if the Identity/Device Profile Type exists in the system.

If the Identity/Device Profile Type must be created for the PBX classification, the following procedure can be used to create the appropriate Identity/Device Profile Type for the PBX classification.

Step	Details	Purpose
Step 1	Log into the Cisco BroadWorks web configuration interface as a system administrator.	You must be logged into Cisco BroadWorks as a system administrator to view the attributes of an Identity/Profile Type in the system.
Step 2	Under the *Resources* tab in the left-side navigation, select the **Identity/Device Profile Types** link.	This is the search page for all of the Identity/Identity/Profile Type defined in the system.
Step 3	Click **Add**.	Add the Identity/Device Profile Type.
Step 4	Enter the Identity/Device Profile name for the specific PBX classification. Select the appropriate Signaling Address type for the specific PBX classification. Select the appropriate policies for the specific PBX classification. Click **OK**.	Create the Identity/Device Profile Type in the system.

25.2.1 Generic SIP IP-PBX Identity/Device Profile Type for Type A – SIP Registering PBX

The Identity/Device Profile Type for the *Type A – SIP Registering PBX classification is Generic SIP IP-PBX single registration*.

Note that this is the same Identity/Device Profile Type used for the *Type B – SIP Non-Registering PBX*. The profile type contains both the Registration policy and Static Registration policy to accommodate both PBX classifications in a single profile type.

The *Generic SIP IP-PBX single registration* Identity/Profile Type uses the Intelligent Proxy Addressing Signaling Address type.

The *Generic SIP IP-PBX single registration* Identity/Profile Type must have the following policies enabled:

- Registration Capable
- Pilot Trunk Mode
- PBX Integration

25.2.2 Generic SIP IP-PBX Identity/Device Profile Type for Type B – SIP Non-registering PBX

The Identity/Device Profile Type for the *Type B – SIP Non-registering PBX* classification is *Generic SIP IP-PBX single registration*.

Note that this is the same Identity/Device Profile Type used for the *Type A – SIP Registering PBX*. The profile type contains both the Registration policy and Static Registration policy to accommodate both PBX classifications in a single profile type.

The *Generic SIP IP-PBX single registration* Identity/Profile Type uses the *Intelligent Proxy Addressing Signaling Address* type.

The *Generic SIP IP-PBX single registration* Identity/Profile Type must have the following policies enabled:

- Static Registration Capable
- Pilot Trunk Mode
- PBX Integration

25.2.3 Generic SIP IP-PBX Identity/Device Profile Type for Type C – SIP Registering PBX with Modified Request-URI Header

The Identity/Device Profile Type for the *Type C – SIP Registering PBX* with modified *Request-URI* header classification is *Generic SIP IP-PBX*.

Note that this is the same Identity/Device Profile Type used for the *Type D – SIP Non-registering PBX* with modified *Request-URI* header. The profile type contains both the Registration policy and Static Registration policy to accommodate both PBX classifications in a single profile type.

The *Generic SIP IP-PBX* Identity/Profile Type uses the *Intelligent Proxy Addressing Signaling Address* type.

The *Generic SIP IP-PBX* Identity/Profile Type must have the following policies enabled:

- Registration Capable
- PBX Integration
- User Trunk Mode

25.2.4 Generic SIP IP-PBX Identity/Device Profile Type for Type D – SIP Non-registering PBX with Modified Request-URI Header

The Identity/Device Profile Type for the *Type D – SIP Non-Registering PBX* with modified *Request-URI* header classification is *Generic SIP IP-PBX*.

Note that this is the same Identity/Device Profile Type used for the *Type C – SIP Registering PBX* with modified *Request-URI* header. The profile type contains both the Registration policy and Static Registration policy to accommodate both PBX classifications in a single profile type.

The *Generic SIP IP-PBX* Identity/Profile Type uses the *Intelligent Proxy Addressing Signaling Address* type.

The *Generic SIP IP-PBX* Identity/Profile Type must have the following policies enabled:

- Static Registration Capable
- PBX Integration
- User Trunk Mode

25.2.5 Generic SIP TDM-PBX Identity/Device Profile Type for Type E – Device Addressing PBX

The Identity/Device Profile Type for the *Type E – Device Addressing PBX is Generic SIP TDM-PBX*.

The *Generic SIP TDM-PBX* Identity/Profile Type uses the *Intelligent Device Addressing Signaling Address* type.

The *Generic SIP TDM-PBX* Identity/Profile Type must have the following policies:

- PBX Integration
- User Trunk Mode

25.2.6 Generic SIP IP-PBX Identity/Device Profile Type for Type F – Subscriber Registering PBX

The Identity/Device Profile Type for the Type F – Subscriber registering PBX is *Generic SIP IP-PBX*.

Note that this is the same Identity/Device Profile Type used for the *Type C – SIP Registering PBX* with modified *Request-URI* and *Type D - SIP Non-registering PBX* with modified *Request-URI*.

The *Generic SIP IP-PBX* Identity/Profile Type uses the *Intelligent Proxy Addressing Signaling Address* type.

The *Generic SIP IP-PBX* Identity/Profile Type must have the following policies enabled:

- Registration Capable
- PBX Integration
- User Trunk Mode

25.2.7 Generic SIP IP-PBX Identity/Device Profile Type for Type G – SIP Registering PBX with Pilot Contact Route Header

The Identity/Device Profile Type for the *Type G – SIP Registering PBX with pilot contact Route Header* is *Generic SIP IP-PBX Proxy*

Note that this is the same Identity/Device Profile Type used for the *Type H – SIP Non-Registering PBX with pilot contact Route Header*. The profile type contains both the Registration policy and Static Registration policy to accommodate both PBX classifications in a single profile type.

The *Generic SIP IP-PBX Proxy* Identity/Profile Type uses the Intelligent Proxy Addressing Signaling Address type.

The *Generic SIP IP-PBX Proxy* Identity/Profile Type must have the following policies enabled:

- Registration Capable
- Proxy Trunk Mode
- PBX Integration

25.2.8 Generic SIP IP-PBX Identity/Device Profile Type for Type H – SIP Non-Registering PBX with Pilot Contact Route Header

The Identity/Device Profile Type for the *Type H – SIP Non-Registering PBX with pilot contact Route Header* is *Generic SIP IP-PBX Proxy*

Note that this is the same Identity/Device Profile Type used for the *Type G – SIP Registering PBX with pilot contact Route Header*.

The *Generic SIP IP-PBX Proxy* Identity/Profile Type uses the Intelligent Proxy Addressing Signaling Address type.

The *Generic SIP IP-PBX Proxy* Identity/Profile Type must have the following policies enabled:

- Static Registration Capable
- Proxy Trunk Mode
- PBX Integration

Acronyms and Abbreviations

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

ACL	Access Control List
AoR	Address of Record
ARPU	Average Revenue Per Unit
ATI	Alternate Trunk Identity
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BTLU	Business Trunking License Unit
CDR	Call Detail Record
CFNA	Call Forwarding No Answer
CFNR	Call Forwarding Not Reachable
CLI	Command Line Interface
CLID	Calling Line ID
CLIR	Calling Line Identification Restriction
CNG	Customer Network Gateway
COLR	Connected Line Identification Restriction
CSCF	Call Session Control Function
CSV	Comma-separated value
DID	Direct Inward Dialing
DN	Directory Number
DNS	Domain Name System
DoS	Denial of Service
DTG	Destination Trunk Group
ETSI	European Telecommunications Standards Institute
FAC	Feature Access Code
FQDN	Fully Qualified Domain Name
FXS	Foreign eXchange Subscriber
GIN	Generate Implicit Numbers
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Function
IAD	Integrated Access Device
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISC	IMS Service Control

ISP	Internet Service Provider
IVR	Interactive Voice Response
KTS	Key Telephony System
MGCF	Media Gateway Control Function
NAPTR	Naming Authority Pointer
NMS	Network Management System
OOTB	Out-of-the-Blue
OTG	Originating Trunk Group
P-CSCF	Proxy Call Session Control Function
PAI	P-Asserted-Identity
PBX	Private Branch Exchange
PM	Performance Measurement
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
PUI	Public User Identity
QoS	Quality of Service
S-CSCF	Serving – Call Session Control Function
SBC	Session Border Controller
SCA	Shared Call Appearance
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UC	Unified Communications
UE	User Equipment
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VTR	Verify Translation and Routing
WAN	Wide Area Network

References

[1] Cisco Systems, Inc. 2019. *Cisco BroadWorks SIP Access Interface Interworking Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[2] Cisco Systems, Inc. 2019. *Cisco BroadWorks SIP Network Interface Interworking Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[3] Cisco Systems, Inc. 2019. *Cisco BroadWorks AS Mode ISC Interface Specification, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[4] Cisco Systems, Inc. 2019. *Cisco BroadWorks AS Mode IP Multimedia Subsystem Solution Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[5] Cisco Systems, Inc. 2019. *Cisco BroadWorks Device Management Configuration Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[6] Cisco Systems, Inc. 2019. *Cisco BroadWorks Application Server Group Web Interface Administration Guide – Part 1, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[7] Cisco Systems, Inc. 2019. *Cisco BroadWorks Application Server Enterprise Web Interface Administration Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[8] Cisco Systems, Inc. 2019. *Cisco BroadWorks Container Options Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[9] Cisco Systems, Inc. 2019. *Cisco BroadWorks Treatment Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[10] Cisco Systems, Inc. 2019. *Cisco BroadWorks Call Processing Policies Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[11] Cisco Systems, Inc. 2019. *Cisco BroadWorks Communication Barring – Fixed Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[12] Cisco Systems, Inc. 2019. *Cisco BroadWorks Business Trunking Configuration Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[13] Cisco Systems, Inc. 2019. *Cisco BroadWorks SIP Business Trunking Interworking Guide, Release 23.0*. Available from Cisco at xchange.broadsoft.com.

[14] Cisco Systems, Inc. 2013. *Calling Line Identity Compliance Enhancements Feature Description, Release 18.0*. Available from Cisco Systems at xchange.broadsoft.com.

[15] SIP Forum. 2011. *SIPconnect 1.1 Technical Recommendation*. Available from http://www.sipforum.org/.

[16] Roach, A.B., "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)", RFC 6140, Internet Engineering Task Force, March 2011. Available from http://www.ietf.org/.

[17] Gurbani, V., Jennings, C., "Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)", RFC 4904, Internet Engineering Task Force, June 2007. Available from http://www.ietf.org/.

[18] 3rd Generation Partnership Project (3GPP). 2018. *TS 24.525 V15.0.0 Technical Specification Group Core Network and Terminals; Business trunking; Architecture and functional description (Release 15)*. Available at http://www.3gpp.org/.

[19] Cisco Systems, Inc. 2014. *Enterprise Trunk Enhancements Feature Description, Release 21.0*. Available from Cisco Systems at xchange.broadsoft.com.

[20] Cisco Systems, Inc. 2015. *Direct Route Service Feature Description, Release 22.0.* Available from Cisco Systems at xchange.broadsoft.com.

[21] Cisco Systems, Inc. 2018. *Terminating Alternate Trunk Identity Feature Description, Release 23.0.* Available from Cisco Systems at xchange.broadsoft.com.

[22] Cisco Systems, Inc. 2018. *Unmapped Sessions for Trunking Users Feature Description, Release 23.0.* Available from Cisco Systems at xchange.broadsoft.com.

[23] Cisco Systems, Inc. 2018. *Physical Location for SIP Trunking Users Feature Description, Release 23.0.* Available from Cisco Systems at xchange.broadsoft.com.

[24] Cisco Systems, Inc. 2018. *SIP Trunking Enhancements Feature Description, Release 23.0.* Available from Cisco Systems at xchange.broadsoft.com.

Index