PERIMETA SBC
MEDIA SESSION CONTROLLER

INFRASTRUCTURES ARE EVOLVING, MESSAGES ARE INCREASING AND TRAFFIC PATTERNS ARE CHANGING. PERIMETA REPRESENTS THE FIRST IN A NEW GENERATION OF SESSION BORDER CONTROLLER (SBC) PLATFORMS CAPABLE OF MEETING THE DEVELOPING ACCESS AND INTERCONNECT REQUIREMENTS OF NEXT GENERATION WIRELINE AND WIRELESS NETWORKS.

• Architected for distributed signaling & media
• Flexible hardware/software deployment models
• Security
• Policing

• Quality-of-Service
• Accessibility
• Interworking
• Analysis

PERIMETA
Purpose-built for distributed deployments within both the control and transport layers of emerging next-generation networks, the Perimeta architecture comprises two distinct components: a Signaling Session Controller (SSC) and Media Session Controller (MSC). Data volumes are intensifying and the relationship between signaling and media is becoming increasingly divided. Conforming to 3GPP specifications for decomposed SBC functions, our unique solution enables independent, cost effective scaling of these critical control elements.

Where consolidation of these individual components is preferred, the Perimeta Integrated Session Controller (ISC) combines both SSC and MSC elements within a single platform, without sacrificing performance or scalability.

DISTRIBUTED ARCHITECTURE, INTENSE PERFORMANCE
The Media Session Controller is specifically designed to handle the rapidly rising data rates and number of IP endpoints in next generation networks. Decoupled from the task of processing an ever increasing number of SIP signaling messages, the MSC is ideally suited for media-rich unified communications environments, where not only wideband audio but bandwidth-intensive high definition video is making up a larger percentage of fixed and mobile broadband calls.

MSC platforms perform the role of an IMS-AGW or Tr-GW function. The MSC is controlled by one or more Perimeta Signaling Session Controllers or Integrated Session Controllers over a standard H.248 reference interface.

UNIQUE SOFTWARE + STANDARD HARDWARE = FLEXIBILITY
Perimeta is the only session border controller architected as a pure software solution. It is a critical component in the march towards network functions virtualization (NFV) and in helping to transition operators into being true software telcos. Unlike other SBCs, Perimeta is not dependent on any proprietary equipment, such as DSPs. Instead, Perimeta can run on any standard server hardware.

Perimeta leverages the unprecedented processing power of today's standard hardware to produce unrivalled performance and scalability, even without specialized hardware. Running the Perimeta SBC on highly scalable standardized and open platforms allows you to protect and enable a network of any size with much lower Capex and Opex compared with SBCs that rely on specialized hardware.
PERFORMANCE

The Perimeta MSC has been designed for performance. Leveraging interrupt mitigation and zero copy packet extraction techniques, the MSCs multi-core, multi-threaded software architecture delivers superior packet throughput while performing high-touch functions such as packet marking and remarking.

Perimeta’s unique software-based architecture is designed to take full advantage of today’s standard multi-core servers and cloud computing resources, offering extremely high performance across a range of hardware and virtualized environments.

Perimeta is available on Metaswitch’s own high-availability ATCA hardware, and works seamlessly on a range of servers from Dell, HP and Cisco. For performance ratings and hardware specifications, see the Perimeta Performance and Hardware Specifications document.

CO-LOCATION OR GEOGRAPHIC DISPERSAL

Scaled independently of the signaling controller, Perimeta Media Session Controllers may be either collocated with the SSC/ISC function or geographically dispersed around an access network. As the MSC is scaled independently of the signaling controller, network operators can realize significant cost saving when building-out next generation networks.

CONTROL

Perimeta provides granular connection admission control and rate limiting, enabling the MSC to intelligently manage and restrict bandwidth use by both interconnect peers and individuals.

Critical to maintaining strict quality of service guarantees, the MSC can also read then mark or re-mark the IP differentiated services code point (DSCP) field. This ensures the expedited forwarding of voice and assured forwarding of video streams by upstream and downstream network switch/router elements.

TRANSCODING

Perimeta’s comprehensive media transcoding function simplifies communication between different networks and endpoints, dynamically routing media traffic through the most efficient transcoding path, always guaranteeing the highest quality of experience. Choose between software transcoding for simplicity and scalability on any platform, and hardware transcoding with DSPs on compatible platforms for density and power efficiency. For more info go to www.metaswitch.com/sbc-transcoding.

ANALYSIS

Perimeta is the first session border controller to export detailed unsampled call quality records to the MetaView Service Assurance Server. Combining these with records collected from other network elements and endpoints, MetaView can provide objective quality of experience measurements while delivering a comprehensive end-to-end view of overall network performance.

The MSC delivers total visibility without degrading router performance or implementing costly network analytics components.
PERIMETA MEDIA SESSION CONTROLLER SPECIFICATIONS

**SIGNALLING & CONTROL**
- H.248

**MEDIA**
- IPv6-IPv4 Interworking
- QoS and Bandwidth Enforcement
- SRTP-RTP Interworking
- SRTP Pass-through
- DTMF Interworking
- NAT Traversal
- 3GPP IMS-AGW and Tr-GW
- Software transcoding on all Perimeta platforms
- Hardware DSP transcoding on compatible Perimeta COTS platforms (requires full-height PCIe card slot for each DSP board)
- MSRP for RCS / RCS-e
- Lawful intercept

**SECURITY**
- DoS/DDoS Detection and Protection
- Bandwidth policing
- Topology hiding
- SRTP
- Alarm on attack
- Separation of management and data traffic

**MANAGEMENT**
- Command-line interface
- SNMPv2c
- Secured management access (SSH, SFTP, SCP)
- Bulk configuration and staging (configuration cloning, export and restore of configuration snapshot)
- VQM reporting
- Northbound APIs for configuration

**REDUNDANCY**
- 1:1 redundant service interface
- 1:1 redundant management interface