



## Acme Packet session border controllers in the enterprise

*Acme Packet session border controllers enable the delivery of trusted, first-class enterprise IP telephony today and Unified Communications tomorrow*

**Whitepaper**

### Introduction

Large enterprises have been expanding their deployments of IP telephony (IPT) for several years now. Planning has already begun to extend the benefits of interactive communications over IP beyond voice services to include real-time presence-based voice, videoconferencing, chat/instant messaging, multimedia collaboration, telepresence, and more. With encouragement from major IT vendors, some enterprises will achieve this objective by deploying suites of integrated real-time applications over IP—often referred to as Unified Communications (UC)—as well as core business applications enhanced with interactive communications capabilities, e.g., CRM enabled with click-to-call and call recording features.

Delivering these real-time, interactive communications services and applications over IP will be critical to fostering business agility, boosting employee accessibility and efficiency, improving customer service, and reducing IT capital and operating costs. But significant challenges in security, interoperability, service assurance and regulatory compliance emerge once enterprises begin migrating voice and video away from service provider TDM services and converging them on IP networks.

Session border controllers (SBCs), product solutions extensively used by service providers to address these shortcomings, are now being deployed by enterprises to enable the delivery of secure, high-quality, real-time interactive communications, including IPT and UC. Similarly, service providers are using SBCs in new outsourced interactive communications offerings for enterprises such as hosted contact centers and hosted Voice over IP (VoIP) services.

## Business challenges

The business world is now global, 24/7/365, mobile, and real-time. The emergence of new economic powerhouses like India and China has intensified the competition for customer loyalty and money. The advent of a more globalized economy has meant both improved availability of lower-cost labor and the entry of agile new competitors unburdened by legacy IT infrastructure. Meanwhile, customer expectations of the level of service their vendors provide are rising. Any enterprise that hopes to survive in this environment must optimize the efficiency of its internal and customer-facing business processes by reducing “human latency”; the time it takes to identify, access and connect the best-available employees to make decisions, address customer needs and solve problems quickly.

In this newly competitive environment, enterprises face a broad spectrum of challenges, including how to:

- Equip employees with better real-time communications tools to improve the speed and efficiency with which they interact with each other and with customers; this includes adding real-time communications features to core business and productivity applications
- Build customer loyalty by optimizing business processes such as order entry and inquiry/problem resolution, enabling customers to quickly reach the right employees via the best available communications channels
- Respond to economic and competitive pressures by reducing infrastructure costs, notably by using IT selectively to simplify, optimize and drive cost out of overhead business processes (e.g., travel, communications)
- Identify processes and skills that are core to the business, and selectively outsource the rest
- Minimize the enterprise’s exposure to risk with appropriate investments in security and business continuity while achieving compliance with all relevant government and commercial regulatory requirements

## Technology trends and challenges

IT strategists working to arm the enterprise with the tools it needs to survive in an increasingly competitive world must address several overarching technology trends and challenges.

**The transition from TDM-based telecommunications to VoIP is mainstream.** VoIP’s ability to reduce costs and improve communications efficiency is widely recognized as essential to competitive parity. Gartner research shows that “voice and data convergence based on IP telephony will be underway in more than 95 percent of large companies by 2010.” IP PBXs are now widely deployed, though many still operate as islands disconnected from the broader enterprise telephony environment.

**New interactive communications imperatives are accelerating the transition to IP.** Enterprises are working to add mobile, remote and home-based workers to the enterprise IP telephony environment. They plan to upgrade existing tools with real-time capabilities like instant messaging, presence, videoconferencing, and multimedia collaboration and integrate UC with business applications. IP infrastructure is simultaneously becoming more complex and more critical to the business, heightening its need for security, reliability and availability.

**Regulatory and commercial compliance issues bring their own challenges.** Enterprises are struggling to migrate compliance-oriented systems and features from their TDM environments into the IP world, including privacy, call recording, emergency services, and domain separation.

**Migrating the contact center to IP and interactive communications is a new focus.** Enterprises are moving to equip their contact center agents with IP telephony, to integrate chat, voice and video into agent-supporting applications and to migrate call recording to the IP environment. Contact center virtualization across geographically distributed sites, including home-based contact center agents, is the future.

**The widespread deployment of IP telephony has revealed cracks in IP and security infrastructure originally designed for non-real-time data.** Real-time interactive IP communications are initiated from both inside and outside of the enterprise security perimeter, putting new stresses on the network. Traffic patterns are dramatically different, marked by two-way flows of more continuous, less bursty traffic. The multi-protocol, real-time nature and criticality of this new traffic is exposing gaps in network security. Fairly simple-to-mount attacks, such as signaling overloads, can cause catastrophic failures in IP telephony elements. This new universe of threats demands more sophisticated, stateful defense mechanisms.

Routers, firewalls and network intrusion prevention systems have major deficiencies for real-time interactive IP communications. For example, they cannot dynamically correct VoIP interoperability issues, perform deep packet inspection (DPI) of VoIP packets or media, nor track session state to recover from network failures and thereby provide uninterrupted service.

## New control requirements

To successfully deliver IP telephony throughout the enterprise and prepare for additional interactive communications services, enterprises must focus on additional controls for their IPT/UC infrastructure in five key areas:

### Security

IPT/UC infrastructure must be protected from DoS/DDoS attacks, overload of signaling and media elements, intrusions by malware like viruses, worms and spam for Internet telephony (SPIT), and directed attacks that exploit knowledge of network topology and addressing conventions. Identity and session privacy must be protected where necessary with signaling and/or media encryption. Problems associated with unauthorized access—e.g., DoS/DDoS attacks, identity and information theft, and service fraud—must be minimized.

### Application reach maximization

Enterprise IPT/UC applications must extend to remote offices as well as individual users who are mobile, located in small offices, or working from home offices. They must integrate with hosted VoIP services and VoIP-enabled applications, including audio and videoconferencing services, contact center services, IP Centrex services used to augment premise-based systems for certain sites or divisions, and VoIP-enabled business applications such as salesforce.com. In many enterprises, IP PBXs from multiple vendors have been deployed as the result of decentralized IT planning or growth through acquisition. This results in a patchwork of trunk-side signaling protocols and varying implementations of signaling protocols.

These requirements demand interworking capabilities to mediate technology differences in signaling protocols (e.g., SIP vs. H.323), vendor implementations of signaling protocols (e.g., Nortel SIP vs. Avaya SIP), transport protocols (TCP, UDP and SCTP), encryption protocols (TLS, MTLS, SRTP and IPsec), and codecs (G.711, G.729 A/B, G.729 E, G.723.1, G.726, G.728, iLBC). The SBC should also offer a means to translate between overlapping private IP address spaces, different dial plans and different versions of IP (IPv4 vs. IPv6).

### SLA assurance

Given the criticality of the business processes that IPT and UC support, the network and application infrastructure must exhibit very high levels of service quality and availability. Defending signaling elements from malicious attacks and extraordinary but non-malicious network events (e.g., re-registration floods) is one key component of SLA assurance. Other key components include policy-based admission control and load balancing for IPT and UC servers; quality of service (QoS) marking and VLAN mapping to assign VoIP traffic to appropriate paths through the network; and QoS and Answer Seizure Ratio (ASR) reporting capabilities to monitor network performance for voice quality and service provider SLA compliance.

### Cost optimization

With the downturn-driven renewed focus on cost control, enterprises must deploy interworking and protocol normalization to maximize the shelf life of their existing IPT infrastructure. Other cost-reduction mechanisms include policy-based routing at the network border to yield optimal efficiency and economy in the use of service providers.

### Regulatory compliance

Mechanisms deployed in the TDM environment to effect governmental and commercial regulatory compliance must be supported in the IP environment. Such mechanisms include call recording, call prioritization for emergency services (E9-1-1), National Security/Emergency Preparedness (NS/EP) in government agencies, and domain separation between business groups or operations such as financial services research and trading.

## Acme Packet Enterprise session border control solutions

Acme Packet® SBCs enable enterprises to control four critical IP network borders to their data centers that host IPT/UC infrastructure, as shown in Figure 1:

- **IP trunking border**—connections to service provider IP networks linking the enterprise to the outside world of PSTN and IP endpoints
- **Private network border**—connections to internal employees located on the enterprise campus LAN and in remote offices connected via private WAN services such as MPLS VPNs
- **Internet border**—connections to small offices, users working from home and mobile employees over the public Internet
- **Hosted services interconnect border**—private connections to service providers or Application Service Providers (ASP) that offer hosted IP-based audio and videoconferencing services, IP contact center services, IP Centrex to augment premise-based systems for certain sites, business groups or divisions and VoIP-enabled business applications such as salesforce.com.

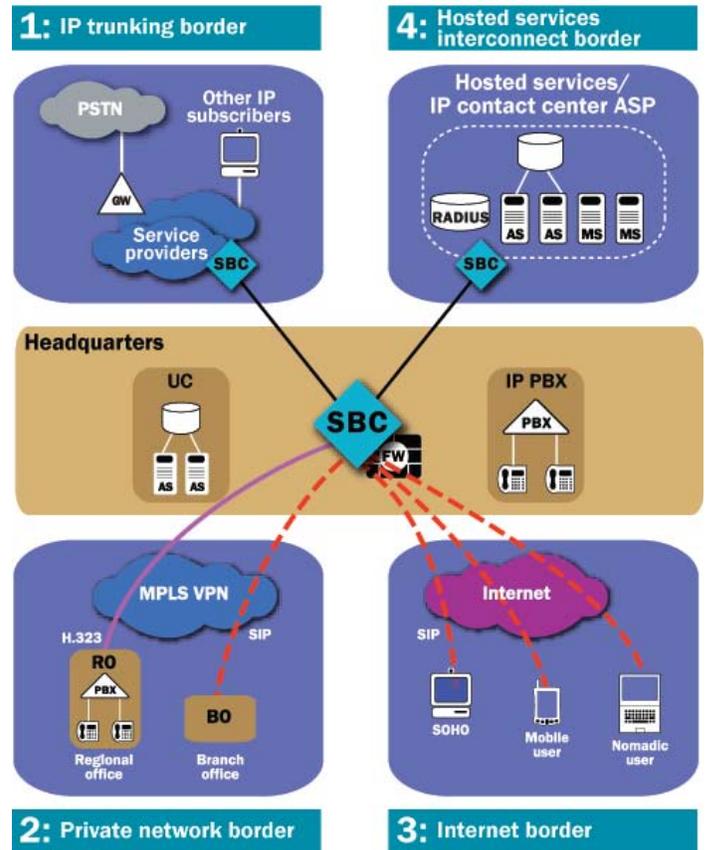


Figure 1: The four critical IP network borders of the Enterprise data center

### 1: IP trunking border

The first critical border that must be controlled is the IP trunking border that connects the enterprise to the outside world. This border is located between the private enterprise network where mission-critical IP PBXs and UC servers reside, and to one or more IP trunks connecting it to service provider IP networks. These networks link to the PSTN via media gateways and to external IP endpoints. Enterprises are increasingly using IP trunks to replace TDM trunks to realize a number of cost-saving and operational advantages (see sidebar).

While these advantages have obvious benefits for the enterprise, IP trunks do present some challenges. First, the service provider's IP network, like any IP network, cannot be trusted. It provides an attack vector for signaling and media overloads, DoS/DDoS attacks, viruses and worms that can cripple IP PBXs and UC servers, sap network performance and call quality and compromise the confidentiality of voice and UC traffic. Next, the IP trunking service may use signaling, networking protocols, encryption methods and codecs that are incompatible with enterprise IPT/UC infrastructure. These incompatibilities must be mediated.

On the plus side, the IP trunking border provides a logical place to add routing intelligence to the IPT/UC environment, improving the enterprise's ability to recover from network failures, choose the most cost-effective service providers and routes for IPT/UC sessions and generate reports necessary for traffic management and planning. It's also a convenient place to interface to regulatory compliance systems like IP call recording systems.

#### Benefits of IP trunking

Replacing an ISDN-PRI, T1/E1 or larger TDM trunk with one or more IP trunks allows enterprises to:

- Reduce call termination costs by letting IP trunks route each call over the service provider IP backbone to the remote media gateway closest to the call's destination
- Reduce capital and operating costs by eliminating media gateways and TDM trunks, and by supporting voice applications on the existing data network
- Add network fault tolerance (also referred to as geo-redundancy) by provisioning multiple IP trunks to diverse PoPs and/or diverse service providers
- Simplify operations by relegating media gateway and PSTN interconnection management to the service provider
- Cut the time to provision and deploy IP interconnects to a matter of days, as opposed to the months typically needed to provision and deploy TDM services.

To effectively take advantage of IP trunking services, enterprises must deploy SBCs to perform the following functions:

## Security

The SBC must perform a number of functions to defend IPT and UC servers (as well as itself) against DoS/DDoS attacks and overloads. It should enforce access control policies by limiting incoming sessions to the IP addresses of service provider peer SBCs. Network Address Translation (NAT) must be employed to hide the topology of IPT/UC servers and internal endpoints, thereby defending against directed attacks and protecting user privacy. The SBC should inspect traffic coming from the IP trunk to eliminate viruses, worms and SPIT, and eliminate fraud by preventing unauthorized use of the IP trunk. And the SBC must provide intrusion monitoring and reporting capabilities to validate service provider security compliance.

## Application reach maximization

The SBC must provide signaling protocol interworking to bridge incompatibilities between enterprise IPT/UC servers and service provider IP trunks, including SIP trunk to H.323 IP PBX interworking, H.323 trunk to H.323 or SIP IP PBX interworking, and interworking between differing vendor implementations of SIP. Other required types of interworking may include: transport protocol interworking for TCP, UDP and SCTP; encryption protocol interworking for TLS, MTLs, SRTP, and IPsec; and response code translations. The SBC may also need to provide IP address translation between overlapping private IP address spaces or between IPv4 and IPv6 addresses. In sessions where each endpoint uses a different codec or frame rate, transcoding or transrating may be necessary.

## SLA assurance

The SBC must assure the uptime and performance of the enterprise IPT/UC infrastructure. It should support geo-redundancy by enabling the deployment of IP trunks to diverse service provider PoPs, then detecting and routing around failed network elements and connections. The SBC must monitor the health of logically-adjacent elements (router, session agent, peer SBC) and then reroute and redistribute traffic when those elements suffer performance degradation or failure. To ensure high session quality, admission control must be asserted to prevent trunk saturation and IPT/UC signaling element overload. The SBC must also provide transport control for incoming sessions with QoS marking and VLAN mapping, and monitoring capabilities like QoS and ASR reporting to help the enterprise validate service provider SLA compliance.

## Cost optimization

The SBC must help the enterprise reduce service provider charges for IPT and UC traffic via flexible session routing policies based on a variety of metrics, including least-cost routing, observed call quality, and codec types. The SBC should also provide flexible usage reporting for cost accounting and traffic planning purposes.

## Regulatory compliance

The SBC must be able to identify emergency sessions (E9-1-1), add location information to them, exempt them from admission control policies and route them with priority to the appropriate emergency center. It should provide a replication mechanism to support IP call recording for compliance with regulatory agencies and mandates like the Securities and Exchange Commission (SEC), Health Insurance Portability and Accountability Act (HIPAA) and Federal Rules of Civil Procedure (FRCP).

## 2: Private network border

The second critical border is the private network border. This border straddles the private, secure WAN (typically MPLS VPNs) or LAN connections that link the enterprise data centers where IP PBXs and UC servers reside, to users at headquarters, regional offices and branch offices. IPT/UC servers and endpoints interconnected over a private WAN and/or headquarters campus LAN generally conform to either of two topologies:

- Centralized session control—the private network interconnects all enterprise IP phones and UC endpoints to a group of IPT/UC servers in a central data center location. An enterprise needing business continuity may have a second, physically separate, data center with failover from one to the other in disaster scenarios like data center, network or service provider outages.
- Distributed session control—the private network connects IP phones and UC endpoints to many geographically distributed IPT/UC servers located at headquarters and in regional offices, and interconnects the distributed IPT/UC signaling elements to one another.

The private network border presents several challenges, foremost of which is the security risk of attacks on IPT/UC infrastructure from inside the enterprise network. Despite the inherent untrustworthiness of IP networks, IPT/UC infrastructure has become essential to many mission-critical, revenue-generating business processes. This makes attacking IPT/UC servers and endpoints more profitable or rewarding for employees motivated by financial gain or malice.

Criminals are also increasingly employing insider strategies to attack IPT/UC infrastructure rather than attempting to penetrate the data center's external defenses. For example, a criminal might lodge malware (like a click-to-call worm embedded in a document) in the laptop of a mobile employee working in an airport wireless hotspot. A successful attack could then be propagated the next time the employee connected to the enterprise network from his desk inside the network security perimeter.

Another significant challenge is IPT/UC technical incompatibility issues in distributed session control environments. For a variety of reasons—growth through acquisition, decentralized IT planning, etc.—many enterprises end up owning IP PBXs from multiple vendors, resulting in a patchwork of trunk-side signaling protocols and varying implementations of signaling protocols. Discontinuous or overlapping IP address spaces and incompatible dial plans are also common stumbling blocks for large enterprises trying to broaden the reach of their IPT/UC applications and services.

High service level requirements and regulatory issues present further hurdles to IPT/UC with centralized session control. Access to backup IPT/UC servers in a large campus site must be preserved even in the face of extraordinary events, e.g., a router failure that makes the primary IP PBX unreachable. To maximize call quality, transport network latency must be minimized by releasing media peer-to-peer when endpoints are in the same network, rather than keeping the media flow centrally “hair-pinned”. Local emergency services calling must also be supported, even if the caller's primary IP PBX is geographically distant.

To overcome these challenges, enterprises need to deploy SBCs on the private network border to perform the following functions:

### **Security**

The SBC must defend IPT/UC servers from attacks and overloads originating from inside the private network. It should police sessions to avert both non-malicious and malicious attacks, and employ NAT to hide the topology and IP addresses of signaling and media elements and thereby thwart directed attacks. The SBC should also provide monitoring and reporting for anomaly detection and post-attack forensics. It must also defend itself from attacks and overloads; otherwise, a successful DoS/DDoS attack on the SBC would leave IPT/UC infrastructure vulnerable.

### **Application reach maximization**

In distributed session control topologies, the SBC must bridge a variety of gaps in IPT/UC infrastructure, like incompatible or differently-implemented trunk-side signaling protocols. The SBC should provide protocol interworking between call control elements for signaling normalization, repair, and interworking between differing vendor implementations of signaling protocols, e.g., Nortel SIP and Avaya SIP, and different signaling protocols, e.g., SIP and H.323. Transport protocol interworking (for TCP, UDP and SCTP) and encryption protocol interworking (for TLS, MTLS, SRTP, and IPsec) may also be required. The SBC should also unify discontinuous dial plans and provide interworking for overlapping IP addresses—public to private, private to private, or VPN to VPN.

### **SLA assurance**

The SBC must maintain the uptime and performance of the enterprise IPT/UC infrastructure via session admission control policies that intelligently assess available bandwidth and session agent capacity in terms of maximum number of allowed sessions or maximum rate of session establishment. It should monitor the health of logically-adjacent elements (router, SIP registrar, session agent) and reroute and redistribute traffic when those elements suffer performance degradation or failure. After a massive power failure at a large site, the SBC should gracefully and statefully manage the ensuing avalanche of endpoint re-registrations. In both centralized and distributed session control topologies, media between endpoints should be established peer-to-peer whenever possible to improve session quality by reducing packet latency, jitter and loss.

### **Cost optimization**

The SBC must provide flexible usage reporting for cost accounting and traffic planning purposes. It should provide signaling interworking to extend the useful life of existing IP PBX infrastructure. Through policy enforcement of authentication and authorization servers, the SBC should deny unauthorized use of enterprise network resources, e.g., bandwidth-intensive telepresence sessions.

### **Regulatory compliance**

For internal employees, the SBC must identify emergency sessions (E9-1-1), add location information to them, exempt them from admission control policies and route them with priority to the appropriate emergency center. The SBC should also support domain separation (e.g., separation of investment banking from research operations) by supporting VPNs at layers 2 and 3.

### 3: Internet border

The third critical enterprise border is the Internet border, defined by Internet connections from the data center to small branch offices, users working from home and mobile employees.

Enterprise remote and mobile workers have the same need to connect to centralized IPT/UC resources as employees in headquarters and regional offices. But these users face some obstacles associated with their reliance on inexpensive and ubiquitous, yet insecure and unreliable, Internet connections.

Compared to threats associated with the IP trunking and private network borders, the Internet border carries significantly higher security risks. The enterprise must carefully mitigate the many threats that attend all inbound Internet traffic, including DoS/DDoS attacks and overloads on session control elements. VoIP-specific malware—viruses, worms, and SPIT—is also a significant threat. Depending upon industry and employee role, and given the heightened ease of eavesdropping on the Internet, call privacy may be critical for business reasons or compulsory for regulatory compliance. However, end-to-end encryption may not be supported by all IP phones, media gateways or voice mail servers.

Further, many remote users must originate and receive VoIP calls and UC sessions from behind NAT gateways/firewalls. Successful enterprise VoIP traversal of these devices requires configuration changes to the local gateway that are too complex for most employees.

Finally, given the highly variable quality and speed of the various public Internet links that a typical remote user's IP telephony and UC traffic must traverse, session quality across the Internet border can vary significantly. Session quality for larger offices must be monitored regularly to determine whether upgrading from an Internet connection to private network connection would be appropriate.

To address these challenges, enterprises need to deploy SBCs on the Internet border to perform the following functions:

#### Security

The SBC must protect IPT/UC signaling and media elements and itself from the broad range of attacks that originate on Internet-connected endpoints, including DoS/DDoS attacks, overloads, and VoIP-specific malware like viruses, worms, and SPIT. NAT should be used to hide the topology and IP addresses of signaling and media elements and thereby thwart directed attacks. The SBC should also provide monitoring and reporting for anomaly detection and post-attack forensics. Where appropriate, the SBC must support encryption of signaling and media for confidential remote user sessions.

#### Application reach maximization

The SBC must provide hosted NAT traversal so that remote users can make enterprise VoIP calls and establish UC sessions without having to reconfigure their local NAT/firewall devices.

#### SLA assurance

The SBC must perform a variety of functions to give Internet-connected users high-performance, highly available access without exposing enterprise IPT/UC elements to DoS/DDoS attacks and signaling overloads. The same mechanisms required on the private network border are also critical on this access border, including session admission control; media release between endpoints; router, SIP registrar and session agent failure detection, re-routing and recovery; and overload control. To ensure that sessions receive the appropriate priority on the private network side of this border, the SBC must control QoS marking or VLAN mapping. It should also provide quality of experience (QoE) reporting to help planners understand when a remote-site Internet connection needs to be upgraded to a private WAN connection.

#### Regulatory compliance

For remote office and teleworker connections, the SBC must enable enterprise compliance with government regulations, including emergency session (E9-1-1) control. It should also support encryption as needed for compliance with government and commercial privacy regulations.

## 4: Hosted services interconnect border

The fourth critical border is the hosted services interconnect border, encompassing private network connections from the enterprise to ASPs and providers of hosted IP services. Applications and hosted services offered by these providers may include IP-based audio and videoconferencing services, IP contact center services, IP Centrex to augment premise-based systems for certain sites or divisions and VoIP-enabled business applications such as salesforce.com.

Because security is so critical to the business of hosting providers and ASPs, the risk associated with this border is low compared to the Internet border. Nonetheless, if the hosted application is critical to the enterprise, protecting the performance and availability of this border will likewise be critical. In some cases, hosted services may have network and protocol incompatibilities that must be mediated.

To overcome these challenges, enterprises need to deploy SBCs on the hosted services interconnect border to perform the following functions:

### Security

The SBC must perform a number of functions to defend IPT and UC servers (as well as itself) against DoS/DDoS attacks and overloads originating in the hosting provider's network. The SBC should enforce access control by limiting incoming sessions to the IP address of the hosting provider's peer SBC. It must employ NAT to hide the topology of the enterprise's IPT/UC servers and endpoints, thereby preventing directed attacks and protecting user privacy. The SBC should inspect incoming traffic from the hosting provider to eliminate viruses, worms and SPIT, and defend against fraudulent use of the hosting provider's services. It must also provide intrusion monitoring and reporting capabilities to validate the hosting provider's security compliance.

### Application reach maximization

The SBC may need to mediate incompatible or differently-implemented trunk-side signaling protocols between the enterprise and the hosting provider. It should provide protocol interworking between call control elements for signaling normalization, repair, and interworking between differing vendor implementations of signaling protocols, e.g., Cisco SIP and Genesys SIP, and different signaling protocols, e.g., SIP and H.323. Transport and encryption protocol interworking, IP address space and response code translations, and transcoding and transrating may be required.

### SLA assurance

The SBC must ensure the uptime and performance of the connection between the enterprise IPT/UC environment and the hosting provider through several mechanisms. It should support geo-redundancy by enabling the deployment of diverse connections between the two, and detecting and routing around failed network elements and connections. It should monitor the health of logically-adjacent elements (router, session agent, peer SBC) and reroute and redistribute traffic when those elements suffer performance degradation or failure. To ensure high quality sessions, the SBC must provide admission control to prevent trunk saturation and IPT/UC signaling element overload. The SBC should also provide transport control for incoming sessions with QoS marking and VLAN mapping, and monitoring capabilities like QoS and ASR reporting to validate hosting provider SLA compliance.

## Summary

Enterprise IPT is now mainstream, and UC will soon follow. Both are critical components of enterprise IT strategies to improve business agility, increase employee efficiency and responsiveness, build customer satisfaction and loyalty, and reduce overhead costs. Clearly, they are becoming indispensable tools for success in a newly-competitive global marketplace.

But full-scale deployment of enterprise IPT has revealed deficiencies in network and security infrastructure originally deployed for non-real-time data. Consequently, enterprises must add further controls to their IPT/UC infrastructure to improve its security, extend its application reach, meet service level commitments, optimize capital and operating costs, and comply with relevant commercial and government regulations.

Enterprises should follow the example set by service providers that have already encountered and addressed these same issues: deploy SBCs to control the four key borders of their IPT/UC infrastructure. Using SBCs to control the IP trunking, private network, Internet, and hosted services interconnect borders, enterprises can deliver the network security, availability, and performance necessary for the successful deployment of IPT today and UC tomorrow.



71 Third Avenue  
Burlington, MA 01803 USA

© 2008 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.

t +1.781.328.4400  
f +1.781.425.5077  
www.acmepacket.com

07/15/08