

# How to Leverage SIP Trunks, Session Border Control and Session Management for Cost Savings and UC Deployment

1 June 2010

Jay Lassman, Bern Elliot

Gartner RAS Core Research Note G00200653

SIP trunks, session border control and session management can help IT organizations support an increasing number of secure, low-cost, reliable communications channels with high connection quality. They can also facilitate deployment of unified communications services and applications.

## Overview

Session Initiation Protocol (SIP) is a foundational component of a unified communications (UC) environment that supports voice, instant messaging (IM), presence, video, unified messaging and collaboration. The implementation of SIP trunks, session border control and session management can help the IT organization support an increasing number of secure, low-cost, reliable communications channels with high transmission quality.

## Key Findings

- SIP trunks can cost at least 28% less than Primary Rate Interface (PRI) trunks with comparable throughput. The aggregation of SIP trunks in the enterprise yields further cost improvements due to centralized trunking and applications, as well as economies of scale.
- Session border controllers (SBCs) can reduce SIP-based denial of service (DoS) threats that originate from within and outside an organization, and provide interoperability with various versions of SIP being used by service providers and enterprises.
- The complementary functions of session management and session border control improve enterprise communications security, UC application deployment, operational efficiency and reliability.

## Recommendations

- When deploying SIP trunks, avoid single points of failure for aggregated trunk configurations; consider more than one aggregation point to meet a geographically dispersed enterprise footprint; and maintain local direct inward dialing (DID) for consumer-centric business operations.

- When evaluating an SBC, confirm that it not only prevents DoS and distributed denial of service (DDoS) attacks, but also enables toll cost optimization. Ensure that the solution can function as an integral part of the enterprise UC solution, and provides comprehensive UC infrastructure protection and disaster recovery features.
- Verify that the SBC provider has experience resolving integration and interoperability issues in a UC environment, and that the solution's licensing model provides for cost-effective growth.
- Implement session management for dial plan normalization, interconnection with disparate platforms and endpoints, call admission control, toll cost optimization, and UC application deployment and policy management.

## Table of Contents

### Analysis

- 1.0 Introduction
- 2.0 SIP Adoption Drivers
- 3.0 SIP Trunking
  - 3.1 SIP Versus PRI Costs
  - 3.2 SIP Trunk Aggregation Issues
- 4.0 Session Border Control and Session Management
  - 4.1 Session Border Control Overview
  - 4.2 Session Manager Overview
- 5.0 Session Border Control Versus Session Management
- 6.0 SBC Functions
  - 6.1 SIP Trunk Interoperability
    - 6.1.1 SBC Interoperability and Flexibility
  - 6.2 SIP Trunk Security
    - 6.2.1 "Defense in Depth" Model Enhances Enterprise Security
    - 6.2.2 ALG for All SIP Signaling and Media Traffic
  - 6.3 SIP Trunk Control
    - 6.3.1 Increases Call Routing Options for Enterprises
  - 6.4 SBC Evaluation Criteria
- 7.0 Session Manager Functions
  - 7.1 Communications Session Manager Evaluation Criteria
- 8.0 Federation
- 9.0 Bottom Line

## List of Tables

Table 1. Annual North American Savings Projection: \$4471.20 (28%) for Each 23-Channel PRI Replaced

Table 2. Comparison of SBC and Session Manager Functions

## List of Figures

Figure 1. Example of SBC Deployment

Figure 2. Example of Session Manager Deployment

## Analysis

### 1.0 Introduction

This document was revised on 2 June 2010. For more information, see the [Corrections](http://gartner.com/technology/.../article8.html) page on [gartner.com/technology/.../article8.html](http://gartner.com/technology/.../article8.html)

gartner.com.

Internet Protocol (IP)-based communications is enabling the convergence, transport and management of multiple communications modes — such as voice, video, text, IM, presence and multimedia messaging — across a common network. With adoption growing, the enterprise, and specifically the IT organization, is challenged to support an increasing number of secure, low-cost, reliable communications channels with high call quality.

SIP has emerged as the protocol for implementing a cost-effective, standards-based converged communications network that also integrates with legacy communications environments and many traditional protocols. SIP is actively supported by the Internet Engineering Task Force (IETF), as well as industry groups, to make sure SIP works across enterprises that use a variety of architectures, standards and products. While it's important to recognize that SIP is a standard, not all SIP is the same. Service providers, as well as customer premises equipment manufacturers, all support their own forms of SIP.

[⚡ Back to Table of Contents](#)

## 2.0 SIP Adoption Drivers

SIP is a foundational component of a UC environment intended to support current and emerging applications for video and collaboration, and is becoming the standard protocol for UC deployments. Using SIP trunks as the transport within public and private networks, combined with session border control and communications session management, can help an enterprise:

- Improve communications system security, reliability and performance
- Optimize costs
- Deploy location-independent UC services and applications

[⚡ Back to Table of Contents](#)

## 3.0 SIP Trunking

### 3.1 SIP Versus PRI Costs

The PRI has been the standard for connecting PBXs to the public switched telephone network (PSTN) for years. A PRI in North America multiplexes 23 64 Kbps voice channels and one 64 Kbps signaling channel across a T1 link (or 30 64 Kbps voice channels across an E1 link in Europe). Because this is done via time division multiplexing (TDM), it does not take advantage of the gaps in conversations when no traffic is sent. Packetized IP traffic can take advantage of the statistical nature of traffic flow, and conversation gaps do not consume bandwidth. Experience with SIP trunking suggests that at least 50 conversations can be supported on a single T1 line; some customers have attained 70 conversations with no audible impact. Our high-level calculations suggest that there is at least a 28% savings when migrating to SIP trunking, but the savings could be greater when considering that a SIP trunk can support twice as many sessions as a PRI. The challenge has been that not all central offices support SIP trunking, and not all enterprises have SIP trunking capabilities on their voice systems.

The following example (for North America) compares the costs of PRI facilities with SIP trunk facilities that can carry the equivalent traffic. Potential operating expenditure (opex) reductions result from fewer trunk requirements and lower rates (see Table 1).

#### **PRI Cost**

- About \$1,325 per PRI per month with 20,000 long distance (LD) minutes
- About \$57.60 per channel per month with 870 LD minutes

#### **SIP Trunk Cost**

- \$450 per access, plus \$15 per channel per month plus \$0.02 LD per minute off network
- \$41.40 per session per month with 870 off network LD minutes

**Table 1. Annual North American Savings Projection:  
\$4471.20 (28%) for Each 23-Channel PRI Replaced**

| Transport Cost                             | PRI     | SIP     | Difference |
|--|---------|---------|------------|
| <i>PRI channel per month</i>               | \$57.60 | *       | *          |
| <i>Equivalent SIP connection per month</i> | *       | \$41.40 | *          |
| <i>Monthly savings projection</i>          | *       | *       | \$16.20    |

Source: Gartner (June 2010)

[↩ Back to List of Tables](#)  
[↩ Back to Table of Contents](#)

Gartner estimates the annual savings projection for other global regions will be within 15% to 28%. Cost optimization can also be gained by aggregating large numbers of SIP trunks into strategically chosen centralized locations. Furthermore, centralizing contact center call treatment allows better customer service, leveraging contact center staff, and can minimize disruption of customer-facing branch staff.

While cost optimization is important, organizations should also understand that SIP is a foundational component of a UC environment that supports voice, IM, presence, video, unified messaging and collaboration. The implementation of SIP trunks, session border control and session management can help IT organizations support an increasing number of secure, low-cost, reliable communications channels with high transmission quality.

As the example indicates, there is a clear opportunity for enterprises as they migrate to IP PBXs. For most enterprises, the migration to an IP PBX is a multimonth project. Very early in the project, organizations should be working with a carrier or secondary provider to ensure that SIP trunking is available where needed when the project cuts over to an IP PBX. The following list is a sampling of service providers that support SIP trunks:

- AT&T
- Cable & Wireless
- CBeyond
- Chief Telecom
- Global Crossing
- KT (formerly Korea Telecom)
- Orange (France Telecom)
- Paetec
- Verizon Business

[↩ Back to Table of Contents](#)

## 3.2 SIP Trunk Aggregation Issues

While it is very cost-effective to aggregate a large number of SIP trunks at a central location, it's important to:

- Avoid single points of failure for aggregated trunks.
- Maintain local DIDs for consumer-centric business operations (e.g., local branch phone numbers).
- Maintain local branch trunks for survivability.
- Consider more than one aggregation point to meet geographically dispersed enterprise footprints.

- ◆ Recognize that regional and international availability of SIP trunking is variable.

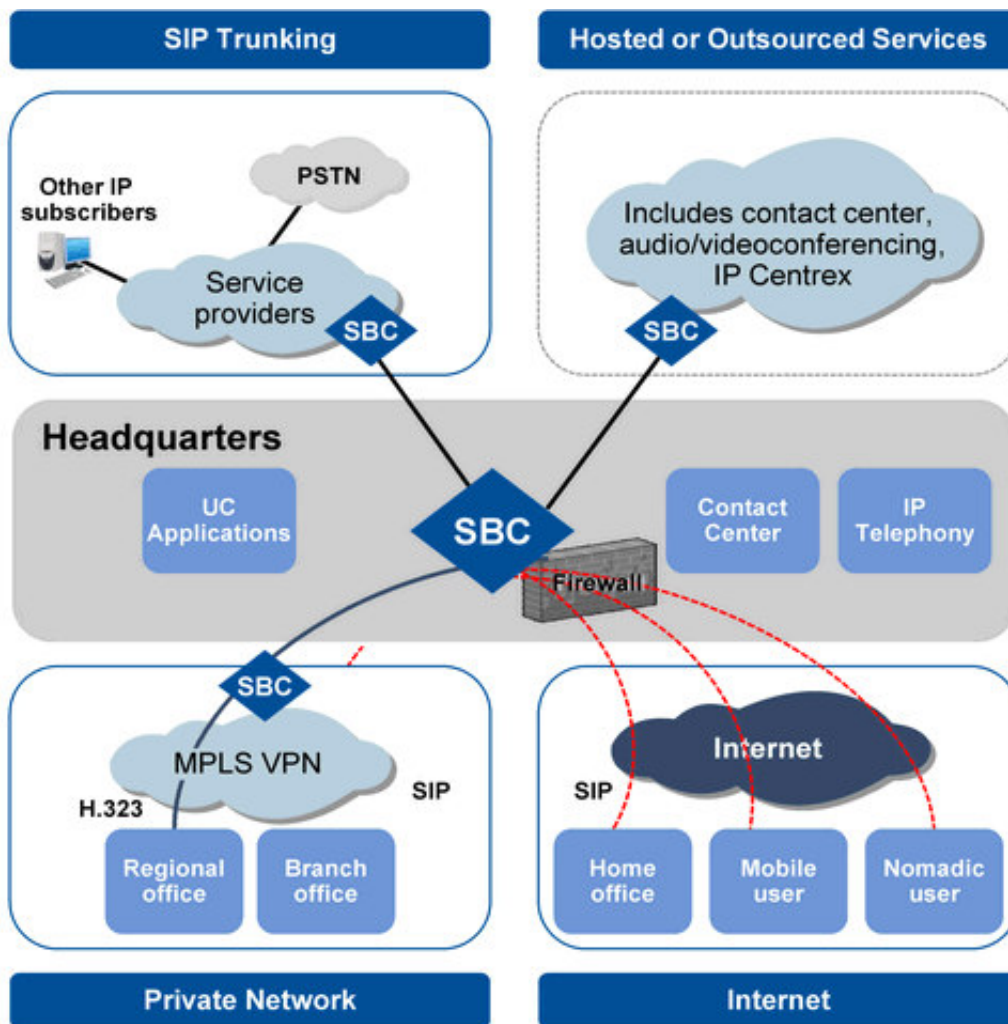
[⚡ Back to Table of Contents](#)

## 4.0 Session Border Control and Session Management

### 4.1 Session Border Control Overview

SBCs provide a secure, controlled connection for points between networks that provide interactive, IP-based communications like SIP-based UC. As shown in Figure 1, the SBC is usually found at the border between the enterprise communications network and the service provider's SIP trunking network, which can constitute a combination of the SIP trunking border and hosted services border.

**Figure 1. Example of SBC Deployment**



Source: Acme Packet (May 2010)

[Back to List of Figures](#)  
[Back to Table of Contents](#)

SBCs can:

- ◆ Control signaling and media streams involved in setting up, conducting, and tearing down telephone or other interactive media communications
- ◆ Be used to control and secure communications with Internet-based remote workers or even

internal networks

- Provide security and address many issues that are inherent to interconnecting different communications networks, including protocol interworking and transcoding, ensuring connection quality, managing network-related costs and regulatory compliance

In addition, SBCs work in parallel with data firewalls that handle non-SIP traffic and provide stronger security protection than a SIP application layer gateway (ALG) firewall, and are often deployed in conjunction with data firewalls.

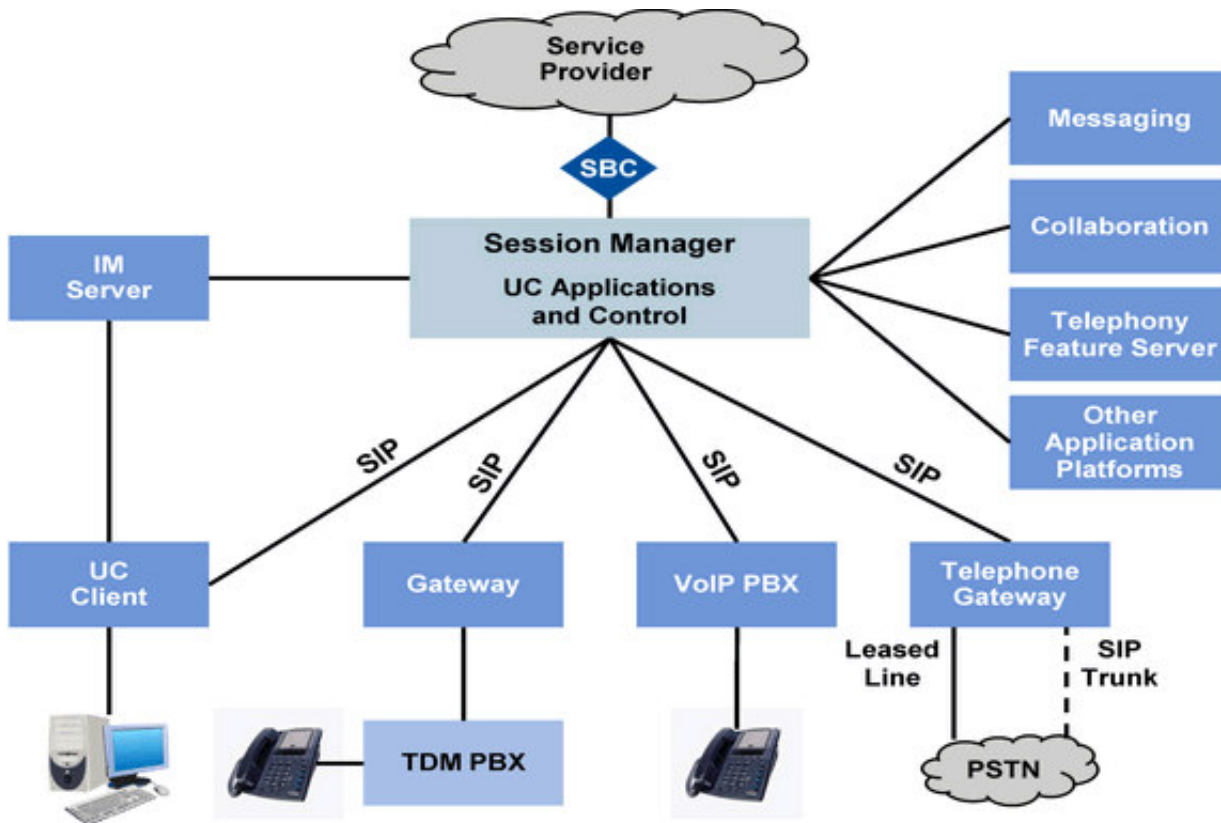
Requirements are not limited to wired systems. Smartphones have become more pervasive and include voice over IP (VoIP) technologies like Wi-Fi. As these devices traverse internal and external networks, SBCs that understand these transitions have emerged. Organizations that want to leverage voice over cellular and VoIP, voice over Wi-Fi (VoWi-Fi) and third-generation (3G) networks will need to consider the security implications. Accordingly, in addition to supporting SIP, new classes of SBCs are dealing with the security issues across multiple physical network types. For example, Agito Networks, a vendor of enterprise mobile communication gateways that supports fixed-mobile convergence (FMC), provides capabilities that augment security when there are handoffs between private Wi-Fi networks and public cellular networks. Furthermore, IP PBX vendors are beginning to add this functionality using software clients, of which Avaya's one-X Mobile is an example. However, these capabilities are not yet formalized into a complete multinetwork solution that offers roaming, security and protocol management.

[↩ Back to Table of Contents](#)

## 4.2 Session Manager Overview

Session managers are positioned within a private network for midsize to large enterprisewide UC, collaboration and contact center applications. They help save money for toll charges, aggregate trunks and enable dial plan integration for a multivendor implementation. They also enable employee-specific access, authentication, endpoint registration services and application integration services. An important distinction between an SBC and a session manager is that the session manager is situated within the private network (see Figure 2), whereas the SBC is almost always located between a public network and a private network. In addition, a session management operation depends on signaling, rather than using media streams. The private network can comprise transport between a central location and distributed sites, as well as from the central location to the Internet.

### Figure 2. Example of Session Manager Deployment



Source: Avaya (May 2010)

- [⚡ Back to List of Figures](#)
- [⚡ Back to Table of Contents](#)

## 5.0 Session Border Control Versus Session Management

Table 2 summarizes when to use an SBC or session manager, and whether there is overlap between the two.

**Table 2. Comparison of SBC and Session Manager Functions**

| Function Description  | SBC   | Session Manager                     | Potential Overlap |
|---|---|-------------------------------------|-------------------|
| <b>Architecture</b>   |   |                                     |                   |
| Network location  | Border between trusted and mistrusted network | Internal to private trusted network | No                |
| Signaling control (call forking, SIP normalization, identity control, etc.) | Between networks                              | Within enterprise                   | Yes               |
| Media control   | Yes   | No                                  | No                |
| <b>Interworking</b>   |   |                                     |                   |
| Media manipulations (codec conversions, media forking, etc.)                | Yes   | No                                  | No                |
| Codec and protocol interworking   | Yes   | No                                  | No                |
| Network address translation   | Yes   | No                                  | No                |
| <b>Operations Support</b>   |   |                                     |                   |
| Session detail recording (call detail recording)                            | Yes (Edge)                                    | Yes (Core)                          | Yes               |

|  |                            |                                |     |
|--|----------------------------|--------------------------------|-----|
| SIP debugging and tracing                                      | Between networks           | Within enterprise              | No  |
| <b>IP PBX Traffic Optimization</b>                             |                            |                                |     |
| Endpoint registration, authentication and location services    | No                         | Yes                            | No  |
| Binds users to applications                                    | No                         | Yes                            | No  |
| Centralized dial plan  | No                         | Yes                            | No  |
| Application-aware routing (application sequencing)             | No                         | Yes                            | No  |
| Media replication for call session recording                   | Yes                        | No                             | Yes |
| Session routing  | Yes                        | Yes                            | Yes |
| <b>Policy Management</b>                                       |                            |                                |     |
| Policy scope   | Within network             | Personnel-specific             | Yes |
| Directory interfaces   | No                         | Yes                            | No  |
| External policy interfaces                                     | No                         | Yes                            | No  |
| Routing policy management                                      | No                         | Yes                            | Yes |
| <b>Security</b>  |                            |                                |     |
| Transport Layer Security (TLS) signaling security              | Between networks           | Within enterprise              | No  |
| Configurable SIP/network firewalls with deep packet inspection | Between networks           | Within enterprise              | No  |
| Call admission control   | Yes (to external networks) | Yes (within the enterprise)    | Yes |
| Identity-based access control                                  | No                         | Yes                            | No  |
| DoS/DDoS protection  | Yes                        | Yes (mainly within enterprise) | Yes |
| Topology hiding  | Yes                        | No                             | No  |
| Intrusion detection reporting                                  | Yes                        | No                             | No  |
| Emergency notification prioritization                          | Yes                        | No                             | Yes |
| <b>Service Assurance</b>                                       |                            |                                |     |
| Load balance communications services                           | No                         | Yes                            | Yes |
| Business continuity/disaster recovery features                 | Yes                        | Yes                            | Yes |

**Source: Gartner (June 2010)**

[❖ Back to List of Tables](#)  
[❖ Back to Table of Contents](#)

## 6.0 SBC Functions

In addition to protection against DoS and DDoS threats, SBCs allow a range of other beneficial functions. We list some of the leading benefits.

[Back to Table of Contents](#)

### 6.1 SIP Trunk Interoperability

IP PBXs are not always able to connect directly to carrier SIP trunks. An SBC acts as a [gartner.com/technology/.../article8.html](http://gartner.com/technology/.../article8.html)

IP PBXs are not always able to connect directly to carrier SIP trunks. An SBC acts as a demarcation point between the service provider and the enterprise. In many cases, an SBC provides a smaller operational impact to the service provider and the enterprise by terminating the SIP trunk on an SBC, rather than directly to a PBX that may be operational. For example:

- Variations exist in SIP implementations.
- H.323 is the only available IP interface.

[↩ Back to Table of Contents](#)

### 6.1.1 SBC Interoperability and Flexibility

- Complete SIP header manipulation rule (HMR) capabilities to interwork different SIP dialects between PBX and carrier SIP trunking elements
- Full H.323 — SIP interworking
- Media transcoding and dual-tone multifrequency (DTMF) format (INFO/2833) interworking
- Signaling transport (User Datagram Protocol [UDP]/TCP/Transport Layer Security [TLS]) and media encryption (Real-Time Transport Protocol [RTP]/Secure RTP [SRTP]) interworking
- Interoperability with all the major PBX and UC vendors and SIP trunk carriers supports virtually any SIP or H.323-capable PBX or UC platform, so they can talk to any carrier SIP trunk service

[↩ Back to Table of Contents](#)

## 6.2 SIP Trunk Security

### 6.2.1 "Defense in Depth" Model Enhances Enterprise Security

- Like e-mail and Web applications, SIP-based communications applications have unique security requirements and vulnerabilities.

[↩ Back to Table of Contents](#)

### 6.2.2 ALG for All SIP Signaling and Media Traffic

- SBCs are similar to ALGs used for enterprise IT applications today.
- SBC features include dynamic port control, full SIP firewall and DDOS protection.

[↩ Back to Table of Contents](#)

## 6.3 SIP Trunk Control

### 6.3.1 Increases Call Routing Options for Enterprises

- Supports least cost routing, call quality-based routing and time-of-date routing options
- Provides connection admission and emission control
- Enhances failover and load-balancing capabilities
- Provides called and calling number digit normalization

[Back to Table of Contents](#)

## 6.4 SBC Evaluation Criteria

The SBC market includes vendors such as:

- Acme Packet
- AudioCodes

- AudioCodes
- Cisco
- Ingate
- Sipera
- Sonus Networks
- Thomson

Gartner estimates that Acme is the SBC market share leader, with 50% in 2009. Avaya also has SBC products within its UC portfolio. During the evaluation process, ensure that the SBC solution:

- Has been thoroughly tested and documented as an integral part of the enterprise UC solution, including common use cases, such as SIP trunking, remote worker, remote contact center agent, video, etc.
- Has been incorporated into the certification configurations of the enterprise UC solution with the SIP trunk service provider
- Provides support and maintenance services for UC
- Has a large installed base in the service provider market, ensuring the enterprise deployment of the SBC will mesh well with the service provider's SBC
- Provides a full set of security features, including prevention of DoS and DDoS attacks
- Supports UC infrastructure resiliency and disaster recovery features
- Scales well from about 25 to many thousands of concurrent sessions in two specific use cases:
  - In small sites, such as remote branches, and large sites, such as centralized data centers
  - During early stage deployments with planned growth for later-stage deployments
- Can be deployed in a stand-alone configuration for data networking applications, or for converged voice and data applications
- Supports high-traffic, high-availability enterprise and contact center use cases
- Offers pricing and a licensing model that enables cost-effective future growth
- Supports interoperability with a range of session manager and voice platform vendors

Gartner estimates that the incremental cost of adding session border control for 2,000 users and 200 simultaneous sessions is \$0.65 per user per month, based on a three-year amortization period.

[↩ Back to Table of Contents](#)

## 7.0 Session Manager Functions

The following summarizes session manager functions:

- Dial plan "normalization" unification and virtualization
- Centralizing the management of alternate, time-of-day and least-cost routing
- Integration with third-party PBX, SBC and SIP gateway equipment by normalizing SIP to standard SIP for use by all core applications
- Providing UC policy control for directory and class of service
- Enabling real-time deployment of UC applications; the ability to bind applications to selected users allows application development and trials on production systems without risk
- Support for carrier arbitrage
- Load balancing across application servers — in the same data center and across data centers
- Communication with disparate UC platforms and endpoints
- Application policy enforcement at the user level
- Ability to manage and report on a single communication session end-to-end, across multiple legs and connections providing global session/call detailed reporting at an enterprise level
- Provide debugging tools for sessions across the enterprise that has cross multiple nodes, devices and locations

[Back to Table of Contents](#)

## 7.1 Communications Session Manager Evaluation Criteria

Avaya and Cisco offer platforms specifically developed to support a broad range of session management capabilities for their respective flagship UC product lines. However, session management functions are evolving within the SIP-based enterprise voice communications portfolios of providers such as Aastra, NEC and Siemens.

During the evaluation process, ensure that the session management solution:

- Supports integration with a range of voice platforms directly via SIP or SIP gateways
- Includes capabilities for "normalizing" SIP from different service providers for use throughout the enterprise core
- Supports centralized dial plan management by unifying disparate dial plans of PBXs throughout the enterprise into a single dial plan across a multivendor architecture
- Enables routing for on-network and tail-end hop-off calls to bypass the PSTN
- Enables an administrator to specify per user policies for time of day, white list and black lists
- Allows the direct registration of SIP phones to the centralized core
- Supports the same routing, policy management, dial plan, capabilities, etc., for contact center applications
- Has a pricing and licensing model that supports cost-effective growth
- Supports scalability up to hundreds of sites and thousands of endpoints
- Offers cost-effective redundancy options that also fit into business continuity and disaster recovery plans
- Supports interoperability with a range of SBC, voice platform vendors and IP phones

Gartner estimates that the incremental cost of adding session management to a 2,000-user organization is \$0.50 per user per month, based on a three-year amortization period. Some vendors bundle session management prices into premium user licenses that can reduce the cost for the same 2,000-user organization to less than \$0.25 per user per month.

[↩ Back to Table of Contents](#)

## 8.0 Federation

The concept of "federation" is to permit different companies to have open, end-to-end SIP communications among end users. Session managers and SBCs facilitate the implementation and operation of secure federated environments, and manage the connections that allow the federation of communications services.

The SBC provides security from external DoS and intrusion detection reporting attacks. They also ensure that packets only pass between approved networks.

The communications session manager ensures policy enforcement per employee and per application, including access, authentication and authorization.

Additional capabilities session managers and SBCs offer include:

- Compliance enforcement, session recording
- Call admission control
- Interoperation between different SIP protocols
- Session prioritization
- Linkage of different directory/dial plan islands into a single, unified dial plan

[Back to Table of Contents](#)

## 9.0 Bottom Line

While organizations can use SIP trunks, SBCs and communications session managers separately, these components also perform a wide range of complementary functions. Combined use supports

enhanced security, presents opportunities for cost optimization, and improves system performance as well as reliability. Organizations that are deploying UC and have mission-critical contact center investments should consider SIP trunks, SBCs and session managers as integral components of their enterprise communications strategies.

[❖ Back to Table of Contents](#)

*© 2010 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.*