



Acme Packet session border controllers in MSF Release 3 architecture

Whitepaper

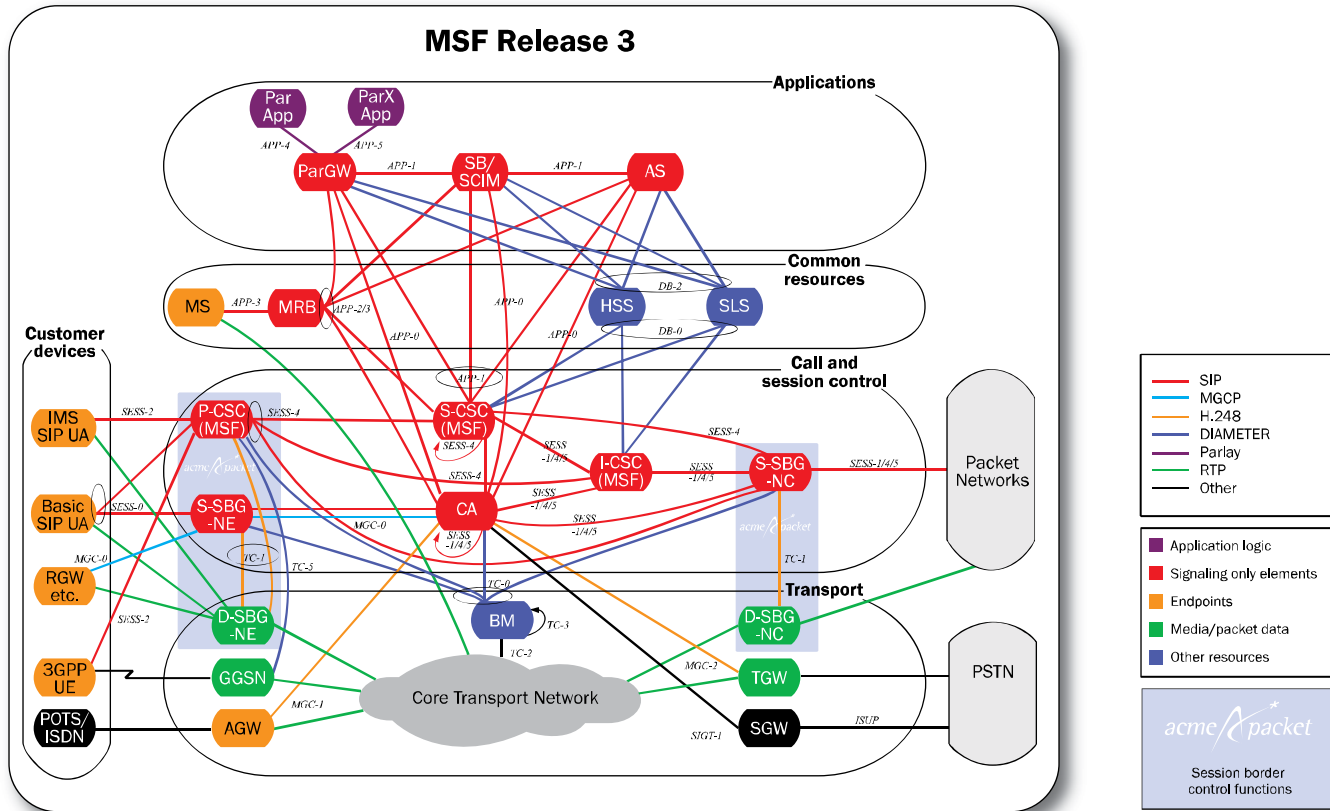
Introduction

Acme Packet® has defined the role of session border controllers (SBCs) within the next-generation, converged fixed-mobile Multi-Service Forum (MSF) architecture. Within this architecture, SBCs provide service providers with support for delivering real-time interactive IP-based voice, video and multimedia sessions in five critical areas – security, service reach maximization, SLA assurance, revenue and cost optimization, and regulatory compliance.

Role of SBCs within MSF Release 3 architecture

MSF Release 3 is an architecture defined by the MSF for the delivery of real-time voice, video and multimedia services using SIP and other standards based protocols to initiate and control service delivery over packet-switched networks with a focus on wireline and wireless access networks. This architecture leverages work from 3GPP/IMS and ETSI/TISPAN to enable service providers to leverage a common core service delivery infrastructure for both wireline and wireless access networks. This enables service providers to accelerate support for the service delivery requirements of converged fixed-mobile services.

Within the MSF architecture, the two different types of SBCs – the Access SBC and the Interconnect SBC – play very important roles by integrating signaling and media control. The functional responsibilities of these products are illustrated and further described below.



SBC role in extended MSF Release 3 architecture

Access Session Border Controller (A-SBC)

The Access SBC satisfies the requirements at the border where subscribers access the MSF core. It integrates three functional elements from the MSF architecture.

- **Proxy Call and Session Controller (MSF-specified)** – is the SIP signaling contact point, the outbound/inbound “proxy,” for subscribers within MSF. However, the term “proxy” is deceiving since to fulfill its complete set of responsibilities it must be able to proactively initiate SIP requests. This requires implementation as a SIP Back-to-Back User Agent (SIP B2BUA), not a simple SIP proxy. The P-CSC (MSF) is responsible for forwarding SIP registration messages from the subscriber’s endpoint, the User Equipment (UE), in a visited network to the Interrogating-CSC (I-CSC (MSF)) and subsequent call set-up requests and responses to the Serving-CSC (S-CSC (MSF)). The P-CSC (MSF) maintains the mapping between logical subscriber SIP URI address and physical UE IP address and a security association, for both authentication and confidentiality, with the UE using TLS or IPsec for example. It supports emergency call (E911) local routing within the visited network, accounting, session timers and admission control. Admission control requires an interface to an external Bandwidth Manager (BM). The P-CSC (MSF) interacts with D-SBG-NE for control of the boundary at the transport layers including pinhole firewall, NAPT and numerous other features.

- **Signaling Session Border Gateway, Network Edge (S-SBG-NE)** – provides overall control of the boundary between subscribers and service provider networks. It provides security for the MSF core in terms of signaling information by performing signaling-based topology hiding, signaling rate policing, IPv4-IPv6 interworking and session screening based upon source and destination signaling addresses. The S-SBG-NE performs protocol and address interworking when connecting non-SIP or non-IPv6 networks. It maintains security associations between itself and SIP UAs and performs admission control and bandwidth allocation using a local policy function or via the BM. Lastly, the S-SBG-NE interacts with D-SBG-NE for control of the boundary at the transport layers including pinhole firewall, NATP and numerous other features.
- **Data Session Border Gateway, Network Edge (D-SBG-NE)** – controls the transport boundary at layers 3 and 4 between service provider networks. This function acts as a pinhole firewall and NAT device protecting the service provider's MSF core. It controls access by packet filtering on IP address/port and opening/closing gates (pinholes) into the network. It uses Network Address and Port Translations (NAPT) to hide the IP addresses/ports of the service elements in the IMS core. QoS packet marking, bandwidth policing, usage metering and QoS measurements for the media flows are additional features supported by the D-SBG-NE. For wireline networks it provides network-based NAT traversal for the media flows.

Interconnect Session Border Controller (I-SBC)

The Interconnect SBC addresses the requirements at the boundary where different service provider networks interconnect or "peer." It integrates two functional elements from the MSF architecture:

- **Signaling Session Border Gateway, Network Core (S-SBG-NC)** – provides overall control of the boundary between different service provider networks. It provides security for the MSF core in terms of signaling information by performing signaling-based topology hiding, signaling rate policing, IPv4-IPv6 interworking and session screening based upon source and destination signaling addresses. The S-SBG-NC performs protocol and address interworking when connecting non-SIP or non-IPv6 networks. It maintains security associations between itself and SIP UAs, performs admission control and bandwidth allocation using a local policy function or via the BM, and generates call detail records (CDRs). Lastly, the S-SBG-NC interacts with D-SBG-NC for control of the boundary at the transport layers including pinhole firewall, NATP and numerous other features.
- **Data Session Border Gateway, Network Core (D-SBG-NC)** – controls the transport boundary at layers 3 and 4 between service provider networks. This function acts as a pinhole firewall and NAT device protecting the service provider's MSF core. It controls access by packet filtering on IP address/port and opening/closing gates (pinholes) into the network. It uses Network Address and Port Translations (NAPT) to hide the IP addresses/ports of the service elements in the MSF core. QoS packet marking, bandwidth policing, usage metering and QoS measurements for the media flows are additional features supported by the D-SBG-NC.

Acme Packet SBCs support critical missing requirements

Acme Packet SBCs provide essential capabilities that have yet to be defined within the MSF specification. These capabilities are required to provide a secure, reliable and manageable network architecture.

- **Comprehensive security** – Acme Packet SBCs provide critical security functions and features that are currently outside the scope of MSF Release 3, but are required for the successful and secure delivery of services. These critical security features include DoS/DDoS self protection for the border functional elements. Acme Packet border elements also provide DoS/DDoS prevention for core CSC functional elements.
- **Signaling overload control** – Acme Packet SBCs provide critical signaling overload protection via the P-CSC (MSF), S-SBG-NE and S-SBG-NC to protect the core CSC (MSF) elements that are currently outside the scope of MSF. These capabilities include call rate limiting, code gapping and detection of automated dialing platforms. Acme Packet SBCs can perform selective destination/source admission control to prevent signaling overload from flash mass calling events such as American Idol voting.
- **Enterprise access requirements** – MSF is currently specified for residential and mobile wireless services where a single UE is connecting to the network. Acme Packet SBCs provide critical functional capabilities that allow the MSF architecture to be leveraged by enterprise customers. These include the SBCs ability to bridge overlapping MPLS VPN and IP addresses and perform surrogate registrations for endpoints aggregated behind an IP PBX or access gateway. To ensure the seamless connectivity of legacy equipment Acme Packet SBCs provide access protocol interworking for H.323 PBX to SIP trunk connectivity and DTMF translation between SIP signaling-based to RTP media-based (RFC 2833) DTMF.
- **Transcoding (wireline-wireless, wireline-wireline)** – Acme Packet SBCs extend the MSF architecture to provide transcoding capabilities that enable disparate codecs from wireline or wireless networks to seamlessly interoperate. Acme Packet SBCs can transcode (translate) and transrate (change frames sizes) for the wireline codecs G.711 a-law & mu-law, G.723.1, G.726, G.728, G.729 A/B, G.729 E, and iLBC, as well as the wireless codecs AMR, AMR-WB, GSM EFR, GSM FR, EVRC and SMV. They also support fax interworking between G.711 and T.38.

SBC product selection and physical deployment considerations

Acme Packet SBCs may be implemented using an integrated architecture with signaling and media control in the same physical platform or a decomposed architecture that offers separate physical signaling and media control products for the functional elements described earlier. In the decomposed architecture, Acme Packet's products fulfill the access and interconnect SBC roles. In the access role, Acme Packet products perform the functions of the D-SBG-NE (media control) under the supervision of the P-CSC (MSF) (signaling control). In the interconnect SBC role, Acme Packet products perform the functions of the D-SBG-NC (media control) under the supervision of the S-SBG-NC (signaling control). In both cases the elements use H.248 as the control protocol between products.

The key considerations when selecting a product and defining the physical deployment architecture are:

- **Security** – SBCs prevent DoS and DDoS attacks on core MSF elements by dynamically discovering and blocking malicious signaling and media attacks or non-malicious overloads (e.g. endpoint re-registering very frequently). Advanced SBCs using hardware-based features, like Acme Packet's SBCs, can protect themselves against attack without loss of service and create a security perimeter that protects upstream elements (I/S-CSC) from DoS/DDoS attacks and signaling overloads.
- **Scalability** – SBCs provide a distributed edge processing function for signaling control (P-CSC (MSF), S-SBG-NE and S-SBG-NC) offloading connection and encryption management (e.g. TCP, TLS, IPsec), NAT traversal processing and other processor-intensive tasks from core MSF elements (I/S-CSC). The SBC also performs local policy decision functions in order to off-load the core BM. These decisions include enforcing the maximum bandwidth per subscriber, access network, core network or interconnect link. From a SIP signaling perspective, Acme Packet SBCs can also control the number of sessions or rate of session establishment per subscriber, access network, interconnect link or session agent/group.
- **Resiliency (geographic location)** – SBCs increase network resiliency by deploying signaling control functions (P-CSC (MSF), S-SBG-NE and S-SBG-NC) at the access and interconnect network borders. These devices provide a logical breakout point for emergency calls, prevent DoS/DDoS attacks from reaching the core network and minimize the impact of a single P-CSC (MSF) failure or a centralized I/S-CSC site disaster by providing simplified subscriber re-routing capabilities.
- **Cost** – SBCs incorporate multiple MSF products resulting in fewer network elements, fewer networking protocols and more robust fault and performance management (e.g. media QoS monitoring incorporated with session layer accounting), resulting in lower operational costs. Acme Packet SBCs also leverage hardware-based acceleration for processor intensive functions (DoS/DDoS protection, encryption, QoS monitoring/reporting) to reduce capital expenditures by scaling more efficiently.

Net-Net

Acme Packet SBCs perform the critical functions of the access and interconnect SBCs as defined in the MSF Release 3 architecture. In these roles the Acme Packet SBCs enable service providers to create a border architecture that delivers increased security, scalability and resiliency, while reducing operating and capital expenditure costs.

Acme Packet SBCs also provide critical functions that are outside the scope of the MSF specification, including security, signaling overload control, enterprise access requirements and transcoding. These valuable capabilities enable service providers to extend the reach of their NGN investment while better protecting their network and users.

Finally, Acme Packet SBCs allow the service provider to select the preferred deployment model – integrated or decomposed – that satisfies their unique requirements for creating a secure and scalable border. These deployment options enable the service provider to design an access architecture that optimizes operational and capital expenditures, while enhancing the service provider's ability to deliver real-time voice, video and multimedia services.



71 Third Avenue
Burlington, MA 01803 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com