WHITE PAPER

The Need for Session Delivery Networks

Executive Summary Service providers, enterprises and contact centers continue to build IP-based infrastructure to lower their operating costs and introduce new IP-enabled offerings such as VoIP, video-over-IP and instant messaging (IM). In order to overcome the limitations inherent in using the Internet or another best-effort, unsecured IP network for session-based voice, video, data and unified communications, more-and-more service providers and enterprises are turning to session delivery networks, which layer complementary intelligence and controls over an IP transport network.

With the IP transport network providing basic packet routing and delivery services, the overlay session delivery network provides critical session border control and session management functions that ensure prioritized, secure and trusted delivery of a broad range of services and applications. Acme Packet® offers proven session delivery network solutions that enable the trusted, first-class delivery of next-generation voice, data and unified communications (UC) services and applications across IP networks that bridge the gap between the underlying IP transport network and applications and services.

WHITE PAPER

The Need for Session Delivery Networks

Industry Dynamics Drive Demand for IP Communications

Service providers traditionally have delivered voice and data services over two separate networks: the public switched telephone network (PSTN) and the Internet. Similarly, enterprises have used the PSTN for voice services and the Internet for data applications. The PSTN provides high reliability and security but is costly to operate and is limited in its ability to support high-bandwidth video and other interactive multimedia services.

The Internet is capable of cost-effectively transmitting any form of traffic that is IP-based—including interactive voice, video and data—but it transmits traffic only on a best-effort basis because all traffic is given the same priority. Internet-based services are also subject to disruptive and fraudulent behavior, including identity theft, viruses, spam and hacking. Both service providers and enterprises are migrating to a single IP network architecture to serve as the foundation for their next-generation voice, video, multimedia and data services and applications. To provide secure and high-quality interactive communications on a converged IP network, service providers and enterprises must be able to control the communications flows that comprise communication sessions.

IP networks were initially designed to provide reliable delivery of data services such as file downloads and website traffic that are not sensitive to latency or time delay. If data packets are lost or misdirected, an IP network exhibits tremendous resiliency in re-transmitting and eventually executing the desired user request. However, IP networks were not originally designed to meet the real-time communications needs of interactive voice and video and provide the levels of security, QoS and reliability demanded by these types of services. Managing two distinct networks is not a viable economic alternative, and as a result service providers and enterprises have begun to migrate to a single IP network architecture to serve as the foundation for their next-generation services and applications.

What is a Session?

A session is a communications interaction that has a defined beginning and end, and is effective only when transmitted in real time without latency or delays.

A session is initiated using signaling messages. These messages establish a virtual connection between the participants' PCs, IP phones, smart phones, tablets or other IP devices. In addition, they negotiate the IP addresses used for the session's media streams and control messages as well as the codecs used to digitize analog voice and video. Various codecs are required for voice and video, and they involve trade-offs between quality and bandwidth efficiency. Once the call is initiated, media streams and control messages flow in both directions between participants. Signaling messages also are used to transfer a call, place a call on hold and terminate a session.

Every session includes three sets of bidirectional communication flows:

- *Session signaling messages, which are used to initiate, modify or terminate a session*
- *Media streams, which are data packets containing the actual media being exchanged*
- *Media control messages, which are used to compile information to report on QoS levels*

The Need for a New IP Overlay Network

In order to enable session-based communication, control of the session from its origination point to its defined end point is required. No single IP network extends far enough to enable that level of control, and the Internet lacks the fundamental QoS and security mechanisms necessary to consistently deliver the security and quality of real-time multimedia communications that consumers and businesses require.

What's more, the delivery of session-based communications is complicated by the following characteristics of today's IP networks:

- The identities of the participants are difficult to ascertain and security needs are complex
- The number of session signaling protocols, codecs and related standards continues to grow
- Addressing schemes are not consistent or compatible across networks
- Bandwidth and signaling element resources are finite
- Interactive communications service provider business models and regulatory compliance requirements continue to evolve and require network flexibility

Additionally, unlike typical data communications, not all session-based communications can be treated with the same priority. For example, a 911 call or a high-quality enterprise videoconference should take priority over viewers calling into a reality television program.

To overcome these challenges and truly enable session-based communications that end-users trust, service providers and enterprises must be able to assure secure and high-quality interactive communications across one-or-more networks. To deliver such communications requires a new IP overlay network—a session delivery network.

Session Delivery Networks: Implementing Critical Control Functions

Session delivery networks implement the critical controls functions to allow service providers and enterprise networks to deliver trusted, first-class interactive communications across IP network borders:

Security

Session delivery network solutions need to protect themselves, softswitches, IMS cores, IP PBXs, UC servers and other service delivery infrastructure elements, as well as customer networks, systems and relationships. This includes providing DoS/DDoS protection from malicious attacks and non-malicious overloads. They authenticate and authorize users, discover user location and exchange this information with other network elements, and must be able to ensure session privacy.

Service and Application Interoperability and Control

Proven interoperability is needed to maximize the different types of applications, networks and devices supported by session delivery network solutions. They must enable data applications to initiate and control communications, and enable sessions to traverse existing data firewall devices, bridge private networks using overlapping IP addresses and VPNs, mediate between different signaling, transport and encryption protocols, convert between incompatible codecs and translate signaling layer telephone numbers, addresses and response codes.

SLA Assurance

Session delivery networks play a critical role in assuring service capacity and quality. They enable data center disaster recovery and perform admission control to ensure that both the network and service infrastructure have the capacity to support a session with high quality. They perform optimal load balancing for session signaling elements and application servers. They also monitor and report actual session quality to determine compliance with performance specifications set forth in SLAs between service providers and enterprises and their external or internal customers. They also enable contact centers to record calls and sessions for quality assurance.

Regulatory Compliance

Session delivery networks enable compliance with government-mandated regulations worldwide, including emergency services such as E911, national government priority services such as Government Emergency Telecommunications Service (GETS) and lawful intercept such as the Communications Assistance for Law Enforcement Act (CALEA). They also enable enterprises to record calls for regulatory compliance.

Cost and Revenue Management

Session delivery networks must be able to enable organizations to increase revenues and control costs by protecting against both bandwidth and QoS theft by routing sessions optimally to minimize costs and by providing accounting, charging and related mechanisms to maximize billable sessions.

Session Delivery Network Products from Acme Packet

Session delivery network solutions from Acme Packet are architected using one-or-more products within our Net-Net® product family and they allow service providers and enterprise networks to implement the critical control functions needed to deploy service delivery networks.

Session Border Controllers

Session border controllers (SBC) are the cornerstones of session delivery networks. They provide critical control functions in the delivery of high-quality interactive communications across IP network borders. A "session" is any real-time, interactive voice, video or multimedia communication using IP session-layer signaling protocols such as SIP, H.323, MGCP, Megaco/H.248, MSRP and RTSP. The "border" is any IP-IP network border such as those between service provider and enterprise, residential or mobile customer/subscriber; between two service providers; or between enterprise and service provider managed networks and the public untrusted, unmanaged Internet.

The "control" functions satisfy requirements in the areas of security, interoperability, availability, quality and regulatory compliance.

Acme Packet's Net-Net SBC product family includes the Net-Net Session Director (SD), Net-Net Signaling Firewall (SF) and Net- Net Border Gateway (BG). The Net-Net SD integrates signaling and media controls in a single standalone system, while the Net- Net SF and BG operate as "decomposed" SBCs; the Net-Net SF delivers security and other SIP signaling controls. The Net-Net BG operates in tandem with an external signaling element to control only the media within interactive communications sessions.

Session Managers

Session managers are centralized signaling elements in both service provider and enterprise networks that interface employee/subscriber databases and application servers to the session delivery network. They support user authentication, authorization, registration and location discovery; application orchestration; session routing; and accounting/charging services.

Net-Net SIP Multimedia-Xpress (SMX) adds core IMS session manager functions to Acme Packet's Net-Net access SBCs to create an integrated session delivery solution.

Multiservice Security Gateways

Multiservice security gateways (MSGs) securely connect subscribers using the untrusted Internet or WiFi access networks to their mobile voice and data services. They are deployed at the border between the mobile network and the Internet or WiFi access network. They transport both voice and data services and address a wide array of fixed-mobile convergence solutions, including UMA and SIP, WiFi and femto/picocell access points. They authenticate endpoints, secure the voice and data traffic within IPsec tunnels to ensure privacy and protect against theft, and defend against DoS/DDoS attacks on the mobile service infrastructure at the TCP/IP and IPsec networking levels to deliver non-stop service.

The Net-Net Security Gateway offers industry-leading security gateway capabilities in terms of architectural flexibility, capacity, performance, functionality, carrier-class availability and manageability.

Diameter Signaling Controllers

Diameter signaling controllers (DSCs) enable the exchange of subscriber profile information within service provider LTE and IMS networks and across LTE network borders. Diameter signaling messages are used to exchange subscriber authentication, authorization and location information among different LTE and IMS network elements. For each subscriber data, voice, video or multimedia session, Diameter signaling is used to exchange QoS and charging information. By aggregating and controlling Diameter signaling messages, DSCs streamline LTE and IMS network deployments, assuring service availability and security.

Net-Net Diameter Director leverages Acme Packet's Net-Net OS software to offer industry-leading DSC capabilities in terms of signaling control, security, scalability, dynamic routing and carrier-class availability. It supports multiple applications, including core Diameter routing and overload control, LTE data and VoLTE roaming and federated service delivery.

Session-aware Load Balancers

Session-aware load balancers (SLBs) are used to scale the capacity of access SBCs, interconnect SBCs, MSGs and interconnect DSC deployments at network borders. SLBs provide a single point of contact (IP address) for a service provider's own subscribers or sessions coming from other networks. SLBs then dynamically and adaptively load balance traffic across two-or-more SBC, MSG or DSC elements. SLBs are session-aware since traffic is only re-balanced when there is no active session, dialog or transaction in process. Load balancing decisions incorporate a number of parameters including system capacity and current system load, availability and health score.

The Net-Net Session-aware Load Balancer features carrier-class high-availability to ensure no loss of active sessions in the event of single system failures. The Net-Net SLB and its associated clusters provide a superior solution in terms of scalability, dynamic adaptive load balancing, redundancy and management compared to traditional Layer 3/Layer 5 web server load balancers and SIP redirect servers.

Session Routing Proxies

Session routing proxies (SRPs) centralize and consolidate routing control for SIP-based voice, video, IM and multimedia sessions. SRPs direct traffic to-and-from other SIP signaling elements in the network, including mobile switching centers, Class 4 and 5 softswitches, CSCF servers and access and interconnect session border controllers. They reduce costs by addressing scaling problems when SIP routing decisions become complex and require a dynamic, real-time routing decision for each individual session for multiple sources and destinations within a network.

The Net-Net Session Router is the core element in our Open Session Routing architecture and works in conjunction with a world-class ecosystem of routing database products and services from our partners.

Application Session Controllers

Application session controllers (ASCs) enable enterprises to streamline business processes by integrating their applications with IP communications services. By adding interactive voice, video, IM and multimedia communications to applications, enterprises can eliminate inefficiencies and improve collaboration, productivity and customer service.

The Net-Net Application Session Controller (ASC) is an advanced middleware platform that leverages existing web development frameworks and toolsets to communications-enable business processes or web pages.

Session Recorders

Session recorders are designed to record IP voice, video, chat and UC sessions for regulatory compliance and contact center quality assurance. They also enable service providers to offer new cloud-based session recording services for their SIP trunking or hosted UC service customers.

The Net-Net Interactive Session Recorder (ISR) is a complete software-based IP session recording solution that records, stores and archives voice, video and multimedia communications.

Conclusion

Managing applications and services over the PSTN and an IP network is not an economically viable long-term solution, and evolving to a converged IP network requires the ability to guarantee real-time, secure delivery of high-quality, session-based communications. By relying on the IP transport network to prove packet routing services, an overlay session delivery network provides critical session border control and session management functions that ensure prioritized, secure and trusted delivery of a broad range of services and applications. Service delivery networks enable: security; service and application interoperability and control; SLA assurance; regulatory compliance; and cost and revenue management of interactive IP communications in service provider, enterprise and contact center networks.

Acme Packet is the leader in session delivery network solutions for trusted first-class voice, video and UC, and continues to satisfy the evolving session delivery network requirements of enterprises and fixed line, mobile and over-the-top service providers. Our network deployments position us to gain valuable knowledge that we can use to expand our product portfolio and enhance our features and functionality and we facilitate and promote service interconnections and federations among our customers and implement new technologies to enhance product performance and scalability.

Acme Packet actively contributes to architecture and the standards definition processes, and we utilize our breadth and depth of experience with session delivery network deployments to support the evolving standards for next-generation IP networks for service providers and enterprise networks. Learn more about our family of products for service providers and for enterprises, and for more information about our service delivery network solutions, visit www.acmepacket.com.

100 Crosby Drive
Bedford, MA 01730 USA
t +1 781.328.4400
f +1 781.275.8800
www.acmepacket.com
06/04/12