

Hosted IP communications services solutions

application note

Improving collaboration & productivity with hosted IP communications services

Businesses are turning to hosted service providers and new cloud-based services for a wide range of IP communications needs from audio and video conferencing solutions to virtual contact center offerings. By leveraging the expertise and capital investments of an experienced service provider, enterprises can improve business agility while reducing CAPEX and OPEX. When deploying hosted IP communications services, businesses must ensure their IP telephony and Unified Communications (UC) solutions interoperate seamlessly with the hosted service provider infrastructure, confidential communications remain safe and secure and their end-users enjoy outstanding service quality. Acme Packet Enterprise Session Border Controllers (E-SBCs) are specifically designed to ensure the successful implementation of hosted IP communications services. The solutions deliver:

- Strong security by safeguarding user confidentiality and privacy, and protecting enterprise IT assets
- Easy interoperability by resolving multi-vendor compatibility issues and enabling multi-protocol interworking
- Assured reliability by enforcing service quality and enabling high availability services

Acme Packet E-SBCs allow businesses to enjoy all the features and benefits of a hosted or cloud-based communications service without sacrificing reliability or integrity. Acme Packet offers a complete portfolio of solutions for hosted IP communications services suitable for virtually any business regardless of size or industry.

Service Providers offer a wide range of hosted IP communications solutions

Enterprises are turning to hosted service providers for a wide variety of IP communications solutions including:

- HD IP video conferencing services that enhance collaboration and reduce expenses and lost productivity due to travel
- Audio conferencing services that enable multiparty communications without the burden of a conventional on-site system
- IP contact center services for implementing virtual contact centers that span geographies and leverage home workers and offshore agents
- IP Centrex services that provide enterprise-class telephony features without the expense and maintenance hassles of an on-site office phone system
- UC services which provide presence-enabled voice, video, and multimedia capabilities to improve collaboration and productivity

Hosted IP communications services reduce cost and improve business agility

Hosted IP communications services offer a variety of functional and business benefits. By deploying hosted IP communications services enterprises can:

- Save CAPEX and OPEX by reducing on-site equipment and simplifying network planning, operations and management
- Protect and enhance existing IT assets by adding cloud-based services to premises-based UC and IP telephony solutions
- Improve productivity and collaboration with state-of-the art communications features such as high-definition video conferencing, on-line meetings, and communications-enabled business processes
- Leverage the Internet to extend corporate communications services to small offices, remote workers and mobile professionals and to implement cost-effective disaster recovery and business continuity plans
- Improve business agility and business innovation by enabling services, features and users on-demand and by allowing valuable IT resources to focus on strategic initiatives
- Avoid risk, business interruptions and technology obsolescence with carrier-class availability and non-disruptive service upgrades and feature updates

Session Initiation Protocol – the foundation for hosted IP communications services

The Session Initiation Protocol (SIP) has emerged as the standard protocol for controlling interactive communications over IP networks and serves as the foundation for contemporary hosted IP communications services. By standardizing on SIP, hosted service providers are able to support a wide variety of enterprise IP telephony systems and endpoints, and offer customers greater choice and flexibility. Enterprise networks and service provider networks are typically connected via SIP trunks.

As with any new technology, enterprises must consider a number of technical matters when implementing hosted IP communications services and interfacing private enterprise networks with shared service provider networks. Interactive IP communications introduces security, interoperability and reliability issues which are beyond the scope of existing IP networking solutions. Conventional IP firewalls, application layer gateways (ALGs) and IP security appliances weren't designed with real-time interactive IP communications in mind and leave the enterprise vulnerable to a variety of security threats. IP traffic shapers, load balancers, bandwidth management solutions and policy management systems weren't designed to control interactive voice or video sessions, and can't guarantee high-quality rich media experiences. IP routers, firewalls and application layer gateways can't resolve the multi-vendor interoperability and multi-protocol interworking issues businesses often encounter when interfacing with hosted service providers.

The unique role of the enterprise SBC

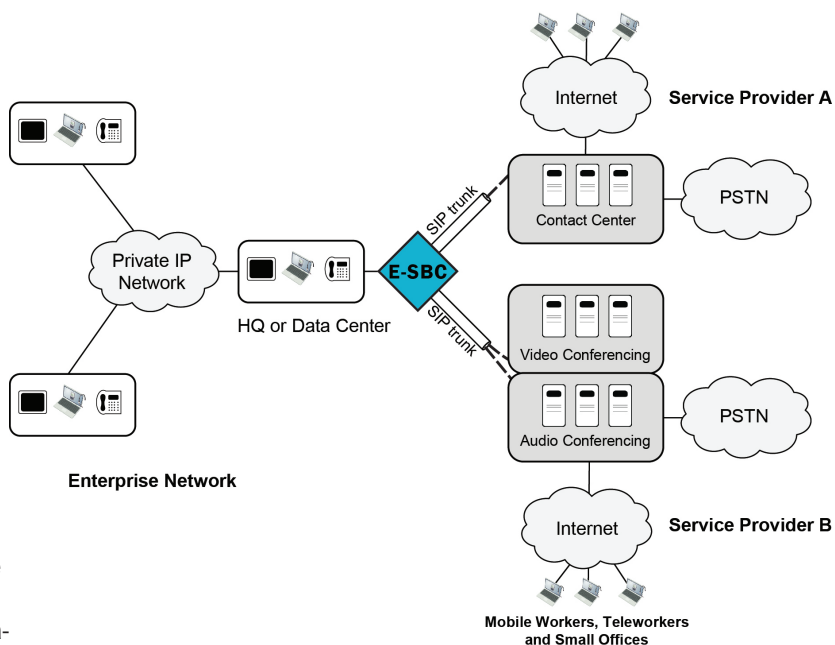
SBCs are typically deployed in both the service provider data center and at the customer premise for ultimate security and control. Enterprise SBCs and service provider SBCs perform different functions. The service provider SBC is intended to protect, control and segregate the service provider infrastructure. The E-SBC is intended to protect and control the enterprise network. Leading IP telephony and UC vendors including Avaya, Cisco, Siemens and Alcatel-Lucent strongly recommend businesses install enterprise SBCs to safeguard and control SIP trunking borders. E-SBCs perform a range of critical functions including the following:

- E-SBCs protect the enterprise against a wide range of internal and external security threats including threats originating from the service provider network
- E-SBCs can be dual homed for load balancing or service provider diversity or to enable service continuity in the event of facility failures
- E-SBCs allow enterprises to configure custom QoS parameters and session routing and call admission control settings to enforce compliance with corporate security policies and business practices
- E-SBCs are vital for troubleshooting problems and isolating voice and video quality issues within the enterprise network domain

Acme Packet E-SBCs protect and control hosted IP communications services

When implementing hosted services, enterprises must put systems in place to safeguard IT assets and confidential information, mitigate interoperability and interworking issues, protect against service outages and maintain the high service levels users have come to expect from the corporate phone system and premises-based communications solutions.

Acme Packet E-SBCs are specifically designed to address the unique security, interoperability and reliability challenges that accompany the implementation of hosted IP communications services. Enterprises typically install E-SBCs at IP communications service provider network borders in the same way they install firewalls at IP network borders.



Acme Packet E-SBCs provide extensive security features to protect enterprise IT assets and safeguard the confidentiality and integrity of enterprise communications, and provide extensive protocol normalization features to help enterprises avoid hosted service interoperability and compatibility issues. In addition, Acme Packet E-SBCs are based on a highly-available architecture and are capable of rerouting sessions around trunk or service failures to ensure hosted service availability. Key features and functions include:

Feature	Function
Security	
<ul style="list-style-type: none"> Granular access control 	<ul style="list-style-type: none"> Prevent fraud and service theft
<ul style="list-style-type: none"> IP address and SIP signaling concealment 	<ul style="list-style-type: none"> Safeguard privacy and confidentiality
<ul style="list-style-type: none"> Layer 3-5 topology hiding and signaling overload controls 	<ul style="list-style-type: none"> Prevent reconnaissance scans and DoS/DDoS attacks
<ul style="list-style-type: none"> IP telephony spam protection 	<ul style="list-style-type: none"> Mitigate nuisance calls
<ul style="list-style-type: none"> Stateful deep packet inspection 	<ul style="list-style-type: none"> Remove malicious viruses and worms from SIP messages
<ul style="list-style-type: none"> Signaling and media encryption 	<ul style="list-style-type: none"> Prevent eavesdropping, hijacking and impersonation
Interoperability	
<ul style="list-style-type: none"> SIP message normalization Response code translation SDP and DTMF manipulation Number and URI manipulation Signaling message header manipulation 	<ul style="list-style-type: none"> Resolve multi-vendor interoperability issues
<ul style="list-style-type: none"> Transport interworking (TCP, UDP, SCTP) Encryption interworking (TLS, MTLS, SRTP, IPsec) NAT and firewall traversal IP address translation: private/public, IPv4/IPv6 Transcoding 	<ul style="list-style-type: none"> Interconnect autonomous IP telephony islands Implement end-to-end IP communications
Reliability	
<ul style="list-style-type: none"> Stateful signaling & media failover 	<ul style="list-style-type: none"> Enable high availability
<ul style="list-style-type: none"> QoS marking, VLAN mapping, access control 	<ul style="list-style-type: none"> Guarantee service quality
<ul style="list-style-type: none"> Registration storm avoidance Call rate limit enforcement 	<ul style="list-style-type: none"> Prevent network and system overload
<ul style="list-style-type: none"> Trunk load balancing 	<ul style="list-style-type: none"> Optimize performance
<ul style="list-style-type: none"> Stateful session routing 	<ul style="list-style-type: none"> Circumvent equipment and facility failures



100 Crosby Drive
Bedford, MA 01730 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com

© 2011 Acme Packet, Inc. All rights reserved. Acme Packet, Session-Aware Networking, Net-Net and related marks are trademarks of Acme Packet. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Acme Packet without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Acme Packet assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Acme Packet, Acme Packet has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.

03/09/11