

FINAL FOR IMMEDIATE RELEASE



Media Contact: Annalisa Ouellette
Acme Packet
+1 781-328-4436
aouellette@acmepacket.com

SUPERCOMM 2005, Booth #33049

**Acme Packet Defines Role of Session Border Controllers
in Converged Fixed-Mobile IMS Architecture**

Access and Interconnect session border controllers integrate critical functional elements of IMS architecture defined by 3GPP and extended by ETSI

BURLINGTON, MA – June 3, 2005 – Acme Packet® today defined the role of session border controllers within the next-generation, converged fixed-mobile IMS architecture defined by 3GPP and extended by ETSI TISPA. Within this architecture, session border controllers provide service providers with critical support for real-time interactive IP-based voice, video and multimedia sessions in five areas - security, service reach maximization, SLA assurance, revenue and profit protection, and regulatory and law enforcement.

Within the extended IMS architecture, two different types of session border controllers integrating signaling and media control play very important roles. The Access Session Border Controller satisfies the requirements at the border where subscribers access the IMS core. It incorporates two functional elements from the IMS architecture - the Proxy-Call Session Control Function and the Access Border Gateway Function. The Interconnect Session Border Controller addresses the requirements at the boundary where different service provider networks interconnect or “peer.” It incorporates three functional elements from the architecture - the Interconnect Border Control Function, Inter-working Function and Interconnect Border Gateway Function. Both session border controllers support external interfaces to policy servers for admission control as defined by the IMS Policy Decision Function and the ETSI Resource and Admission Control Subsystem (see separate Acme Packet press release on policy server interface support). Both of these session border controller product definitions tightly integrate signaling and media control in a single platform.

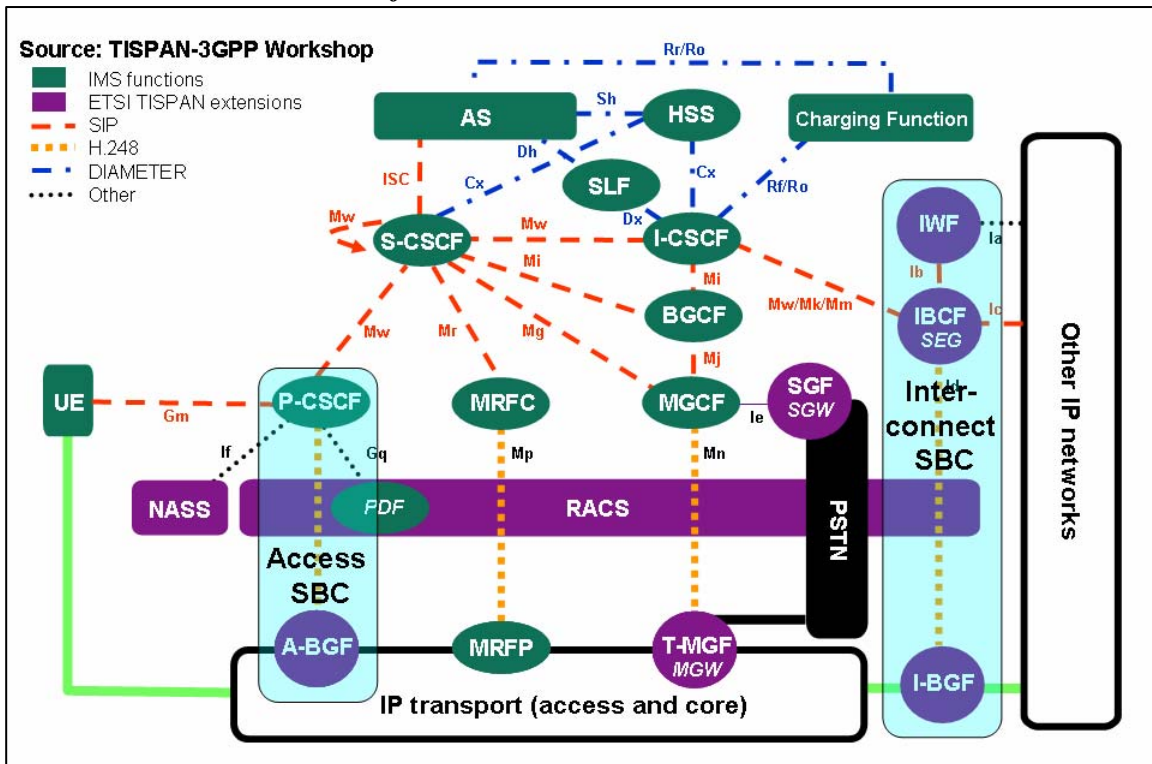
Alternatively, session border control may be implemented using a distributed architecture using separate physical signaling and media control products for the functional elements described above. In this architecture, Acme Packet’s products fulfill the role of the BGF elements under the supervision of the P-CSCF or IBCF elements using H.248 as the control protocol between products.

Session border controllers in IMS

Within the extended IMS architecture, two different types of session border controllers (SBC) that integrate signaling and media control - the Access SBC and the Interconnect SBC - play very important roles. The functional responsibilities of these products are illustrated and further described below. The tight integration of signaling and media control provides several architectural benefits:

- Security – SBC prevents DoS attacks on core IMS 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, can protect themselves against attack without loss of service.
- Scalability – SBC provides distributed edge processing function for signaling and media offloading core IMS elements for connection and encryption management (e.g. TCP, TLS, IPSec), NAT traversal processing and other processor-intensive tasks.
- Manageability - SBC incorporates multiple IMS functions 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).

Role of session border controllers in IMS



Interconnect Session Border Controller

This session border controller addresses the requirements at the boundary where different service provider networks interconnect or “peer.” It integrates three functional elements from the ETSI TISPAN architecture:

- **Interconnect Border Control Function (IBCF)** – provides overall control of the boundary between different service provider networks. It provides security for the IMS core in terms of signaling information by implementing a Topology-Hiding Inter-network Gateway (THIG) sub-function. This sub-function performs signaling-based topology hiding, IPv4-IPv6 inter-working and session screening based upon source and destination signaling addresses. The IBCF also invokes the Inter-Working Function (described below) when connecting non-SIP or non-IPv6 networks, and performs admission control and bandwidth allocation using local policies or via interface to ETSI TISPAN Resource and Admission Control Subsystem (RACS). Lastly, the IBCF interacts with I-BGF (described below) for control of the boundary at the transport layers including pinhole firewall, NAT and numerous other features.
- **Inter-Working Function (IWF)** – provides signaling protocol inter-working between the SIP-based IMS network and other service provider networks using H.323 or different SIP profiles.
- **Interconnect Border Gateway Function (I-BGF)** - 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 IMS 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 & signaling rate policing, usage metering and QoS measurements for the media flows are additional features supported by the I-BGF.

Access Session Border Controller

This session border controller satisfies the requirements at the border where subscribers access the IMS core. It integrates two functional elements from the IMS and ETSI TISPAN architectures.

- **Proxy-Call Session Control Function (P-CSCF)** – is the SIP signaling contact point, the outbound/inbound “proxy,” for subscribers within IMS as defined by 3GPP. 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-CSCF is responsible for forwarding SIP registration messages from the subscriber’s endpoint, the User Element (UE), in a visited network to the Interrogating-CSCF (I-CSCF) and subsequent call set-up requests and responses to the Serving-CSCF (S-CSCF). The P-CSCF 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 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 IMS Policy Decision Function (PDF)/ESTI TISpan Resource and Admission Control Subsystem (RACS). The P-CSCF interacts with A-BGF (described below) for control of the boundary at the transport layers including pinhole firewall, NAT and numerous other features. In addition, for wireline networks, ETSI's RACS is responsible for network-based NAT traversal.

- **Access Border Gateway Function (A-BGF)** – controls the transport boundary at layers 3 and 4 between subscribers and the service provider's network. It performs all of the functions and features of the I-BGF. In addition, in wireline networks, it provides network-based NAT traversal for the media flows.

Support for distributed session border control architecture

Alternatively, session border control may be implemented using a distributed architecture using separate physical signaling and media control products for the functional elements described above. In this architecture, Acme Packet's products fulfill the role of the A-BGF and I-BGF elements under the supervision of the P-CSCF or IBCF elements using H.248 as the control protocol between products.

#####

About Acme Packet

Acme Packet, the leader in session border control, enables service providers to deliver premium, interactive communications - voice, video and multimedia sessions - across IP network borders. Our Net-Net family has been selected by 9 of the top 10, and 16 of the top 25 service providers in the world to satisfy critical security, service assurance and law enforcement requirements in wireline, cable and wireless networks. These deployments support all applications - from trunking to hosted enterprise and residential services; all protocols – SIP, H.323, MGCP/NCS and H.248; and all border points - interconnect, access network and data center. For more information, contact us at +1 781.328.4400, or visit www.acmepacket.com.